Engineering 33 (2024) 35–46

Contents lists available at ScienceDirect

Engineering

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

Research
Safety for Intelligent and Connected Vehicles—Article

Ensuring Secure Platooning of Constrained Intelligent and Connected Vehicles Against Byzantine Attacks: A Distributed MPC Framework

Henglai Wei [a,b], Hui Zhang [b,*], Kamal AI-Haddad [c], Yang Shi [a,*]

[a] Department of Mechanical Engineering, University of Victoria, Victoria, BC V8W 3P6, Canada
[b] School of Transportation Science and Engineering, Beihang University, Beijing 100191, China
[c] École de Technologie Supérieure, University of Quebec, Montreal, QC H3C 1K3, Canada

ARTICLE INFO

Article history:
Received 17 November 2022
Revised 28 February 2023
Accepted 12 October 2023
Available online 7 December 2023

Keywords:
Model predictive control
Resilient control
Platoon control
Intelligent and connected vehicle
Byzantine attacks

ABSTRACT

This study investigates resilient platoon control for constrained intelligent and connected vehicles (ICVs) against F-local Byzantine attacks. We introduce a resilient distributed model-predictive platooning control framework for such ICVs. This framework seamlessly integrates the predesigned optimal control with distributed model predictive control (DMPC) optimization and introduces a unique distributed attack detector to ensure the reliability of the transmitted information among vehicles. Notably, our strategy uses previously broadcasted information and a specialized convex set, termed the "resilience set", to identify unreliable data. This approach significantly eases graph robustness prerequisites, requiring only an $(F+1)$-robust graph, in contrast to the established mean sequence reduced algorithms, which require a minimum $(2F+1)$-robust graph. Additionally, we introduce a verification algorithm to restore trust in vehicles under minor attacks, further reducing communication network robustness. Our analysis demonstrates the recursive feasibility of the DMPC optimization. Furthermore, the proposed method achieves exceptional control performance by minimizing the discrepancies between the DMPC control inputs and predesigned platoon control inputs, while ensuring constraint compliance and cybersecurity. Simulation results verify the effectiveness of our theoretical findings.

1. Introduction

Platoon control in intelligent and connected vehicles (ICVs) has garnered significant attention owing to its potential to reduce fuel consumption and increase transportation system efficiency. Although several commendable platoon control strategies have emerged [1], practical challenges remain. Information communicated over public vehicle-to-vehicle (V2V) networks is susceptible to malicious intrusions and cyberattacks, rendering ICVs vulnerable. Traditional platoon control methods often fail in security-centric ICVs, especially for constraints demanding heightened security assurances.

Secure platoon control is crucial when malicious vehicles in the network disregard established communication protocols, thereby misleading their counterparts. Byzantine attacks manifest when one or several vehicles deliberately disseminate deceptive data within the ICV network, jeopardizing platoon coordination, and possibly leading to collisions. The urgency to devise innovative control algorithms and detection mechanisms capable of addressing this malicious behavior cannot be overstated; they are vital for the safety and security of platoon systems. Given the computational complexity and inherently distributed structure of ICVs, distributed control approaches are appropriate. Thus, developing a resilient distributed platoon control system to prevent cyberattacks is of paramount importance.

Numerous secure control methods for ICVs under cyberattacks have emerged. Comprehensive overviews of this topic are available in Refs. [2–4].

Malicious cyberattacks targeting communication channels tend to undermine data availability, integrity, and confidentiality, as detailed in Refs. [5–8]. Recognizing this threat, various secure control schemes have emerged for ICVs to counteract the detrimental effects of diverse cyberattacks, such as denial-of-service (DoS), deception, and eavesdropping attacks. For example, ICVs under DoS attacks were investigated in Ref. [9]. DoS attacks manifest as time delays, and researchers have used a combination of adaptive estimation and sliding mode control techniques to detect and

* Corresponding authors.
E-mail addresses: huizhang285@buaa.edu.cn (H. Zhang), yshi@uvic.ca (Y. Shi).

https://doi.org/10.1016/j.eng.2023.10.007

gauge the impact of such attacks. Furthermore, DoS attacks represented by packet dropouts were examined in Ref. [10]. A resilient cooperative adaptive cruise control system was developed, pinpointing the resilience boundary against the most permissible consecutive packet dropouts. This subject has also received attention in recent studies [11–13]. Deception attacks on data integrity such as replay [14] and false data injection (FDI) attacks [15–17] pose challenges. In Ref. [14], a dynamic tracking controller melds the output feedback control with a robust reset control to counteract replay attacks that appear as significant random communication delays. For FDI attacks, two distinct detection mechanisms are prominent: one introduces a cloud-based sandboxing technique to assess and segregate adversarial attacks in ICV scenarios [15], and the other elucidates a partial differential equation-based observer to detect FDI attacks and determine their injection points in the ICV platoon [16]. Additionally, strides in privacy-preserving control methods for ICVs concerning data confidentiality have become evident [18,19]. Specifically, proposed a differentially private data streaming approach that integrates noise within the data streams among vehicles [18].

In the following discussion, we briefly outline developments related to attacks executed on agents. A dominant strategy for addressing resilient control challenges is prevention, which is invoked before the onset of attacks; comprehensive insights into this methodology can be found in Refs. [20–23]. Byzantine-resilient distributed observers were conceptualized for a fully distributed implementation, as highlighted in Ref. [24]. The mean sequence reduced (MSR) algorithm [25] empowers multi-agent systems (MASs) with bounded adversaries to attain resilient control objectives, provided that the communication graph meets certain robustness criteria. Specifically, the MSR algorithm shifts through the state values of neighboring systems, discarding outliers, and using the remaining conventional values to update the control input. Although several adaptations of MSR-type resilient algorithms for MAS have emerged under attack scenarios [20,26,27], these often face complications owing to coupled system states, complicating attack detection. Additionally, the bulk of the existing work primarily focuses on the theoretical facets of the resilient consensus of MAS. By contrast, research offering security assurances that are explicitly tailored for practical ICVs in the context of Byzantine attacks remains underexplored.

Conversely, distributed model predictive control (DMPC) has gained substantial attention owing to its exceptional capabilities in constraint management and computational resource optimization, as evidenced in Refs. [28,29]. DMPC approaches for tackling cooperative stabilization challenges in MASs were explored in Ref. [30], whereas solutions addressing consensus issues in cooperative systems appeared in Refs. [31,32]. Despite their merits, existing DMPC methodologies lack in the context of security-sensitive operations. This highlights the necessity for a unified and resilient DMPC-based strategy to safeguard ICVs against cyberattacks.

This study addresses platoon control in ICVs under physical constraints and Byzantine attacks, in which malicious information is transmitted between vehicles. Meeting both the constraint satisfaction and security demands of ICVs is a nontrivial task that requires the co-design of an effective control strategy and reliable attack detection mechanism.

(1) We develop a resilient distributed model predictive platoon control (RDMP2C) for constrained ICVs. This framework allows vehicles to detect and identify malicious information, thereby ensuring that they consistently meet the desired platoon control objectives. By integrating the predesigned optimal control with DMPC optimization, our approach ensures both superior control performance and constraint adherence.

(2) To address the challenge of high communication network robustness requirements in the existing resilient distributed control algorithms for ICVs under Byzantine attacks [25,33], we designed a distributed attack detector based on previously broadcast information and a resilience set. Communication links are characterized by different levels of thrust based on the intensity of Byzantine attacks, and a novel second verification algorithm is designed to restore the thrust of communication links that are not severely attacked.

(3) We establish sufficient conditions for the recursive feasibility of the RDMP2C algorithm and the stability of the closed-loop ICV system. Notably, our method is the first attempt to concurrently address the cybersecurity, constraints, and control performance of constrained ICVs under potential attacks. Even during Byzantine attacks, our method maintains closed-loop stability and security in ICVs with reduced reliance on network robustness.

The remainder of this paper is organized as follows. Section 2 presents some basic preliminaries and formulates the resilient platoon control problem. In Section 3, we present the distributed detection algorithms for Byzantine attacks. In Section 4, we propose the RDMP2C framework for constrained ICVs. In Section 5, we prove the theoretical properties, including the recursive feasibility and closed-loop stability. Section 6 presents the simulation results and Section 7 concludes the paper.

2. Preliminaries and problem formulation

2.1. Communication networks

A directed graph $\mathcal{G}(t)=\{\mathcal{V},\mathcal{E}(t),\mathcal{A}(t)\}$ is used to describe the information exchange among the ICVs, in which $\mathcal{V}=\{1,2,\cdots,M\}$ denotes the vertex set, $M\in\mathbb{N}$, $\mathcal{E}(t)\subseteq\{(i,j)\mid i,j\in\mathcal{V},i\neq j\}$ represents the edge set, $t\in\mathbb{N}$, $\mathbb{N}$ denotes the set of nonnegative integers and $\mathcal{A}(t)=\left[a_{ij}(t)\right]\in\mathbb{R}^{n\times n}$ represents the adjacency matrix with $a_{ij}(t)>\alpha$, $0<\alpha<1$. An edge (j,i) with $a_{ij}(t)\neq 0$ implies that vehicle j can send information to vehicle i at time t. The in-degree of vehicle i is denoted by $\deg_i=\sum_{j=1,\,j\neq i}^{M}a_{ij}(t)$. For the in-degree matrix $\mathcal{D}(t)=\mathrm{diag}(\deg_1,\cdots,\deg_M)$, the Laplacian matrix is given as $\mathcal{L}(t)\in\mathbb{R}^{n\times n}=\mathcal{D}(t)-\mathcal{A}(t)$. The neighbors of vehicle i are denoted by $\mathcal{N}_i(t)=\left\{v_j\in\mathcal{V}(t)\mid(v_i,v_j)\in\mathcal{E}(t),i\neq j\right\}$. Only a subset of follower vehicles can receive information from leader vehicle 0 in this work. The corresponding pinning matrix is given as $G=\mathrm{diag}(g_{10},\cdots,g_{M0})$ with a pinning gain g_{i0}. Follower vehicle i receives information from the preceding vehicles $i-1$ and $i-2$, $i=\{2,\cdots,M\}$. The notations of r-reachable set and r-robustness introduced in Ref. [25] characterize graph robustness properties.

Definition 1. (r-reachable set). Given a graph $\mathcal{G}$ and a nonempty subset $\mathcal{S}\subset\mathcal{V}$, the set $\mathcal{S}$ is r-reachable if $\exists\, i\in\mathcal{S}$ such that $|\mathcal{V}_i\setminus\mathcal{S}|\geq r$, $r\in\mathbb{N}$.

Definition 2. (r-robust graph). A nonempty graph $\mathcal{G}$ is r-robust ($r<M$) if at least one of the subsets is r-reachable for any pair of nonempty disjoint subsets $\mathcal{V}$, at least one of the subsets is r-reachable.

2.2. ICV longitudinal dynamics

For precise control over the longitudinal dynamics, we adopt certain assumptions [34]. We neglect the longitudinal slip of the tire, assume a rigid and symmetric vehicle, and disregard any lateral effects. These assumptions streamline the model, ensuring that longitudinal dynamics are both predictable and accurately controllable. The longitudinal dynamics of vehicle i, $i\in\mathcal{V}$, are detailed in Ref. [34].

$$\begin{cases} \dot{s}_i(t) = \mu_i(t) \\ \dot{\mu}_i(t) = \frac{1}{m}\left(\frac{\eta F_i(t)}{R_w} - C_A \mu_i^2(t) - mgf\right) \\ \tau \dot{F}_i(t) + F_i(t) = F_{i,\text{des}}(t) \end{cases} \tag{1}$$

where s_i and μ_i are, respectively, the position and the velocity along the longitudinal axis; η is the mechanical efficiency of the driveline; R_w is the tire radius; C_A is the aerodynamic drag coefficient; m is the vehicle mass; g is the gravity constant; f is the rolling resistance; F_i is the actual driving torque; $F_{i,\text{des}}$ is the desired driving torque; and τ is the inertial lag of the longitudinal dynamic of the vehicle. A feedback linearization technique is adopted to transform the nonlinear longitudinal dynamics Eq. (1) into a linear system model as follows:

$$F_{i,\text{des}}(t) = \frac{R_w}{\eta}\left(C_A \mu_i(t)\left(\mu_i(t) + 2\tau \dot{\mu}_i(t)\right)\right) + mgf + mu_i(t)) \tag{2}$$

in which $u_i(t)$ denotes the control input. For acceleration $a_i(t) = \dot{\mu}_i(t)$ of vehicle i:

$$a_i(t) + \tau \dot{a}_i(t) = u_i(t) \tag{3}$$

From Eqs. (1)–(3), we obtain the compact form

$$\dot{x}_i(t) = \boldsymbol{A_c} x_i(t) + \boldsymbol{B_c} u_i(t) \tag{4}$$

in which $x_i = \text{col}(s_i, \mu_i, a_i)$,

$$\boldsymbol{A_c} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, \text{ and } \boldsymbol{B_c} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} \tag{5}$$

The dynamics of the vehicle Eq. (4) in discrete time follows

$$x_i(t+1) = \boldsymbol{A_d} x_i(t) + \boldsymbol{B_d} u_i(t) \tag{6}$$

where

$$\boldsymbol{A_d} = \begin{bmatrix} 1 & T & 0.5T^2 \\ 0 & 1 & T \\ 0 & 0 & 1 - \frac{T}{\tau} \end{bmatrix}, \text{ and } \boldsymbol{B_d} = \begin{bmatrix} 0 \\ 0 \\ \frac{T}{\tau} \end{bmatrix} \tag{7}$$

with T being the sampling period. For the sake of notation simplicity, we abbreviate $\boldsymbol{A_d}$ and $\boldsymbol{B_d}$ as $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively.

Note that the ICV in Eq. (6) is subject to the state and control input constraints.

$$x_i \in \mathcal{X}_i \text{ and } u_i \in \mathcal{U}_i \tag{8}$$

in which the sets $\mathcal{X}_i = \{x \in \mathbb{R}^3 \mid x_{\min} \le x \le x_{\max}\}$ and $\mathcal{U}_i = \{u \in \mathbb{R}^1 \mid u_{\min} \le u \le u_{\max}\}$ are compact and contain the origin as the interior point, with the state bounds $x_{\min}, x_{\max}$ and control input bounds $u_{\min}, u_{\max}$.

2.3. Byzantine attack model

This subsection describes the characterization of the Byzantine attack model. Here, a vehicle under Byzantine attack is called a Byzantine vehicle. If a vehicle is free of attack, it is called a normal vehicle and always obeys a predefined control strategy. Let $\mathcal{V}_N \subset \mathcal{V}$ and $\mathcal{V}_A \subset \mathcal{V}$ denote the set of normal and Byzantine vehicles, respectively. The cardinality of the normal vehicle set is denoted as $|\mathcal{V}_N|$. The cardinality of the Byzantine vehicle set is denoted as $|\mathcal{V}_A|$.

In the following section, we introduce the notations for Byzantine vehicles, normal vehicles, and F-local Byzantine attacks [25].

Definition 3. (Byzantine vehicle). Vehicle i, $i \in \mathcal{V}$ in Eq. (4) is Byzantine if it broadcasts arbitrarily different state values to its neighbors.

Definition 4. (Normal vehicle). Vehicle i, $i \in \mathcal{V}$ in Eq. (4) is normal if it updates and broadcasts its state values based on the designed control protocol.

Definition 5. (F-local Byzantine attacks). Given graph $\mathcal{G}$ and a number $F \in \mathbb{N}$, if the number of Byzantine vehicles in the neighborhood of the normal vehicle i, $i \in \mathcal{V}_N$ is no more than F, that is, $|\mathcal{N}_i \cap \mathcal{V}_A| \le F$, then we say that the ICV is subject to F-local Byzantine attacks.

ICVs typically have inter-vehicle communication networks, such as V2V and intra-vehicle networks (e.g., controller area networks) for controller–sensor communication. Moreover, these vehicles have an array of sensors dedicated to perception [2]. However, although these connected networks and sensors enhance intra- and inter-vehicle communication, they also present vulnerabilities. These can become entry points for adversarial Byzantine attacks, causing arbitrary system updates. Notably, a vehicle under malicious attack transmits identical state values to all neighboring vehicles [25]. Consequently, this malicious vehicle can be regarded as a specific example of a Byzantine vehicle.

In the realm of vehicle platooning, Byzantine attacks pose a significant risk, as they occur when an adversarial vehicle disseminates deceptive data, such as its position, speed, or acceleration, to other vehicles within the platoon. Such misinformation can throw off the synchronized movement of a platoon, creating operational inefficiencies and potential safety hazards. Risks escalate if the compromised vehicle is situated at the front of the platoon, where it has considerable influence over the entire formation. Addressing the challenges posed by Byzantine attacks on vehicle platooning systems involves a two-pronged approach. First, control strategies must be designed to preserve the stability and security of the platoon, even in the face of malicious actors within the ranks. Second, these strategies must demonstrate resilience to different types of adversarial incursions. Achieving this resilience requires the creation of innovative control algorithms and robust detection mechanisms capable of identifying and mitigating malicious activities.

Byzantine attacks can occur in various manners during platoon operations, ranging from FDI and packet loss to more elaborate replay attacks. The perpetrators of these attacks could be insiders with access to the communication systems or external agents of the platoon. Furthermore, these attacks can vary in duration and frequency, whether intermittent or sustained.

Let t_k^i denote the Byzantine attack time instant for vehicle i, with $i \in \mathcal{V}$, $k \in \mathbb{N}_{\ge 1}$, and $\mathbb{N}_{\ge 1}$ being the set of integers in interval $[1, +\infty)$. We define $H_i > 0$ as the duration of the Byzantine attack, and vehicle i is attacked by a Byzantine attacker during $\mathbb{N}_{[t_k^i, t_k^i + H_i]}$. Following are the assumptions for the Byzantine attack model and ICVs:

Assumption 1. Constants $F \in \mathbb{N}$ *and* $W \in \mathbb{N}$ exist such that: ① the attack duration satisfies $H_i \le W$ for $k \in \mathbb{N}_{\ge 1}$; ② the intensity of malicious Byzantine attacks remains unchanged in the attack duration $\mathbb{N}_{[t_k^i, t_k^i + H_i]}$; ③ the ICVs in Eq. (6) are subject to F-local Byzantine attacks, and the upper bound F is available for the normal vehicles; ④ the lead vehicle 0 is attack-free.

Given the limited energy of adversarial cyberattacks, assuming the number of Byzantine attacks F and maximum attack duration W for the ICV is reasonable. A similar assumption can be made in the DoS attack results [35,36].

2.4. Problem formulation

This work aims to develop a resilient and distributed platoon control framework such that constrained ICVs under F-local Byzantine attacks achieve the following two objectives:

(1) Resilient platoon: Byzantine vehicles can be detected and isolated. Normal vehicle i, $i \in \mathcal{V}_N$ keeps a desired distance from lead vehicle 0 and tracks the speed of lead vehicle 0, that is,

$\lim_{t\to\infty}|s_i(t)-s_0(t)|=d_{i0}$ and $\lim_{t\to\infty}|\mu_i(t)-\mu_0(t)|=0$, where $d_{i0}=id$ and the constant $d>0$ is the desired gap between two consecutive vehicles.

(2) Constraint satisfaction: normal vehicle i, $i\in\mathcal{V}_N$

$$x_i(t+1)=\boldsymbol{A}x_i(t)+\boldsymbol{B}u_i(t) \tag{9}$$

satisfies the physical constraints in Eq. (8) for all $t\in\mathbb{N}$.

3. Distributed detection algorithms for Byzantine attacks

The proposed RDMP2C framework for ICV in the right lane is outlined in Fig. 1. Each follower vehicle comprises five parts: the broadcaster (block a), controlled vehicle (block b), DMPC controller (block c), attack detector (block d), and receiver (block e). The information transmitted between vehicles is broadcast and received by a broadcaster and receiver, respectively. The attack detector is responsible for determining malicious information and retaining normal information from its neighbors. Given normal broadcast information, the optimal platoon control input u_i^* is generated for vehicle i by solving the DMPC problem (see Section 4).

Before discussing the distributed detection algorithms for ICVs under Byzantine attacks, we introduce two pivotal sets: the estimation error set and the resilience set. The estimation error set was meticulously designed and integrated into the DMPC problem to facilitate parallel execution of the distributed control algorithm. Building upon the estimation error set, we design a tube $X_i(t)$, $i\in\mathcal{V}$ centered around the prior broadcast state sequence. This tube constrains the current broadcast state sequence shared among vehicles. Expanding the estimation error set, we formulate a resilience set to detect and identify potential attacks targeting vehicles. Consequently, the resilience tube $R_i(t)$, $i\in\mathcal{V}$ leveraging the previously broadcast predicted state sequence and the resilience set, is structured within the attack detector (the attack detection mechanism) (block d) for vehicle i.

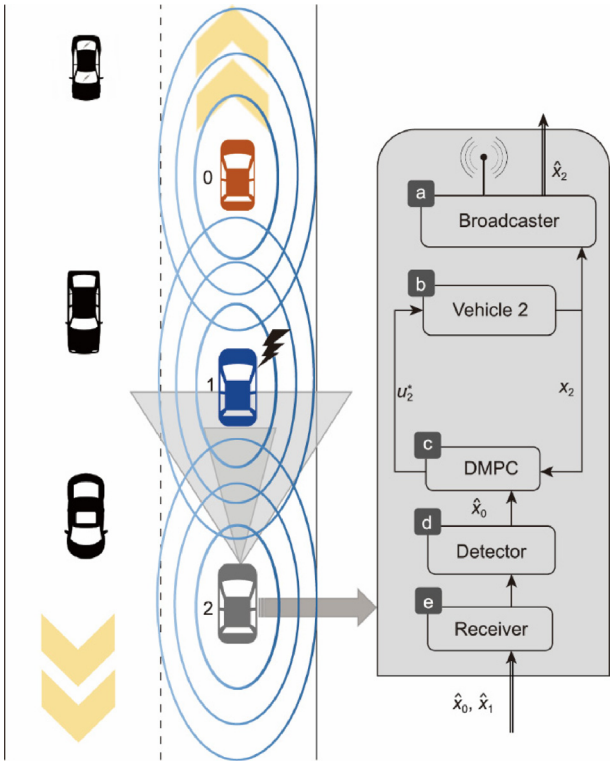

Fig. 1. RDMP2C scheme for the constrained ICV in the right lane (consisting of three vehicles with leader vehicle 0 and follower vehicles 1 and 2; $\mathcal{N}_1=\{0,2\}$, $\mathcal{N}_2=\{0,1\}$). The information is broadcast among vehicles via the V2V networks. Note that vehicle 1 is attacked.

3.1. Estimation error set

Typically, cooperative agents calculate the optimal predicted state sequences and exchange them simultaneously [37,38]. However, this approach is not feasible in practice. To address this problem, the predicted states of each vehicle broadcast at the previous time instant t (termed as "the assumed predicted states") are used to estimate the current predicted system states at time $t+1$, $t\in\mathbb{N}_{\geq 0}$. Consequently, vehicles can implement distributed control algorithms simultaneously. Let $\hat{\boldsymbol{x}}_i(t+1)=\{\hat{x}_i(t+1|t+1),\hat{x}_i(t+2|t+1),\ldots\}$ be the assumed predicted state sequence of vehicle i, $i\in\mathcal{V}$ hereafter, which is used to estimate the current optimal predicted state sequence $\boldsymbol{x}_i^*(t+1)=\{x_i^*(t+1|t+1),x_i^*(t+2|t+1),\ldots\}$ at time $t+1$. More precisely, $\hat{x}_i(t+1+k|t+1)$ is given by

$$\hat{x}_i(t+k|t+1)=x_i^*(t+k|t) \tag{10}$$

where $k,t\in\mathbb{N}_{\geq 0}$, and $\boldsymbol{x}_i^*(t)$ denotes the optimal predicted state sequence generated by solving the DMPC problem $\mathcal{P}_i$. As indicated in Eq. (10), the assumed predicted states exchanged among the ICV inevitably lead to estimation errors. In this case, the estimation errors induced by a more practical transmission were treated as external disturbances. Note that an estimation error set Δ used to limit the estimation error $e_i(t+k|t)=\hat{x}_i(t+k|t)-x_i^*(t+k|t)$ is specified for the ICV, aiming at achieving the desired formation. The estimation error set plays an important role in the ICV that distributively performs the control algorithm. Accordingly, the optimized predicted states of vehicle i, $i\in\mathcal{V}$ are required to lie in a specified neighborhood of the assumed predicted states for $k\in\mathbb{N}_{\geq 0}$,

$$x_i(t+k|t)-\hat{x}_i(t+k|t)\in\Delta \tag{11}$$

in which the estimation error set $\Delta=\{\delta\in\mathbb{R}^3\mid\|\delta\|<\eta\}$ is convex and contains the origin, with $\eta>0$ and $\|\cdot\|$ denoting the Euclidean norm.

Inspired by the tube-based MPC for linear systems with external disturbances, the estimation errors between the current optimal predicted states and assumed states are treated as external disturbances. Constraint Eq. (11) is incorporated into the robust DMPC optimization problem $\mathcal{P}_i$ to constrain the optimal predicted state sequence $x_i(t+k|t)$ within the predesigned tube $X_i(t)$ centered along the assumed state $\hat{x}_i(t+k|t)$. Moreover, this constraint ensures that the robust DMPC optimization problem can be solved in a distributed fashion. Note that the estimation error set provides consistency between the intended behaviors of a vehicle and what makes the neighbors believe how it will behave from the perspective of the broadcaster (the vehicle is the broadcaster when it broadcasts the predicted states to its neighbors; likewise, the receiver refers to the vehicle that receives the predicted states from its neighbors) (block a).

3.2. Resilience set

As achieving resilient platoon control requires reliable and secure information from neighboring vehicles, each vehicle must be able to detect adversarial vehicles and communication links. To identify potential Byzantine attacks, we construct a resilience set for the distributed attack detector (block d), as shown in Fig. 1. For communication networks $\mathcal{G}(t)$ of the ICV that can afford resilience against F-local Byzantine vehicles, each normal vehicle must detect and discard adversarial interconnections to eliminate adverse effects; otherwise, resilient platoon control of the ICV

cannot be guaranteed. To this end, the resilience set $\mathcal{R}$ is designed based on the estimation error set to detect and identify Byzantine adversaries. More precisely, resilience set $\mathcal{R}$ is given by

$$\mathcal{R} = \sigma \Delta \tag{12}$$

where the constant $\sigma > 1$ is a resilience parameter. The design parameter σ reflects the ability of the ICV to tolerate cyber-attacks.

Next, based on the estimation error set and resilience set, vehicle i, $i \in \mathcal{V}$ categorizes the received predicted state sequence from neighbors j, $j \in \mathcal{N}_i(t)$ into three levels: normal, recoverable, and adversarial communication.

(1) Normal communication: If the assumed predicted state sequence of neighbors $\widehat{\boldsymbol{x}}_j(t)$, $j \in \mathcal{N}_i(t)$ transmitted from vehicle j to vehicle i satisfies

$$\widehat{x}_j(t+k|t) - \widehat{x}_j(t+k|t-1) \in \Delta \tag{13}$$

with $k \in \mathbb{N}_{\geq 0}$, then the communication link (j,i) is normal at time t. From Eq. (13), it can be seen that the assumed predicted state sequence $\widehat{\boldsymbol{x}}_j(t-1)$ broadcast at time $t-1$ serves as the center of the tube $X_i(t)$.

(2) Recoverable communication: The adversarial predicted state sequence of neighbors $\widehat{\boldsymbol{x}}_j(t)$ may be in the resilience tube that centers along the previous broadcast assumed predicted state sequence $\widehat{\boldsymbol{x}}_j(t-1)$, with $k \in \mathbb{N}_{\geq 0}$. If the assumed predicted-state sequence $\widehat{\boldsymbol{x}}_j(t)$ satisfies

$$\widehat{x}_j(t+k|t) - \widehat{x}_j(t+k|t-1) \in \mathcal{R} \setminus \Delta \tag{14}$$

with $k \in \mathbb{N}_{\geq 0}$, then the communication link (j,i) is adversarial but recoverable at time t. $\mathcal{R} \setminus \Delta := \{x \in \mathbb{R}^3 \mid x \in \mathcal{R}, x \notin \Delta\}$. Let $\mathcal{N}_i^r(t)$ denote the set of all recoverable communication links, with $\mathcal{N}_i^r(t) \subset \mathcal{N}_i(t)$. The weight $a_{ij}(t)$ used in the platoon control design becomes $a_{ij}(t) = a_{ij}(t-1)/\sigma$, which dynamically adjusts the level of trust in the corresponding communication link/channel among the ICV.

(3) Adversarial communication: If the received assumed predicted state sequence $\widehat{\boldsymbol{x}}_j(t)$ satisfies

$$\widehat{x}_j(t+k|t) - \widehat{x}_j(t+k|t-1) \notin \mathcal{R} \tag{15}$$

with $k \in \mathbb{N}_{\geq 0}$, then the communication link (j,i) is adversarial. The adversarial predicted state information is discarded and not used in the platoon control design for vehicle i (which implies $a_{ij}(t) = 0$).

This study assumes no Byzantine attacks on the ICV at the initial time $t = 0$. For vehicle i, $i \in \mathcal{V}$, the corresponding trustworthiness weight at the initial time 0, with $a_{ij}(0) = 1/|\mathcal{N}_i(0)|$. At time t, the trustworthiness weight becomes:

$$a_{ij}(t) = \begin{cases} a_{ij}(t-1) & j \in \mathcal{N}_i^n(t) \\ a_{ij}(t-1) \cdot \sigma^{-1} & j \in \mathcal{N}_i^r(t) \\ 0 & j \in \mathcal{N}_i^m(t) \end{cases} \tag{16}$$

where $\mathcal{N}_i^n(t)$, $\mathcal{N}_i^r(t)$, and $\mathcal{N}_i^m(t)$ represent the normal, recoverable, and adversarial neighboring sets, respectively.

Note that normal vehicles do not require an exact determination of which of their neighboring vehicles is adversarial. Only the adversarial communication induced by Byzantine adversaries must be detected based on the assumed predicted states broadcast at the last time instant, estimation error set, and resilience set.

3.3. Distributed detection algorithm

In this subsection, we present the distributed attack detection algorithm and the second verification algorithm for ICV in the presence of F-local Byzantine attacks.

MSR-type algorithms [20,25,39] usually require each agent to gather the neighboring state information, sort the received information, and discard the $2F$ extreme system state values. These algorithms collect and detect adversarial agents in a centralized manner, which is a requirement for robust communication networks. More precisely, the communication network $\mathcal{G}(t)$ is at least $(2F+1)$-robust. In contrast, the proposed detection algorithm distributively detects broadcast information from neighbors, which significantly relaxes the restriction on network robustness. Each normal vehicle only ignores at most F received neighbors' information for the ICV in the presence of F-local Byzantine attacks.

Algorithm 1 summarizes the implementation of the distributed attack detection scheme for vehicle i, $i \in \mathcal{V}$ at time t in this paper.

Algorithm 1: Distributed attack detection algorithm

Input: The estimation error set Δ, the resilience parameter σ, the neighboring sets $\mathcal{N}_i^r(t-1)$, $\mathcal{N}_i(t-1)$, the assumed predicted states $\widehat{\boldsymbol{x}}_j(t-1)$, $k \in \mathbb{N}_{\geq 0}$ and $a_{ij}(t-1)$, with $a_{ij}(0) = 1/|\mathcal{N}_i(0)|$.

Output: The neighboring sets $\mathcal{N}_i^r(t)$, $\mathcal{N}_i(t)$ and the weight $a_{ij}(t)$, $j \in \mathcal{N}_i(t)$.

for $j = 1$ to $|\mathcal{N}_i(t-1)|$
  Receive the assumed predicted states $\widehat{\boldsymbol{x}}_j(t)$;
  if the condition Eq. (15) holds **then**
    $a_{ij}(t) \leftarrow 0$ and $|\mathcal{N}_i(t)| \leftarrow |\mathcal{N}_i(t-1)| - 1$;
  else if the condition Eq. (14) holds **then**
    $a_{ij}(t) \leftarrow a_{ij}(t-1)/\sigma$, $|\mathcal{N}_i(t)| \leftarrow |\mathcal{N}_i(t-1)|$;
    $|\mathcal{N}_i^r(t)| \leftarrow |\mathcal{N}_i^r(t-1)| + 1$;
  else
    $a_{ij}(t) \leftarrow a_{ij}(t-1)$ and $|\mathcal{N}_i(t)| \leftarrow |\mathcal{N}_i(t-1)|$;
  end if
end for
return $a_{ij}(t)$, $\mathcal{N}_i(t)$ and $\mathcal{N}_i^r(t)$.

Before proceeding, we make the following remarks on Algorithm 1.

Redundant network interconnections are crucial for a resilient ICV platoon under F-local Byzantine attacks. Typically, MSR-type algorithms filter adversarial information from neighbors by discarding $2F$ suspicious system state values at each time step, which requires the communication network to be at least $(2F+1)$-robust [20,24,40]. By contrast, our distributed attack detection algorithm relaxes the network robustness requirement from $(2F+1)$ to $(F+1)$. Owing to the resilience set and assumed predicted states, each normal vehicle can detect the received neighbor information under relaxed graph robustness. This constitutes a distinct contribution to this study.

Applying Algorithm 1 identifies and ignores severely adversarial assumed predicted states from neighbors, as indicated in Eq. (15), in the distributed control strategy. Now, let us consider the special case (slight cyberattacks) where the broadcast assumed predicted states violate the estimation error set while remaining within the resilience set, as given in Eq. (14). In Algorithm 1, instead of discarding this information directly, we dynamically adjust the edge weight $a_{ij}(t)$ of the adjacency matrix $\mathcal{A}(t)$ to eliminate the adverse effects of Byzantine attacks. A question arises naturally: If the communication link $a_{ij}(t)$, $j \in \mathcal{N}_i^r(t)$ becomes normal, is it possible to recover the confidence weight? To address this problem, we provide a "second verification" mechanism for recovering less severe communication links. Under this verification mechanism, if attacks recur in the same communication channel/link and vehicles broadcast the misbehaving assumed predicted state given in Eq. (15), we consider the vehicle vulnerable and discard it. Conversely, if Byzantine attacks Eq. (14) occur at time t_k^i, then we will restore the trust-

worthiness of the associated vehicle and communication links at $t = t_k^i + W$ based on Algorithm 1.

This algorithm is referred to as the second verification algorithm and is summarized in Algorithm 2.

Algorithm 2: Second verification algorithm

Input: The assumed predicted state sequence $\widehat{\boldsymbol{x}}_j(t)$ of vehicle j, $j \in \mathcal{N}_i^r(t_k^i)$, $t_k^i \in \mathbb{N}_{\geq 1}$, The resilience set $\mathcal{R}$ and $\mathcal{N}_i^r(t)$.
Output: $a_{ij}(t)$, $\mathcal{N}_i^r(t)$ and $\mathcal{N}_i(t)$.
1: **for** $t \in \mathbb{N}_{[t_k^i+1, t_k^i+W]}$
2: $\quad a_{ij}(t) \leftarrow a_{ij}(t-1)$;
3: **end for**
4: $a_{ij}(t) \leftarrow \sigma a_{ij}(t_k^i)$, $t = t_k^i + W$;
5: $|\mathcal{N}_i^r(t)| \leftarrow |\mathcal{N}_i^r(t_k^i)| - 1$;
6: **return** $a_{ij}(t)$, $\mathcal{N}_i(t)$ and $\mathcal{N}_i^r(t)$.

The detection and isolation mechanism (i.e., detecting attacks and isolating corrupted communication links/agents) for MAS under cyberattacks has recently gained attention [20,41]. In contrast to these existing attack detection methodologies, the proposed secondary verification algorithm enhances the resilience of the system to a higher number of Byzantine attacks without increasing the robustness threshold of the network.

4. Resilient DMPC-based platoon control

In this section, we present a DMPC-based platoon control algorithm for constrained ICVs in the presence of F-local Byzantine attacks. Inspired by the "pre-stabilizing" control method [42], the proposed control policy $u_i(t) = \varkappa_i(t) + c_i^*(t)$ is designed in two steps:

(1) Pre-design the optimal platoon control strategy $\varkappa_i(t)$ for the unconstrained ICV based on the reliable predicted state information from the normal neighbors and the updated communication network $\mathcal{G}(t)$.

(2) Design the DMPC optimization problem $\mathcal{P}_i$ for vehicle i, $i \in \mathcal{V}$ to explicitly handle the estimation errors and the physical constraints, including the state and control input constraints. Solving the DMPC optimization problem $\mathcal{P}_i$ yields the optimal control input $c_i^*(t)$.

4.1. Pre-designed platoon control

At time t, communication network $\mathcal{G}(t)$ may be updated when Byzantine attacks occur. In this work, we design an optimal platoon control $\varkappa_i(t)$ for the unconstrained ICV to achieve optimal control performance. Specifically, the predesigned optimal platoon control for vehicle i depends on the relative states with its normal neighbors, that is,

$$\varkappa_i(t) = \boldsymbol{K}(t)\left[\sum_{j\in\mathcal{N}_i(t)} a_{ij}(t)\big(x_i(t) - x_j(t)\big) + g_{i0}(x_i(t) - x_0(t))\right] \tag{17}$$

where $\boldsymbol{K}(t)$ denotes the predesigned optimal control gain matrix. For vehicle i, the assumed predicted states of neighbors $\widehat{x}_j(t)$ are employed to construct the predesigned optimal platoon control law. Consequently, the predesigned platoon control input in Eq. (17) can be written as follows:

$$\widehat{\varkappa}_i(t) = \boldsymbol{K}(t)\left[\sum_{j\in\mathcal{N}_i(t)} a_{ij}(t)\big(x_i(t) - \widehat{x}_j(t)\big) + g_{i0}(x_i(t) - x_0(t))\right] \tag{18}$$

Once the Byzantine vehicles are detected by Algorithm 1 and Algorithm 2, information from these vehicles is discarded. That is, Byzantine vehicles were isolated from the ICV, yielding a time-dependent communication network, $\mathcal{G}(t)$. When the communication networks change, we update the predesigned optimal control gain matrix $\boldsymbol{K}(t)$, using various methods outlined in Refs. [43,44].

4.2. DMPC for constrained ICVs

At time t, the cost function $J_i(\boldsymbol{c}_i(t))$ for vehicle i, $i \in \mathcal{V}$ is designed as

$$J_i(\boldsymbol{c}_i(t)) = \sum_{k=0}^{\infty} \|c_i(t+k|t)\|_Q^2 \tag{19}$$

where the weighting matrix Q is positive definite and $\boldsymbol{c}_i(t) = \mathrm{col}(c_i(t|t), \ldots, c_i(t+k|t), \ldots)$ denotes the control sequence. Note that $[c_1^{\mathrm{T}}, \ldots, c_n^{\mathrm{T}}]^{\mathrm{T}}$ is written as $\mathrm{col}(c_1, \ldots, c_n)$ and $\|c_i\|_Q^2$ denotes the weighted Euclidean norm $c_i{}^{\mathrm{T}} Q c_i$.

At time t, given the current system state $x_i(t)$ of each vehicle i, $i \in \mathcal{V}$ and its neighbors' assumed states $\widehat{\boldsymbol{x}}_j(t)$, $j \in \mathcal{N}_i(t)$, the DMPC problem $\mathcal{P}_i$ is given as

$$\begin{aligned} &\min_{\boldsymbol{c}_i(t)} J_i(\boldsymbol{c}_i(t)) \\ &\text{s.t. } x_i(t|t) = x_i(t) \end{aligned} \tag{20a}$$

$$x_i(t+k+1|t) = \boldsymbol{A}x_i(t+k|t) + \boldsymbol{B}u_i(t+k|t) \tag{20b}$$

$$u_i(t+k|t) = \widehat{\varkappa}_i(t+k|t) + c_i(t+k|t) \tag{20c}$$

$$u_i(t+k|t) \in \mathcal{U}_i \tag{20d}$$

$$x_i(t+k|t) \in \mathcal{X}_i \tag{20e}$$

$$x_i(t+k|t) - \widehat{x}_i(t+k|t) \in \Delta \tag{20f}$$

where $k \in \mathbb{N}_{\geq 0}$. $x_i(t)$ denotes the state x at time t, and $x_i(t+k|t)$ denotes the predicted state at future time $t+k$ determined at time t. Let $\boldsymbol{c}_i^*(t) = \mathrm{col}(c_i^*(t|t), \ldots, c_i^*(t+k|t), \ldots)$ be the optimal solution to problem $\mathcal{P}_i$ at time t. Then, we obtain the optimal control input for vehicle i

$$\begin{aligned} u_i^*(t+k|t) = &\boldsymbol{K}(t)\Big[\textstyle\sum_{j\in\mathcal{N}_i(t)} a_{ij}(t)\big(x_i^*(t+k|t) - \widehat{x}_j(t+k|t)\big) + \\ &g_{i0}(x_i(t+k|t) - x_0(t+k|t))\Big] + c_i^*(t+k|t) \end{aligned} \tag{21}$$

where $k \in \mathbb{N}_{\geq 0}$, the optimal control input sequence at time t is $\boldsymbol{u}_i^*(t) = \mathrm{col}(u_i^*(t|t), \ldots, u_i^*(t+k|t), \ldots)$ and the corresponding optimal predicted state becomes

$$x_i^*(t+k+1|t) = \boldsymbol{A}x_i^*(t+k|t) + \boldsymbol{B}u_i^*(t+k|t) \tag{22}$$

where $t \in \mathbb{N}$, the optimal state sequence is denoted by $\boldsymbol{x}_i^*(t) = \mathrm{col}(x_i^*(t|t), \ldots, x_i^*(t+k|t), \ldots)$. Furthermore, applying the first term of the optimal control input in Eq. (21) to the vehicle system in Eq. (4) yields

$$x_i(t+1) = \boldsymbol{A}x_i(t) + \boldsymbol{B}u_i^*(t|t) \tag{23}$$

with $c_i(t) = c_i^*(t|t)$.

In what follows, some discussions of computation, stability, and optimality are provided.

(1) Discussion on computation and stability. The DMPC problem with an infinite prediction horizon usually has a high computational resource requirement, facilitating theoretical analysis, for example, feasibility and stability analysis. In practical applications, we use a DMPC problem with a sufficiently long finite prediction horizon to estimate an infinite prediction horizon case [45]. The

stability analysis of finite horizon DMPC for ICV deserves further investigation.

(2) Discussion on optimality and constraint satisfaction. For an unconstrained ICV, a predesigned platoon control law is optimal for a specific cost function [44]. By contrast, the proposed DMPC-based platoon control gradually converges to the optimal control input and achieves suboptimal platoon control performance. Therefore, the algorithm handles physical constraints and achieves a trade-off between optimality and constraint satisfaction.

The overall RDMP2C algorithm for vehicle i, $i \in \mathcal{V}$ is summarized in Algorithm 3.

Algorithm 3: RDMP2C Algorithm

Require: The weighting matrix Q, the set Δ, the initial assumed state $\widehat{x}_i(k|0) = \boldsymbol{A}^k x_i(0)$, $k \in \mathbb{N}_{\geq 0}$ and other related parameters. Set $t = 1$.

1: **while** vehicle i, the control is not stopped
2: Measure the current system state $x_i(t)$;
3: Receive and evaluate the assumed state trajectories of neighbors $\widehat{\boldsymbol{x}}_j(t)$, $j \in \mathcal{N}_i(t)$ as in Algorithms 1 and 2;
4: Solve the problem $\mathcal{P}_i$ Eq. (20) to generate the optimal control inputs $\boldsymbol{c}_i^*(t)$, and optimal predicted states $\boldsymbol{x}_i^*(t)$;
5: Apply control input $u_i^*(t|t)$ to vehicle i;
6: Broadcast the assumed predicted sequence $\widehat{x}_i(t+k|t)$, $t \in \mathbb{N}_{\geq 0}$ as in Eq. (10) to vehicle j, $j \in \mathcal{N}_i(t)$;
7: $t = t + 1$;
8: **end while**

Note that each vehicle verifies the information from its neighbors in step 2 of Algorithm 3 based on Algorithms 1 and 2 at each time step. When the communication networks change, the predesigned platoon control gain matrix $\boldsymbol{K}(t)$ in Eq. (21) is recalculated and updated.

5. Theoretical analysis

In this section, the recursive feasibility of Algorithm 3 and the convergence analysis of the ICV under Byzantine attacks are discussed. We first present three technical lemmas before proceeding with the feasibility and convergence analyses in Theorem 1.

The following lemma on the nonnegative sequences $\{\alpha_k\}$, $\{\beta_k\}$, and $\{\gamma_k\}$ are fundamental to the resilient platoon analysis, and the proof can be found in Ref. [46].

Lemma 1. Let $\{\alpha_k\}$, $\{\beta_k\}$ and $\{\gamma_k\}$ be nonnegative sequences, suppose $\sum_{k=1}^{\infty}\gamma_k < \infty$ and

$$\alpha_k \leq \alpha_{k-1} - \beta_{k-1} + \gamma_{k-1},\ \forall k \in \mathbb{N}_{\geq 1} \tag{24}$$

then the sequence $\{\alpha_k\}$ converges and $\sum_{k=1}^{\infty}\beta_k < \infty$.

Let $\widetilde{\boldsymbol{c}}_i(t+1)$ be the candidate control input sequence for optimization problem $\mathcal{P}_i$ at time $t+1$. Depending on whether the ICV is under attack at time $t+1$, two candidate input sequences $\widetilde{\boldsymbol{c}}_i(t+1)$ can be constructed.

Case 1. The network $\mathcal{G}(t+1)$ does not change at time $t+1$.

A candidate input sequence $\widetilde{\boldsymbol{c}}_i(t+1)$ at $t+1$ is then created by dropping the first input and appending a terminal zero element of the optimal control at t,

$$\widetilde{c}_i(t+1+k|t+1) = c_i^*(t+1+k|t),\ k \in \mathbb{N}_{\geq 0} \tag{25}$$

Case 2. The network $\mathcal{G}(t+1)$ changes at time $t+1$.

A candidate input sequence $\widetilde{\boldsymbol{c}}_i(t+1)$ is constructed based on the optimal control sequence $u_i^*(t+k|t)$, that is

$$\begin{aligned}\widetilde{c}_i(t+1+k|t+1) = \ & u_i^*(t+1+k|t) - \\ & \boldsymbol{K}(t+1)\textstyle\sum_{j\in\mathcal{N}_i(t+1)} a_{ij}(t+1)\times \\ & \big(\widetilde{x}_i(t+1+k|t+1) - \widehat{x}_j(t+1+k|t+1)\big) + \\ & g_{i0}(\widetilde{x}_i(t+1+k|t+1) - x_0(t+1+k|t+1))\end{aligned} \tag{26}$$

Lemma 2. For the ICV in the presence of F-local Byzantine attacks, if the initial state $x_i(0)$ is feasible and $\sum_{k=0}^{\infty}\|c_i(t+k|t)\|_Q^2 < \infty$, $t \in \mathbb{N}_{\geq 0}$, then the control sequence $c_i(t)$ satisfies $\lim_{t\to\infty} c_i(t) = 0$.

Proof of Lemma 2. To prove the convergence of $c_i(t)$ as $t \to \infty$, we introduce the following function

$$V_i(t) = J_i(\boldsymbol{c}_i^*(t)) = \sum_{k=0}^{\infty}\|c_i^*(t+k|t)\|_Q^2 \tag{27}$$

By choosing the control input sequence $\widetilde{\boldsymbol{c}}_i(t+1) = \mathrm{col}(c_i^*(t+1|t), c_i^*(t+2|t), \ldots)$ for the ICV when there are no attacks at $t+1$, the following relationship can be obtained:

$$\widetilde{V}_i(t+1) = \sum_{k=0}^{\infty}\|\widetilde{c}_i(t+1+k|t+1)\|_Q^2 = V_i(t) - \|c_i^*(t|t)\|_Q^2 \tag{28}$$

The control input sequence $\widetilde{\boldsymbol{c}}_i(t+1)$ is feasible but not necessarily an optimal solution to the problem $\mathcal{P}_i$ at $t+1$. Then, one has

$$V_i(t+1) \leq \widetilde{V}_i(t+1) = V_i(t) - \|c_i^*(t|t)\|_Q^2 \tag{29}$$

It holds that

$$V_i(t+1) - V_i(t) \leq -\|c_i^*(t|t)\|_Q^2 \tag{30}$$

Note that there are at most F-local Byzantine attacks for vehicle i, $i \in \mathcal{V}$, which implies that the control input candidate in Eq. (26) is adopted no more than F times during the time interval $\mathbb{N}_{[1,t_F^i]}$. Additionally, $\overleftarrow{C}_i = 2\sum_{\tau=1}^{F}\sum_{k=0}^{\infty}\|\widetilde{c}_i(t_\tau^i + k|t_\tau^i)\|_Q^2 < \infty$, with $\tau \in \mathbb{N}_{[1,F]}$.

Upon summing up $V_i(t+1) - V_i(t)$ in Eq. (30) from $t = 0$ to k, we obtain

$$\begin{aligned}\lim_{k\to\infty}\sum_{t=0}^{k}(V_i(t+1) - V_i(t)) &= \lim_{k\to\infty} V_i(k+1) - V_i(0) + \overleftarrow{C}_i \\ &\leqslant -\lim_{k\to\infty}\sum_{t=0, t\neq t_\tau^i}^{k}\|c_i^*(t|t)\|_Q^2 + \overleftarrow{C}_i\end{aligned} \tag{31}$$

and $V_i(t)$ as $t \to \infty$, satisfies

$$0 \leqslant V_i(\infty) \leqslant V_i(t) - \lim_{k\to\infty}\sum_{t=0}^{k}\|c_i^*(t|t)\|_Q^2 + \overleftarrow{C}_i < \infty \tag{32}$$

in which $V_i(\infty) = \lim_{t\to\infty} V_i(t)$. From Lemma 1, we obtain that $V_i(t)$ converges as $t \to \infty$. Therefore, we have $\lim_{t\to\infty}\|c_i^*(t|t)\|_Q^2 = 0$, which implies that $\lim_{t\to\infty}\|c_i(t)\| = 0$.

Lemma 3. For any given scalar $\theta \in (0,1)$, suppose that the summable sequence $\{\kappa(t)\}$ satisfies $\lim_{t\to\infty}\kappa(t) = 0$, then it holds that $\lim_{k\to\infty}\sum_{t=0}^{k}\theta^{k-t}\kappa(t) = 0$.

The main theoretical results of ICV under the RDMP2C algorithm are as follows. Note that $\rho(\boldsymbol{S})$ represents its spectral radius of the matrix $\boldsymbol{S}$.

Theorem 1. Consider constrained ICV Eq. (6) in the presence of F-local Byzantine attacks. Suppose that the communication network $\mathcal{G}$ is $(F+1)$-robust, and Byzantine attacks can be detected using Algorithms 1 and 2. If the conditions $\rho(\lim_{p\to\infty}\sum_{s=0}^{p}\boldsymbol{A}_K^{p-s}\boldsymbol{B}\boldsymbol{K}(t))\leq 1$, $\rho(A_K)<1$ are satisfied, with $\boldsymbol{A}_K=\boldsymbol{A}+\boldsymbol{B}\boldsymbol{K}(t)$, and the optimization problem $\mathcal{P}_i$ is feasible at t, $i\in\mathcal{V}_N(t)$, $t\in\mathbb{N}_{\geq 0}$, then

(1) the optimization problem has a feasible solution at $t+1$;
(2) the normal vehicles achieve resilient platoon, with $i,j\in\mathcal{V}_N(t)$ and $v'=|\mathcal{V}_N(t)|$.

Proof of Theorem 1. (1) Proof of the recursive feasibility. For case 1 (i.e., network $\mathcal{G}(t+1)$ does not change), the proof directly follows the proof in Ref. [47] and is omitted here.

For case 2 (i.e., the network $\mathcal{G}(t+1)$ changes), the control input $\widetilde{\boldsymbol{u}}_i(t+1)=\mathrm{col}(\widetilde{u}_i(t+1|t+1),\widetilde{u}_i(t+1+2|t+1),\ldots)$ becomes

$$\widetilde{u}_i(t+1+k|t+1)=u_i^*(t+1+k|t) \tag{33}$$

where $k\in\mathbb{N}_{\geq 0}$. The constraint $\widetilde{u}_i(t+1+k|t+1)\in\mathcal{U}_i$ holds at time $t+1$.

With the initial condition $\widetilde{x}_i(t+1|t+1)=x_i^*(t+1|t)$ and the control inputs in Eq. (33), the corresponding system state $\widetilde{x}_i(t+1+k|t+1)$ becomes

$$\widetilde{x}_i(t+1+k|t+1)=x_i^*(t+1+k|t) \tag{34}$$

where $k\in\mathbb{N}_{\geq 0}$. Hence, constraints Eqs. (20e) and (20f) hold.

From Eqs. (33) and (34), the feasibility is established at time $t+1$ when attacks occur.

(2) Proof of the convergence for the resilient platoon.

By substituting Eq. (21) into Eq. (4), we obtain

$$\boldsymbol{x}(t+1)=(I_{v'}\otimes\boldsymbol{A}+\mathscr{L}_G\otimes\boldsymbol{B}\boldsymbol{K})\boldsymbol{x}(t)+(I_M\otimes\boldsymbol{B})\boldsymbol{c}(t) \tag{35}$$

where $\boldsymbol{x}(t)=\mathrm{col}(x_1(t),x_2(t),\ldots,x_{v'}(t))$, $\mathscr{L}_G=\mathscr{L}+\boldsymbol{G}$, $\boldsymbol{G}=\boldsymbol{G}(t)$, $\mathscr{L}=\mathscr{L}(t)$, $\mathbf{c}(t)=\mathrm{col}(c_1(t),c_2(t),\ldots,c_{v'}(t))$, $\boldsymbol{K}=\boldsymbol{K}(t)$, $I_{v'}\in\mathbb{R}^{v'\times v'}$ is the identity matrix, and the symbol $\otimes$ denotes the Kronecker product. The corresponding variables and matrices for normal vehicles in Eq. (35) have compatible dimensions.

The state of the leader vehicle 0 is $x_0(t)\in\mathbb{R}^n$,

$$x_0(t+1)=\boldsymbol{A}x_0(t)+\boldsymbol{B}u_0(t) \tag{36}$$

Define $\check{x}_i(t)=x_i(t)+d_{i0}$, $\zeta_i(t)=\check{x}_i(t)-x_0(t)$ and $\zeta=\mathrm{col}(\zeta_1,\zeta_2,\ldots,\zeta_{v'})$, $i\in\mathcal{V}_N(t)$, then we have

$$\boldsymbol{\zeta}(t+1)=(I_{v'}\otimes\boldsymbol{A}+\mathscr{L}_G\otimes\boldsymbol{B}\boldsymbol{K})\boldsymbol{\zeta}(t)+(I_{v'}\otimes\boldsymbol{B})\boldsymbol{c}(t)+(I_{v'}\otimes\boldsymbol{B})\boldsymbol{u}_0(t) \tag{37}$$

in which $\boldsymbol{u}_0(t)=\mathbf{1}\otimes u_0(t)$ and $\mathbf{1}$ is a compatible vector with all elements to be 1.

There always exists an orthogonal matrix $\boldsymbol{U}=[\mathbf{1}/\sqrt{v'},U_2,\ldots,U_{v'}]\in\mathbb{R}^{v'\times v'}$ such that the Laplacian matrix is diagonalized, that is, $\boldsymbol{U}^{\mathrm{T}}\mathscr{L}_G\boldsymbol{U}=\mathrm{diag}(0,\lambda_2,\ldots,\lambda_{v'})$, where U_i, $i\in\mathbb{N}_{[2,v']}$ is an orthogonal eigenvector of $\mathscr{L}_G$.

Using the property of Kronecker product, one obtains

$$\begin{aligned}&\left(U^{\mathrm{T}}\otimes I_n\right)(I_{v'}\otimes\boldsymbol{A}+\mathscr{L}_G\otimes\boldsymbol{B}\boldsymbol{K})(\boldsymbol{U}\otimes I_n)\\&=\mathrm{diag}(\boldsymbol{A},\boldsymbol{A}+\lambda_2\boldsymbol{B}\boldsymbol{K},\ldots,\boldsymbol{A}+\lambda_{v'}\boldsymbol{B}\boldsymbol{K})\end{aligned} \tag{38}$$

Define $\widetilde{\boldsymbol{\zeta}}(t)=\mathrm{col}\left(\widetilde{\zeta}_1(t),\widetilde{\zeta}_2(t),\ldots,\widetilde{\zeta}_{v'}\right)=\left(\boldsymbol{U}^{\mathrm{T}}\otimes I_n\right)\boldsymbol{\zeta}(t)$, then Eq. (37) is expressed by

$$\begin{aligned}\widetilde{\boldsymbol{\zeta}}(t+1)=&\,\mathrm{diag}(\boldsymbol{A},\boldsymbol{A}+\lambda_2\boldsymbol{B}\boldsymbol{K},\ldots,\boldsymbol{A}+\lambda_{v'}\boldsymbol{B}\boldsymbol{K})\widetilde{\boldsymbol{\zeta}}(t)+\\&\left(\boldsymbol{U}^{\mathrm{T}}\otimes I_n\right)(I_{v'}\otimes\boldsymbol{B})\boldsymbol{c}(t)-\left(\boldsymbol{U}^{\mathrm{T}}\otimes I_n\right)(I_{v'}\otimes\boldsymbol{B})\boldsymbol{u}_0(t)\end{aligned} \tag{39}$$

Next, we define the transition matrix $\boldsymbol{\Phi}=\mathrm{diag}(\boldsymbol{A},\boldsymbol{A}+\lambda_2\boldsymbol{B}\boldsymbol{K},\ldots,\boldsymbol{A}+\lambda_{v'}\boldsymbol{B}\boldsymbol{K})$ and $\mathscr{B}=\left(\boldsymbol{U}^{\mathrm{T}}\otimes I_n\right)(I_{v'}\otimes\boldsymbol{B})$, then Eq. (37) becomes

$$\widetilde{\boldsymbol{\zeta}}(t+1)=\boldsymbol{\Phi}\widetilde{\boldsymbol{\zeta}}(t)+\mathscr{B}\boldsymbol{c}(t)-\mathscr{B}\boldsymbol{u}_0(t) \tag{40}$$

which implies that $\widetilde{\boldsymbol{\zeta}}(t)=\boldsymbol{\Phi}^t\widetilde{\boldsymbol{\zeta}}(0)+\sum_{k=0}^{t-1}\boldsymbol{\Phi}^k\mathscr{B}\mathbf{c}(t-1-k)-\sum_{k=0}^{t-1}\boldsymbol{\Phi}^k\mathscr{B}\boldsymbol{u}_0(t-1-k)$, $t\in\mathbb{N}_{\geq 1}$.

It holds that $\widetilde{\zeta}_1(t)=1/\sqrt{v'}\left(\sum_{i=1}^{v'}\zeta_i(t)\right)=0$. Also, owing to $\rho(\boldsymbol{A}+\lambda_i\boldsymbol{B}\boldsymbol{K})<1$, $i\in\mathbb{N}_{[2,v']}$, we obtain the term $\lim_{t\to\infty}\boldsymbol{\Phi}^t\widetilde{\boldsymbol{\zeta}}(0)=0$.

In light of $\rho(\boldsymbol{A}+\lambda_i\boldsymbol{B}\boldsymbol{K})<1$, there always exists a constant $\beta\in(0,1)$, such that

$$\|\boldsymbol{\Phi}^t\|\leq\beta^t<1 \tag{41}$$

Define $E(t-1-k)=\|I_{v'}\otimes\boldsymbol{B}\|\|\mathbf{c}(t-1-k)\|$. Using the Cauchy–Schwarz inequality and Eq. (41), we have

$$\begin{aligned}\lim_{t\to\infty}\textstyle\sum_{k=0}^{t-1}\boldsymbol{\Phi}^k\mathscr{B}\mathbf{c}(t-1-k)&\leq\lim_{t\to\infty}\textstyle\sum_{k=0}^{t-1}\|\Phi^k\|E(t-1-k)\\&\leq\lim_{t\to\infty}\textstyle\sum_{k=0}^{t-1}\beta^kE(t-1-k)\end{aligned} \tag{42}$$

From Lemmas 2 and 3, we obtain

$$\lim_{t\to\infty}\sum_{k=0}^{t-1}\boldsymbol{\Phi}^k\mathscr{B}\mathbf{c}(t-1-k)=0 \tag{43}$$

Similarly, it holds that

$$\lim_{t\to\infty}\sum_{k=0}^{t-1}\boldsymbol{\Phi}^k\mathscr{B}\boldsymbol{u}_0(t-1-k)=0 \tag{44}$$

Therefore, the constrained ICVs under F-local Byzantine attacks achieve a platoon control objective with guaranteed resilience. The proof is completed.

Although most current studies on platoon control emphasize error dynamics and require vehicles to receive information from the leader, practical limitations can impede some vehicles from accessing the leader's data because of restricted communication ranges. In contrast, only a portion of the follower vehicles are required to obtain information from the leader in the proposed platoon control design, making this work more general and practical.

6. Simulation

In this section, we describe numerical simulations to verify the effectiveness of the proposed RDMP2C strategy for ICV under 1-local Byzantine attacks. A platoon consisting of seven vehicles moves along a single lane with a fixed distance gap d = 5 m. The longitudinal dynamics of vehicle i, $i=0,\cdots,6$ are given by

$$x_i(t+1)=\boldsymbol{A}x_i(t)+\boldsymbol{B}u_i(t) \tag{45}$$

where $x_i(t)=[s_i(t),v_i(t),a_i(t)]^{\mathrm{T}}\in\mathbb{R}^3$ includes the position $s_i(t)$, the speed $v_i(t)$ and the acceleration $a_i(t)$.

$$\boldsymbol{A}=\begin{bmatrix}1&T&0.5T^2\\0&1&T\\0&0&1-\frac{T}{\tau}\end{bmatrix}\text{ and }\boldsymbol{B}=\begin{bmatrix}0\\0\\\frac{T}{\tau}\end{bmatrix} \tag{46}$$

where $T=0.2$ and $\tau=0.6$ are the sampling time and vehicle engine constant, respectively. The control input constraints are $|u_i(t)|\leq 3$. The vehicle system constraints are given as $0\leq v_i(t)\leq 20$ m·s^{-1} and $|a_i(t)|\leqslant 3$ m·s^{-2}. Lead vehicle 0 starts at a low speed, accelerates to reach a speed of 18 m·s^{-1}, and keeps a constant speed. That is,

$$v_0(t)=\begin{cases}10\text{ m}\cdot\text{s}^{-1} & t\leqslant 2\text{ s}\\10+2t\text{ m}\cdot\text{s}^{-1} & 2\text{ s}<t\leqslant 6\text{ s}\\18\text{ m}\cdot\text{s}^{-1} & 14\text{ s}<t\leqslant 6\text{ s}\end{cases} \tag{47}$$

with $s_0(0) = 0$ and $a_0(0) = 0$. Only a portion of follower vehicles can receive information from the lead vehicle 0. The initial states of six vehicles are $x_1(0) = [-5.2, 20, -0.4]^{\mathrm{T}}$, $x_2(0) = [-10.3, 20, -0.4]^{\mathrm{T}}$, $x_3(0) = [-15.9, 20, -0.2]^{\mathrm{T}}$, $x_4(0) = [-20.7, 20, 0.2]^{\mathrm{T}}$, $x_5(0) = [-25.7, 20, 0.3]^{\mathrm{T}}$, and $x_6(0) = [-30.7, 20, -0.1]^{\mathrm{T}}$, respectively. The 2-robust communication network among ICV is described by the neighboring sets: $\mathcal{N}_1(0) = \{0, 2\}$, $\mathcal{N}_2(0) = \{0, 1\}$, $\mathcal{N}_3(0) = \{1, 2\}$, $\mathcal{N}_4(0) = \{2, 3\}$, $\mathcal{N}_5(0) = \{3, 4\}$, and $\mathcal{N}_6(0) = \{4, 5\}$.

Ensuring safety and rational driving exploration and exploitation are crucial for the online evolution of autonomous driving. These principles are the key factors affecting the safety, comfort, and trust of drivers and passengers in online autonomous driving. This section introduces the corresponding modeling methods for these two principles, including predictive safe-driving envelope modeling and a rational exploration and exploitation scheme.

Table 1
Two types of Byzantine attacks.

Attack type	Attack duration	Attack intensity	Vehicle index
Byzantine attack A_1	$\mathbb{N}_{[36,40]}$	$-0.7 + 1.4\mathrm{rand}(3,1)$	5
Byzantine attack A_2	$\mathbb{N}_{[51,55]}$	$-3.0 + 6.0\mathrm{rand}(3,1)$	3

The prediction horizon is chosen as $N = 12$ and the estimation error set is $\Delta = \{x \in \mathbb{R}^3 \mid \|x\| \leq 0.5\}$, using a weighting matrix $\Psi = 1$. Following the method in Ref. [44], the pre-designed consensus gain matrix is designed as $K(0) = [-0.4042, -1.0015, -0.5387]$.

Two Byzantine attacks, A_1 and A_2 are randomly generated and injected into follower vehicle 5 and vehicle 3, respectively, as listed in Table 1. The resilience parameter is chosen as $\sigma = 1.6$, and the maximum attack duration is $W = 5$. The four simulation scenarios (S_1, S_2, S_3 and S_4) listed in Table 2 [44,48] are designed to verify the platoon control performance of the proposed framework.

In the first two baseline scenarios, the ICVs are simulated without considering Byzantine attacks. In S_1, we simulate the pre-designed consensus-based platoon control method (PCPC) [44]. The results, including the system states, system error states, and control inputs, are presented in Fig. 2. Fig. 2(a) demonstrates that follower vehicles maintain the desired relative distance and consistent speed. However, the PCPC method cannot guarantee constraint satisfaction in terms of physical constraints including the speed, acceleration, and control input constraints (Figs. 2(b), (c), and (f)).

In S_2, we test the DMPC method [48] for a constrained ICV without Byzantine attacks, to facilitate comparison. The simulation results shown in Fig. 3 demonstrate that the DMPC method achieves the platoon control objective while guaranteeing constraint satisfaction.

Table 2
Simulation scenarios.

Conditions	Scenario 1 (S_1)	Scenario 2 (S_2)	Scenario 3 (S_3)	Scenario 4 (S_4)
ICV under attack A_1	–	–	√	√
ICV under attack A_2	–	–	√	√
ICV with normal communication	√	√	√	√
Attack detection mechanism	–	–	–	√
Control method	PCPC [44]	DMPC [48]	DMPC [48]	RDMP2C

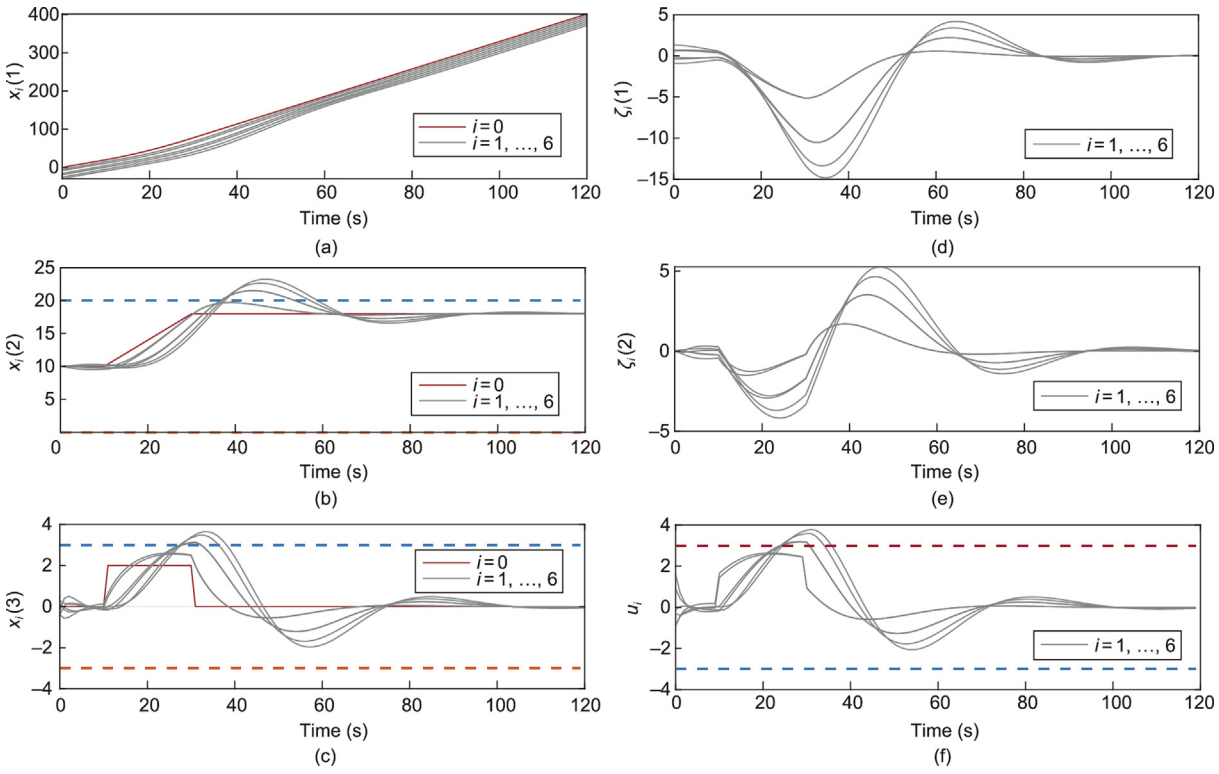

Fig. 2. ICV system states and control input signals under the PCPC method in S_1. The ICVs (one leader vehicle 0 with a red line and six follower vehicles with gray lines) are attack-free. Panel (a) depicts the position of seven vehicles. Panel (b) plots the vehicle velocities. The dashed lines represent the bound of the velocity. Panel (c) shows the acceleration of the ICV. Here, the dashed lines denote the bound of the acceleration speed. Panels (d) and (e) display the corresponding position errors and velocity errors of six follower vehicles, respectively. In panel (f), we provide the control input signals of six follower vehicles.

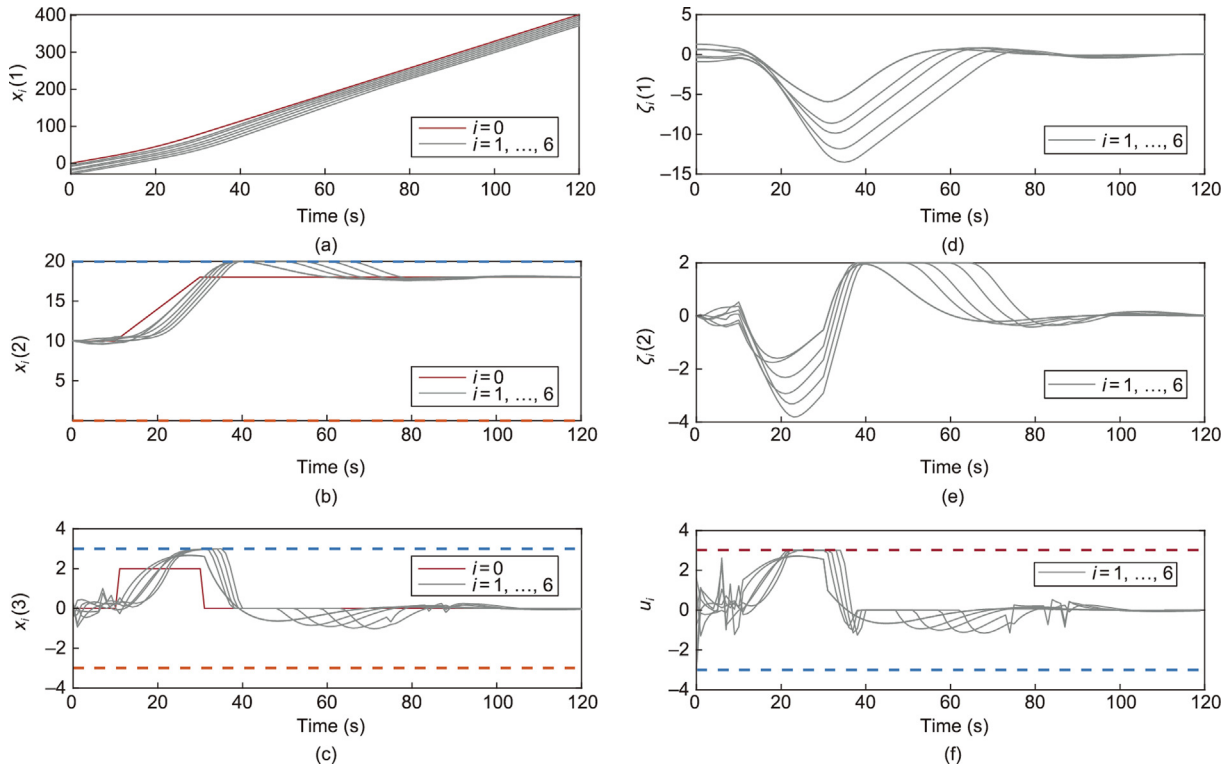

Fig. 3. ICV system states and control input signals under the DMPC method in S_2. The ICVs (one leader vehicle 0 with a red line and six follower vehicles with gray lines) are attack-free. Panel (a) depicts the position of seven vehicles. Panel (b) plots the vehicle velocities. The dashed lines represent the bound of the velocity. Panel (c) shows the acceleration of the ICV. Here, the dashed lines denote the bound of the acceleration speed. Panels (d) and (e) display the corresponding position errors and velocity errors of six follower vehicles, respectively. In panel (f), we provide the control input signals of six follower vehicles.

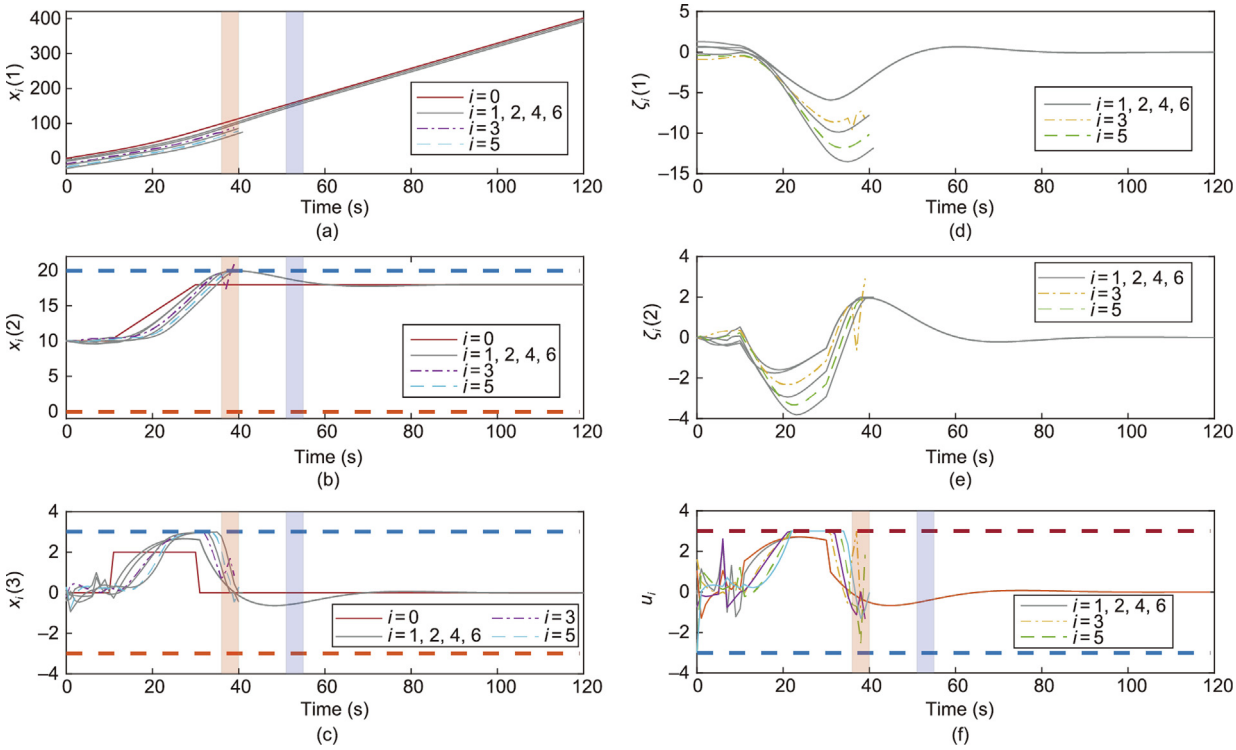

Fig. 4. ICV system states and control input signals under the DMPC method in S_3. The ICV (one leader vehicle 0 with a red line and six follower vehicles with gray lines) are under $F = 1$ local Byzantine attack. Panel (a) depicts the position of seven vehicles. Panel (b) plots the vehicle velocities. The dashed lines represent the bound of the velocity. Panel (c) shows the acceleration of the ICV. Here, the dashed lines denote the bound of the acceleration speed. Panels (d) and (e) display the corresponding position errors and velocity errors of six follower vehicles, respectively. In panel (f), we provide the control input signals of six follower vehicles. The red and blue areas represent the periods under the Byzantine attack A_1 and A_2, respectively.

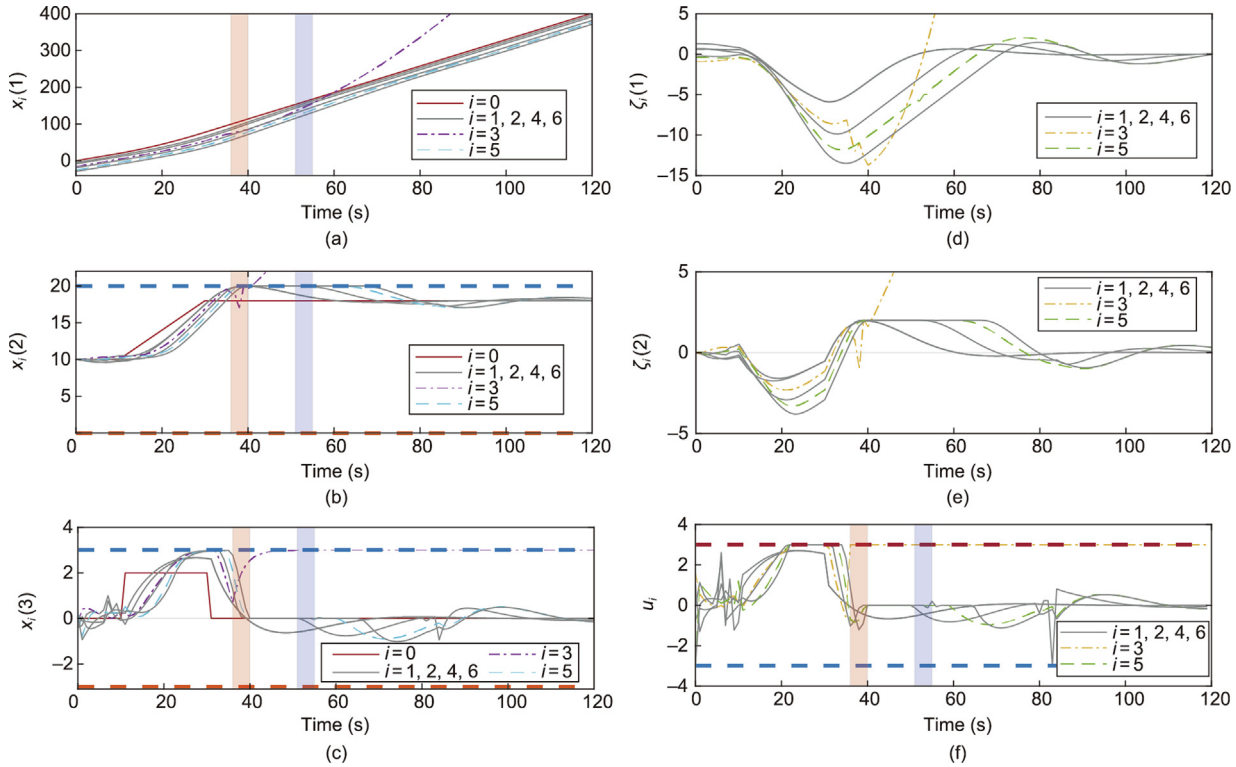

Fig. 5. Vehicle system states and control input signals in S_4. The ICVs (one leader vehicle 0 with a red line and six follower vehicles with gray lines) are under $F = 1$ local Byzantine attack. Panel (a) depicts the position of seven vehicles. Panel (b) plots the vehicle velocities. The dashed lines represent the bound of the velocity. Panel (c) shows the acceleration of the ICV. Here, the dashed lines denote the bound of the acceleration speed. Panels (d) and (e) display the corresponding position errors and velocity errors of six follower vehicles, respectively. In panel (f), we provide the control input signals of six follower vehicles. The red and blue areas represent the periods under the Byzantine attack A_1 and A_2, respectively.

In the last two scenarios, the ICVs are attacked by two types of Byzantine attackers (see Table 1). In S_3, the DMPC method cannot achieve resilient platoon control without an attack detection mechanism. In Figs. 4(a) and (d), follower vehicles $i = 3, ..., 6$ do not operate normally and stop operating. More precisely, the normal follower vehicles $i = 4, ..., 6$ cannot maintain the desired spacing and stability when Byzantine attacker A_2 attacks vehicle 3.

In S_4, the proposed RDMP2C framework is simulated, and the results are shown in Fig. 5. The stability and resilience of the ICV are guaranteed under the proposed RDMP2C. Because of the distributed attack detection algorithms, the adversarial information from vehicle 3 is detected and discarded. Consequently, the following normal vehicles $i = 4, \cdots, 6$ retain the desired resilient platoon behavior. Further, in the second verification algorithm, normal vehicles can achieve resilient platoon control when vehicle 5 is attacked by slight attacker A_1.

Therefore, the proposed RDMP2C algorithm achieves a trade-off between optimality and constraint satisfaction while ensuring the resilience of the ICV under F-local Byzantine attacks. The main advantages of the proposed algorithm with respect to resilient control algorithms [11–14,16,17] lie in its ability to handle Byzantine attacks on constrained vehicles. The aforementioned resilient control algorithms ensure only the resilience of the ICV under DoS or FDI attacks. Moreover, the network robustness requirement is significantly relaxed compared to MSR-type algorithms [20,39]. Resilient platoon control is achieved over an $(F + 1)$-robust graph despite F-local Byzantine attacks.

7. Conclusions

This paper presented a resilient DMPC-based platoon control framework for constrained ICV under F-local Byzantine attacks. A distributed Byzantine attack detection mechanism was developed to enable each vehicle to detect a Byzantine attack by relying only on the $(F + 1)$-robust graph. Communication among ICV was classified into different types based on the attack intensity: normal, recoverable, and adversarial communication. Based on the resilience set and parameters, we developed a second verification algorithm to recover the communication channels under slight attacks, which offered the opportunity to further relax the robustness requirements of communication networks. The proposed resilient platoon control strategy, which took advantage of the predesigned optimal control and DMPC optimization, ensured robust constraint satisfaction and optimized platoon control performance. A rigorous theoretical analysis was conducted, including recursive feasibility and closed-loop stability. The simulation results verified the effectiveness of the proposed algorithm.

This study suggests several directions for future research. This study examines longitudinal ICV under local Byzantine attacks. The proposed RDMP2C framework can be extended to handle constrained ICV in more complex environments such as time-varying communication networks [26]. Also, we expect that the proposed approach can be applied to address the flexible ICV platoon problem as demonstrated in Ref. [49]. Furthermore, advanced machine learning methods like graph neural networks [50] hold promise for detecting adversarial cyberattacks on ICVs in intricate real-world situations.

Acknowledgments

The authors acknowledge the financial support from the Natural Sciences and Engineering Research Council of Canada (NSERC) and thank the anonymous reviewers for their valuable suggestions.

Compliance with ethics guidelines

Henglai Wei, Hui Zhang, Kamal AI-Haddad, and Yang Shi declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Feng S, Zhang Y, Li SE, Cao Z, Liu HX, Li L. String stability for vehicular platoon control: definitions and analysis methods. Annu Rev Control 2019;47:81–97.
[2] Ju Z, Zhang H, Li X, Chen X, Han J, Yang M. A survey on attack detection and resilience for connected and automated vehicles: from vehicle dynamics and control perspective. IEEE Trans Intell Veh 2022;7(4):815–37.
[3] Limbasiya T, Teng KZ, Chattopadhyay S, Zhou J. A systematic survey of attack detection and prevention in connected and autonomous vehicles. Veh Commun 2022;37:100515.
[4] Sun X, Yu FR, Zhang P. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans Intell Transp Syst 2022;23(7):6240–59.
[5] Sandberg H, Gupta V, Johansson KH. Secure networked control systems. Annu Rev Control Robot Auton Syst 2022;5(1):445–64.
[6] Zhang D, Feng G, Shi Y, Srinivasan D. Physical safety and cyber security analysis of multi-agent systems: a survey of recent advances. IEEE/CAA J Autom Sin 2021;8(2):319–33.
[7] Chen J, Shi Y. Stochastic model predictive control framework for resilient cyber-physical systems: review and perspectives. Phil Trans R Soc A 2021;379 (2207):20200371.
[8] Zhou C, Hu B, Shi Y, Tian YC, Li X, Zhao Y. A unified architectural approach for cyberattack-resilient industrial control systems. Proc IEEE 2021;109(4):517–41.
[9] Abdollahi Biron Z, Dey S, Pisu P. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Trans Intell Transp Syst 2018;19(12):3893–902.
[10] Merco R, Ferrante F, Pisu P. A hybrid controller for DOS-resilient string-stable vehicle platoons. IEEE Trans Intell Transp Syst 2021;22(3):1697–707.
[11] Xiao S, Ge X, Han QL, Zhang Y. Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks. IEEE Trans Cybern 2022;52(11):12003–15.
[12] Zhang D, Shen YP, Zhou SQ, Dong XW, Yu L. Distributed secure platoon control of connected vehicles subject to DoS attack: theory and application. IEEE Trans Syst Man Cybern Syst 2021;51(11):7269–78.
[13] Zhao Y, Liu Z, Wong WS. Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances. IEEE Trans Intell Transp Syst 2022;23(8):10945–56.
[14] Xu X, Li X, Dong P, Liu Y, Zhang H. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. IEEE Trans Veh Technol 2021;70(6):5524–36.
[15] Zhao C, Gill JS, Pisu P, Comert G. Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing. IEEE Trans Intell Transp Syst 2022;23(7):9078–88.
[16] Biroon RA, Biron ZA, Pisu P. False data injection attack in a platoon of CACC: real-time detection and isolation with a PDE approach. IEEE Trans Intell Transp Syst 2022;23(7):8692–703.
[17] Ju Z, Zhang H, Tan Y. Distributed deception attack detection in platoon-based connected vehicle systems. IEEE Trans Veh Technol 2020;69(5):4609–20.
[18] Ghane S, Jolfaei A, Kulik L, Ramamohanarao K, Puthal D. Preserving privacy in the internet of connected vehicles. IEEE Trans Intell Transp Syst 2021;22 (8):5018–27.
[19] Aladwan MN, Awaysheh FM, Alawadi S, Alazab M, Pena TF, Cabaleiro JC. TrustE-VC: trustworthy evaluation framework for industrial connected vehicles in the cloud. IEEE Trans Ind Inform 2020;16(9):6203–13.
[20] Dibaji SM, Ishii H. Resilient consensus of second-order agent networks: asynchronous update rules with delays. Automatica 2017;81:123–32.
[21] Ruan M, Gao H, Wang Y. Secure and privacy-preserving consensus. IEEE Trans Autom Control 2019;64(10):4035–49.
[22] Hadjicostis CN, Domínguez-García AD. Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus. IEEE Trans Autom Control 2020;65(9):3887–94.
[23] Fang W, Zamani M, Chen Z. Secure and privacy preserving consensus for second-order systems based on Paillier encryption. Syst Control Lett 2021;148:104869.
[24] Mitra A, Sundaram S. Byzantine-resilient distributed observers for LTI systems. Automatica 2019;108:108487.
[25] LeBlanc HJ, Zhang H, Koutsoukos X, Sundaram S. Resilient asymptotic consensus in robust networks. IEEE J Sel Areas Commun 2013;31 (4):766–81.
[26] Usevitch J, Panagou D. Resilient leader-follower consensus to arbitrary reference values in time-varying graphs. IEEE Trans Autom Control 2020;65 (4):1755–62.
[27] Fiore D, Russo G. Resilient consensus for multi-agent systems subject to differential privacy requirements. Automatica 2019;106:18–26.
[28] Wei H, Zhang K, Shi Y. Self-triggered min–max DMPC for asynchronous multiagent systems with communication delays. IEEE Trans Ind Inform 2022;18(10):6809–17.
[29] Shi Y, Zhang K. Advanced model predictive control framework for autonomous intelligent mechatronic systems: a tutorial overview and perspectives. Annu Rev Control 2021;52:170–96.
[30] Dunbar WB, Murray RM. Distributed receding horizon control for multi-vehicle formation stabilization. Automatica 2006;42(4):549–58.
[31] Li H, Shi Y, Yan W, Liu F. Receding horizon consensus of general linear multi-agent systems with input constraints: an inverse optimality approach. Automatica 2018;91:10–6.
[32] Wang Q, Duan Z, Lv Y, Wang Q, Chen G. Linear quadratic optimal consensus of discrete-time multi-agent systems with optimal steady state: a distributed model predictive control approach. Automatica 2021;127:109505.
[33] Ishii H, Zhu Q. Security and resilience of control systems: theory and applications. Cham: Springer; 2022.
[34] Zheng Y, Li S, Wang J, Cao D, Li K. Stability and scalability of homogeneous vehicular platoon: study on the influence of information flow topologies. IEEE Trans Intell Transp Syst 2016;17(1):14–26.
[35] Deng C, Zhang D, Feng G. Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks. Automatica 2022;139:110172.
[36] Lu AY, Yang GH. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Autom Control 2018;63(6):1813–20.
[37] Müller MA, Reble M, Allgöwer F. Cooperative control of dynamically decoupled systems via distributed model predictive control. Int J Robust Nonlinear Control 2012;22(12):1376–97.
[38] Wang Z, Ong CJ. Distributed model predictive control of linear discrete-time systems with local and global constraints. Automatica 2017;81:184–95.
[39] Mustafa A, Modares H, Moghadam R. Resilient synchronization of distributed multi-agent systems under attacks. Automatica 2020;115:108869.
[40] Dibaji SM, Ishii H, Tempo R. Resilient randomized quantized consensus. IEEE Trans Autom Control 2018;63(8):2508–22.
[41] Usevitch J, Panagou D. Determining r- and (r, s)-robustness of digraphs using mixed integer linear programming. Automatica 2020;111:108586.
[42] Chisci L, Rossiter JA, Zappa G. Systems with persistent disturbances: predictive control with restricted constraints. Automatica 2001;37(7):1019–28.
[43] You K, Xie L. Network topology and communication data rate for consensusability of discrete-time multi-agent systems. IEEE Trans Autom Control 2011;56(10):2262–75.
[44] Movric KH, Lewis FL. Cooperative optimal control for multi-agent systems on directed graph topologies. IEEE Trans Autom Control 2014;59(3):769–74.
[45] Boccia A, Grüne L, Worthmann K. Stability and feasibility of state constrained MPC without stabilizing terminal constraints. Syst Control Lett 2014;72:14–21.
[46] Chang TH, Nedić A, Scaglione A. Distributed constrained optimization by consensus-based primal-dual perturbation method. IEEE Trans Autom Control 2014;59(6):1524–38.
[47] Wei H, Liu C, Shi Y. A robust distributed model predictive control framework for consensus of multi-agent systems with input constraints and varying delays. 2022. arXiv:2209.08785.
[48] Wei H, Sun Q, Chen J, Shi Y. Robust distributed model predictive platooning control for heterogeneous autonomous surface vehicles. Control Eng Pract 2021;107:104655.
[49] Liu P, Kurt A, Ozguner U. Distributed model predictive control for cooperative and flexible vehicle platooning. IEEE Trans Control Syst Technol 2019;27 (3):1115–28.
[50] Wang Y, Liu Y, Shen Z. Revisiting item promotion in GNN-based collaborative filtering: a masked targeted topological attack perspective. Proc AAAI Conf Artif Intell 2023;37(12):15206–14.