Safeguard Vehicle Platooning Based on Resilient Control Against False Data Injection Attacks

Chengcheng Zhao, *Member, IEEE*, Ruijie Ma, Mengzhi Wang, *Member, IEEE*, Jinming Xu, *Member, IEEE*, and Lin Cai, *Fellow, IEEE*

***Abstract*— This paper investigates secure control for homogeneous vehicle platoons in the presence of false data injection attacks with low communication and computation costs. We consider a scenario where each vehicle within the platoon transmits a local state vector to multiple neighboring vehicles. By leveraging these shared vectors from both preceding and following vehicles, we propose a novel and effective resilient controller for vehicle platoons against node/communication link attacks. More specifically, each vehicle determines the local state deviation vectors from neighboring vehicles. It then eliminates the vectors that are farthest from the origin, with the number of removed vectors equivalent to the maximum number of attacks. This approach offers a considerable advantage by mitigating the effects of abnormality and manipulation, making it robust against arbitrary information tampering within a pre-defined upper boundary for manipulated broadcast information. Importantly, we establish specific conditions for the proposed resilient design to guarantee the internal stability of the vehicle platoon under attacks. Extensive simulations and experiments involving four TurtleBot3s are conducted to demonstrate the effectiveness of the proposed resilient controller.**

***Index Terms*— Vehicle platooning, attack resilience, stability analysis.**

I. Introduction

With continuous progress in autonomous driving and vehicle-to-vehicle (V2V) communication technologies, the concept of vehicle platooning has emerged as an extensively studied topic in both academia and industry. Vehicle platooning refers to a coordinated group of vehicles traveling closely together. This groundbreaking technology holds immense potential for revolutionizing the transportation industry, as it can effectively reduce traffic congestion, enhance fuel efficiency, and improve road safety. However, due to the high integration of communication and control, it also raises critical security challenges that need to be addressed.

From the perspective of every single car within a vehicle platoon, modern cars are equipped with complex distributed computer systems. These systems with diverse processors interconnected through internal networks like Controller Area Network (CAN) offer significant benefits in terms of efficiency, safety, and cost. However, it has also introduced new surfaces for potential attacks. One such vulnerability is remote attackers exploiting the vehicle's network for location tracking and audio extraction, using methods like Bluetooth and cellular technology [1]. From the perspective of Cooperative Adaptive Cruise Control (CACC) functionality, its reliable performance is heavily reliant on vehicular communications. However, the vulnerability of these communications poses a significant threat to the overall security of the platoon system. Specifically, the effectiveness of CACC hinges on information exchange between vehicles, allowing for coordinated and synchronized actions. Unfortunately, the susceptibility of vehicular communications introduces a potential entry point for external attacks, thereby jeopardizing the entire platoon system's security and even causing fatality. Although much research and industry efforts have been made to secure vehicular communications [2], it is still a challenging issue to address and also hinders the realistic deployment of vehicular communications [3]. It should be pointed out that with the growth of vehicle platoon system complexity, the attack surface increases accordingly. It is desirable to improve the resilience of the control strategy in the vehicle platoon, as here resilience means the capacity to withstand or to recover quickly from misbehaving hardware and software, malfunctioning communication processes, etc.

With the seamless connection between cyberspace (e.g., V2V and CAN communications) and physical space (e.g., vehicle dynamics) in vehicle platoons, communication delay sensitivity, and control safety-critical become more severe in the presence of cyber attacks. Resilient control design faces two kinds of challenges. First, under CACC, vehicles follow their predecessor through local controllers with information from neighbors via sensing and communication techniques. The global formation of the vehicle platoon is safety critical and usually requires a short period and low delay V2V communication. During the whole control period, it is hard for vehicles to verify the integrity of local sensors

Manuscript received 19 September 2023; revised 13 February 2024 and 21 May 2024; accepted 26 June 2024. Date of publication 17 July 2024; date of current version 1 November 2024. This work was supported in part by the National Natural Science Foundation of China under Grant 62273305, in part by Zhejiang Provincial Natural Science Foundation under Grant LZ22F030010, and in part by the Young Elite Scientist Sponsorship Program by the Cast of China Association for Science and Technology under Grant YESS20210158. The Associate Editor for this article was R. Malekian. *(Corresponding author: Chengcheng Zhao.)*

Chengcheng Zhao, Ruijie Ma, and Jinming Xu are with the College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: chengchengzhao@zju.edu.cn; maruijie13@zju.edu.cn; jimmyxu@zju.edu.cn).

Mengzhi Wang is with the College of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China (e-mail: wangmz@buct.edu.cn).

Lin Cai is with the Department of Electrical Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada (e-mail: cai@ece.uvic.ca).

Digital Object Identifier 10.1109/TITS.2024.3424687

or local communication information. Meanwhile, platooning is a delay-sensitive application since safety-critical control poses strict deadlines for message delivery in the vehicle platoon. The applied security mechanisms must consider these constraints and impose low processing and messaging overhead, which can limit the usage of cryptographic methods. Moreover, it is possible for the attacker to break through these cryptographic-based integrity verification methods due to the broadcast characteristics of V2V communications. Secondly, since vehicle platooning is a safety-critical control system, it requires a resilient design to meet the system stability requirements theoretically at the first stage. As a resilient control strategy has to be effective for different attack manipulation mechanisms, the system modeling and analysis is hard. Thus, we aim to design an effective resilient controller for vehicle platooning under node/communication manipulation attacks, where the communication information integrity is damaged.

Some research attention has been dedicated to resilient control for vehicle platoons under false data injection (FDI) attacks. In the context of cloud-based vehicle platooning, researchers have proposed the implementation of a health monitoring system and a human-robot interaction system to effectively detect and mitigate the impact of communication abnormalities caused by disturbances or attacks [4], [5]. It is important to note that these scenarios require a control center. Furthermore, in the case of Adaptive Cruise Control (ACC), which is not scalable for multiple vehicles, certain researchers have focused on developing attack detection and mitigation methods against sensor Denial-of-Service (DoS) and delay injection attacks in a single car [6], [7]. Regarding CACC, safeguards have been established, such as switching to ACC once an attack is detected or implementing slide mode control-based resilient controllers, to ensure system safety even with one misbehaving car [8], [9]. To address multiple sensor or communication attacks, both secure state estimation-based and reachable set-based resilient strategies have been proposed. However, these strategies often require a significant computational cost or are limited to specific network topology and a limited number of attacks [10], [11], [12], [13]. It should be noted that most of these designs are only applicable to the vehicle platoon, where each vehicle utilizes information from a single predecessor for control. In addition, other approaches have been explored, such as leveraging channel redundancy, Blockchain technology, machine learning methods, etc., to detect and mitigate false data injection attacks [14], [15], [16]. However, these methods may incur additional costs in terms of communication and data collection.

Because each vehicle in a platoon can possess a large communication range of up to one kilometer and can utilize information from multiple neighbors for local control, there is potential to exploit information redundancy and enhance the resilient design to reduce the adverse effects of attacks. Thus, our objective is to propose a novel attack-resilient control algorithm for CACC. We consider the homogeneous vehicle platoon under FDI attacks, where each vehicle sends a local state vector to communicate with neighbors and uses received information to realize resilient control. The effectiveness of the proposed resilient controller is demonstrated through both simulations and experiments. Our contributions are threefold.

- We investigate the resilience control design issue for vehicle platoons against FDI in communication links or nodes, where each vehicle sends a local state vector to communication neighbors and uses received information for control and the number of manipulated communication links or nodes is limited.
- We propose a distributed attack robust controller for the vehicle platoon. Under the proposed resilient methods, each vehicle only compares the local state vector distances among neighbors and leverages the filtered information for local control.
- We use the discrete-time model to show that the vehicle platoon can achieve global stability. The relationship between the resilience, the number of manipulated links/nodes, and the stability is revealed.

The following structure guides the rest of this paper. Section II provides a summary of related work. Section III presents the preliminaries and problem formulation. Section IV outlines the system design. In Section V, we analyze the performance of the system. Numerical studies to validate the main results are presented in Section VI and the resilient control algorithm is experimentally implemented on a platoon system composed of four TurtleBot3s in Section VII. Finally, Section VIII concludes the paper and provides a glimpse into future work.

II. Related Work

Recently, much attention has been paid to the security issues of vehicle platoons. Ju et al. provided a comprehensive survey about the security of vehicle platoons [17]. We can roughly categorize the existing work into three main streams, i.e., attack modeling [18], [19], attack detection [20], [21], [22], and resilient control. Typically, resilient control design for vehicle platoon systems can be broadly divided into two categories: those against information unavailability (e.g., DoS attacks) and those against integrity attacks (e.g., FDI). For an overview of resilient control in networked control systems, interested readers can consult the survey [23].

A. DoS Attacks

Various approaches have been developed to mitigate the effect of DoS attacks on vehicle platoons, each tailored to specific system models and control performance requirements. For instance, Biron et al. developed a distributed resilient control strategy based on the adaptive observer and a delay estimator for CACC against DoS attacks [24]. In addition, much attention has been paid to vehicle platooning with nonlinearities, uncertainties, disturbances, or multiple DoS attacks [25], [26]. Liu et al. proposed self-organization mechanisms, i.e., resilient control strategies, against heterogeneous vehicles, acceleration limits, and communication failures [27], which work when DoS attacks can be viewed as communication failures.

B. Integrity Attacks

In the context of integrity attacks, e.g., FDI attacks, researchers have investigated countermeasures for four categories of attacks, i.e., controller manipulation attacks, sensor attacks, communication manipulation attacks, and communication-sensor deception attacks. Under controller manipulation attacks, the control input or control gain in the vehicle can be arbitrarily manipulated under physical constraints. To defend against such attacks, different defense strategies have been studied. These include attack detection and switching to ACC mode [8], slide mode control based secure control [9], [28], reachability-based safe control [10], and learning-based attack detection, identification and recovery [29]. In particular, DeBruhl et al. proposed a model-based method to detect internal controller attacks and switch to adaptive cruise control for safe vehicle platooning with the predecessor following information flow, where each vehicle uses broadcast information via the secure dedicated short-range communication for detection [8]. Concerning sensor attacks, it is typically assumed that communication is secure. Several countermeasures have been explored, including secure state estimation using sensor redundancy [11], secure communication-based state estimation [13], [14], [30]. Security is guaranteed only when the number of deceived sensors is limited. For instance, Yang et al. developed a sensor-redundancy-based state estimation method against sensor attacks for vehicle platooning with the predecessor following information flow [11]. In the case of communication manipulation attacks, attackers compromise only the communication link and arbitrarily modify communication data, assuming sensor data is secure. Defense strategies include communication profile pattern recognition based secure policy [31], human-involved attack detection and recovery [5], ACC and CACC switching via game [32]. As an illustration, Petrillo et al. developed a secure adaptive control against simultaneous communication delays and cyber-attacks for vehicle platooning with general communication topology, where enough data for the case without cyberattacks is required to construct trusted information about the average distance, speed, and acceleration of the formation [31]. The secure control ensures that only the secure information will be used for local control. Boddupalli et al. conducted a comprehensive investigation of machine learning-based resilient CACC, which focused on different attacks that underlie V2X communication technology [33]. To defend against communication manipulation attacks or sensor attacks, Raja et al. integrated Blockchain with a Multi-Agent Deep Reinforcement Learning method to enhance the fuel efficiency and throughput of gap-following CACC [15]. Considering communication-sensor deception attacks, Mousavinejad et al. proposed a set-membership filtering-based attack detection and recovery method for vehicle platoons with the predecessor following information flow [12]. However, these strategies are often limited to specific network topology or induce much computation and communication load to the system. In addition, Pirani et al. studied how communication connectivity affects the resilience of the commonly used distributed estimation and control in vehicle platooning, where the constant spacing is considered [34].

Note that in the case of platoons with general communication topologies, such as the topology under which each vehicle received information from multiple front and back vehicles, each communication link may be susceptible to attacks. Designing control strategies that can ensure the resilience of the platoon system with general communication interaction and low communication and computation overhead is still an open problem.

III. Problem Formulation

In this section, we first provide the vehicle model and communication network model among all vehicles. Then, the platoon controller and the FDI attack model are presented followed by the problems of interest. Some of the important notations are given below.

Notations: Let $\mathbb{R}$ and $\mathbb{Z}$ represent the set of real numbers and the set of integers, respectively. The set of integers greater than or equal to some integer $q \in \mathbb{Z}$ is denoted as $\mathbb{Z}_{\geq q}$. Let $\mathbb{R}^{m\times n}$ be an $m \times n$ real matrix set. The transpose of matrix A is denoted by $A^\top$, where A is a vector or matrix. We use I_N to stand for the identity matrix of dimension N. The cardinality of a set $\mathcal{V}$ is denoted by $|\mathcal{V}|$. Let $\|\cdot\|$ represent the Euclidean norm of a vector or matrix. The continuous function $\alpha : [0, c) \to [0, \infty)$ is said to be a class $\mathcal{K}$ function if it is strictly increasing and $\alpha(0) = 0$. If $\mathbb{Z}$ is equipped with counting measure, then $\ell_p(\mathbb{Z})$ consists of all sequences $\{x(k) \in \mathbb{R} : k \in \mathbb{Z}\}$ such that $\|\{x(k)\}\|_{\ell_p}^p = \sum_{k=0}^{\infty} |x(k)|^p < \infty$, and we can denote the sequence norm by $(\sum_{k=0}^{\infty} |x(k)|^p)^{1/p}$.

A. Vehicle Longitudinal Dynamic Model

We focus on the longitudinal dynamics and a 3rd-order state-space model for each vehicle i is provided as

$$\dot{s}_i(t) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix} s_i(t) + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} u_i(t), \quad (1)$$

where τ is the inertial delay, $s_i(t) = \begin{bmatrix} q_i(t) & v_i(t) & a_i(t) \end{bmatrix}^\top$, and $u_i(t)$ is the control input of vehicle i at time t. Note that the vehicle platoon is assumed to be homogeneous, meaning that τ is identical for all vehicles. Then, the vehicle dynamics in (1) can be discretized as

$$s_i(k+1) = As_i(k) + Bu_i(k), \quad (2)$$

where $A = \begin{bmatrix} 1 & \xi & \frac{\xi^2}{2} \\ 0 & 1 & \xi \\ 0 & 0 & 1 - \frac{\xi}{\tau} \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ \frac{\xi}{\tau} \end{bmatrix}$, ξ is the sampling time, and $s_i(k)$ and $u_i(k)$ are the state and control input of vehicle i at time slot k, respectively.

B. Network Model

Consider a vehicle platoon of $N+1$ vehicles, including a leading vehicle and N following vehicles. The vehicles in the platoon are identified in sequence from the leading vehicle to the vehicle at the end as $\{0, 1, 2, \cdots, N\}$. The communication topology among the following vehicles is modeled by a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, where $\mathcal{V} = \{1, \ldots, N\}$ is the set of the following vehicles and $\mathcal{E} = \mathcal{V} \times \mathcal{V}$ is the edge set. If vehicle i can obtain the information of vehicle j, then we have $(j, i) \in \mathcal{E}$ and $(j, i) \notin \mathcal{E}$ otherwise. The adjacent matrix of graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ is defined as $\mathcal{A} = \left[\mathcal{A}_{ij}\right] \in \mathbb{R}^{N\times N}$, where $a_{ij} = 1$ if and only if $(j, i) \in \mathcal{E}$ and $a_{ij} = 0$ otherwise. Note that self-loop is not considered, i.e., $a_{ii} = 0$. If vehicle i can obtain the information from vehicle j, i.e., $a_{ij} = 1$, vehicle j is said to be the neighbor of vehicle i, and the neighbor set of vehicle i is denoted by $\mathbb{N}_i = \left\{j \,\middle|\, a_{ij} = 1, j \in \mathcal{V}\right\}$. Let the in-degree of vehicle i be $d_i = \sum_{j=1}^{N} a_{ij}$, $i \in \{1, \ldots, N\}$, and then we have the in-degree diagonal matrix $\mathcal{D} = \text{diag}\{d_1, \ldots, d_N\} \in \mathbb{R}^{N\times N}$. The Laplacian matrix $\mathcal{L} = \left[l_{ij}\right] \in \mathbb{R}^{N\times N}$ is defined by $\mathcal{L} = \mathcal{D} - \mathcal{A}$. The communication graph is considered strongly connected if there is a directed communication path for any pair of vehicles in the platoon. To model the communication from the leader to followers, we define an augmented graph $\tilde{\mathcal{G}} = \left\{\tilde{\mathcal{V}}, \tilde{\mathcal{E}}\right\}$ with all vehicles $\tilde{\mathcal{V}} = \{0, 1, \ldots, N\}$ and edge set $\tilde{\mathcal{E}} = \tilde{\mathcal{V}} \times \tilde{\mathcal{V}}$. A diagonal matrix associated with the augmented graph $\tilde{\mathcal{G}}$ is called the pinning matrix $P = \text{diag}\{p_1, \ldots, p_N\}$, where $p_i = 1$ if $(0, i) \in \tilde{\mathcal{E}}$ and $p_i = 0$ otherwise. It characterizes the existence of the information flow from the leader to the following vehicles. The leader accessible set of vehicle i is defined as $\mathbb{P}_i$, where $\mathbb{P}_i = \{0\}$ for $p_i = 1$ and $\mathbb{P}_i = \emptyset$ otherwise.

C. Platoon Controller

We assume that the leading vehicle does not receive information from the followers, meaning that its state would not be affected by the followers, and the driving state of the leader can be considered as constant velocity type over a short period of time, i.e., $s_0 = v_0 t$. The objective of longitudinal control of a platoon is to maintain a rigid formation by the specified spacing policy between any two consecutive vehicles while tracking the velocity of the leading vehicle. The control objective can be described as

$$\begin{cases} \lim\limits_{k\to\infty} \left\| q_i(k) - q_{i-1}(k) - d_{i,i-1}(k) \right\| = 0, \\ \lim\limits_{k\to\infty} \left\| v_i(k) - v_0(k) \right\| = 0, \\ \lim\limits_{k\to\infty} \left\| a_i(k) - a_0(k) \right\| = 0. \end{cases} \tag{3}$$

where $d_{i,i-1}(k)$ is the desirable distance between vehicle i and its predecessor $i-1$, $i = 1, 2, \ldots, N$. Here, we use the constant time headway (CTH) policy, which means the desired distance between two consecutive vehicles varies with the vehicle velocity, i.e., $d_{i,i-1}(k) = -(d + h v_i(k))$, where d is the standstill gap and $h > 0$ is the constant headway time. For any pair of vehicles i and j, the desired spacing distance is denoted by

$$d_{i,j}(k) = \begin{cases} -\sum_{n=j+1}^{i} \left(d + h v_n(k)\right), & j < i \\ \sum_{n=i+1}^{j} \left(d + h v_n(k)\right), & j > i \end{cases} \tag{4}$$

The distributed controller can only use the vehicle's local information, i.e., the information obtained from its neighborhood. Let $\mathbb{I}_i = \mathbb{N}_i \cup \mathbb{P}_i$ be the neighbor set of vehicle i. The control input $u_i(k)$ in (2) is implemented using a consensus-based linear controller below

$$\begin{aligned} u_i(k) = -\sum\nolimits_{j\in\mathbb{I}_i} [&\kappa_q \left(q_i(k) - q_{i,j}(k) - d_{i,j}(k)\right) \\ &+ \kappa_v \left(v_i(k) - v_{i,j}(k)\right) + \kappa_a \left(a_i(k) - a_{i,j}(k)\right)], \end{aligned} \tag{5}$$

where $\kappa_\#$, $\# \in \{q, v, a\}$ is the controller gain, $q_{i,j}(k)$, $v_{i,j}(k)$, and $a_{i,j}(k)$ represent the position, velocity, and acceleration information sent by vehicle j to vehicle i at time k, respectively.

D. False Data Injection Attack Model

In vehicle platoon control, each vehicle uses sensors and other devices to measure vehicle state and shares information with its neighbors through a wireless network. However, the process of information transmission may be subject to cyber-attacks, resulting in false neighbor information. Therefore, the feedback information of vehicle i from vehicle j under FDI attacks can be expressed as

$$\begin{cases} q_{i,j}(k) = q_j(k) + \delta_{i,j}^q(k), \\ v_{i,j}(k) = v_j(k) + \delta_{i,j}^v(k), \\ a_{i,j}(k) = a_j(k) + \delta_{i,j}^a(k), \end{cases} \tag{6}$$

where $\delta_{i,j}(k) = [\delta_{i,j}^q(k) \ \delta_{i,j}^v(k) \ \delta_{i,j}^a(k)]^\top$ is the injected information and can be any value if the information is manipulated by the attacker. In practice, we can make an assumption on the upper limit of the number of malicious nodes in the communication network. A common attack model is called the F-total model defined below.

Definition 1: The set of malicious nodes $M \subset \mathcal{V}$ follows the F-total malicious model if it contains at most F nodes in the network, i.e., $|M| \le F$, $F \in \mathbb{Z}_{\ge 0}$.

Remark 1: This assumption is justified considering that the adversary usually has limited resources. To launch a successful FDI attack, the adversary needs to make substantial efforts. Precisely, before FDI attacks, adversaries must undertake a series of penetration tests to uncover the network's topology and vulnerabilities. Subsequently, reverse engineering is applied to decipher communication protocol formats for crafting deceptive data packets. Hence, it is reasonable to assume the maximum number of tolerable attacks. On the other hand, under such an assumption, we can further obtain a fundamental theoretical guarantee for the control performance. It should be pointed out that vehicles in the platoon can use radars and it can be difficult to deploy spoofing attacks against commercial automotive radars operating in the mmWave frequency range. The difficulties lie in the complexity of synchronizing to the victim's carrier frequency and the issue of minimizing self-interference

stemming from coupling and reflections [35]. But it should be mentioned that many efforts have been made to solve these issues. For example, in [36], commercial off-the-shelf hardware is used to successfully interfere with automotive-grade frequency-modulated continuous wave radars operating in the commonly used 77GHz frequency band, which is deployed in real-world scenarios. We can conclude that our model also works in the case that the adversary compromises both communication links and local radars, which results in manipulated positions, velocities, and accelerations.

Problem of Interests: We consider that each malicious vehicle conducts normal control like normal vehicles to avoid collisions. Note that once the attack behavior is detected without being identified, it is important for vehicles to execute resilient control to make the platoon control safe. We aim to solve the following issues:

- How can we utilize the information redundancy to realize resilient control when the number of manipulated vehicles/communication links is limited?
- How will the attack and the resilient design affect the stability of the vehicle platoon?

IV. Resilient Controller Design

In this section, we first provide a distributed resilient control algorithm and then give the system model for vehicle platoon under the proposed resilient control algorithm.

A. Resilient Control Algorithm

Inspired by MSR techniques, we design a resilient controller for the vehicle platoon to deal with the information tampering attack in the communication process. Specifically, each vehicle i received information $s_{i,j}(k) = [q_j(k) + \delta^q_{i,j}(k)\ v_j(k) + \delta^v_{i,j}(k)\ a_j(k) + \delta^a_{i,j}(k)]^\top$ from communication neighbors $j \in \mathbb{N}_i$, which may be manipulated by the attacker. If the communication link $(j,i) \in \mathcal{E}$ is manipulated, we do not have $\delta^q_{i,j}(k) = 0$, $\delta^v_{i,j}(k) = 0$, $\delta^a_{i,j}(k) = 0$ for all k, and $\delta^q_{i,j}(k) = \delta^v_{i,j}(k) = \delta^a_{i,j}(k) = 0$ for all k otherwise. Then, vehicle i calculates the tracking error vector $\bar{s}_{i_j}(k) = [q_j(k)+\delta^q_{i,j}(k)-q_i(k)-d_{j,i}(k)\ v_j(k)+\delta^v_{i,j}(k)-v_i(k)\ a_j(k)+\delta^a_{i,j}(k)-a_i(k)]^\top$. As the all these tracking error vectors should converge to zero, we compare their norm values to select safe neighboring states for local control. Since there are at most F false neighbor states, if each vehicle always uses $|\mathbb{N}_i| - F$ neighboring states with the smallest norms, we can filter out the arbitrarily manipulated states. Thus, the resilience of the platoon under FDI can be guaranteed. The details can be found in Algorithm 1 (Algo. 1).

Note that each vehicle only needs to broadcast its unencrypted local state including position, velocity, and acceleration to its neighbors. Compared with encryption and description algorithms, the communication load is lightweight. In addition, under Algo. 1, each vehicle only needs to execute three-dimensional vector subtraction, three-dimensional vector norm calculation, an algorithm designed to sort based on vector norms with the number of vector norms matching the number of neighboring vehicles, and then the weighted combination for filtered information. During each iteration, for each node with m neighbors, the time complexity can be $\mathcal{O}(m \log m)$. Thus, the running time of Algo. 1 is short, making it easily deployable.

Algorithm 1 Resilient Platoon Control Algorithm

Initialization: Initialize $s_i(0)$ and broadcast to neighbors.
Iteration:

1. Obtain states $s_{i,j}(k)$, $j \in \mathbb{N}_i$ from neighbors;
2. Convert $s_{i,j}(k)$ to tracking error vectors $\bar{s}_{i_j}(k)$ and calculate the norm of vectors by $\|\bar{s}_{i_j}(k)\|$, and form a sorted list;
3. Remove the state sent by neighbors j with the largest F norm values in the sorted list to obtain the set of remaining neighbors $\mathbb{N}_{i,\text{rem}}$;
4. Calculate the control input by
$$\bar{u}_i(k) = -\sum_{j\in\mathbb{I}_{i,\text{rem}}} \left[\kappa_q\left(q_i(k) - q_{i,j}(k) - d_{i,j}(k)\right) + \kappa_v\left(v_i(k) - v_{i,j}(k)\right) + \kappa_a\left(a_i(k) - a_{i,j}(k)\right)\right],$$
where $\mathbb{I}_{i,\text{rem}} = \mathbb{N}_{i,\text{rem}} \cup \mathbb{P}_i$;
5. Update the states of vehicle i according to
$$s_i(k+1) = As_i(k) + B\bar{u}_i(k).$$

Output: The local position, velocity, and acceleration

B. Platoon Model With Resilient Controller

Here, we first introduce a definition of network robustness as follows.

Definition 2: A directed graph $\mathcal{G}$ is (r,s)-robust (r, $s < N$) if for every pair of nonempty disjoint subsets $\mathcal{S}_1$, $\mathcal{S}_2 \subset \mathcal{V}$ at least one of the following conditions is satisfied: 1) $\chi^r_{\mathcal{S}_1} = \mathcal{S}_1$; 2) $\chi^r_{\mathcal{S}_2} = \mathcal{S}_2$; 3) $\left|\chi^r_{\mathcal{S}_1}\right| + \left|\chi^r_{\mathcal{S}_2}\right| \geq s$, where $\chi^r_{\mathcal{S}_i}$ is the set of all nodes in $\mathcal{S}_i$ which have at least r incoming edges from outside of $\mathcal{S}_i$. Typically, r-robust graph means that given the nonempty, nontrivial graph, for every pair of nonempty disjoint subsets, at least one of the subsets is r-reachable.

Then, to transform the platoon system into a closed system form, we define tracking errors for vehicle i,

$$\begin{cases} \tilde{q}_i(k) = q_i(k) - q_0(k) - d_{i,0}(k), \ \tilde{v}_i(k) = v_i(k) - v_0(k), \\ \tilde{a}_i(k) = a_i(k) - a_0(k), \end{cases} \tag{7}$$

where $d_{i,0}(k) = -(\sum_{n=1}^{i}(d + hv_n(k)))$ is the desirable distance between vehicle i and the leader. Similarly, we have $\tilde{q}_{i,j}(k)$, $\tilde{v}_{i,j}(k)$, and $\tilde{a}_{i,j}(k)$. Let $\tilde{q}(k) = [\tilde{q}_1^\top(k)\ \cdots\ \tilde{q}_N^\top(k)]^\top$, $\tilde{v}^\top(k) = [\tilde{v}_1^\top(k)\ \cdots\ \tilde{v}_N^\top(k)]^\top$, and $\tilde{a}(k) = [\tilde{a}_1^\top(k)\ \cdots\ \tilde{a}_N^\top(k)]^\top$. Considering the vehicle platoon with vehicle dynamics in (2), control input in Algo. 1, $v_0(k) = c$, and $a_0(k) = 0$ in an ideal communication network, we have

$$\begin{bmatrix} \tilde{q}(k+1) \\ \tilde{v}(k+1) \\ \tilde{a}(k+1) \end{bmatrix} = \begin{bmatrix} I_N & \xi I_N & \frac{\xi^2}{2}I_N + \xi H \\ 0_N & I_N & \xi I_N \\ 0_N & 0_N & (1-\frac{\xi}{\tau})I_N \end{bmatrix} \begin{bmatrix} \tilde{q}(k) \\ \tilde{v}(k) \\ \tilde{a}(k) \end{bmatrix} + \begin{bmatrix} 0_N \\ 0_N \\ \frac{\xi}{\tau}I_N \end{bmatrix} \bar{u}(k), \tag{8}$$

where $H \in \mathbb{R}^{N\times N}$ is a lower triangular matrix with all entries in/below the main diagonal equal to h. Then, we have

$$\begin{aligned}\bar{u}_i(k) &= \sum_{j=1}^{N}\mathcal{A}_{ij}(k)(\kappa_q(\tilde{q}_{i,j}(k)-\tilde{q}_i(k))+\kappa_v(\tilde{v}_{i,j}(k)-\tilde{v}_i(k))\\ &\quad+\kappa_a(\tilde{a}_{i,j}(k)-\tilde{a}_i(k))\\ &\quad+P_{ii}(-\kappa_q\tilde{q}_i(k)-\kappa_v\tilde{v}_i(k)-\kappa_a\tilde{a}_i(k))\\ &= \underbrace{\sum_{j=1}^{N}\mathcal{A}_{ij}(k)(\kappa_q(\tilde{q}_j(k)-\tilde{q}_i(k))+\kappa_v(\tilde{v}_j(k)-\tilde{v}_i(k))}_{(1a)}\\ &\quad\underbrace{+\kappa_a(\tilde{a}_j(k)-\tilde{a}_i(k))}_{(1b)}\\ &\quad\underbrace{+P_{ii}(-\kappa_q\tilde{q}_i(k)-\kappa_v\tilde{v}_i(k)-\kappa_a\tilde{a}_i(k))}_{(1c)}\\ &\quad+\underbrace{\sum_{j=1}^{N}\mathcal{A}_{ij}(k)(\kappa_q\delta^q_{i,j}(k)+\kappa_v\delta^v_{i,j}(k)+\kappa_a\delta^a_{i,j}(k))}_{(2)}.\end{aligned}$$

Let $x(k)=\left[\tilde{q}(k)^\top \quad \tilde{v}(k)^\top \quad \tilde{a}(k)^\top\right]^\top \in \mathbb{R}^{3N}$. Hence, the compact form of the input (1a), (1b), and (1c) in $\bar{u}_i(k)$ can be written as

$$\begin{aligned}\bar{u}^{(1)}(k) &= -\kappa_q(\mathcal{L}(k)+P)\tilde{q}(k)-\kappa_v(\mathcal{L}(k)+P)\tilde{v}(k)\\ &\quad-\kappa_a(\mathcal{L}(k)+P)\tilde{a}(k)\\ &= -\kappa_q\mathcal{L}_P(k)\tilde{q}(k)-\kappa_v\mathcal{L}_P(k)\tilde{v}(k)-\kappa_a\mathcal{L}_P(k)\tilde{a}(k)\\ &= \begin{bmatrix}-\kappa_q\mathcal{L}_P(k) & -\kappa_v\mathcal{L}_P(k) & -\kappa_a\mathcal{L}_P(k)\end{bmatrix}x(k), \quad (9)\end{aligned}$$

where $\mathcal{L}_P(k)=\mathcal{L}(k)+P$ and $x(k)=[\tilde{q}(k)\ \tilde{v}(k)\ \tilde{a}(k)]^\top$. Meanwhile, the part (2) of $\bar{u}_i(k)$ can be written in the compact form below

$$\begin{aligned}\bar{u}^{(2)}(k) &= -\kappa_q\bar{\mathcal{L}}(k)\delta^q(k)-\kappa_v\bar{\mathcal{L}}(k)\delta^v(k)-\kappa_a\bar{\mathcal{L}}(k)\delta^a(k)\\ &= \begin{bmatrix}-\kappa_q\bar{\mathcal{L}}(k) & -\kappa_v\bar{\mathcal{L}}(k) & -\kappa_a\bar{\mathcal{L}}(k)\end{bmatrix}\delta(k), \quad (10)\end{aligned}$$

where $\bar{\mathcal{L}}(k)\in\mathbb{R}^{N\times|\mathcal{E}|}$ with $\bar{\mathcal{L}}_{ij}(k)$ representing the relationship between vehilce i and the edge j. Let $\delta(k)=[\delta^q(k)^\top,\delta^v(k)^\top,\delta^a(k)^\top]^\top\in\mathbb{R}^{3|\mathcal{E}|}$, where $\delta^q(k),\delta^v(k),\delta^a(k)\in\mathbb{R}^{|\mathcal{E}|}$. Specifically, we give each edge in the communication graph of the vehicle platoon an ID, i.e., $\{1,\ldots,|\mathcal{E}|\}$, and then we can obtain the corresponding $\delta^q(k),\delta^v(k),\delta^a(k)$. Combining (8), (9), and (10), we obtain the following closed-loop system

$$\begin{aligned}&x(k+1)\\ &=\begin{bmatrix}I_N & \xi I_N & \frac{\xi^2}{2}I_N+\xi H\\ 0_N & I_N & \xi I_N\\ 0_N & 0_N & (1-\frac{\xi}{\tau})I_N\end{bmatrix}x(k)\\ &\quad+\begin{bmatrix}0_N\\0_N\\\frac{\xi}{\tau}I_N\end{bmatrix}\begin{bmatrix}-\kappa_q\mathcal{L}_P(k) & -\kappa_v\mathcal{L}_P(k) & -\kappa_a\mathcal{L}_P(k)\end{bmatrix}x(k)\\ &\quad+\begin{bmatrix}0_N\\0_N\\\frac{\xi}{\tau}I_N\end{bmatrix}\begin{bmatrix}-\kappa_q\bar{\mathcal{L}}(k) & -\kappa_v\bar{\mathcal{L}}(k) & -\kappa_a\bar{\mathcal{L}}(k)\end{bmatrix}\delta(k)\\ &= W(k)x(k)+C(k)\delta(k), \quad (11)\end{aligned}$$

where

$$W(k)=\begin{bmatrix}I_N & \xi I_N & \frac{\xi^2}{2}I_N+\xi H\\ 0_N & I_N & \xi I_N\\ -\frac{\xi}{\tau}\kappa_q\mathcal{L}_P(k) & -\frac{\xi}{\tau}\kappa_v\mathcal{L}_P(k) & (1-\frac{\xi}{\tau})I_N-\frac{\xi}{\tau}\kappa_a\mathcal{L}_P(k)\end{bmatrix}$$

and

$$C(k)=\begin{bmatrix}0_{N\times|\mathcal{E}|} & 0_{N\times|\mathcal{E}|} & 0_{N\times|\mathcal{E}|}\\ 0_{N\times|\mathcal{E}|} & 0_{N\times|\mathcal{E}|} & 0_{N\times|\mathcal{E}|}\\ -\frac{\xi}{\tau}\kappa_q\bar{\mathcal{L}}(k) & -\frac{\xi}{\tau}\kappa_v\bar{\mathcal{L}}(k) & -\frac{\xi}{\tau}\kappa_a\bar{\mathcal{L}}(k)\end{bmatrix}.$$

V. Performance Analysis

In this section, we provide some assumptions and then obtain sufficient conditions to guarantee the system's stability.

Assumption 1: The attacks happen in the communication process, where the communication information is modified by the external attacker. At most F vehicles' information can be altered by the attacker. For the manipulated vehicles' information, the received information by their different neighbors can be different.

Assumption 2: The leading vehicle's information is always trustable and safe, which means that the attacker cannot manipulate the information broadcast by the leading vehicle.

Remark 2: Assumption 2 can be guaranteed by the security and authentication mechanism since the leading vehicle's information is quite important. We have to admit that we can only have security under some assumptions. In the considered problem, we aim to guarantee the security of the vehicle platoon by designing a resilient controller where the leading vehicle's information is assumed to be secure. On the other hand, this is not an unrealistic assumption since mature security and authentication mechanisms can be used. However, if all vehicles rely on these methods, it can lead to high communication and computation costs. This is the reason that we consider designing a lightweight resilient controller without any security and authentication mechanisms for local communication and computation.

Lemma 1: Without any attacks, if $\|W(i)\|<1$, $\forall i$, then we have $\lim_{k\to\infty}x(k)=0$ for the platoon system (11).

Lemma 2: Under attacks, for the platoon system (11), if we have $\lim_{k\to\infty}x(k)=0$, then there must hold $\lim_{k\to\infty}\delta(k)=0$.

To show the stability of the platoon system, we first consider the case that $C(k)\delta(k)\equiv 0$, i.e., no attack. Specifically, we can obtain the system dynamics below

$$x(k+1)=W(k)x(k). \quad (12)$$

Without the resilient design, we have the system model as

$$x(k+1)=Wx(k), \quad (13)$$

where

$$W = \begin{bmatrix} I_N & \xi I_N & \frac{\xi^2}{2} I_N + \xi H \\ 0_N & I_N & \xi I_N \\ -\frac{\xi}{\tau}\kappa_q \mathcal{L}_P & -\frac{\xi}{\tau}\kappa_v \mathcal{L}_P & (1-\frac{\xi}{\tau}) I_N - \frac{\xi}{\tau}\kappa_a \mathcal{L}_P \end{bmatrix}$$

with original time-invariant Laplace matrix $\mathcal{L}$ and the P matrix.

Lemma 3 [37]: The system (13) can achieve asymptotic stability if and only if

$$\max_{i=1,2,\cdots,3N} (|\lambda_i(W)|) < 1, \tag{14}$$

where $\lambda_i(W)$ denotes the ith eigenvalue of W. When multiple predecessors' information is used by the following vehicles, the condition becomes $|a_2 + a_0| < 1 + a_1$, $|a_2 - 3a_0| < 2 - a_1$, $a_0^2 + a_1 - a_0 a_2 < 1$, where r_i is the number of vehicle i's neighbors and $\forall i$

$$\begin{aligned} a_2 &= \frac{\xi(\kappa_a r_i + 1)}{\tau} - 3, \\ a_1 &= \frac{\xi^3 \kappa_q r_i}{2\tau} + \frac{\xi^2 \kappa_q h r_i}{\tau} + \frac{\xi^2 \kappa_v r_i}{\tau} - \frac{2\xi \kappa_a r_i}{\tau} - \frac{2\xi}{\tau} + 3, \\ a_0 &= 1 + \frac{\xi}{\tau} + \frac{\xi \kappa_a r_i}{\tau} - \frac{\xi \kappa_v r_i}{\tau} + \frac{\xi^3 \kappa_q r_i}{2\tau} - \frac{\xi^2 \kappa_q h r_i}{\tau}. \end{aligned} \tag{15}$$

Lemma 4 [38]: Suppose system $x(k+1) = Wx(k)$ is asymptotically stable. The system $x(k+1) = (W + W'(k))x(k)$, $W'(k) = W(k) - W$, is asymptotically stable if there exist a positive constant α and a sufficiently small constant $\epsilon > 0$ such that $W'(k)$ satisfies $\sum_{j=k_0}^{k-1} \|W'(k)\| \le \epsilon(k - k_0) + \alpha, \forall k \ge k_0, \forall k_0 \ge 0$.

Then, we can further derive the following results.

Lemma 5: Suppose that the communication graph is strongly connected. Under Algo. 1, the states of system (12) converge to zero if (14) holds and there exist a positive constant α and a sufficiently small constant $\epsilon > 0$ such that

$$\frac{\xi}{\tau}\sqrt{(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)} \sum_{j=k_0}^{k-1} \rho(\mathcal{L}'_P(k)) \le \epsilon(k - k_0) + \alpha, \ \forall k \ge k_0, \quad \forall k_0 \ge 0, \tag{16}$$

where $\mathcal{L}'_P(k) = -\mathcal{L}_P(k) + \mathcal{L}_P$.

Proof: From (12) and (13), we have

$$\begin{aligned} x(k+1) &= W(k)x(k) = (W + W(k) - W)x(k) \\ &= (W + W'(k))x(k), \end{aligned} \tag{17}$$

where $W'(k) = W(k) - W$, i.e.,

$$W'(k) = \begin{bmatrix} 0_N & 0_N & 0_N \\ 0_N & 0_N & 0_N \\ \frac{\xi}{\tau}\kappa_q \mathcal{L}'_P(k) & \frac{\xi}{\tau}\kappa_v \mathcal{L}'_P(k) & \frac{\xi}{\tau}\kappa_a \mathcal{L}'_P(k) \end{bmatrix}.$$

Then, we have

$$W'(k)W'^{\top}(k) = \begin{bmatrix} 0_N & 0_N & 0_N \\ 0_N & 0_N & 0_N \\ 0_N & 0_N & \frac{\xi^2}{\tau^2}(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)\mathcal{L}'_P(k)\mathcal{L}'^{\top}_P(k) \end{bmatrix}.$$

From Lemma 3 in [37], we can obtain the sufficient condition (14) to ensure that the system $x(k+1) = Wx(k)$ is asymptotically stable. The platoon under Algo. 1 without any attacks can be viewed as the system $x(k+1) = Wx(k)$ perturbed by the matrix $W'(k)$. Since the communication graph of the platoon is strongly connected, we have $\|W'(k)\| = \frac{\xi}{\tau}\sqrt{(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)\rho(\mathcal{L}'_P(k))}$, where $\rho(\mathcal{L}'_P(k))$ denotes the singular value of matrix $\mathcal{L}'_P(k)$. Then, by Lemma 4, we have the sufficient condition (16) to ensure the stability of the system $x(k+1) = W(k)x(k)$. Thus, we have completed the proof. □

Remark 3: The condition (16) can hold when we have a smaller sample time ξ. If for all k, the graph having the Laplace matrix $\mathcal{L}'_P(k)$ is undirected and we have at most $\bar{F}$ compromised communication links, by [39], we have the upper bound of $\max(|\lambda_i(\mathcal{L}'_P(k))|)$ as $\max(|\lambda_i(\mathcal{L}'_P(k))|) \le \max\{d'_i + d'_j - |N'_i \cap N'_j| : 1 \le i < j \le N, (i,j) \in \mathcal{E}\} \le \bar{F}$, where d'_i, $\forall i$ is the corresponding degree and N'_i is the corresponding neighbors set of vehicle i. The condition in (16) can be further derived as $\frac{\xi}{\tau}\sqrt{(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)}\bar{F} \le \epsilon + \alpha/(k - k_0), \forall k \ge k_0$.

Theorem 1: Under Algo. 1 and Assumptions 1 and 2, given $F+1$-robustness graph $\mathcal{G}$, all vehicles in the platoon can achieve stability under attacks if (14) holds, there exist a positive constant α and a sufficiently small constant $\epsilon > 0$ such that (16) holds, and $\sqrt{\bar{F}\frac{\xi^2}{\tau^2}(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)}$ is small enough, where $\bar{F}$ is the maximum number of communication links that are manipulated by at most F manipulated vehicles.

Proof: Since $\delta(k)$ is the false data injected on the manipulated communication links, it must be upper-bounded by the proposed resilient method. It means that each vehicle i uses the injected information $\delta_{i,j}(k) = [\delta^q_{i,j}(k); \delta^v_{i,j}(k); \delta^a_{i,j}(k)]$ from communication neighboring vehicle j if and only if $\delta_{i,j}(k)$ is less than or equals to the maximum norm distance between neighboring vehicles and itself. Let $x_i(k) = [\tilde{q}_i(k); \tilde{v}_i(k); \tilde{a}_i(k)]$, for all i. Then, we have

$$\|\delta_{i,j}(k)\| \le \max\{\|x_i(k) - x_j(k)\|\}, \quad \forall j \in \mathcal{N}_i. \tag{18}$$

The maximum number of communication links that can be manipulated, i.e., $\bar{F}$. As $\|x(k)\|^2 = \|x_1(k)\|^2 + \ldots + \|x_N(k)\|^2$, one infers

$$\begin{aligned} \|C(k)\delta(k)\|^2 &\le \bar{F}\frac{\xi^2}{\tau^2}(\kappa_q^2 + \kappa_v^2 + \kappa_a^2) \max_{\forall i,j}\{\|x_i(k) - x_j(k)\|\} \\ &\le \bar{F}\frac{\xi^2}{\tau^2}(\kappa_q^2 + \kappa_v^2 + \kappa_a^2) \max_{\forall i,j}\{\|x_i(k)\|^2 + \|x_j(k)\|^2\} \\ &\le \bar{F}\frac{\xi^2}{\tau^2}(\kappa_q^2 + \kappa_v^2 + \kappa_a^2)\beta(k)\|x(k)\|^2, \end{aligned}$$

where $\beta(k) = \frac{\max\{\|x_i(k)\|^2 + \|x_j(k)\|^2\}}{\|x(k)\|^2}$, $0 < \beta(k) \le 1$ with $\lim_{k\to\infty} \beta(k) = 1$. Let $\Phi(k, k_0) = \Pi_{i=0}^{k-k_0-1} W(k_0 + i)$, where $k > k_0$, and $\Phi(k_0, k_0) = I$. Consequently, we have

$$\|x(k)\| = \|\Phi(k, k_0)x(k_0) + \sum_{i=k_0}^{k-1} \Phi(k, i+1)C(i)\delta(i)\|.$$

There exist constants $\phi > 0$ and $\varphi \in (0, 1)$ such that $\forall k_0$

$$\begin{aligned}\|x(k)\| &\le \|\Phi(k, k_0)\|\|x(k_0)\| + \sum_{i=k_0}^{k-1} \|\Phi(k, i+1)\|\|C(i)\delta(i)\| \\ &\le \phi\varphi^{(k-k_0)}\|x(k_0)\| + \sum_{i=k_0}^{k-1} \phi\varphi^{(k-i-1)}\|C(i)\delta(i)\| \\ &\le \phi\varphi^{(k-k_0)}\|x(k_0)\| \\ &\quad + \sum_{i=k_0}^{k-1} \phi\varphi^{(k-i-1)}\frac{\xi}{\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}\|x(i)\|.\end{aligned}$$

Using Gronwall-Bellman inequality on the above inequality, we have

$$\|x(k)\| \le \phi\varphi^{(k-k_0)}\|x(k_0)\|\exp\Big(\sum_{i=k_0}^{k-1}\frac{\phi}{\varphi}\frac{\xi}{\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}\Big). \tag{19}$$

Thus,

$$\begin{aligned}\|x(k)\| &\le \phi\varphi^{(k-k_0)}\|x(k_0)\|\exp\Big((k-k_0)\frac{\phi}{\varphi}\frac{\xi}{\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}\Big) \\ &\le \phi\varphi^{(k-k_0)}\exp\Big((k-k_0)\frac{\phi}{\varphi}\frac{\xi}{\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}\Big)\|x(k_0)\| \\ &\le \phi\Big(\varphi\exp\Big(\frac{\phi\xi}{\varphi\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}\Big)\Big)^{(k-k_0)}\|x(k_0)\|.\end{aligned} \tag{20}$$

If $\sqrt{\bar{F}\frac{\xi^2}{\tau^2}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}$ is small enough, $\varphi\exp(\frac{\phi\xi}{\varphi\tau}\sqrt{\bar{F}(\kappa_q^2+\kappa_v^2+\kappa_a^2)}) < 1$. Thus, we can conclude that all states of the system can converge to zero. Thus, we have completed the proof. □

Remark 4: From Theorem 1, it becomes evident that the control gains (κ_q, κ_v, κ_a), the time sampling interval (ξ), and the inertial delay of the vehicle's longitudinal dynamics (τ) are adjustable parameters within the platoon system. To enhance system stability in the face of potential attacks and to provide flexibility in selecting control gains, it is better to use a smaller time sampling time ξ. Importantly, the proposed solution remains robust without making any assumptions about the attacker's error message. Furthermore, in practical scenarios, communication messages may occasionally suffer loss or significant delays due to impairments in the communication channel, and the proposed solution effectively addresses such situations. Given the increased complexity of distributed control in heterogeneous vehicle platoons, an adaptive design is often necessary to address dynamic heterogeneity. In such cases, the resilient control design must be tailored to the specific system. When the adaptive design relies on communication information, a potential vulnerability in our work, it becomes imperative to prioritize the resilience of the adaptive design part. This involves integrating it effectively with the distributed resilient control input component.

Remark 5: We consider that the leader vehicle faces a bounded disturbance, i.e., $\|u_0(k)\| \le c_u$ and $\|a_0(0)\| \le c_a$, where $c_u \ge 0$ and $c_a \ge 0$ are constants. Consequently, $a_0(k) \equiv 0$ does not hold for all k. We have

$$\begin{bmatrix}\tilde{q}(k+1)\\ \tilde{v}(k+1)\\ \tilde{a}(k+1)\end{bmatrix} = \begin{bmatrix}I_N & \xi I_N & \frac{\xi^2}{2}I_N + \xi H\\ 0_N & I_N & \tau I_N\\ 0_N & 0_N & (1-\frac{\xi}{\tau})I_N\end{bmatrix}\begin{bmatrix}\tilde{q}(k)\\ \tilde{v}(k)\\ \tilde{a}(k)\end{bmatrix} + \begin{bmatrix}0_N\\ 0_N\\ \frac{\xi}{\tau}I_N\end{bmatrix}\bar{u}(k) + \begin{bmatrix}\xi H\\ 0_N\\ 0_N\end{bmatrix}1_N a_0(k). \tag{21}$$

As a significant property of the vehicle platoon system, string stability is designed to prevent the amplification of disturbances in the upstream direction. The existing literature has proposed various types of definitions and analysis methods for string stability, tailored to different domains, disturbance types, and information flow topology (IFT), either in terms of stability properties or performance criteria. Different definitions of string stability including Lyapunov-like, input-to-output-like, and input-to-state-like string stability, can be chosen to adapt to specific systems [40]. Lyapunov-like string stability only considers the response to initial condition disturbances, neglecting external disturbance to the platoon system, which limits its practicality. Input-to-output-like string stability, which usually can be expressed as $||e_{q_i}(t)||_\infty \le ||e_{q_{i-1}(t)}||_\infty$, $\forall i \in \mathcal{V}$, only applies to linear systems with zero initial conditions. But these two types of string stability are not suitable for our resilient vehicle platoon system as the system is nonlinear and has external disturbances. Note that ℓ_p string stability belongs to input-to-state-like string stability, which is the most suitable definition for our resilient platoon system. First, ℓ_p string stability makes few assumptions on platoon systems and applies to all types of information flow topology and disturbances. A key feature of resilient control is that the topology is time-varying, which also makes the $s-$domain methods inapplicable. On the other hand, this class of definitions captures three key properties, i.e., 1) boundedness of state fluctuations; 2) convergence of state fluctuations caused by initial condition disturbances; and 3) boundedness and convergence hold for any platoon length, aligning with the initial focus of string stability. The detailed definition is provided below.

Definition 3: The platoon system (21) is ℓ_p-string stable if there exists a $\mathcal{K}$ function α and constants $c > 0$, $c_\omega > 0$, $\kappa_\omega > 0$ such that for any initial disturbance $e_{q1}(0)$ and new disturbance $a_0(k)$ satisfying

$$|e_{q1}(0)| < c \text{ and } \|a_0(k)\|_{\ell_\infty} < c_\omega,$$

the solution $e_{qi}(k)$, $\forall i \in \mathcal{V}$, exists for all $k \ge 0$ and satisfies

$$\|e_{qi}(k)\|_{\ell_p} \le \alpha(|e_{q1}(0)|) + \kappa_\omega c_\omega.$$

Combining (21) and (11), we can derive

$$\begin{aligned}&x(k+1)\\ &= W(k)x(k) + C(k)\delta(k) + \begin{bmatrix}\xi H\\ 0_{N\times N}\\ 0_{N\times N}\end{bmatrix}1_N a_0(k)\\ &= W(k)x(k)\end{aligned}$$

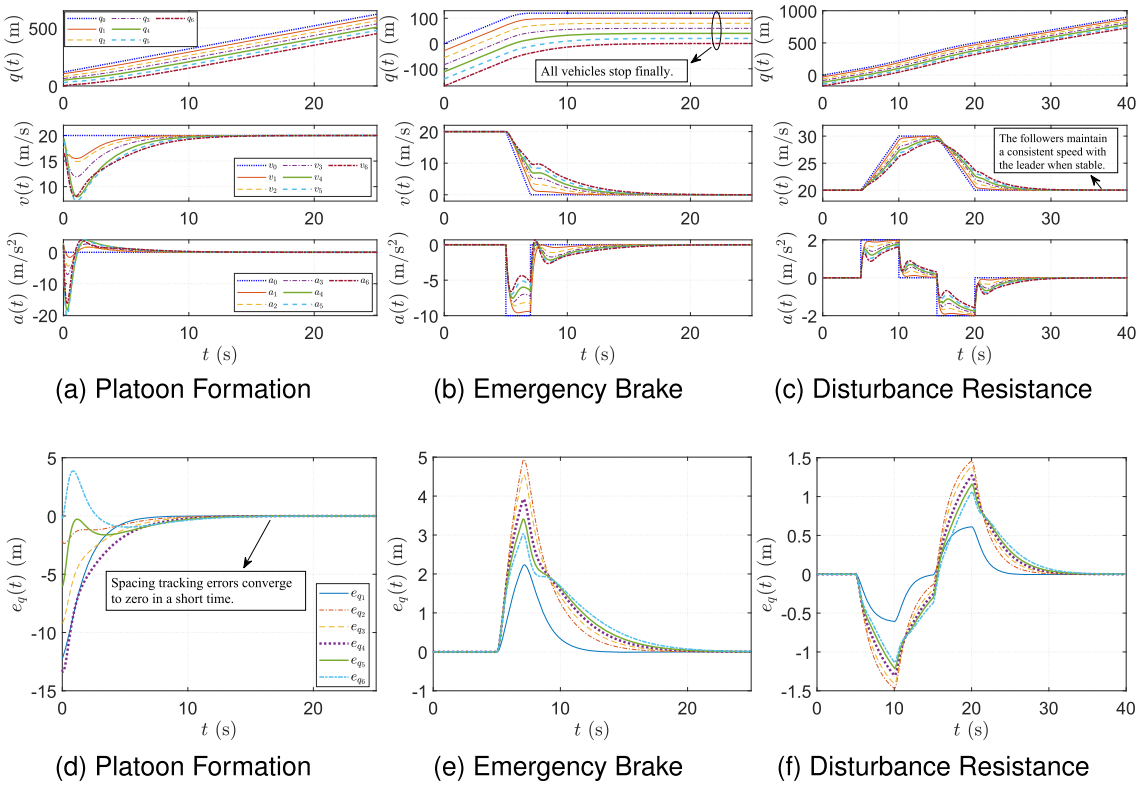


Fig. 1. Performance of vehicle platoon without attacks. (a) (b) (c) state dynamics of vehicle platoons under different cases. (d) (e) (f) tracking errors of vehicle platoons under different cases. Note that the legends for (a), (b), and (c) are the same, as are the legends for (d), (e), and (f).

$$+\begin{bmatrix} 0_{N\times M} & 0_{N\times M} & 0_{N\times M} & \xi H \\ 0_{N\times M} & 0_{N\times M} & 0_{N\times M} & 0_{N\times N} \\ -\frac{\xi}{\tau}\kappa_q\bar{\mathcal{L}}(k) & -\frac{\xi}{\tau}\kappa_v\bar{\mathcal{L}}(k) & -\frac{\xi}{\tau}\kappa_a\bar{\mathcal{L}}(k) & 0_{N\times N} \end{bmatrix} \times \begin{bmatrix} \delta(k) \\ 1_N a_0(k) \end{bmatrix} \tag{22}$$

The challenges for further analysis lie in: 1) We have two kinds of disturbances in the platoon system, i.e., the disturbance from the designed resilient control algorithm and that caused by the acceleration of the leading vehicle, which makes the string stability hard to analyze; 2) Since the disturbance from the designed resilient control algorithm does not have an analytical expression, it is difficult to further analyze the string stability of the system. We admit that we may require extra input design to guarantee string stability. String stability guaranteed controller design and theoretical analysis remains a challenging open issue.

VI. Simulation Results

In this section, we conduct extensive simulations to illustrate the performance of the proposed resilient controller for cases without/with FDI attacks.

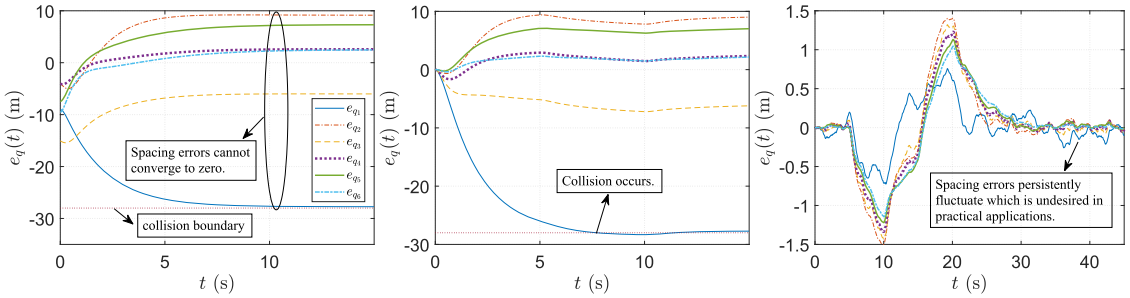
A. Performance Without FDI Attacks

In this part, we demonstrate the performance of the vehicle platoon under the proposed controller in the absence of attacks. We consider a vehicle platoon consisting of $N = 6$ followers and the desired inter-vehicle distance is $d + hv_i(k)$, where $d = 20\,\text{m}$, $h = 0.4\,\text{s}$. The inertial delay of the longitudinal dynamic model is set as $\tau = 0.5\,\text{s}$, while the sample period is $\xi = 0.01\,\text{s}$. We choose the controller gains $\kappa_q = 2$, $\kappa_v = 4$, and $\kappa_a = 2$. Furthermore, each following vehicle can communicate with its two nearest neighbors and the leader.

1) Platoon Formation: In this case, the leading vehicle moves at a constant speed, where $v_0(0) = 20\,\text{m/s}$ and $a_0(0) = 0\,\text{m/s}^2$. The initial positions, velocities, and accelerations of the following vehicles are set as $q_i(0) = 20*(N-i)+10*\text{rand}(1)\,\text{m}$, $v_i(0) = 15+5*\text{rand}(1)\,\text{m/s}$, $a_i(0) = 2+10*\text{rand}(1)\,\text{m/s}^2$, where rand(1) represents a random number in the interval $[0, 1]$ and $1 \le i \le N$. From Fig. 1a and Fig. 1d, we observe that the vehicle platoon system achieves stable formation in the absence of attacks when the leading vehicle moves at a constant speed.

2) Emergency Brake: Possible emergencies require the vehicle platoon to respond promptly to the braking of the leading vehicle, ensuring the safety of the platoon. Here, the initial state of the platoon is set as the desired state, i.e., the initial spacing errors and velocity errors are equal to 0. The leading vehicle moves at the same speed as case 1), and suddenly brakes in the 5 s, i.e., $a_0(t) = -10\,\text{m/s}^2$ until it stops. As is shown in Fig. 1b and Fig. 1e, all vehicles stop in 20 seconds and all relative distances converge to the standstill distance without collisions.

3) Disturbance Resistance (DR): In this case, we investigate the anti-interference ability of the system. The speed changes of the leading vehicle can be viewed as disturbances in the platoon. The system initially maintains the ideal inter-vehicle distance and moves at a constant speed. Then the leader's acceleration is set as $a_0(t) = 2\,\text{m/s}^2$ and $a_0(t) =$



(a) Formation with Fixed $\delta(k)$ (b) DR with Fixed $\delta(k)$ (c) DR with Random $\delta(k)$

Fig. 2. Performance of the vehicle platoon without resilient control under node attacks. (a) (b) (c) depict tracking errors of vehicle platoons under different scenarios. Note that the legends for (a), (b), and (c) are the same.

$-2\,\mathrm{m/s^2}$ when $5 < t \leq 10\,\mathrm{s}$ and $15 < t \leq 20\,\mathrm{s}$, respectively, to observe the control of the vehicle platoon under disturbances. Fig. 1c and Fig. 1f show that the motion of all vehicles is stable when the leader is disturbed.

B. Performance Under FDI Attacks

In this part, we conduct simulations to verify the performance of Algo. 1 under node/edge attacks.

1) Node Attacks: Suppose that each malicious vehicle sends the same tampered information to all its neighbors except itself and normally receives neighbors' information, and uses its own true state value for local control. Each following vehicle can communicate with its 2 nearest neighbors. Then, we consider bidirectional topology $\mathcal{L}_1$ and unidirectional topology $\mathcal{L}_2$ to characterize the inter-vehicle communication among vehicles,

$$\mathcal{L}_1 = \begin{bmatrix} 2 & -1 & -1 & 0 & \cdots & 0 \\ -1 & 3 & -1 & -1 & \cdots & 0 \\ -1 & -1 & 4 & -1 & \cdots & 0 \\ 0 & -1 & -1 & 4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2 \end{bmatrix},$$

$$\mathcal{L}_2 = \begin{bmatrix} 2 & -1 & -1 & 0 & \cdots & 0 \\ -1 & 2 & -1 & 0 & \cdots & 0 \\ -1 & -1 & 2 & 0 & \cdots & 0 \\ 0 & -1 & -1 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 2 \end{bmatrix}$$

In the bidirectional topology, each vehicle communicates with its front and back two nearest neighbors, as shown in $\mathcal{L}_1$, which is $(2, 2)$-robust. A 2-robust topology is also guaranteed in the unidirectional topology $\mathcal{L}_2$. In addition, under the F-total attack model, the vehicle will eliminate F received state vectors to ensure resilience. Therefore, to ensure that the information of the leader can be transmitted to the following vehicles, it is necessary to have no less than $F + 1$ following vehicles communicate directly with the leader vehicle. Here, we discuss the pinning matrix for the following two cases:

1) $\mathcal{P}_1 = \mathrm{diag}\left\{\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}\right\}$;
2) $\mathcal{P}_2 = \mathrm{diag}\left\{\begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \end{bmatrix}\right\}$.

The attacker manipulates the information sent by a certain vehicle while retaining the platoon parameters used in Section VI-A. The false data injected is set as a random number in certain ranges, i.e., $\delta^q(k) \in [-5, 5]$, $\delta^v(k) \in [-2.5, 2.5]$, $\delta^a(k) \in [-0.5, 0.5]$. The different platoon scenarios are given in Table I.

TABLE I
PARAMETERS OF DIFFERENT SCENARIO

Scenario	$\mathcal{N}$	$\mathcal{L}$	$\mathcal{P}$	Attack
S1	6	$\mathcal{L}_1$	$\mathcal{P}_1$	vehicle 2
S2	6	$\mathcal{L}_1$	$\mathcal{P}_2$	vehicle 2
S3	6	$\mathcal{L}_2$	$\mathcal{P}_2$	vehicle 2
S4	20	$\mathcal{L}_1$	$\mathcal{P}_1$	vehicle 2

The platoon control without resilience is initially tested under node attacks. To better illustrate the impact of FDI attacks on the security of vehicles, we set the injected false data as a fixed vector, i.e. $\delta(k) = [15, 10, 5]^\top$. Under condition S1, we examine the formation and disturbance resistance of the vehicle platoon. As shown in Figs. 2a and 2b, the platoon without resilient control fails to maintain the desired inter-vehicle distance and even crashes under attacks. This indicates that conventional consensus algorithms are incapable of countering FDI attacks. Fig. 2c shows the disturbance resistance of the vehicle platoon in the case where the injected false data randomly fluctuates within the narrow range set earlier. It can be observed that although crashes do not occur within the platoon, spacing errors persistently fluctuate, failing to converge to zero. This is undesirable in practical applications.

Next, we examine the resilient platoon control algorithm. The leading vehicle moves at a constant speed and the initial conditions of the vehicle platoon are the same as in Section VI. A-1). Fig. 3 shows the formation process of the platoon with attacks for the S1-S4 scenarios, and all achieve stable vehicle platoons with ideal spacing. Comparing the control effects in different scenarios, we find that the convergence speed of the undirected topology is slower than that of the one-way topology, and the more vehicles that directly communicate with the leader, i.e., larger $|\mathcal{P}|$, the faster the convergence speed. In addition, compared with the other vehicles, there is a certain fluctuation in the acceleration of the following vehicles 1, 3, and 4, as they communicate directly with the manipulated vehicle 2. When the platoon scale grows to $N = 20$ with the same communication topology in S1, the stability of the

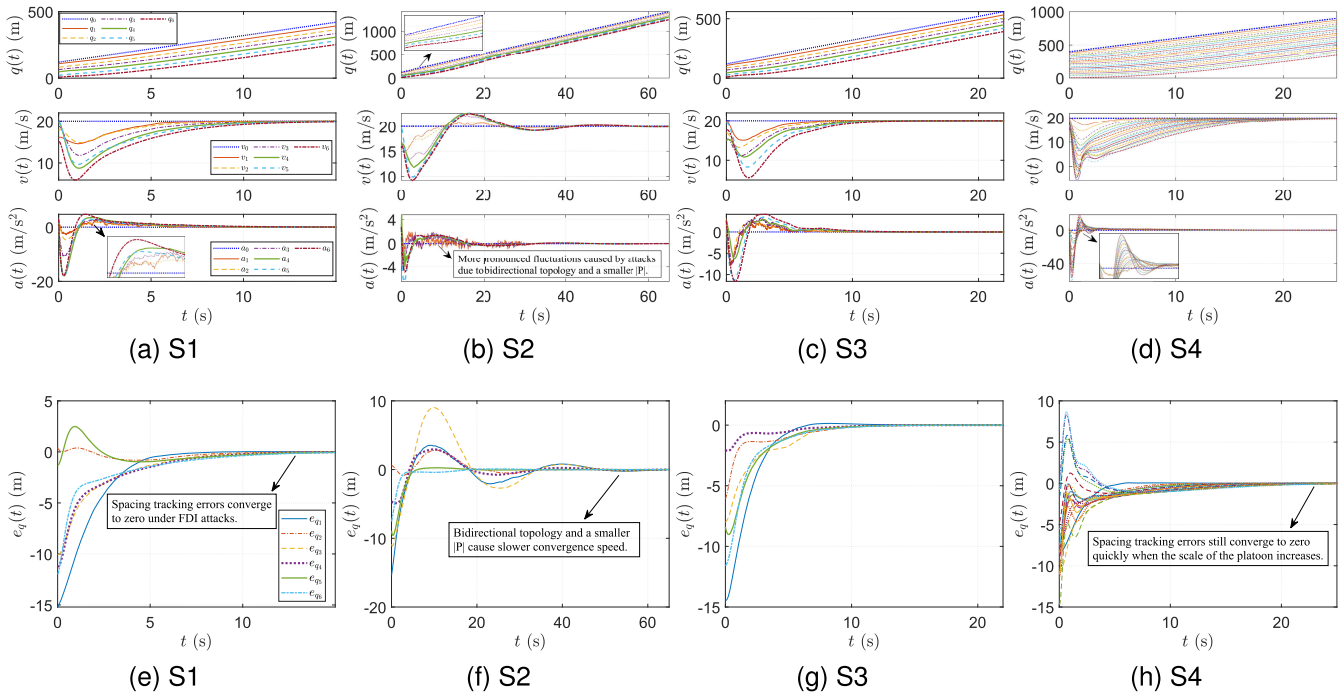


Fig. 3. Platoon stability with node attacks. (a) (b) (c) (d) state the dynamics of vehicle platoons under different cases. (d) (e) (f) (h) depict tracking errors of vehicle platoons under different cases. Note that the legends for (a), (b), (c), and (d) are the same, as are the legends for (e), (f), (g), and (h).

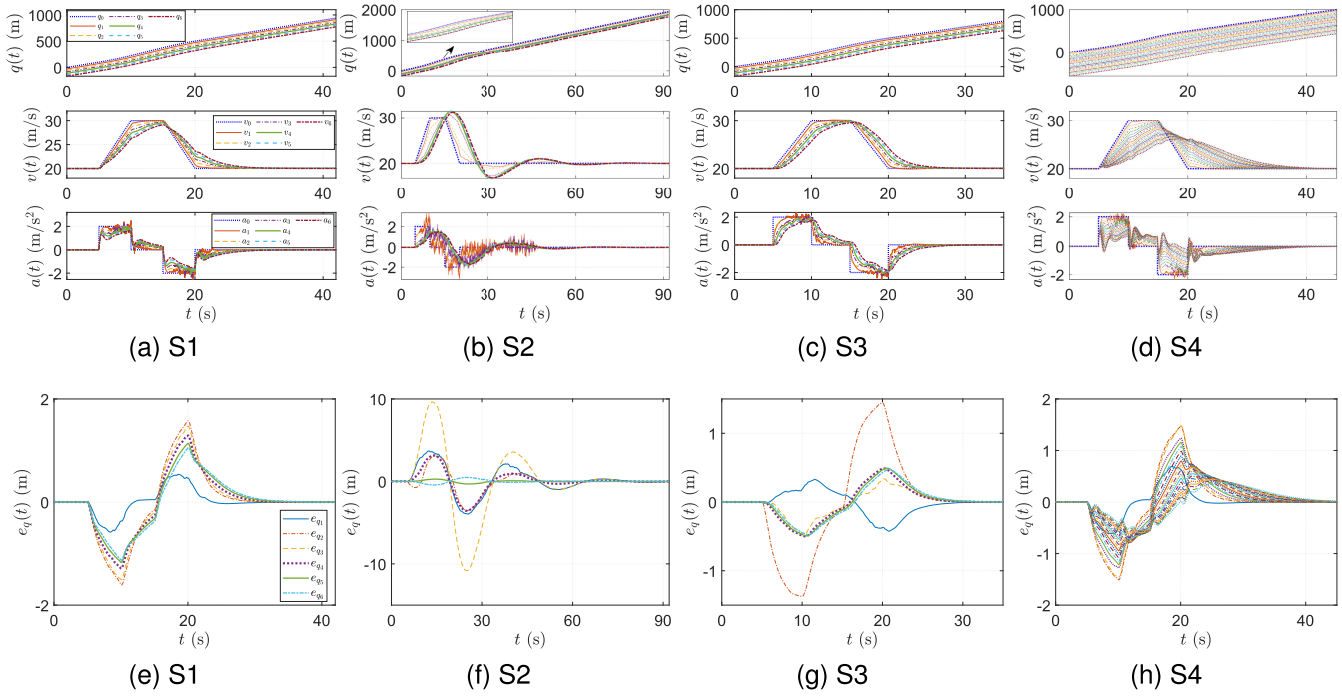
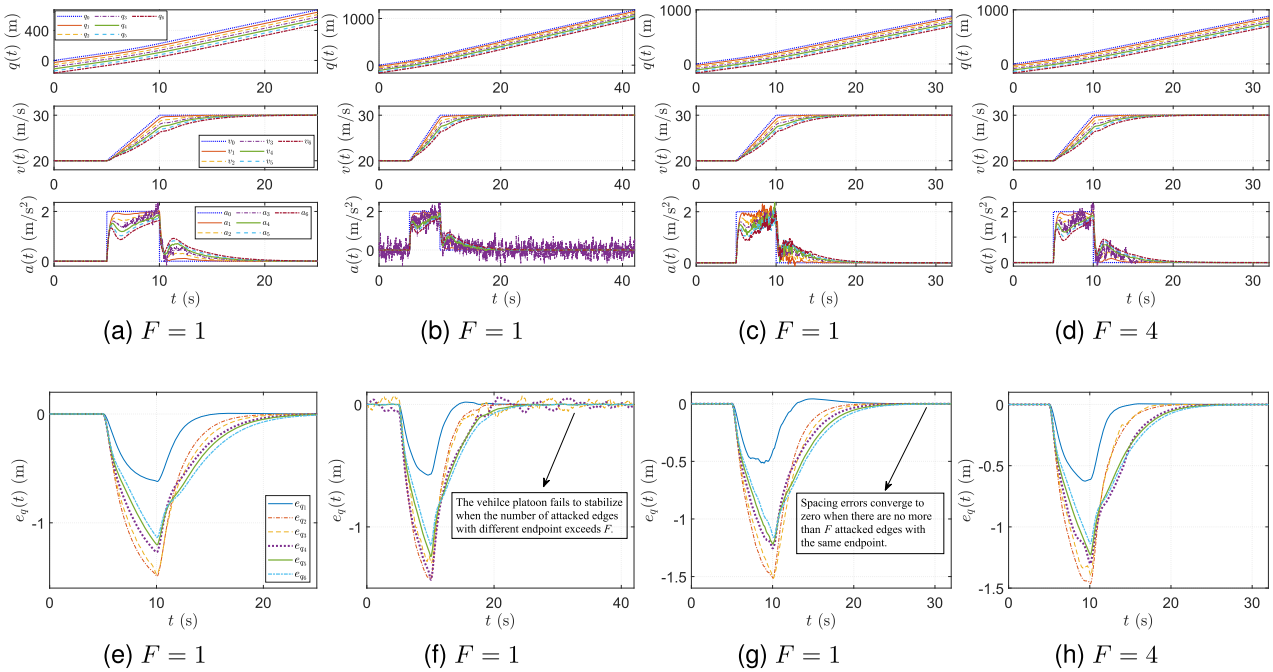


Fig. 4. Platoon stability with node attacks when the leader is disturbed. (a) (b) (c) (d) state dynamics of vehicle platoons under different scenarios. (e) (f) (g) (h) tracking errors of vehicle platoons under different scenarios. Note that the legends for (a), (b), (c), and (d) are the same, as are the legends for (e), (f), (g), and (h).

platoon system can still be achieved in a short period, as shown in Figs. 3d and 3h. Thus, the scalability of Algo. 1 is also guaranteed.

Next, we examine the vehicle platoon under the S1-S4 scenarios when the leading vehicle has disturbances to verify the DR performance. The initial state of the platoon is ideal, and the trajectory of the leading vehicle is the same as Section VI. A-3). All other simulation parameters remain consistent with those specified previously. It can be seen from Fig. 4 that Algo. 1 enables all vehicles to achieve safe and stable driving with ideal inter-vehicle distance under different scenarios.



(a) $F = 1$ (b) $F = 1$ (c) $F = 1$ (d) $F = 4$

(e) $F = 1$ (f) $F = 1$ (g) $F = 1$ (h) $F = 4$

Fig. 5. Platoon stability with edge attacks when the leader is disturbed. (a) (e) state dynamics and tracking errors of the vehicle platoon under single edge $(2, 3)$ attack. (b) (f) state dynamics and tracking errors of the vehicle platoon under two edge $(2, 3)$, $(5, 3)$ attacks with the same endpoint. (c) (g) state dynamics and tracking errors of the vehicle platoon under six edge $(2, 1)$, $(3, 2)$, $(1, 3)$, $(3, 4)$, $(4, 5)$, $(5, 6)$ attacks with different endpoints. (d) (h) state dynamics and tracking errors of the fully connected vehicle platoon under 4 edge $(1, 3)$, $(2, 3)$, $(4, 3)$, $(5, 3)$ attacks with the same endpoints and $F = 4$. Note that the legends for (a), (b), (c), and (d) are the same, as are the legends for (e), (f), (g), and (h).

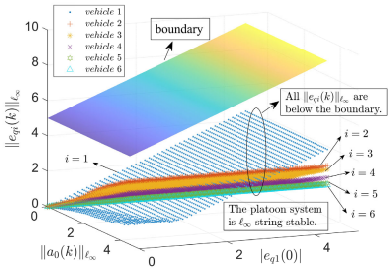


Fig. 6. ℓ_∞-string stability of the vehicle platoon system.

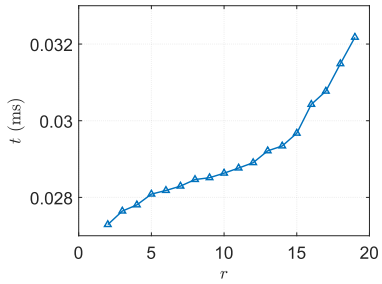


Fig. 7. The running time of Algo. 1 for a single vehicle with different numbers of neighbors.

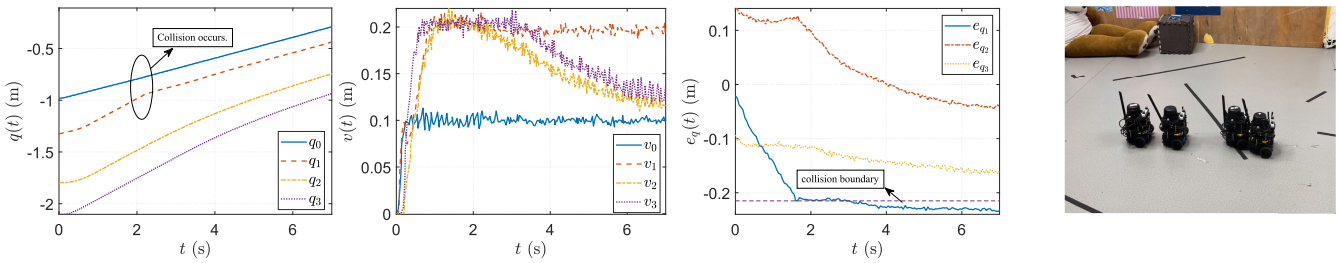
2) Edge Attacks: In this part, we consider arbitrary edge attacks, where the transmitted information is tampered with, and investigate the effectiveness of Algo. 1. When an attacker manipulates the information of any directed link, both the source and sink of the attacked edge may be different. We continue to use the parameters in Section VI-A and the scenario of S1 in Table I. We set $F = 1$, the initial state errors of the system are zero, and the trajectory of the leading vehicle satisfies

$$v_0 = \begin{cases} 20\,\mathrm{m/s}, & 0 \le t \le 5\,\mathrm{s} \\ 20 + 2\,(t-5)\ \mathrm{m/s}, & 5\,\mathrm{s} < t < 10\,\mathrm{s} \\ 30\,\mathrm{m/s}, & t \ge 10\,\mathrm{s} \end{cases}$$

When a single edge $(2, 3)$ is under attacks, it can be seen from Figs. 5a and 5e that the system can achieve stability with the proposed resilient controller. Affected by the attacker, vehicle 3 experiences some fluctuation in acceleration, but it gradually converges to zero as the system stabilizes. However, when both edges $(2, 3)$ and $(5, 3)$ are simultaneously compromised, the system fails to stabilize, as shown in Figs. 5b and 5f. Similarly, it should be pointed out that when the number of attacked edges exceeds F, as long as the sinks of the edges are different or, in other words, there are no more than F attacked edges with the same endpoint, the vehicle platoon can still move stably with ideal inter-vehicle distance. The simulation results shown in Figs. 5c and 5g validate this viewpoint.

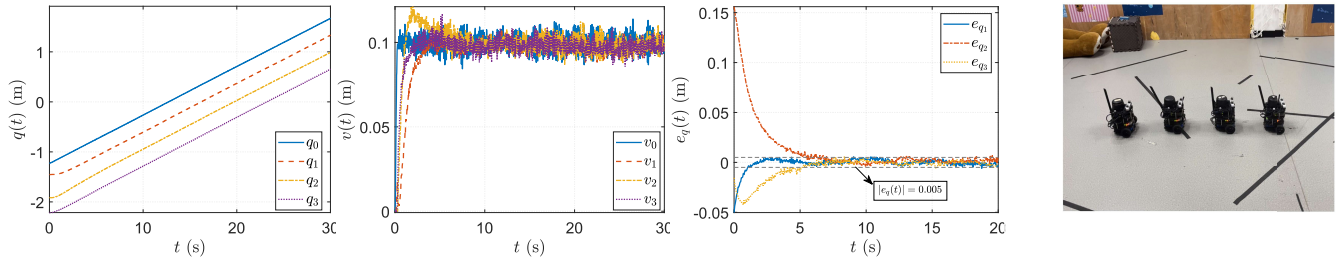
Then, we consider a fully connected vehicle platoon, where all following vehicles can communicate with each other. We set $F = 4$. We also consider the worst-case attack scenario that can be tolerated, where all four attacked edges have the same sink $i = 3$. From Figs. 5d and 5h, we observe that all vehicles achieve stability under attacks, verifying the effectiveness of Algo. 1.

The ℓ_p-string stability of the platoon system under the proposed resilient control is also evaluated via scenario S1 with a nonzero initial tracking error of vehicle 1, i.e., $e_{q1}(0)$, and the nonzero acceleration perturbation of the leading



(a) Position of vehicles (b) Velocity of vehicles (c) Tracking errors (d) Platoon at 3s

Fig. 8. Vehicle platoon dynamics and tracking errors with **non-resilient controller** (5) under FDI attacks: tb3_1 crashes into the leader at approximately 3 s.



(a) Position of vehicles (b) Velocity of vehicles (c) Tracking errors (d) Platoon at 8s

Fig. 9. Vehicle platoon dynamics and tracking errors with **Algo. 1** under FDI attacks: stable formation forms around 8 s.

TABLE II
RUNNING TIME OF ALGO.1 UNDER DIFFERENT SCENARIOS

Scenario	Node ($F = 1$)			
	$N = 6$		$N = 20$	
	formation	DR	formation	DR
S1	0.023 ms	0.023 ms	0.028 ms	0.029 ms
S2	0.022 ms	0.023 ms	0.028 ms	0.028 ms
S3	0.022 ms	0.023 ms	0.027 ms	0.027 ms

vehicle. The initial state is set as the desired state, except for the following vehicle 1 which has a tracking error $e_{q1}(0)$ in the interval $[0, 4.5]$. The trajectory of the leading vehicle is

$$v_0 = \begin{cases} 20\,\text{m/s}, & 0 \le t \le 5\,\text{s} \\ 20 + a_0\,(t-5)\ \text{m/s}, & 5\,\text{s} < t < 10\,\text{s} \\ 30\,\text{m/s}, & t \ge 10\,\text{s} \end{cases}$$

where $a_0 \in [0, 4.5]$. Then, we set $c_\omega = 5$ for $\|a_0(k)\|_{\ell_\infty} < c_\omega$ and $p = \infty$, $\alpha(|e_{q1}(0)|) = |e_{q1}(0)|$, $\kappa_\omega = 1$. The boundary condition for the ℓ_p string stability can be expressed as $\|e_{qi}(k)\|_{\ell_\infty} \le |e_{q1}(0)| + 5$, for $\forall i \in \mathcal{V}$ and $a_0 \in [0, 4.5]$. Since the attack vectors are bounded random values as defined in Section VI-B, we conduct 10 times of simulations and record the results. Note that each simulation results illustrate the ℓ_∞-string stability of the platoon system under Algo. 1. Fig. 6 depicts the average results and illustrates the variation of $\|e_{qi}(k)\|_{\ell_\infty}$ for the vehicle platoon system under different initial tracking error $|e_{q1}(0)|$ and the disturbance of the leader's acceleration a_0. It can be observed from Fig. 6 that when the initial errors and leading vehicle disturbances are bounded, $\|e_{qi}(k)\|_{\ell_\infty}$s of all the following vehicles are less than the boundary condition, indicating that the platoon system is ℓ_∞-string stable.

In the simulation, the MATLAB function ***sortrows*** is used to sort the neighboring states of vehicles, with a time complexity of $\mathcal{O}(m \log m)$ for data points exceeding 32, and $\mathcal{O}(m^2)$ otherwise [41]. The time complexity of Algo. 1 is determined by the sorting algorithm it employs. Extensive simulations have been conducted to demonstrate the running time of Algo. 1, which has been proven to be less than a millisecond. Algo. 1 is written in MATLAB R2019b. All experiments are conducted in Windows 11 with 16 GB of RAM and 12 processor cores. The host machine is an HP Omen 8 Pro laptop with an Intel Core i5-12500H CPU. The simulation time is set to 50 s uniformly, with an iteration time of 0.01 s to test Algo. 1's running time under node attack in different scenarios. The simulations include two performance evaluations for platoon formation and disturbance resistance, as well as two platoon scales. Simulation results about the time required per iteration of a single vehicle are shown in Table II. As seen in Table II, for each vehicle in the platoon, Algo. 1 takes only about 0.2 ms to run per iterative computation.

Since the number of neighbors is the key factor affecting the running time of Algo. 1, we further evaluate Algo. 1 by varying the number of neighbors r (each vehicle has the same number of neighbors here). Fig. 7 depicts the running time of Algo.1 in each iteration for a single vehicle when vehicles have different numbers of neighbors in the platoon system with $N = 20$. It is observed that the running time of Algo. 1 is much less than a millisecond even if r reaches 19.

VII. EXPERIMENTAL RESULTS

Algo. 1 against FDI attacks is implemented on a vehicle platoon experimental platform involving four TurtleBot3 Burger robots and an OptiTrack motion capture system. Specifically, the platoon is composed of one leading vehicle and three following vehicles, labeled as tb3_i, $i \in \{0, 1, 2, 3\}$, respectively. Each TurtleBot3 is equipped with

Ubuntu 18.04 and ROS (Robot Operating System) Melodic, independently carrying out the platoon control tasks. The platoon system uses the ROS communication mechanism to subscribe and publish data to the corresponding topics.

The longitudinal dynamics of TurtleBot3 can be modeled as double integrator dynamics. It is evident that Algo. 1 is applicable to second-order systems with the control law following

$$\bar{u}_i(k) = -\sum\nolimits_{j\in\mathbb{I}_{i,\text{rem}}} \left[\kappa_p\left(p_i(k) - p_{i,j}(k) - d_{i,j}(k)\right) + \kappa_v\left(v_i(k) - v_{i,j}(k)\right)\right] \quad (23)$$

We consider a complete communication topology with

$$\mathcal{L} = \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}, \quad \mathcal{P} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

which ensures the system is (2, 2)-robust. The FDI attack is targeted at tb3_2 with the fixed injected false data $\delta(k) = [0.5, 0.1]^\top$. All vehicles start with zero velocity and have random initial relative distances. After commencement, the leading vehicle tb3_0 moves at a constant speed of $v_0(t) = 0.1\,\text{m/s}$. The parameters of desired inter-vehicle distance are set to $d = 0.3\,\text{m}$ and $h = 0.4\,\text{s}$. Platooning under FDI attacks with non-resilient and resilient control is performed to demonstrate the effectiveness of Algo. 1. It can be observed from Fig. 8 that tb3_1 collided with the leader shortly after its startup, indicating that the platoon system lacks resilience when facing FDI attacks. However, stable platooning can be guaranteed by Algo. 1 as shown in Fig. 9. Note that system noises cause fluctuations in state dynamics, which are small enough. In our case, the tracking error fluctuations essentially remain under 5 millimeters, which is acceptable.

VIII. Conclusion

This study utilized local communication information from multiple links to achieve resilient control for vehicle platoons. The proposed approach allows for distributed deployment with minimal communication costs and delays. The resilient design offers strong robustness against abnormality, enabling tolerance for arbitrary information manipulation within a given upper bound for the manipulated broadcast information. We explicitly provided the conditions for the proposed resilient design that guarantees the stability of the vehicle platoon under attacks. Furthermore, we conducted extensive simulations and experimental results to demonstrate the performance of our design. In the future, we will involve string stability analysis and the development of a control barrier function-based safety design.

References

[1] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Secur.)*, Aug. 2011, pp. 1–16.

[2] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Oct. 2006.

[3] T. Yoshizawa et al., "A survey of security and privacy issues in V2X communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–36, Sep. 2023.

[4] A. Khalil, M. Al Janaideh, K. F. Aljanaideh, and D. Kundur, "Transmissibility-based health monitoring of the future connected autonomous vehicles networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3633–3647, Apr. 2022.

[5] F. Li, C. Wang, D. Mikulski, J. R. Wagner, and Y. Wang, "Unmanned ground vehicle platooning under cyber attacks: A human-robot interaction framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 10, pp. 18113–18128, Oct. 2022.

[6] R. G. Dutta et al., "Estimation of safe sensor measurements of autonomous system under attack," in *Proc. 54th ACM/EDAC/IEEE Design Autom. Conf.*, Austin, TX, USA, Sep. 2017, pp. 1–6.

[7] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Syst. Mag.*, vol. 37, no. 2, pp. 66–81, Apr. 2017.

[8] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy: A study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2015, pp. 1–11.

[9] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *Proc. 1st ACM Workshop Cyber-Phys. Syst.-Secur. PrivaCy*, Oct. 2015, pp. 43–53.

[10] S. H. Kafash, J. Giraldo, C. Murguia, A. A. Cardenas, and J. Ruths, "Constraining attacker capabilities through actuator saturation," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 986–991.

[11] T. Yang and C. Lv, "A secure sensor fusion framework for connected and automated vehicles under sensor attacks," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22357–22365, Nov. 2022.

[12] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2020.

[13] X. He, E. Hashemi, and K. H. Johansson, "Secure platooning of autonomous vehicles under attacked GPS data," 2020, *arXiv:2003.12975*.

[14] T. Yang, C. Murguia, D. Nešić, and C. Lv, "A robust CACC scheme against cyberattacks via multiple Vehicle-to-Vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 9, pp. 11184–11195, 2023.

[15] G. Raja, K. Kottursamy, K. Dev, R. Narayanan, A. Raja, and K. B. V. Karthik, "Blockchain-integrated multiagent deep reinforcement learning for securing cooperative adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9630–9639, Jul. 2022.

[16] H.-T. Sun and C. Peng, "Event-triggered adaptive security path following control for unmanned ground vehicles under sensor attacks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 8500–8509, Aug. 2023.

[17] Z. Ju, H. Zhang, X. Li, X. Chen, J. Han, and M. Yang, "A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective," *IEEE Trans. Intell. Vehicles*, vol. 7, no. 4, pp. 815–837, Dec. 2022.

[18] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat detection for collaborative adaptive cruise control in connected cars," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2018, pp. 184–189.

[19] A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Impact of jamming attacks on vehicular cooperative adaptive cruise control systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 12679–12693, Nov. 2020.

[20] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 5582–5587.

[21] C. Zhao, J. S. Gill, P. Pisu, and G. Comert, "Detection of false data injection attack in connected and automated vehicles via cloud-based sandboxing," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9078–9088, Jul. 2022.

[22] R. A. Biroon, Z. A. Biron, and P. Pisu, "False data injection attack in a platoon of CACC: Real-time detection and isolation with a PDE approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8692–8703, Jul. 2022.

[23] M. Pirani, A. Mitra, and S. Sundaram, "A survey of graph-theoretic approaches for analyzing the resilience of networked control systems," 2022, *arXiv:2205.12498*.

[24] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018.

[25] H. Rezaee, T. Parisini, and M. M. Polycarpou, "Control of vehicular platoons: Stochastic robustness against jamming attacks," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 17041–17046, 2020.
[26] 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, Nov. 2021.
[27] D. Liu, S. Mair, K. Yang, S. Baldi, P. Frasca, and M. Althoff, "Resilience in platoons of cooperative heterogeneous vehicles: Self-organization strategies and provably-correct design," 2023, *arXiv:2305.17443*.
[28] C. Pan, Y. Chen, S. Chen, and I. Ali, "Event-based distributed fixed-time resilient control for heterogeneous vehicular platoon against attack and disturbances," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11858–11868, 2023.
[29] E. Khanapuri, T. Chintalapati, R. Sharma, and R. Gerdes, "Learning based longitudinal vehicle platooning threat detection, identification and mitigation," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 1, pp. 290–300, Jan. 2023.
[30] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, and Y. Jin, "Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 3418–3429, Apr. 2022.
[31] A. Petrillo, A. Pescapé, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134–1149, Mar. 2021.
[32] G. Sun, T. Alpcan, B. I. P. Rubinstein, and S. Camtepe, "To act or not to act: An adversarial game for securing vehicle platoons," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 163–177, 2024.
[33] S. Boddupalli, A. S. Rao, and S. Ray, "Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15655–15672, Sep. 2022.
[34] M. Pirani, S. Baldi, and K. H. Johansson, "Impact of network topology on the resilience of vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15166–15177, Sep. 2022.
[35] R. Chauhan, *A Platform for False Data Injection in Frequency Modulated Continuous Wave Radar*. Logan, UT, USA: Utah State Univ., 2014.
[36] M. Ordean and F. D. Garcia, "Millimeter-wave automotive radar spoofing," 2022, *arXiv:2205.06567*.
[37] C. Zhao, L. Cai, and P. Cheng, "Stability analysis of vehicle platooning with limited communication range and random packet losses," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 262–277, Jan. 2021.
[38] B. Zhou and T. Zhao, "On asymptotic stability of discrete-time linear time-varying systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4274–4281, Aug. 2017.
[39] K. C. Das, "An improved upper bound for Laplacian graph eigenvalues," *Linear Algebra Appl.*, vol. 368, pp. 269–278, Jul. 2003.
[40] S. Feng, Y. Zhang, S. E. Li, Z. Cao, H. X. Liu, and L. Li, "String stability for vehicular platoon control: Definitions and analysis methods," *Annu. Rev. Control*, vol. 47, pp. 81–97, Jan. 2019.
[41] B. McKeeman and L. Shure. (2004). *An Adventure of Sorts-Behind the Scenes of a MATLAB Upgrade*. [Online]. Available: https://ww2.mathworks.cn/company/technical-articles/an-adventure-of-sortsbehind-the-scenes-of-a-matlab-upgrade.html

Chengcheng Zhao (Member, IEEE) received the B.Sc. degree in measurement and control technology and instruments from Hunan University, Changsha, China, in 2013, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2018. She was a Post-Doctoral Fellow with the College of Control Science and Engineering, Zhejiang University, from 2018 to 2021. She is currently a Researcher with the College of Control Science and Engineering, Zhejiang University. Her research interests include consensus and distributed optimization, and security and privacy in networked systems. She received the IEEE PESGM 2017 Best Conference Papers Award, and one of her papers was shortlisted in the IEEE ICCA 2017 Best Student Paper Award Finalist. She is an Editor of *Wireless Networks* and *IET Cyber-Physical Systems: Theory and Applications*.

Ruijie Ma received the B.Sc. degree in automation from Jiangnan University, Wuxi, China, in 2022. She is currently pursuing the M.Sc. degree in control engineering with Zhejiang University, Hangzhou, China. She is a member of the Networked Sensing and Control Group, State Key Laboratory of Industrial Control Technology, Zhejiang University. Her research interests include vehicle formation control and CPS security.

Mengzhi Wang (Member, IEEE) received the B.Sc. degree in automation from Shandong University of Science and Technology, Qingdao, China, in 2011, and the M.Sc. degree in control engineering and the Ph.D. degree in control science and engineering from Beijing Institute of Technology, Beijing, China, in 2013 and 2019, respectively. From 2017 to 2018, he was a Joint Ph.D. Student with the School of Chemical and Materials Engineering, University of Alberta, Edmonton, AB, Canada. From 2019 to 2023, he was a Post-Doctoral Fellow with the School of Control Science and Engineering, Zhejiang University, Hangzhou, China. Since 2024, he has been an Associate Professor with the College of Information Science and Technology, Beijing University of Chemical Technology. His research interests include CPS security, model predictive control, event-triggered control, and data-driven control.

Jinming Xu (Member, IEEE) received the B.S. degree in mechanical engineering from Shandong University, China, in 2009, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University (NTU), Singapore, in 2016. He was a Research Fellow with the EXQUITUS Center, NTU, from 2016 to 2017. He also received post-doctoral training with the Ira A. Fulton Schools of Engineering, Arizona State University, from 2017 to 2018, and the School of Industrial Engineering, Purdue University, from 2018 to 2019. He is currently an Assistant Professor with the College of Control Science and Engineering, Zhejiang University, China. His research interests include distributed optimization and control, machine learning, and network science.

Lin Cai (Fellow, IEEE) has been with the Department of Electrical and Computer Engineering, University of Victoria, since 2005. She is currently a Professor with the Department of Electrical and Computer Engineering, University of Victoria. Her research interests include communications and networking, with a focus on network protocol and architecture design supporting ubiquitous intelligence. She is an NSERC E. W. R. Steacie Memorial Fellow, a Canadian Academy of Engineering (CAE) Fellow, and an Engineering Institute of Canada (EIC) Fellow. In 2020, she was elected as a member of the Royal Society of Canada's College of New Scholars, Artists and Scientists, and the 2020 "Star in Computer Networking and Communications" by N2Women. She served as a Board Member for IEEE Women in Engineering from 2022 to 2024. She will be a Board Member of the IEEE Communications Society (ComSoc) during 2024–2026. She has been elected to serve the IEEE Vehicular Technology Society (VTS) Board of Governors from 2019 to 2024 and served as its VP of Mobile Radio from 2023 to 2024. She received the NSERC Discovery Accelerator Supplement (DAS) Grants in 2010 and 2015. She co-founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter.