Cooperative Adaptive Cruise Control for Connected Vehicle Systems under Composite Attacks

Ahmadreza Jenabzadeh, Zhiguang Feng, Tingwen Huang, *Fellow, IEEE*, Quanmin Zhu, and Yukang Cui

***Abstract*—This paper investigates the cooperative adaptive cruise control (CACC) problem under composite attacks. A novel resilient scheme is proposed for connected vehicle systems to deal with several types of attacks, including denial of service (DoS), camouflage, false-data injection (FDI), and actuator attacks. In contrast to the existing literature dealing with composite attacks, this work not only studies the effect of DoS and FDI attacks on CACC but also investigates the camouflage attacks and unbounded actuator attacks that are intentionally designed to mislead the platoon and jeopardize the dynamics of the vehicles. Also, it is considered that the information of the leader vehicle is not available to the follower vehicles and should be estimated. The proposed scheme is designed based on a two-layer approach to ensure effective CACC with ultimately bounded errors under the mentioned attacks. The presented algorithm is validated using two practical simulation examples.**

***Index Terms*—Connected vehicles, Cooperative adaptive cruise control, Composite attacks, Secure control.**

I. Introduction

INTELLIGENT transportation systems are changing how cities manage traffic by dealing with problems like traffic jams, safety, saving energy, and pollution. With the rising number of vehicles on the road, these issues affect our daily lives and development. Making transportation systems smarter with better scheduling, wireless communication, and automatic controls can solve these problems. Intelligent transportation systems make traffic smoother, enhance road capacity, reduce jams, help self-driving cars, and ensure road safety [1]–[4]. They also save fuel and cut pollution, with methods like managing emissions and controlling energy use in diesel vehicles [5]–[8].

This work was supported by Guangdong Major Project of Basic and Applied Basic Research (2023B0303000009), National Major Scientific Instruments and Equipments Development Project of National Natural Science Foundation of China (62327808), Guangdong Basic and Applied Basic Research Foundation (2024A1515030153), and the Project of Department of Education of Guangdong Province (2022KTSCX105,2023ZDZX4046), Shenzhen Natural Science Fund (Stable Support Plan Program 20231122121608001), and Shenzhen-Hong Kong-Macau Technology Research Programme (SGDX20230821091559019). (*Corresponding author: Yukang Cui.*)

Ahmadreza Jenabzadeh and Yukang Cui are with the College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China, and also with Peng Cheng Laboratory, Shenzhen 518000, China (e-mail: a.jenabzadeh@szu.edu.cn; cuiyukang@szu.edu.cn).

Zhiguang Feng is with the College of Automation, Harbin Engineering University, Harbin 150001, China (e-mail: fengzhiguang@hrbeu.edu.cn).

Tingwen Huang is with the Faculty of Computer Science and Control Engineering, Shenzhen University of Advanced Technology, Shenzhen 518055, China (e-mail: tingwen.huang@qatar.tamu.edu).

Quanmin Zhu is with the School of Engineering, University of the West of England, BS161QY Bristol, U.K. (e-mail: Quan.Zhu@uwe.ac.uk).

One of the fundamental issues in intelligent transportation systems is CACC which aims to maintain a desired distance among vehicles in the connected vehicle systems (CVSs) [9]. By holding the desired inter-vehicle distance, CACC can improve traffic congestion [10], [11]. Also, this technology increases road capacity while saving energy and guaranteeing safety [12]–[14]. It should be mentioned that addressing the CACC problem is a challenging task when CVSs face issues like delays, obstacles, disturbances, and so on. To solve these problems, different strategies have been developed. For example, [15] and [16] worked on improving CACC systems to handle delays in the communication network, making them more reliable. [17] created a method to help vehicles brake together to avoid collisions, which improves safety. Another study by Hu et al. [18] used special controls to keep vehicle groups stable even when disturbances don't match expected patterns. [19] designed a model to make vehicle groups more fuel-efficient while managing delays and input limits. [20] focused on improving how vehicles share information with each other, even when communication is poor. Xie et al. [21] looked into controlling vehicle groups when there is limited communication bandwidth, using learning-based methods. Also, [22] developed a control strategy that keeps CASs safe and functional under faults.

In addition to the aforementioned constraints, CVSs are also vulnerable to different types of attacks since these kinds of systems are considered as a substance subclass of cyber-physical systems. In recent years, CACC under attack has gained considerable attention in the connected vehicles community [23]. For example, a resilient distributed security control scheme was proposed and practically validated for connected vehicles under DoS attacks, which may happen at some sampling time instant and influence the communication links among vehicles [24]. Following this, a control law has been introduced under this kind of attack such that the controller updating frequency is reduced, thereby resulting in saving energy consumption of CVSs [25]. [26] established a control approach for a team of connected vehicles with nonlinear dynamics to accomplish secure tracking of the desired spacing, speed, and acceleration in the presence of deception attacks. In [27], the secure CACC problem was solved for automated vehicles affected by replay attacks. By creating redundancy of inter-vehicle communication paths, attack detection and isolation, and robust control problems have been investigated for CVSs whose communication paths suffer from cyberattacks [28]. A CACC algorithm has been designed against jamming attacks where the attacker sends a jamming signal to channels from a different location to disrupt

communication among vehicles [29]. Using a machine learning approach, a resiliency framework has been developed for CACC under vehicle-to-vehicle attacks [30]. [31] developed a resilient scheme for connected vehicles, assuming the vehicle-to-vehicle communication is under FDI attacks.

The existing works, including [24]–[31], have mostly dealt with the CACC under a single type of attack while the connected vehicles may face composite attacks in practical environments where different types of attacks affect the vehicle platoon at the same time and make the whole system to be unstable. There exist few works that have considered CACC under composite attacks. For instance, [32] studied the CACC problem for connected vehicles with second-order dynamics under multiple cyber-attacks, including DoS attacks and deception attacks. The proposed scheme not only guarantees the CACC of connected vehicles but also was based on the event-triggered scheme resulting in saving communication resources. The results of [32] have been developed based on a sampling period event-triggered approach to reduce the network bandwidth pressure and characterize the effect of DoS attacks [33]. [34] proposed a resilient CACC algorithm for heterogeneous CVSs to prevent delay in the transmission data among vehicles and cope with decreasing the accuracy of receiving information related to follower vehicles affected by FDI and message-delay attacks. In [35], an adaptive scheme was developed for mitigating state-dependent adversarial actuator and sensor attacks while ensuring CACC with uniform ultimate boundedness error.

Upon reviewing the previous works under composite attacks ([32]–[35]), several issues remain to be addressed. Actually, the existing CACC algorithms have primarily been developed for CVSs assuming the availability of information of the leader vehicle. However, this assumption does not hold in some practical environments because of problems like limited energy, limitations in communication ranges, and sensor node faults. Also, a range of attacks has not yet been studied in the context of the dynamics and network of CVSs. One of them is camouflage attacks in which the attacker plans to take control of the vehicle platoon and misleads the vehicles. Another type of attack is unknown unbounded attack signals that are generated by the attackers and injected into the actuator of each follower vehicle to destabilize the platoon dynamics in practice. Therefore, it is important to propose secure and resilient architectures that can guarantee CACC when CVSs face composite attacks, including these two types of attacks in addition to other types of attacks such as DoS and FDI ones while the information of the leader vehicle is unavailable.

Motivated by the explanations provided above, this work solves the CACC problem for CVSs facing composite attacks. To this end, the preliminaries and problem statement are first given in Section II. Then, in Section III, the CACC algorithm is introduced to cope with composite attacks, comprising DoS, camouflage, FDI, and actuator attacks. Utilizing the digital twin approach [36], [37], a dual-layer control scheme comprising a virtual resilient layer (VRL) and cyber-physical layer (CPL) is developed. The VRL as a virtual representation of the CPL possesses the same CPL communication topology and engages in real-time interaction with the CPL. Remarkably, the VRL is equipped with robust security and privacy features, which result in being effective in countering data manipulation attacks like FDI and camouflage attacks in communication networks. Consequently, this paper primarily focuses on designing a defense strategy with two components: the first one is countering DoS attacks on the VRL, and the second one is resisting actuator attacks on the CPL. Finally, Sections IV and V present numerical examples and conclusions to validate and summarize the results of this study. The noteworthy contributions of this paper are as follows:

1) Compared with the existing algorithms of [24]–[35], which deal with the CACC problem under single and double types of attacks, our algorithms are designed to function effectively in the face of composite attacks and efficiently mitigate four types of attacks, such as camouflage and unknown unbounded actuator attacks, that affect communication networks and dynamics of CASs.
2) To establish the proposed resilient framework, this research assumes that the leader vehicle states are not available to any follower vehicle because of practical constraints and should be estimated by a distributed estimator. The resilient approaches in [32]–[35] were developed for scenarios where the leader vehicle is connected to at least one of the follower vehicles, and its states are accessible.
3) In this study, we present a VRL using the digital twin methodology for CVS, aiming to ensure heightened confidentiality and security. This is achievable by deploying the VRL in the Cloud, where it holds less physical significance. By simulating the CVS communication network and estimating states of followers and leader vehicles on this suggested VRL, a substantial portion of attacks on the CPL are effectively impeded.

Notation: The symbol I_η represents a square identity matrix with dimensions $\eta \times \eta$. $\lambda_{\min}(.)$ and $\lambda_{\max}(.)$ express the minimum and the maximum eigenvalues, respectively. The Kronecker product is indicated by $\otimes$. Let R^η denote the dimensional Euclidean space. $R^{\eta_1 \times \eta_2}$ stands for the set of $\eta_1 \times \eta_2$ real matrices. The notation $W > 0$ is employed to express that matrix W is positive definite. The Euclidean norm for vectors is represented by $\|\cdot\|$.

II. Preliminaries and problem definition

A. Communication Graph

The interactions among follower vehicles in CVSs are depicted by an undirected graph denoted as $G = (\vartheta, q, A)$ where the node set is defined as $\vartheta = \{1, 2, ..., v\}$ consists of v follower vehicles, the edge set $q \in \vartheta \times \vartheta = \{(i, j) : i, j \in \vartheta\}$, and the adjacency matrix $A = [a_{ij}] \in R^{v \times v}$. The Laplacian matrix $L = [L_{ij}]$ is defined with elements $L_{ij} = -a_{ij}$ for $i \neq j$ and $L_{ii} = \sum_{j \neq i} a_{ij}$. The second smallest eigenvalue of this matrix is expressed by $\lambda_2(L)$. When vehicles *i* and *j* exchange information with each other, $a_{ij} = a_{ji} > 0$, otherwise, $a_{ij} = 0$. A graph G is considered connected when there is a path from each node to every other node.

This article has been accepted for publication in IEEE Transactions on Intelligent Vehicles. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIV.2024.3469179

B. Vehicles Model

Consider CVSs comprising one leader vehicle and v follower vehicles. The follower vehicles' dynamics are described by

$$\dot{x}_i = Ax_i + Bu_i, \quad i = 1, ..., v, \tag{1}$$

where $u_i \in R^m$ and $x_i \in R^s$ represent the input and the state of vehicle i. $A \in R^{s\times s}$and $B \in R^{s\times m}$ are constant matrices. The leader vehicle's state is assumed to be $\eta \in R^s$ with the dynamics

$$\dot{\eta} = A\eta. \tag{2}$$

The sensing model of the vehicle i is defined as

$$y_i = C\eta. \tag{3}$$

It should be mentioned that the communication among the follower vehicles is bidirectional communication which means every follower vehicle receives/sends relative information from/to both the preceding and the following vehicle as illustrated in Fig. 1. Also, it is assumed that the follower vehicles do not receive any information from the leader vehicle (2) and they should obtain this information using a proposed distributed estimator introduced later.

C. Composite Attacks Description

This paper considers four types of attacks illustrated in Fig. 2 to affect the performance of the CVS as follows:

1) Camouflage attacks: The attacker misleads the vehicles platoon, potentially confusing by disguising itself as the leader vehicle.

2) FDI attacks: These kinds of attackers distort the information exchanged among vehicles. Here, the FDI attack is defined as

$$x_j^c = x_j + x_j^a \tag{4}$$

where x_j represents the true state of neighboring vehicle j, x_j^a stands for the signal of attacker, and x_j^c denotes the disrupted state measurement transmitted to the vehicle i.

3) Actuator attacks: The control input is compromised by the attackers, resulting in the manipulation of the vehicle's control command signal. The attack on actuators is described as

$$u_i^c = u_i + u_i^a \tag{5}$$

where u_i^a denotes the actuator attacker signal and u_i^c represents the compromised control input.

4) DoS attacks: The attacker interrupts the communication links among vehicles and hinders the vehicles from receiving information from their neighbors. This work considers the most destructive DoS attacks, known as zero-topology attacks, that disrupt all communication links on the CPL and VRL during their active attack periods. Assume t_{2k+1} and t_{2k+2} denote the start and end time of the *(2k+1)*-th DoS attack, where $k = 0, 1, 2, \ldots$. Therefore, for any time $t > t_0 \in R$, the time instants set influenced by DoS attacks on the communication network is represented by

$$\Upsilon_A[t_0, t) = \bigcup\nolimits_{k=0,1,2,...} [t_{2k+1}, t_{2k+2}).$$

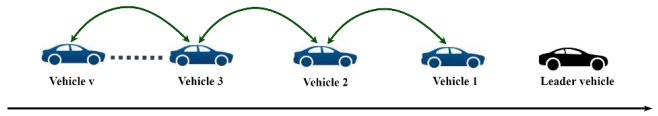


Fig. 1. The communication topology of vehicular platoon

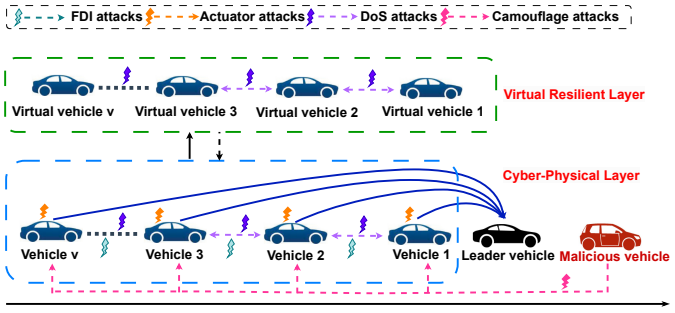


Fig. 2. A double layer scheme.

Furthermore, we define the set of time instants for a safe communication network as

$$\Upsilon_N[t_0, t) = \bigcup\nolimits_{k=0,1,2,...} [t_{2k}, t_{2k+1}).$$

The frequency and duration of DoS Attack are defined in the following definition.

Definition 1 ([38]): For any $t_2 > t_1 \geq t_0$, let $N_a(t_1, t_2)$ and $T_a(t_1, t_2)$ denotes the number and the total time interval of DoS attacks during the time interval $[t_1, t_2)$. Therefore, the attack frequency and attack duration for $t \in [t_1, t_2)$ are defined as

$$F_a(t_1, t_2) = \frac{N_a(t_1, t_2)}{t_2 - t_1},$$
$$T_a(t_1, t_2) \leq T_0 + \frac{t_2 - t_1}{t_a},$$

where $t_a > 1$ and $T_0 > 0$ are constant.

Assumption 1: The actuator attack can be unbounded but its derivative, represented by $\dot{u}_i^a$, is bounded by $\bar{d}$.

D. Problem Definition

Without considering the composite attack, the local CACC error for vehicle i can be defined by

$$\varrho_i(t) = \sum_{j=1}^{v} a_{ij}[x_j - x_i + D_{ij}] + (\eta - x_i + D_{io}) \tag{6}$$

where D_{ij} and D_{io} are the terms to guarantee the expected distance between vehicle i and vehicle j, and between vehicle i and the leader vehicle (2), respectively. However, in the presence of composite attacks, the local CACC error (6) converts to the following form:

$$\bar{\varrho}_i(t) = \sum_{j=1}^{v} d_{ij}[x_j^c - x_i + D_{ij}] + (\eta - x_i + D_{io}) + d_a(\eta_a - x_i + D_{ia}) \tag{7}$$

where d_{ij} stands for the edge weight influenced by the DoS attacks, with $d_{ij} = 0$ for denied communications and $d_{ij} = a_{ij}$ for normal communications. Additionally, d_a indicates the edge weight affected by the camouflage attack on vehicle i. Here, it should be mentioned that although each of four types of attacks related to composite attacks is able to have a hugely destructive effect on CVSs and even result in instability of the whole system, this work studies the effect of the composite attacks which have the destructive influence of all these four types at the same time and can damage more to the system compared to a single type of attack due to the following reasons: 1) Highly aggressive: The composite attacks discussed in this paper are highly aggressive and target both the communication and actuation channels of the vehicular platoon. This is evident from (5) and the difference between equations (6) and (7). Such attacks pose a significant threat to the overall CVS. 2) Highly coupling: The various types of attacks are interconnected and challenging to suppress simultaneously. The local CACC error, a crucial feedback signal in the distributed control scheme, is compromised by DoS attacks, camouflage attacks, and FDI attacks simultaneously, as depicted in equation (7). 3) Potential collusion: There is a possibility of collusion among different kinds of attacks, such as camouflage attacks and FDI attacks, which could mislead the attacked follower. The attacker's goal is to destabilize the whole CVS and jeopardize the string stability of platoons.

The main goal of this work is to establish a resilient scheme for CVSs under composite attacks, with the goal of guaranteeing the desired distance between follower vehicle i described in (1) and the leader vehicle given in equation (2) such that the global CACC error $E_i = x_i - \eta - D_{io}$ is ultimately bounded.

III. Proposed CACC Method Against Composite Attacks

This section introduces a resilient double layer strategy designed to tackle CACC problem under composite attack. Initially, we introduce a VRL capable of effectively resisting FDI, camouflage, and actuator attacks. By using the proposed VRL, a resilient control framework is presented to cope with composite attacks by separating the defense strategy into two parts including protecting follower vehicles (1) from DoS attacks on the VRL as well as actuator attacks on the CPL. The proposed CACC scheme is demonstrated in Fig. 3 where the leader vehicle states and the states of the follower vehicles are reconstructed under DoS attacks on the VRL and transmitted to the distributed control law u_i in the CPL. Also, the actuator attack is estimated on the CPL, and applied to the controller u_i. Utilizing this obtained information on VRL and CPL, the control law u_i can cope with the composite attacks. The details of the proposed control scheme are presented as follows.

A. Virtual Resilient Layer Design Under DoS Attacks

As previously mentioned, the VRL is immune from most of the attack types of composite attacks except for DoS attacks. Therefore, here the goal is to formulate a resilient defense strategy against the DoS attack. To accomplish this objective,

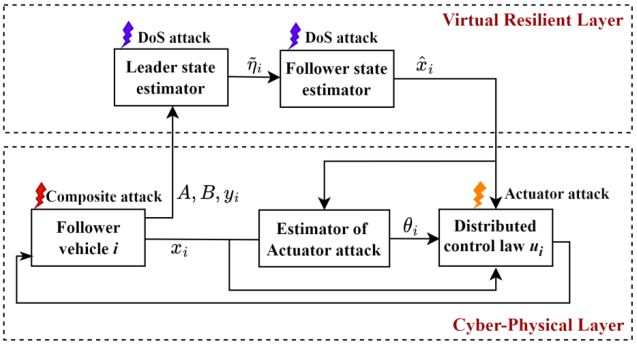


Fig. 3. The proposed CACC framework.

the first step is estimating the states of the leader vehicle (2) by using the proposed distributed estimator

$$\dot{\tilde{\eta}}_i = A\tilde{\eta}_i + Q_i(y_i - C\tilde{\eta}_i) + \Xi_i^{-1}\sum_{j=1}^{v} d_{ij}[\tilde{\eta}_j - \tilde{\eta}_i] \tag{8}$$

where $\tilde{\eta}_i \in R^s$ stands for the estimation of η, $\Xi_i > 0 \in R^{s\times s}$ is a symmetric matrix, and $Q_i = \Xi_i^{-1}C^T$. In the second step, we introduce a distributed resilient estimation algorithm based on the distributed estimator (8) for follower vehicles (1) to estimate the well-tuned state $(\eta + D_{io})$ under DoS attacks. This distributed state estimator on the VRL is represented by the following equation:

$$\dot{\hat{x}}_i = A\hat{x}_i + BB^T\Delta(\sum_{j=1}^{v} d_{ij}[\hat{x}_j - \hat{x}_i + D_{ij}] + (\tilde{\eta}_i - \hat{x}_i + D_{io})) \tag{9}$$

where $\hat{x}_i$ is the i-th follower vehicle's estimation of the actual leader state plus term D_{io}, and $\Delta > 0 \in R^{s\times s}$ is a symmetric matrix. Defining the observer error as $\varsigma_i = \hat{x}_i - \eta - D_{io}$ and the leader vehicle estimation error as $\bar{\eta}_i = \eta - \tilde{\eta}_i$, the error dynamics under normal communication conditions is expressed by

$$\begin{aligned}\dot{\varsigma}_i &= A\varsigma_i + BB^T\Delta(-\sum_{j=1}^{v} a_{ij}[\varsigma_i - \varsigma_j] - (\varsigma_i + \bar{\eta}_i)),\\ \dot{\bar{\eta}}_i &= A\bar{\eta}_i - Q_iC\bar{\eta}_i - \Xi_i^{-1}\sum_{j=1}^{v} a_{ij}[\bar{\eta}_i - \bar{\eta}_j].\end{aligned} \tag{10}$$

Also, during the periods of denied communication, the error dynamics is described as follows:

$$\begin{aligned}\dot{\varsigma}_i &= A\varsigma_i - BB^T\Delta(\varsigma_i + \bar{\eta}_i),\\ \dot{\bar{\eta}}_i &= A\bar{\eta}_i - Q_iC\bar{\eta}_i.\end{aligned} \tag{11}$$

Theorem 1: Consider the leader vehicle (2) and the follower vehicles described in equation (1) faced DoS attacks. By employing the resilient distributed estimators (8) and (9), the errors $\bar{\eta}_i$ and ς_i exponentially converge zero when following conditions hold:

$$\Delta A + A^T\Delta - \Delta BB^T\Delta + M = 0, \tag{12}$$

$$\Xi_i A + A^T\Xi_i - 2C^TC + (\alpha + \varepsilon)I_s < 0, \tag{13}$$

where ε and $\alpha > \lambda_{\max}(\Delta BB^T\Delta)$ are positive constants.

Proof: Select the following Lyapunov function:

$$V = \sum_{i=1}^{v} \varsigma_i^T \Delta \varsigma_i + \sum_{i=1}^{v} \bar{\eta}_i^T \Xi_i \bar{\eta}_i. \tag{14}$$

During the normal communication that no DoS attacks occur, i.e., $t \in \Upsilon_N[t_0, t)$, the derivation of V is obtained as

$$\begin{aligned}\dot{V} =& \sum_{i=1}^{v} 2\varsigma_i^T \Delta (A\varsigma_i + BB^T\Delta(-\sum_{j=1}^{v} a_{ij}[\varsigma_i - \varsigma_j] - (\varsigma_i + \bar{\eta}_i))) \\ &+ \sum_{i=1}^{v} 2\bar{\eta}_i^T \Xi_i (A\bar{\eta}_i - Q_i C\bar{\eta}_i - \Xi_i^{-1} \sum_{j=1}^{v} a_{ij}[\bar{\eta}_i - \bar{\eta}_j]).\end{aligned} \tag{15}$$

Using the inequalities (introduced in [39])

$$\xi_1^T \xi_2 \le \left|\xi_1^T \xi_2\right| \le \|\xi_1\| \, \|\xi_2\|, \tag{16}$$

$$2\|\xi_1\| \, \|\xi_2\| \le \xi_1^T \xi_1 + \xi_2^T \xi_2, \tag{17}$$

we obtain that

$$-2\varsigma_i^T \Delta BB^T \Delta \bar{\eta}_i \le \varsigma_i^T \Delta BB^T \Delta \varsigma_i + \bar{\eta}_i^T \Delta BB^T \Delta \bar{\eta}_i. \tag{18}$$

Choosing a positive constant Ω satisfying $\Omega \le 2\lambda_2(L)$ and replacing (18) in (15), one can get

$$\begin{aligned}\dot{V} \le& \sum_{i=1}^{v} \varsigma_i^T \left(\Delta A + A^T\Delta - (1+\Omega)\Delta BB^T\Delta\right)\varsigma_i \\ &+ \sum_{i=1}^{v} \bar{\eta}_i^T (\Xi_i A + A^T \Xi_i - 2C^T C - \Omega I_s + \Delta BB^T\Delta)\bar{\eta}_i.\end{aligned} \tag{19}$$

Under (12) and (13), one has

$$\begin{aligned}\dot{V} &\le -\sum_{i=1}^{v} \varsigma_i^T \left(M + \Omega \Delta BB^T\Delta\right)\varsigma_i - \sum_{i=1}^{v} \bar{\eta}_i^T ((\Omega+\varepsilon)I)\bar{\eta}_i \\ &\le -\mu_1 \sum_{i=1}^{v} \|\varsigma_i\|^2 - \mu_2 \sum_{i=1}^{v} \|\bar{\eta}_i\|^2 \\ &\le -\bar{\mu}_1 V\end{aligned} \tag{20}$$

in which $\mu_1 = \lambda_{\min}(M + \Omega\Delta BB^T\Delta)$, $\mu_2 = \lambda_{\min}((\Omega+\varepsilon)I)$ and $\bar{\mu}_1 = \frac{\min(\mu_1,\mu_2)}{\lambda_{\max}(P)}$ with $P = diag(\Delta, \Xi_i)$. When communication is disrupted, $t \in \Upsilon_A[t_0, t)$, $\dot{V}$ can be calculated as follows

$$\begin{aligned}\dot{V} =& \sum_{i=1}^{v} 2\varsigma_i^T \Delta \left(A\varsigma_i - BB^T\Delta(\varsigma_i + \bar{\eta}_i)\right) \\ &+ \sum_{i=1}^{v} 2\bar{\eta}_i^T \Xi_i \left(A\bar{\eta}_i - Q_i C\bar{\eta}_i\right).\end{aligned} \tag{21}$$

Utilizing inequalities (16-18), one can derive

$$\begin{aligned}\dot{V} \le& \sum_{i=1}^{v} \varsigma_i^T \left(\Delta A + A^T\Delta - \Delta BB^T\Delta\right)\varsigma_i \\ &+ \sum_{i=1}^{v} \bar{\eta}_i^T (\Xi_i A + A^T\Xi_i - 2C^T C + \Delta BB^T\Delta)\bar{\eta}_i\end{aligned} \tag{22}$$

It follows from (12) and (13) that

$$\begin{aligned}\dot{V} &\le -\sum_{i=1}^{v} \varsigma_i^T M \varsigma_i - \sum_{i=1}^{v} \bar{\eta}_i^T (\varepsilon I)\bar{\eta}_i \\ &\le -\mu_3 \sum_{i=1}^{v} \|\varsigma_i\|^2 - \mu_4 \sum_{i=1}^{v} \|\bar{\eta}_i\|^2 \\ &\le -\bar{\mu}_2 V\end{aligned} \tag{23}$$

where $\mu_3 = \lambda_{\min}(M)$, $\mu_4 = \lambda_{\min}(\varepsilon I_s)$, and $\bar{\mu}_2 = \frac{\min(\mu_3,\mu_4)}{\lambda_{\max}(P)}$. By (20) and (23), one has

$$V(t) \le \begin{cases} e^{-\bar{\mu}_1(t-t_{2k})} V(t_{2k}), & t \in [t_{2k}, t_{2k+1}) \\ e^{-\bar{\mu}_2(t-t_{2k+1})} V(t_{2k+1}), & t \in [t_{2k+1}, t_{2k+2}). \end{cases} \tag{24}$$

Denoting $\bar{\mu} = \begin{cases} -\bar{\mu}_1, & t \in [t_{2k}, t_{2k+1}) \\ -\bar{\mu}_2, & t \in [t_{2k+1}, t_{2k+2}) \end{cases}$, the inequality (24) can be rewritten as

$$V(t) \le e^{\bar{\mu}(t-t_0)} V(t_0). \tag{25}$$

For $t \in \Upsilon_N[t_0, t)$, (25) leads to

$$V(t) \le e^{-\bar{\mu}_1 |\Upsilon_N(t_0,t)| - \bar{\mu}_2 |\Upsilon_A(t_0,t)|} V(t_0). \tag{26}$$

Similarly, we can deduce that (26) holds for $t \in \Upsilon_A[t_0, t)$. Under Definition 1, one gets

$$\begin{aligned}&-\bar{\mu}_1 |\Upsilon_N(t_0,t)| - \bar{\mu}_2 |\Upsilon_A(t_0,t)| \\ =& -\bar{\mu}_1 (t - t_0 - |\Upsilon_A(t_0,t)|) - \bar{\mu}_2 |\Upsilon_A(t_0,t)| \\ \le& -\bar{\mu}_1 (t - t_0) + (\bar{\mu}_1 - \bar{\mu}_2)(T_0 + \frac{t-t_0}{t_a}) \\ \le& -\omega (t - t_0) + (\bar{\mu}_1 - \bar{\mu}_2) T_0\end{aligned} \tag{27}$$

where $\omega = \bar{\mu}_1 - \frac{(\bar{\mu}_1 - \bar{\mu}_2)}{t_a}$. Subsisting (27) into (26), one has

$$\begin{aligned}V(t) &\le e^{-\omega(t-t_0) + (\bar{\mu}_1 - \bar{\mu}_2)T_0} V(t_0) \\ &\le \delta e^{-\omega(t-t_0)}\end{aligned} \tag{28}$$

with $\delta = e^{(\bar{\mu}_1 - \bar{\mu}_2)T_0} V(t_0)$. By Definition 1, it is derived that $\omega > 0$. Therefore, one obtains that $\varsigma_i \to 0$ and $\bar{\eta}_i \to 0$ exponentially for $i = 1, \ldots, v$. ■

B. Resilient Controller Design Under Unbounded Actuator Attacks

In the previous section, we established two distributed estimators for the estimation of the well-tuned state and states of the leader vehicle against DoS attacks. This section aims to present a resilient control framework including the distributed estimators (8) and (9) and a resilient controller to cope with CACC in a scenario involving both DoS and actuator attacks. The proposed distributed control law against actuator attacks (5) is formulated as follows:

$$\begin{cases} u_i(t) = -K\sigma_i - \theta_i, \\ \theta_i = \frac{B^T \Delta \sigma_i}{\left\|\sigma_i^T \Delta B\right\| + \beta} \varrho_i, \\ \dot{\varrho}_i = \left\|\sigma_i^T \Delta B\right\| + l, \end{cases} \tag{29}$$

where $\sigma_i = x_i - \hat{x}_i$ denotes the tracking error, θ_i is the estimation of the actuator attack u_i^a, the parameter β is defined as $\beta = c_1 e^{-c_2 t}$ with positive constants c_1 and c_2, l

stands for a given positive constant, ϱ_i represents an adaptive updating parameter, and the controller gain K is determined as $K = \frac{1}{2}B^T\Delta$.

Theorem 2: Consider v follower vehicles represented by (1) under composite attacks, which encompass unbounded actuator attacks. Under conditions (12)-(13) and Assumption 1, the CACC problem is solved using distributed controllers (29) and the distributed estimation algorithms (8) and (9).

Proof: Theorem 1 demonstrated that the VRL can effectively withstand DoS attacks under relevant conditions. To prove Theorem 2, the convergence of the true state x_i to the estimator state $\hat{x}_i$ should be shown. To this goal, the tracking error dynamics is firstly obtained as follows:

$$\begin{aligned}\dot{\sigma}_i = &A\sigma_i - BK\sigma_i + B\tilde{\theta}_i \\ &+ BB^T\Delta(\sum_{j=1}^{v} d_{ij}[\varsigma_i - \varsigma_j] + (\varsigma_i + \bar{\eta}_i))\end{aligned} \tag{30}$$

where $\tilde{\theta}_i = u_i^a - \theta_i$. Consider a Lyapunov function

$$V_1 = \sum_{i=1}^{v} \sigma_i^T \Delta \sigma_i. \tag{31}$$

The derivation of V_1 can be written as:

$$\begin{aligned}\dot{V}_1 = &\sum_{i=1}^{v} 2\sigma_i^T\Delta(A\sigma_i - BK\sigma_i + B\tilde{\theta}_i \\ &+ BB^T\Delta\bar{\eta}_i + BB^T\Delta(\sum_{j=1}^{v} d_{ij}[\varsigma_i - \varsigma_j] + \varsigma_i))\end{aligned} \tag{32}$$

Using (12) and (18), one obtains

$$\begin{aligned}\dot{V}_1 = &-\sum_{i=1}^{v}\sigma_i^T M\sigma_i + 2\sigma^T\Delta_b B_b B_b^T\Delta_b\Xi\varsigma \\ &+ \sum_{i=1}^{v} 2\sigma_i^T\Delta BB^T\Delta\bar{\eta}_i + \sum_{i=1}^{v} 2\sigma_i^T\Delta B\tilde{\theta}_i \\ \leq &-\lambda_{\min}(M)\|\sigma\|^2 + 2\left\|\sigma^T\right\|\left\|\Delta_b B_b B_b^T\Delta_b\Xi\right\|\|\varsigma\| \\ &+ 2\|\sigma\|\left\|\Delta_b B_b B_b^T\Delta_b\right\|\|\bar{\eta}\| + \sum_{i=1}^{v} 2\sigma_i^T\Delta B\tilde{\theta}_i\end{aligned} \tag{33}$$

where $\Delta_b = I_v \otimes \Delta$ and $\Xi = (L + I_v) \otimes I_s$. In Theorem 1, it was demonstrated that ς and $\bar{\eta}$ converge zero exponentially. Utilizing Young's inequality, one can consequently deduce that

$$\begin{aligned}&2\left\|\sigma^T\right\|\left\|\Delta_b B_b B_b^T\Delta_b\Xi\right\|\|\varsigma\| \leq \\ &\quad\frac{h}{2}\|\sigma\|^2 + \frac{2\left\|\Delta_b B_b B_b^T\Delta_b\Xi\right\|^2}{h}\gamma_1^2 e^{-2\gamma_2 t}, \\ &2\|\sigma\|\left\|\Delta_b B_b B_b^T\Delta_b\right\|\|\bar{\eta}\| \leq \\ &\quad\frac{h}{2}\|\sigma\|^2 + \frac{2\left\|\Delta_b B_b B_b^T\Delta_b\right\|^2}{h}\gamma_3^2 e^{-2\gamma_4 t}\end{aligned} \tag{34}$$

where γ_1, γ_2, γ_3, γ_4 and h are positive constants. In addition, we have

$$\begin{aligned}\sigma_i^T\Delta B\tilde{\theta}_i &= \sigma_i^T\Delta Bu_i^a - \frac{\left\|\sigma_i^T\Delta B\right\|^2}{\left\|\sigma_i^T\Delta B\right\| + \beta}\varrho_i \\ &\leq \left\|\sigma_i^T\Delta B\right\|\|u_i^a\| - \frac{\left\|\sigma_i^T\Delta B\right\|^2}{\left\|\sigma_i^T\Delta B\right\| + \beta}\varrho_i \\ &= \frac{\left\|\sigma_i^T\Delta B\right\|^2(\|u_i^a\| - \varrho_i) + \left\|\sigma_i^T\Delta B\right\|\|u_i^a\|\beta}{\left\|\sigma_i^T\Delta B\right\| + \beta}.\end{aligned} \tag{35}$$

It follows from Assumption 1 that $\frac{d\|u_i^a\|}{dt}$ is bounded. Therefore, one can deduce that $\|u_i^a\|\beta \to 0$. By selecting $\left\|\sigma_i^T\Delta B\right\| + l > \bar{d}$ and employing the fact $\frac{d\|u_i^a\|}{dt} \leq \bar{d}$, one obtains the following inequality:

$$\frac{d\|u_i^a\|}{dt} - \dot{\varrho}_i < 0. \tag{36}$$

Thus, there is $t_1 > 0$ such that for all $t \geq t_1$ one has $\|u_i^a\| - \varrho_i < 0$, which implies

$$\sum_{i=1}^{v} 2\sigma_i^T\Delta B\tilde{\theta}_i < 0. \tag{37}$$

Substituting (34) into (33) and using (37), one can derive

$$\dot{V}_2 \leq -\omega_1\|\sigma\|^2 + \omega_2 \tag{38}$$

where $\omega_1 = \lambda_{\min}(M) - h$, $\omega_2 = \frac{2\left\|\Delta_b B_b B_b^T\Delta_b\Xi\right\|^2}{h}\gamma_1^2 e^{-2\gamma_2 t} + \frac{2\left\|\Delta_b B_b B_b^T\Delta_b\right\|^2}{h}\gamma_3^2 e^{-2\gamma_4 t}$.

Given that matrix M is positive definite, the inequality $\lambda_{\min}(M) > h$ holds for any arbitrary parameter h. Consequently, ω_1 is verified to be positive. Additionally, it is evident that there is an upper bound for ω_2, represented by $\bar{\omega}_2$. Let's define $\omega_3 = \frac{\omega_1}{\lambda_{\max}(\Delta_b)}$. This yields

$$\dot{V}_2 \leq -\omega_3 V_1 + \bar{\omega}_2. \tag{39}$$

Applying the well-known Comparison Lemma, one can derive

$$V_1(t) \leq (V_1(0) - \frac{\bar{\omega}_2}{\omega_3})e^{-\omega_3 t} + \frac{\bar{\omega}_2}{\omega_3}. \tag{40}$$

Considering the inequality $\lambda_{\min}(\Delta_b)\|\sigma\|^2 \leq V_1(t)$, we obtain

$$\|\sigma\|^2 \leq (V_1(0) - \frac{\bar{\omega}_2}{\omega_3})\frac{e^{-\omega_3 t}}{\lambda_{\min}(\Delta_b)} + \frac{\bar{\omega}_2}{\lambda_{\min}(\Delta_b)\omega_3}. \tag{41}$$

Since $e^{-\omega_3 t}$ approaches zero as $t \to \infty$, it can be concluded that σ is ultimately bounded. Thus, the resilient control law (29) guarantees the CACC under unbounded actuator attacks with an ultimately bounded error. ■

Remark 1: It is important to note that the existence of the parameters Ξ_i and Δ depends on the feasibility of LMIs (12) and (13). To obtain Δ, (12) should be solved that need *(A,B)* should be controllable. Additionally, to compute matrix Ξ_i, it is necessary for the LMI (13) to have a solution, implying that the pair *(A,C)* should be observable.

Remark 2: The CACC problem is investigated for CVSs under composite attack in this work but there are also some other practical constraints such as packet loss and network latency which destructively influence CVSs and their effects

on the proposed CACC algorithms should be considered. Based on Theorems 1-2 and their proof, the proposed CACC algorithm is resilient to DoS attacks. Moreover, the considered DoS attack in our paper may last for a long period of time satisfying the mentioned conditions in Definition 1. In fact, when the frequency of communication failure is less than a specific value, the considered DoS attacks may involve scenarios where the network of vehicles is blocked for a specific period of time. It implies the considered DoS attacks usually comprise the category of packet loss since the number of packet losses is usually a member of an integer set, with the number of continuous packet losses being less than a small number. Therefore, the proposed scheme is also able to cope with packet losses since the communication failure frequency caused by packet losses is usually small and meets the conditions related to DoS attacks mentioned in Definition 1.

In addition to packet loss, network latency is one of the main factors influencing the CVS performance. As the connection among the vehicles and between VRL and CPL relies on real-time data transfer to keep them always synchronized, high latency of this communication process can lead to inaccurate system updates in real-time and even instability in the CVS. To deal with communication latency, high-speed wireless network technologies such as 5G wireless communication systems can be used to ensure high transmission rates with high quality resulting in reduced transmission duration and latency. Also, compressing data by decreasing the amount of transmitted data is another method for reducing the transmission latency. This can involve employing various existing data compression techniques or utilizing machine learning algorithms to detect changes in the CVS, transmitting only updates while omitting redundant data transmissions when no updates occur.

IV. Simulation Examples

This section presents two numerical simulations to show the efficiency of the suggested CACC algorithm. The simulations are done on a CVS in which the interaction among vehicles is shown in Fig. 1. First, the CACC problem is studied for a CVS that faces composite attacks and its follower vehicles have the following dynamics [25]:

$$\dot{x}_i = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} x_i + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u_i^c, \ i = 1, ..., 4, \tag{42}$$

where $x_i = \begin{bmatrix} p_i \\ v_i \end{bmatrix}$ is the state of the *i*-th follower vehicle in which p_i and v_i denote its position and velocity, respectively. The leader vehicle is described by [25]:

$$\dot{\eta} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \eta \tag{43}$$

where $\eta = \begin{bmatrix} p_o \\ v_o \end{bmatrix}$ represents the state of the leader vehicle. Meanwhile, the sensing model is defined as:

$$y_i = 3p_o + 2v_o. \tag{44}$$

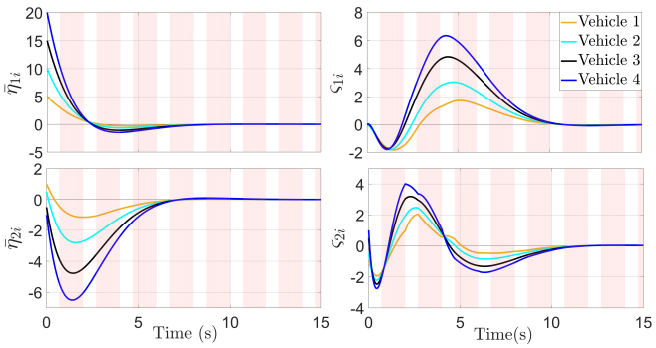


Fig. 4. The estimation error of the states of leader vehicle (43) and the well-tuned states: The duration of the DoS attacks is denoted by the light red blocks.

For this example, D_{ij} and D_{io} are $D_{ij} = \begin{bmatrix} p_{ij} \\ 0 \end{bmatrix}$ and $D_{io} = \begin{bmatrix} p_{io} \\ 0 \end{bmatrix}$ where $p_{ij} = p_i - p_j$ and $p_{io} = p_i - p_o$. It is assumed the desired distance between vehicle *i* and vehicle *j* , and between vehicle *i* and the leader vehicle are 5 and 5i meters that implies $|p_{ij}| = 5$ and $p_{io} = -5i$, respectively. The duration of the time intervals for the DoS attack is defined as $[0.7+2k, 2+2k)s$ for $k = 0, 1, 2, \ldots$, following conditions in Definition 1. The FDI and camouflage attacks are assigned as $x_j^a = [0.4 \sin t \ 0.3t]^T$ and $\eta_a = [0.3e^{0.1t} \ 0.2 \cos t]^T$, respectively. The actuator attack is represented as $u_i^a = 0.5t$ and the simulations employs the following parameters:

$\Xi_i = \begin{bmatrix} 15.1524 & -6.1524 \\ -6.1524 & 21.4572 \end{bmatrix}$, $Q_i = \begin{bmatrix} 0.2669 \\ 0.1697 \end{bmatrix}$, $\Delta = \begin{bmatrix} 1.7321 & 1.0000 \\ 1.0000 & 1.7321 \end{bmatrix}$, $K = [0.5000 \ 0.8660]$, $M = \mathrm{I}_2$, $a_{ij} = 1$, $\alpha = 4.5$, $\varepsilon = 0.5$.

To handle composite attacks including DoS, camouflage, FDI, and actuator attacks, the proposed controller (29) is applied to the CVS (42). As mentioned in the main results section, the proposed CACC algorithm splits the attack resilient problem into two distinct tasks: defending against DoS attacks on the VRL and protecting follower vehicles from actuator attacks on the CPL. It means the CVS (42) with (29) is resilient to FDI and camouflage attacks because the distributed control law (29) does not utilize the information transmitted on the CPL. Fig. 4 illustrates the estimation errors of the states (position and velocity) of the leader vehicle (43) and the well-tuned state in the presence of DoS attacks on the VRL. It is obvious from these figures that the CVS (42) with (29) efficiently cope with DoS attacks on the VRL. To defend against actuator attacks, θ_i in (29) is employed to estimate the actuator attack, with the results shown in Fig. 5. Then, this estimation is used in the controller (29) to remove the effect of the actuator attack. Fig. 6 demonstrates the states of followers and leader vehicles under composite attacks, respectively. This figure verifies that the CACC of connected vehicles (42) and leader vehicle (43) under composite attacks with the proposed scheme is achieved holding a prescribed distance among vehicles of the CVS and tracking a desired velocity with an ultimate bounded error.

This article has been accepted for publication in IEEE Transactions on Intelligent Vehicles. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIV.2024.3469179

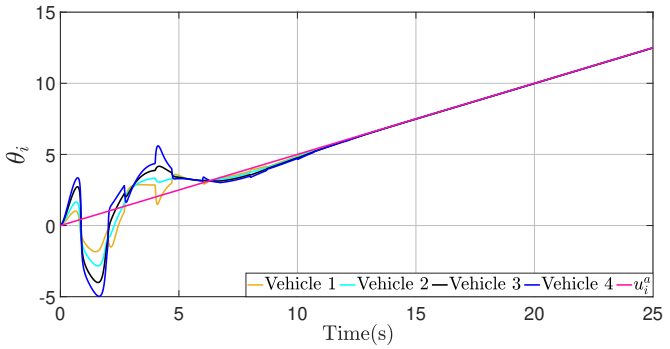


Fig. 5. The actuator attack estimation.

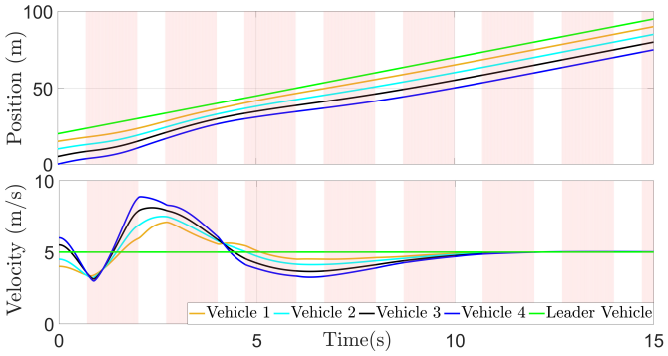


Fig. 6. The states (position and velocity) of the follower vehicles (42) and leader vehicle (43) applying the controller (29).

Compared with the existing CACC algorithms, the proposed approach has a promising performance to cope with composite attacks. To show this, CVS (42) with the proposed CACC scheme (29) is compared with the CACC scheme of [32] in three scenarios. In the first scenario, the proposed CACC approach is compared with the algorithm of [32] under DoS and FDI attacks since the scheme of [32] has been proposed under these two types of attacks. The simulation results of this comparison are shown in Fig. 7 where the proposed scheme achieves CACC while the follower vehicles in (42) using the approach of [32] have a collision based on the position curve in Fig. 7 (b) and fail to guarantee CACC. This is because the approach of [32] has been obtained for a CVS with bounded states while there is not such a condition in our work. In the second scenario, bounded camouflage and actuator attacks are added to DoS and FDI attacks. It means composite attacks including bounded $\eta_a = [0.3\sin t \;\; 0.2\cos t]^T$ and $u_i^a = 0.5\sin t$ are applied to the both CACC algorithms. In this case, the proposed CACC algorithm has a similar performance compared to the first scenario illustrated in Fig. 8 (a) while the scheme of [32] has a higher CACC error shown in Fig. 8 (b). In the third scenario, the controller (29) and the CACC algorithm of [32] have been compared under composite attacks including unbounded camouflage and actuator attacks mentioned at the beginning of this section. The states of followers and leader vehicles for both schemes under this kind of composite attack are illustrated in Fig. 6 and Fig. 9. Also, the CACC errors of these CACC protocols are indicated in Fig. 10 which verifies that the composite attacks with unbounded camouflage and actuator attacks have a considerably higher destructive effect on the performance of the CACC algorithm of [32] compared with the first and second scenarios. These effects are such that not only the desired distance among vehicles is not maintained, but also collisions occur among them. This is even though the desired distance among vehicles is maintained using our proposed algorithm under such destructive composite attacks. This fact can be also seen in Fig. 11 where the norms of CACC errors in the proposed scheme and the CACC approach introduced in [32] for all three scenarios are illustrated. This figure confirms that the CACC error norm related to the CACC algorithm of [32] under composite attacks gradually increases as time goes by while the proposed CACC controller (29) has a bounded CACC error norm and can effectively cope with the

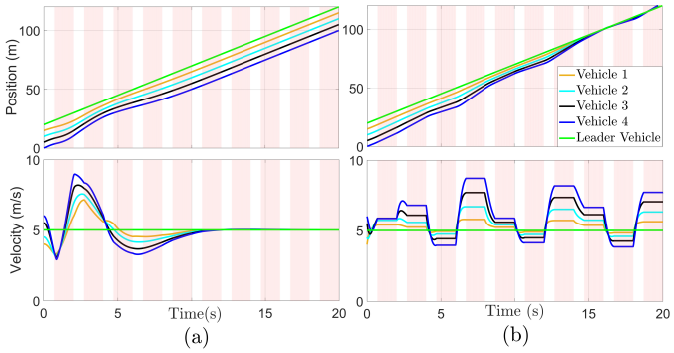


Fig. 7. The states of the follower vehicles (42) and leader vehicle (43) under DoS and FDI attacks using: (a) the proposed CACC scheme, (b) the CACC approach of [32].

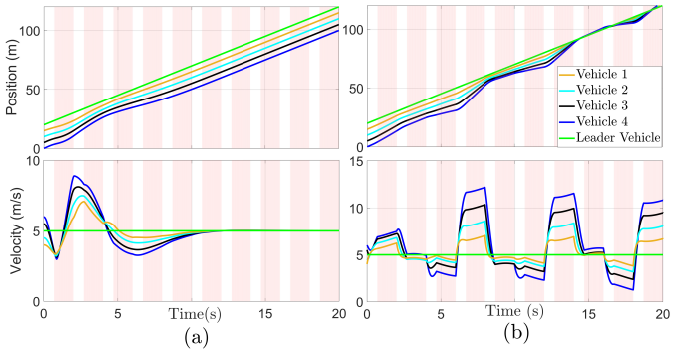


Fig. 8. The states of the follower vehicles (42) and leader vehicle (43) under composite attacks including bounded camouflage and actuator attacks using: (a) the proposed CACC scheme, (b) the CACC approach of [32].

composite attacks. It is worth noting that the CACC controller (29) preserves the desired performance in the three scenarios while the CACC algorithm of [32] has a different performance with the highest error for composite attacks with unbounded camouflage and actuator attacks. This verifies the ability of the proposed CACC algorithm to cope with unbounded and bounded composite attacks.

Next, a practical example is considered for validating the proposed CACC algorithm against composite attacks. In this case, a CVS composed of four vehicles is used in which the dynamics of the *i*-th one is given by [33]:

This article has been accepted for publication in IEEE Transactions on Intelligent Vehicles. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIV.2024.3469179

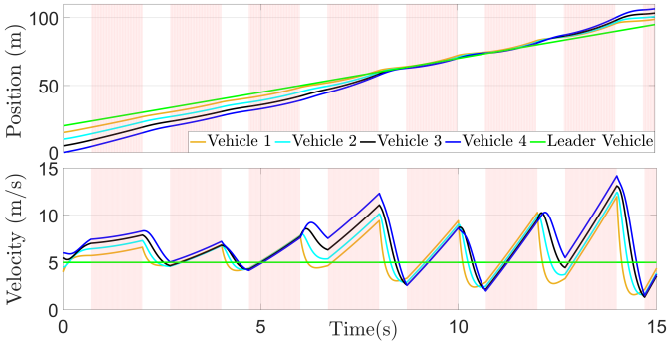


Fig. 9. The states of the follower vehicles (42) and leader vehicle (43) under the CACC approach of [32].

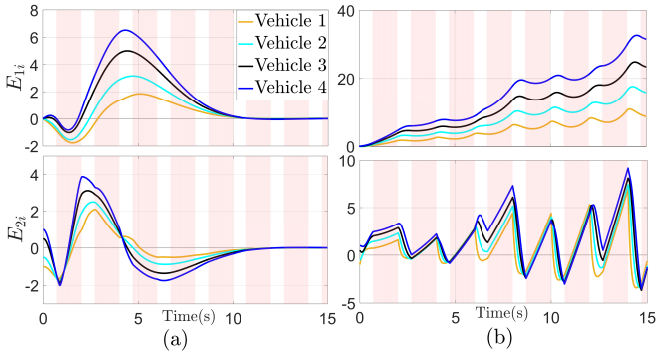


Fig. 10. The CACC errors of follower vehicles in (42) using: (a) the controller (29), (b) the CACC approach of [32].

$$\dot{x}_i = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix} x_i + \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix} u_i^c, \ i = 1, ..., 4. \tag{45}$$

where $x_i = (p_i \ v_i \ a_i)^T$ is the state vector of vehicle i, in which p_i, v_i, and a_i represent the position, velocity, and acceleration of vehicle i, respectively. $\tau = 0.5$ is a time constant relevant to the engine's dynamics. The leader vehicle is given by the dynamical system ([33])

$$\dot{\eta} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix} \eta \tag{46}$$

where $\eta = (p_o \ v_o \ a_o)^T$ is the state vector of the leader vehicle (being p_o, v_o, and a_o the leader position, velocity, and acceleration, respectively). For vehicle i, the measurement equation is defined as

$$y_i = 3p_o + 2v_o + a_o.$$

The composite attacks are considered the same as those of follower vehicles in (42). Here, D_{ij} and D_{io} are defined as $D_{ij} = (p_{ij} \ 0 \ 0)^T$ and $D_{io} = (p_{io} \ 0 \ 0)^T$ with $|p_{ij}| = 20$ and $p_{io} = -20i$, that means the goal is remaining the safe distance 20 meters between vehicles i and j, and distance 20i meters between vehicle i and leader vehicle (46), and all follower vehicles require to maintain the same velocity and acceleration with the leader vehicle. The controller (29) and estimators in (8)-(9) are applied to the CVS including vehicles (45) and (46) with the following parameters:

$$\Xi_i = \begin{bmatrix} 17.9280 & -9.1345 & -6.3771 \\ -9.1345 & 26.5516 & 7.2792 \\ -6.3771 & 7.2792 & 13.5973 \end{bmatrix}, \ Q_i = \begin{bmatrix} 0.2845 \\ 0.1365 \\ 0.1339 \end{bmatrix},$$

$$\Delta = \begin{bmatrix} 2.2650 & 2.0652 & 0.5000 \\ 2.0652 & 4.1777 & 1.1325 \\ 0.5000 & 1.1325 & 0.5326 \end{bmatrix},$$

$K = [0.5000 \ 1.1325 \ 0.5326]$, $a_{ij} = 1$, $\varepsilon = 0.5$, $\alpha = 7.5$. The CACC errors for four vehicles are displayed in Fig. 12, which demonstrate the effectiveness of the suggested CACC scheme. In addition, Fig. 13 shows the states of the followers and leader vehicles under composite attacks, which confirms that the desired distance between vehicles and the velocity and acceleration of all vehicles remain constant. Thus, as mentioned in Theorem 2, the proposed approach can withstand the effect of composite attacks, which ensures CACC with ultimate bounded errors.

As mentioned in Remark 2, network latency is a factor that can negatively affect the CVS performance. Therefore, the proposed CACC performance is investigated under latency here. To this goal, it is assumed that the connection among the follower vehicles and between VRL and CPL are affected by latency. It means the neighboring states of $\tilde{\eta}_j(t)$ and $\hat{x}_j(t)$ related to algorithms (8) and (9) as well as the transmitted states between VRL and CPL, $\hat{x}_i(t)$ in (29), are under delay. In this case, $\tilde{\eta}_j(t)$, $\hat{x}_j(t)$ and $\hat{x}_i(t)$ are replaced by $\tilde{\eta}_j(t-\tau_d)$, $\hat{x}_j(t-\tau_d)$, and $\hat{x}_i(t-\tau_d)$ where τ_d denotes the communication delay caused by network latency. It should be mentioned that the type of communication among vehicles and between VRL and CPL is wireless. Also, it is known that the maximum latency of most of the existing wireless communication networks is 0.2 s, as an example of a maximum of 0.1 s and 0.15 s for 4G and 3G networks under normal operating conditions. Thus, the CVS (45) and the proposed CACC are simulated under different communication delays of 0.1 and 0.2 s. Fig. 14 illustrates the CACC errors of follower vehicles in (45) approving the proposed CACC algorithm can guarantee the string stability of the CACC systems under communication delays of 0.1 s and 0.2 s while preserving the desired distance among vehicles. It is worth noting that the CVS (45) with higher communication delay is also simulated, implying string instability and the existence of some collision among vehicles for $\tau_d > 1.5$.

V. Conclusion

In this study, the CACC problem has been tackled for CVSs with general linear dynamics. Considering the effect of the composite attacks on the dynamics and communication network of CVSs, a defense strategy based on the digital twin technology is developed and a distributed resilient controller is established to effectively protect the CVS from the adverse effects of different types of attacks and maintain the desired distance between vehicles. The obtained results have assured the achievement of the CACC without the availability of the leader vehicle information. The numerical examples have been

This article has been accepted for publication in IEEE Transactions on Intelligent Vehicles. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TIV.2024.3469179

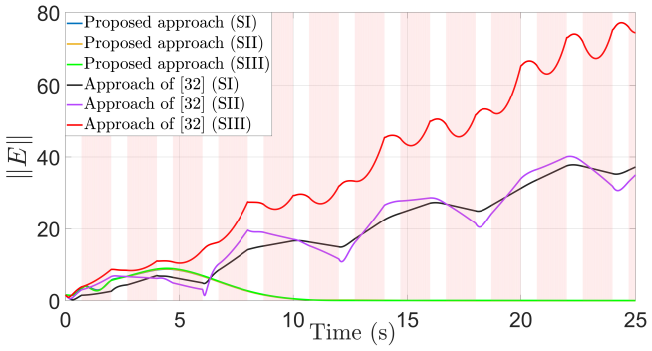


Fig. 11. CACC error norms of the proposed algorithm and CACC approach of [32] for scenario I (SI), scenario II (SII), and scenario III (SIII).

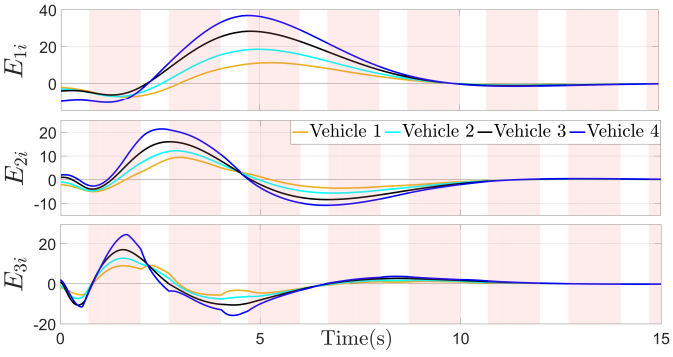


Fig. 12. The CACC errors of follower vehicles in (45).

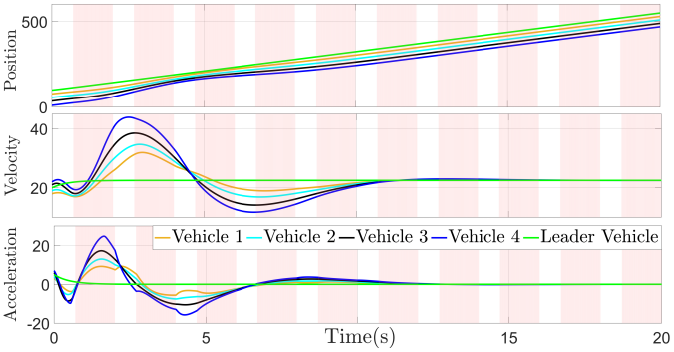


Fig. 13. The states (position and velocity) of the follower vehicles in (45) and leader in vehicle (46).

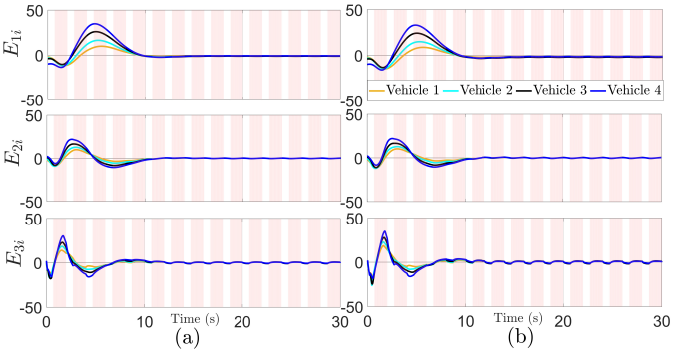


Fig. 14. The CACC errors of the follower vehicles (45) under communication error: (a) $\tau_d = 1$, (b) $\tau_d = 2$.

employed to illustrate the efficiency of the proposed CACC protocol in maintaining the desired inter-vehicle distance under composite attacks.

However, the proposed approach still has some limitations. Firstly, the same dynamics has been utilized for all follower vehicles while considering a heterogeneous vehicle string consisting of follower vehicles with different characteristics can be more practical. Secondly, the communication among the follower vehicles is bidirectional communication which results in more communication burden compared with directional communication. Lastly, even if coping with composite attacks has been addressed, there are still some practical constraints on the system such as bounds on road speed limit, acceleration, and input that are required to be dealt with. In our future studies, we will develop our method for heterogeneous CVSs with directional communication topology considering the aforementioned practical constraints.

REFERENCES

[1] H. Pan, M. Luo, J. Wang, T. Huang, and W. Sun, "A safe motion planning and reliable control framework for autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, 10.1109/TIV.2024.3360418, 2024.

[2] Y. Ma, R. Du, A. Abdelraouf, K. Han, R. Gupta, and Z. Wang, "Driver digital twin for online recognition of distracted driving behaviors," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 2, pp. 3168-3180, 2024.

[3] Z. Zhou, Z. Yang, Y. Zhang, Y. Huang, H. Chen, and Z. Yu, "A comprehensive study of speed prediction in transportation system: From vehicle to traffic," *Iscience*, vol. 25, no. 3, 2022.

[4] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Vehicular Technology Magazine*, vol. 5, no. 1, pp. 77–84, 2010.

[5] Y. Sun, Y. Hu, H. Zhang, H. Chen, and F.-Y. Wang, "A parallel emission regulatory framework for intelligent transportation systems and smart cities," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1017–1020, 2023.

[6] L. Guo, M. Sun, Y. Hu, and H. Chen, "Optimization of fuel economy and emissions through coordinated energy management for connected diesel vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 6, pp. 3593–3604, 2023.

[7] S. Dong et al., "Cooperative eco-driving control of connected multi-vehicles with spatio-temporal constraints," *IEEE Transactions on Intelligent Vehicles*, 10.1109/TIV.2023.3282490, 2023.

[8] A. Hadjigeorgiou and S. Timotheou, "Real-time optimization of fuel-consumption and travel-time of CAVs for cooperative intersection crossing," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 313–329, 2022.

[9] Z. Wang, G. Wu, and M. J. Barth, "A review on cooperative adaptive cruise control (CACC) systems: Architectures, controls, and applications," in *Proceedings of 2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018: IEEE, pp. 2884–2891.

[10] A. Lunge and P. Borkar, "A review on improving traffic flow using cooperative adaptive cruise control system," in *Proceedings of 2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015: IEEE, pp. 1474–1479.

[11] S. Mosharafian and J. M. Velni, "Cooperative adaptive cruise control in a mixed-autonomy traffic system: A hybrid stochastic predictive approach incorporating lane change," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 1, pp. 136-148, 2022.

[12] B. Van Arem, C. J. Van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristics," *IEEE Transactions on Intelligent Transportation Systems*, vol. 7, no. 4, pp. 429-436, 2006.

[13] Y. Kim, J. Guanetti, and F. Borrelli, "Compact cooperative adaptive cruise control for energy saving: Air drag modeling and simulation," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 9838–9848, 2021.

[14] I. Mahdinia, R. Arvin, A. J. Khattak, and A. Ghiasi, "Safety, energy, and emissions impacts of adaptive cruise control and cooperative adaptive cruise control," *Transportation Research Record*, vol. 2674, no. 6, pp. 253–267, 2020.

[15] Y. Zhang, Y. Bai, M. Wang, and J. Hu, "Cooperative adaptive cruise control with robustness against communication delay: An approach in the space domain," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 9, pp. 5496-5507, 2020.
[16] W. Cao, G. Gu, L. Zhang, C. Peng, and H. He, "Analysis and synthesis of cooperative adaptive cruise control against the hetero-integration poly-net loop delays," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 12, pp. 12913–12925, 2023.
[17] M. Hu, J. Li, Y. Bian, J. Wang, B. Xu, and Y. Zhu, "Distributed coordinated brake control for longitudinal collision avoidance of multiple connected automated vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, pp. 745–755, 2022.
[18] M. Hu, X. Wang, Y. Bian, D. Cao, and H. Wang, "Disturbance observer-based cooperative control of vehicle platoons subject to mismatched disturbance," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 4, pp. 2748–2758, 2023.
[19] H. Pan, C. Zhang, and W. Sun, "Fault-tolerant multiplayer tracking control for autonomous vehicle via model-free adaptive dynamic programming," *IEEE Transactions on Reliability*, vol. 72, no. 4, pp. 1395–1406, 2023.
[20] H. Pan, Y. Hong, W. Sun, and Y. Jia, "Deep dual-resolution networks for real-time and accurate semantic segmentation of traffic scenes," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 3, pp. 3448–3460, 2023.
[21] M. Xie, D. Ding, B. Shen, and Y. Song, "Learning-based platooning control of automated vehicles under constrained bit rate," *IEEE Transactions on Intelligent Vehicles*, 10.1109/TIV.2023.3335866, 2023.
[22] B. Wang, Y. Luo, Z. Zhong, and K. Li, "Robust non-fragile fault tolerant control for ensuring the safety of the intended functionality of cooperative adaptive cruise control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 18746–18760, 2022.
[23] 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 Transactions on Intelligent Vehicles*, vol. 7, no. 4, pp. 815–837, 2022.
[24] 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 Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 11, pp. 7269–7278, 2020.
[25] N. Zhao, X. Zhao, M. Chen, G. Zong, and H. Zhang, "Resilient distributed event-triggered platooning control of connected vehicles under denial-of-service attacks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6191–6202, 2023.
[26] Y. Xu, G. Guo, and S. Yu, "An adaptive dynamic programming method for observer-based sliding mode control of connected vehicles subject to deception attacks," *International Journal of Robust and Nonlinear Control*, 10.1002/rnc.7155, 2024.
[27] M. Xie, D. Ding, X. Ge, Q.-L. Han, H. Dong, and Y. Song, "Distributed platooning control of automated vehicles subject to replay attacks based on proportional integral observers," *IEEE/CAA Journal of Automatica Sinica*, 10.1109/JAS.2022.105941, 2022.
[28] T. Yang, C. Murguia, D. Nešić, and C. Lv, "A robust cacc scheme against cyberattacks via multiple vehicle-to-vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11184–11195, 2023.
[29] A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Impact of jamming attacks on vehicular cooperative adaptive cruise control systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 12679–12693, 2020.
[30] S. Boddupalli, A. S. Rao, and S. Ray, "Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15655–15672, 2022.
[31] F. Yang, Z. Gu, L. Hua, and S. Yan, "A resource-aware control approach to vehicle platoons under false data injection attacks," *ISA Transactions*, vol. 131, pp. 367–376, 2022.
[32] Y. Xu and G. Guo, "Event triggered control of connected vehicles under multiple cyber attacks," *Information Sciences*, vol. 582, pp. 778–796, 2022.
[33] N. Zhao, X. Zhao, N. Xu, and L. Zhang, "Resilient event-triggered control of connected automated vehicles under cyber attacks," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 12, pp. 2300–2302, 2023.
[34] Y. Liu, L. Xu, G. Cai, G. Yin, and F. Yan, "Distributed robust platooning control for heterogeneous vehicle group under parametric uncertainty and hybrid attacks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 5, pp. 5677–5689, 2023.
[35] X. Jin, W. M. Haddad, Z. P. Jiang, A. Kanellopoulos, and K. G. Vamvoudakis, "An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons," *International Journal of Adaptive Control and Signal Processing*, vol. 33, no. 12, pp. 1788–1802, 2019.
[36] Q. Zhu and Z. Xu, *Cross-layer design for secure and resilient cyberphysical systems: A decision and game theoretic approach*, Berlin, Germany: Springer, 2020.
[37] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2019.
[38] Z. Feng, G. Wen, and G. Hu, "Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Transactions on Cybernetics*, vol. 47, no. 5, pp. 1273–1284, 2016.
[39] D. S. Bernstein, *Matrix mathematics: Theory, facts, and formulas*. Princeton university press, 2009.

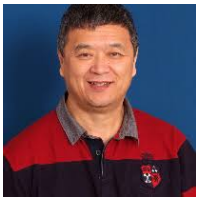
Ahmadreza Jenabzadeh (Member, IEEE) received the M.S. degree in electrical engineering from the Isfahan University of Technology, Isfahan, in 2013, and the Ph.D. degree in electrical engineering from the Shiraz University of Technology, Fars, Iran, in 2018.

He was a Post-Doctoral Fellow with Shanghai Jiao Tong University, Shanghai, China. He is currently a Research Associate Professor at the College of Mechatronics and Control Engineering, Shenzhen University. His research interests include multi-agent systems, machine learning, autonomous vehicles, and secure control.

Zhiguang Feng (Member, IEEE) received the B.S. degree in automation from Qufu Normal University, Rizhao, China, in 2006, the M.S. degree in Control Science and Engineering from Harbin Institute of Technology, Harbin, China, in 2009, and the Ph.D. Degree in the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong, in 2013.

He was a Research Associate in the Department of Mechanical Engineering, University of Hong Kong, Hong Kong, from Oct. 2013 to Feb. 2014. From Mar. 2014 to Apr. 2015, he was a visiting fellow at University of Western Sydney, Australia. He was appointed with Victoria University in Australia as Postdoctoral Research Fellow from Oct. 2015 to Mar. 2017. In 2017, he was promoted Professor at the College of Intelligent Systems Science and Engineering, Harbin Engineering University, Harbin, China. In 2019, he was a Vice-Chancellor's Postdoctoral Research Fellowship at University of Wollongong, NSW, Australia. His research interests include singular systems, time-delay systems, robust control, dissipative control, and reachable set estimation.

Tingwen Huang (Fellow, IEEE) received the B.S. degree in Mathematics from Southwest Normal University (now Southwest University), China, 1990, the M.S. degree in Applied Mathematics from Sichuan University, China, 1993, and the Ph.D. degree in Applied Mathematics from Texas A&M University, College Station, Texas, 2002. After graduating from Texas A&M University, he worked as a Visiting Assistant Professor there. Then he joined Texas A&M University at Qatar (TAMUQ) as an Assistant Professor in August 2003, then he was promoted to Professor in 2013. Dr. Huang's focus areas for research interests include computational intelligence, smart grid, dynamical systems, optimization, and



Quanmin Zhu received the M.Sc. degree in automatic control from Harbin Institute of Technology, Harbin, China, in 1983, and the Ph.D. degree in engineering from the Faculty of Engineering, University of Warwick, Coventry, U.K., in 1989.

He is currently a Professor in control systems with the Department of Engineering Design and Mathematics, University of the West of England, Bristol, U.K. He has authored or coauthored more than 250 papers on these topics, edited various books with Springer, Elsevier, and the other publishers, and provided consultancy to various industries. His main research interests include nonlinear system modelling, identification, and control.

Dr. Zhu is acting as an Editor of *International Journal of Modelling, Identification and Control*, an Editor of *International Journal of Computer Applications in Technology*, an Editor of Complexity, Hindawi, Member of various journal editorial boards, and Editor of Elsevier book series of Emerging Methodologies and applications in modelling, identification and control. He is the founder and president of a series annual international conference on modelling, identification and control.

Yukang Cui (Member, IEEE) received his B.Eng. Degree in Automation from the Harbin Institute of Technology in 2012 and his Ph.D. degree in Mechanical Engineering from the University of Hong Kong in early 2017. During 2017, he was a Research Associate in the Department of Mechanical Engineering at the University of Hong Kong. Since 2018, he has been with the College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. His current research interests include multi-robot cooperative sensing, swarm-robot path planning, multi-agent formation control, and nonlinear time-delay systems.