Letter

Fully Distributed Resilient Cooperative Control of Vehicular Platoon Systems Under DoS Attacks

Lei Ding, *Senior Member, IEEE*, Jie Li, Maojiao Ye, *Member, IEEE*, and Yuan Zhao

Dear Editor,

This letter is concerned with distributed resilient platoon control of multiple vehicles subject to denial-of-service (DoS) attacks. In order to accommodate the effects of DoS attacks, a fully resilient distributed control strategy is presented by designing an adaptive control gain, where any global information of communication topology is no longer required. Then, the conditions of time duration rates and frequency of DoS attacks on stability of vehicular platoons can be characterized. Finally, a numerical simulation example is given to validate the obtained results.

Coordinated platoon control, which aims to drive vehicles to follow each other at a specific predefined distance, is an important technical means in transportation systems to improve traffic safety, alleviate traffic congestion, and improve traffic pollution [1]. In order to achieve such coordinated platoon control, various distributed algorithms have been developed for vehicular platoon systems [2]–[6]. For example, a sampled-data-based cooperative scheme is proposed to achieve platoon control [2]. Based on multi-agent consensus protocols, a decomposition framework was introduced to model, analyze and design platoon systems [3]. An adaptive sliding mode control protocol was developed in [4], where the communication interactions among the vehicles were considered to be uncertain. An optimized control method was proposed for distributed cooperative vehicular platoon systems by considering actuator delays and non-ideal communication conditions [5]. A platooning control scheme with dynamic event-triggered scheduling is presented [6]. However, it should be pointed out that most of existing distributed vehicular platoon control schemes require some Laplacian eigenvalue information associated with the communication graph. In practical situations, it is difficult, costly or even impossible to calculate such global information for each vehicle. Thus, it is desirable for vehicle platoon systems to design a fully distributed control scheme without requiring any knowledge of global information. To address this issue, a fully distributed control strategy was developed for vehicular platoon systems based on an event-triggered communication scenario [7].

Note that communication topologies for distributed control systems are often vulnerable to cyber attacks controlled by malicious actions or accidents [8], [9]. DoS attacks, as one of the most common types of attacks, often cause the paralysis of communication connectivity by blocking the data transmission through communication channels, probably leading to undesirable consequences, such as performance degradation or even head-to-tail collisions [10]. To relax the negative effects caused by DoS attacks, a variety of secure control schemes have been investigated. For example, some network recovery mechanisms was introduced to recover vehicle-to-vehicle (V2V) communication networks damaged by DoS attacks [11]. Moreover, a linear matrix inequality (LMI)-based controller adjustment program was provided in [12]. Based on adaptive and sliding mode control, observer-based approaches were designed to accommodate DoS attacks [13]. Distributed secure control for connected vehicles under DoS attacks was considered [14], [15]. However, such distributed control algorithms [14], [15] are not fully distributed, as the global information of communication topologies is required. Therefore, it is interesting yet challenging to develop a fully distributed resilient control scheme for vehicle systems subject to DoS attacks, which motivates the current study.

Motivated by the above observation, this letter aims to develop fully distributed secure platoon control strategies for multiple vehicle systems subject to DoS attacks. The main contributions of this letter can be summarized as: 1) Different from [14], [15], a fully resilient distributed control scheme under DoS attacks is developed in the letter. By designing adaptive protocols for the control gains, the method does not require any global information. 2) A sufficient condition is derived to ensure the stability of vehicle platoon, where the effects of duration time and frequency of DoS attacks on stability of vehicle platoon can be revealed.

Problem formulation: A group of $N+1$ automated vehicles consisting of N follower vehicles and a leader vehicle labeled by 0 are connected through vehicular ad hoc networks. The longitudinal dynamics of vehicle i can be described as [2]

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad i = 1, \ldots, N \tag{1}$$

where $x_i(t) = [p_i(t), v_i(t), a_i(t)]^T$, $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau_a} \end{bmatrix}$ and $B = [0 \ \ 0 \ \ \frac{1}{\tau_a}]^T$ with $p_i(t)$, $v_i(t)$ and $a_i(t)$ being the position, velocity and acceleration of vehicle i, respectively, τ_a being the inertial time constant of vehicles, and $u_i(t)$ being the control input of vehicle i.

The objective of this letter is to design a fully distributed control law for follower vehicle i such that it can maintain a desired constant spacing $d_{i,i-1}$ with its predecessor $i-1$ while tracking the constant velocity v_0 of the virtual leading vehicle, i.e., $p_i(t) \to p_{i-1}(t) - d_{i,i-1}$, $v_i(t) \to v_0$, where $p_0(t)$ is the position of the leader.

In this letter, exchange information among vehicles can be modeled by a graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{1, 2, \ldots, N\}$ is the set of vehicles. An edge $(i, j)(i \neq j)$ means that vehicles i and j can obtain information from each other, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges. A graph is called an undirected graph if $(i, j) \in \mathcal{E}$ implies $(j, i) \in \mathcal{E}$ for any $i, j \in \mathcal{V}$. A sequence of edges (i, k), $(k, l), \ldots, (p, j)$ is called a path from node i to node j. If there is a path between any two nodes, the graph is connected. $\mathcal{A} = [a_{ij}]$ is the adjacency matrix, where $a_{ij} = 1$ if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$, otherwise. $a_{ii} = 0$ for all $i \in \mathcal{V}$. $N_i = \{j : (i, j) \in \mathcal{E}\}$ is the set of neighbors of node i. Define $D = \text{diag}\{d_1, \ldots, d_N\}$ with $d_i = \sum_{j \in N_i} a_{ij}$ being the degree of node i. The Laplacian matrix of the undirected graph G is defined as $L = D - \mathcal{A}$. In addition, $\bar{G}$ is the graph with N follower vehicles and one leader vehicle. Let $H = \text{diag}\{h_1, h_2, \ldots, h_N\}$, where $h_i = 1$ if follower vehicle i can have direct access to states of leader vehicle 0, and $h_i = 0$, otherwise. Correspondingly, the matrix $\hat{L} = L + H$ is defined for $\bar{G}$.

In this letter, it is assumed that DoS attacks are sometimes imposed on V2V networks, leading to the unavailability of data transmission among some of neighboring vehicles. In this case, the network

Corresponding author: Maojiao Ye.

Citation: L. Ding, J. Li, M. Ye, and Y. Zhao, "Fully distributed resilient cooperative control of vehicular platoon systems under DoS attacks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 5, pp. 937–940, May 2022.

L. Ding and J. Li are with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China (e-mail: dl522@163.com; lijie88njupt@163.com).

M. Ye is with the School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China (e-mail: ye0003ao@e.ntu.edu.sg).

Y. Zhao is with the College of Information Engineering, Dalian University, Dalian 116622, China (e-mail: zycandice@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2022.105578

communication topology of vehicular platoon is not globally reachable any longer, resulting in task failure due to lack of collaboration among some vehicles [15]. To mitigate the negative impact of DoS attacks, a control framework is proposed, where an effective network recovery mechanism can be used to repair connectivity of communication topologies [11]. Therefore, under the framework, the communication topology will be switching. Denote the set of all possible communication topologies by $C = C_m \bigcup C_p$, where $C_m = \{\bar{G}_1, \bar{G}_2, \ldots, \bar{G}_n\}$ is the set of all globally reachable communication topologies, and $C_p = \{\bar{G}_{n+1}, \bar{G}_{n+2}, \ldots, \bar{G}_q\}$ represents the set of all globally unreachable communication topologies due to the impacts of DoS attacks. $\bar{G}_{\sigma(t)}$ which represents time-varying communication topologies is used to characterize the effects of DoS attacks on communication topology, where $\sigma(t) : [0, \infty) \to C$ is a switching signal mapping from t to the set of possible graphs. For $r = \sigma(t) \in C = C_m \bigcup C_p$, $\mathcal{A}_r = [a_{ij}^r]$ is the the adjacent matrix of $\bar{G}_{\sigma(t)}$, and H_r is the pinning matrix with its diagonal element h_i^r.

Remark 1: Different from [14], the effects of DoS attacks can be characterized by a set of switching topologies in this letter. In other words, due to the occurrence of DoS attacks, some data exchange among neighboring vehicles may fail, which is equivalent to the break of their communication links.

Assumption 1: For $\bar{G}_{\sigma(t)}$, $\sigma(t) \in C_m$, the leader vehicle is globally reachable to all follower vehicles.

To quantify the characteristics of switching communication topologies caused by DoS attacks and network recovery mechanisms, $T_p(T_1, T_2)$ and $N_p(T_1, T_2)$ are denoted as the total time and the number of globally unreachable communication topologies during the time period $[T_1, T_2)$. Then, the following definitions [15] are useful to prove the stability of vehicular platoons later.

Definition 1: $T_p(T_1, T_2)/(T_2 - T_1)$ is denoted as the time ratio of globally unreachable communication topologies during the time period $[T_1, T_2)$.

Definition 2: $F_p(T_1, T_2) = N_p(T_1, T_2)/(T_2 - T_1)$ is denoted as the frequency of globally unreachable communication topology during time period $[T_1, T_2)$.

Let $\eta_i^r(t) = \sum_{j=1}^N a_{ij}^r(x_j(t) - x_i(t) - D_{ij}) + h_i^r(x_0(t) - x_i(t) - D_{i0})$, where $D_{i,j} = [d_{i,j}, 0, 0]^T$ with $d_{i,j} = \sum_{l=j}^{i-1} d_{l,l+1}$ being the desirable distance between vehicles i and j. To achieve fully distributed platoon control, the following adaptive control protocol is presented:

$$u_i(t) = -K\Big[\sum_{j=1}^N a_{ij}^r(c_i^r(t)\eta_i^r(t) - c_j^r(t)\eta_j^r(t)) + [h_i^r c_i^r(t)\eta_i^r(t)\Big] \tag{2}$$

$$\dot{c}_i^r(t) = e^{\gamma t}\eta_i^r(t)^T \Gamma \eta_i^r(t), \quad r = \sigma(t) \in C \tag{3}$$

where $c_i^r(t)$ is the adaptive gain of vehicle i, K is the gain matrix to be designed later, the matrix Γ and constant γ are shown later. Denote the error between follower i and leader 0 by $z_i(t) = x_0(t) - x_i(t) - D_{i,0}$, where $x_0(t) = [p_0(t), v_0(t), 0]^T$. Then, one has $\eta_i^r(t) = \sum_{j=1}^N a_{ij}^r(z_i - z_j) + h_i^r z_i(t)$. Let $z(t) = [z_1^T(t), z_2^T(t), \ldots, z_N^T(t)]^T$, and $\hat{C}_r = \text{diag}\{c_1^r, c_2^r, \ldots, c_N^r\}$. Together with (1), (2) and (3), it is easy to obtain that

$$\dot{z}(t) = (I_N \otimes A - \hat{L}_r \hat{C}_r \hat{L}_r \otimes BK)z(t) \tag{4}$$

$$\dot{\hat{C}}_r = e^{\gamma t} z^T(t)(\hat{L}_r \hat{L}_r \otimes \Gamma)z(t) \tag{5}$$

where $\hat{L}_r = L_r + H_r$. Therefore, the platoon control issue considered in this letter can be transformed to design control gain matrices K and Γ for the control protocol (2) such that $\lim_{t\to\infty} z_i(t) = 0$, $i = 1, \ldots, N$.

Main results: In this section, a sufficient condition ensuring stability of vehicular platoons is derived, where the constraints of DoS attacks are characterized.

For a controllable matrix pair (A, B), there exist symmetric positive definite matrices $P > 0$ and $Q > 0$, and constants $\beta > 0$, $\alpha > 0$ such that following inequalities hold:

$$AP + PA^T - BB^T + \beta P \le 0 \tag{6}$$

$$AQ + QA^T + BB^T - \alpha Q \le 0. \tag{7}$$

Next, we state the following main result.

Theorem 1: Under Assumption 1 and $\gamma \ge \beta$, platoon control of vehicular system (1) under DoS attacks can be achieved by fully distributed control law (2), where the control gain matrices are designed by $K = B^T P^{-1}$ and $\Gamma = P^{-1} B B^T P^{-1}$, $r \in C_m$ or $K = B^T Q^{-1}$ and $\Gamma = Q^{-1} B B^T Q^{-1}$, $r \in C_p$ with P and Q being the solutions of (6) and (7), provided that the following conditions are satisfied:

$$\frac{T_p(t_0, t)}{t - t_0} \le \frac{\beta - \zeta^*}{\beta + \alpha}, \quad F_p(t_0, t) \le \frac{\zeta^* - \zeta}{2\ln \varrho} \tag{8}$$

where $\zeta \in (0, \zeta^*)$ with $\zeta^* \in (0, \beta)$, and $\varrho = \max\{\varrho_1, \varrho_2\}$ with $\varrho_1 = \lambda_{\max}(P)/\lambda_{\min}(Q)$ and $\varrho_2 = \lambda_{\max}(Q)/\lambda_{\min}(P)$, $\lambda_{\min}(\cdot)$ and $\lambda_{\max}(\cdot)$ represent the minimum and maximum eigenvalues of a matrix, respectively.

Proof: Choose the Lyapunov function as

$$V(t) = \begin{cases} z^T(t)(I_N \otimes P^{-1})z(t) + \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2, & r \in C_m \\ z^T(t)(I_N \otimes Q^{-1})z(t) + \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2, & r \in C_p \end{cases}$$

where $\bar{c}_r$ is a positive constant. We will discuss two cases as follows.

Case 1: For $r \in C_m$, taking derivative of $V(t)$ along (4) yields

$$\dot{V}(t) = z^T(t)[I_N \otimes (A^T P^{-1} + P^{-1}A) - 2\bar{c}_r \hat{L}_r^2 \otimes P^{-1} B B^T P^{-1}]z(t) - \gamma \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2. \tag{9}$$

Set the constant $\bar{c}_r > 1/2\left[\lambda_{\min}(\hat{L}_r)\right]^2$ and the gain constant $\gamma \ge \beta$. If (6) holds, then

$$\dot{V}(t) \le -\beta z^T(t)(I_N \otimes P^{-1})z(t) - \beta \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2 \le -\beta V(t)$$

which implies that for $r \in C_m$,

$$V(t) \le e^{-\beta(t - t_k)} V(t_k), \ \ t \in [t_k, t_{k+1}). \tag{10}$$

Case 2: For $r \in C_p$, similar to Case 1, one can get

$$\begin{aligned} \dot{V}(t) &= z^T(t)\Big[I_N \otimes (A^T Q^{-1} + Q^{-1}A) - 2\bar{c}_r \hat{L}_r^2 \otimes Q^{-1} B B^T Q^{-1}\Big]z(t) - \gamma \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2 \\ &\le \alpha z^T(t)(I_N \otimes Q^{-1})z(t) + \alpha \sum_{i=1}^N e^{-\gamma t}(c_i^r - \bar{c}_r)^2 \\ &\le \alpha V(t) \end{aligned}$$

where (7) is used. Then, it is easy to obtain that for $r \in C_p$

$$V(t) \le e^{\alpha(t - t_k)} V(t_k), \ \ t \in [t_k, t_{k+1}). \tag{11}$$

Denote the total time duration of globally reachable communication topologies during time period $[t_k, t)$ by $\mathrm{T}_m(t_k, t) = t - t_k - T_p(t_k, t)$. Combining (10) and (11), for $r \in C_m \bigcup C_p$, one has

$$V(t) \le e^{\alpha T_p(t_k, t) - \beta T_m(t_k, t)} V(t_k), \ \ t \in [t_k, t_{k+1}). \tag{12}$$

For any switching time $t = t_k$, it is clear that $x_i(t_k) = x_i(t_k^-)$, which implies $V(t_k) \le \varrho V(t_k^-)$. Then

$$\begin{aligned} V(t) &\le \varrho e^{\alpha T_p(t_k,t)-\beta T_m(t_k,t)} V(t_k^-) \\ &\le \varrho e^{\alpha T_p(t_{k-1},t)-\beta T_m(t_{k-1},t)} V(t_{k-1}) \\ &\le \varrho^2 e^{\alpha T_p(t_{k-1},t)-\beta T_m(t_{k-1},t)} V(t_{k-1}^-) \\ &\le \cdots \le \varrho^{N_a(t_0,t)} e^{\alpha T_p(t_0,t)-\beta T_m(t_0,t)} V(t_0) \end{aligned} \tag{13}$$

in which $N_a(t_0,t)$ is the amount of switching during period $[t_0,t)$. If (8) holds, then

$$\alpha T_p(t_0,t)-\beta T_m(t_0,t) \le -\zeta^*(t-t_0). \tag{14}$$

Similarly, we can derive along (8) that

$$\varrho^{N_a(t_0,t)} = e^{N_a(t_0,t)\ln\varrho} \le e^{2N_p(t_0,t)\ln\varrho} \le e^{(\zeta^*-\zeta)(t-t_0)}. \tag{15}$$

Therefore, one can obtain that $V(t) \le e^{-\zeta(t-t_0)} V(t_0)$, which ensures that $z_i(t) \to 0$ exponentially as $t \to +\infty$. ■

Remark 2: Note that for the sake of analysis simplicity, the vehicle's dynamics (1) are disturbance-free. It should be pointed out that the proposed method can be extended to accommodate vehicle systems under external disturbances. For instance, in the presence of disturbances with limited energy capacity, an H_∞ platooning control method can be developed for vehicle systems, see, e.g., [15].

Remark 3: String stability can be usually regarded as a performance requirement on platoon control [2], [3], which aims to decrease the propagation of spacing errors along platoon, especially in the presence of external disturbances. In practice, this requirement may be relaxed when general communication topologies (rather than one-line communication topologies) are employed. To simplify control design and analysis, the string stability of vehicle systems is not taken into account in this letter.

Remark 4: Note that the control design [14], [15] depends closely on the global information of communication topologies (e.g., their eigenvalues of Laplacian matrices). In contrast, the proposed control scheme (2) and (3) is fully distributed, which is more desirable for practical implementation.

Remark 5: Theorem 1 reveals the relationship among control parameters, attack duration and attack frequency. In fact, the parameter selection is problem-specific according to practical requirements. For example, parameters α and β are associated with the divergence and convergence rates of error system (4) under disconnected and connected graphs, respectively. As a result, an optimal selection of parameters is to maximize β while minimizing α, by which the control gain matrices can be obtained as well.

Numerical example: A platoon of vehicles with 1 leader vehicle and 5 follower vehicles are taken into account. The desired distances between vehicles are set as $d_{i,i-1} = 12$ m for each follower vehicle. Let $\tau_a = 0.58$, $p_0(0) = 0$ m, and $v_0(0) = 55$ m/s. The expected velocity of leader is

$$v_0(t) = \begin{cases} 55, & 0 \le t < 25 \\ 55+2t, & 25 \le t < 35 \\ 75, & 35 \le t < 45 \\ 75-t, & 45 \le t < 55 \\ 65, & 55 \le t < 70. \end{cases} \tag{16}$$

Let $x_1(0) = [-7\ \ 55\ \ 0]^T$, $x_2(0) = [-18\ \ 55\ \ 0]^T$, $x_3(0) = [-33\ \ 55\ \ 0]^T$, $x_4(0) = [-45\ \ 55\ \ 0]^T$, $x_5(0) = [-64\ \ 55\ \ 0]^T$, and Fig. 1 be the communication graphs for the vehicles.

The simulation time period is [0 s, 70 s], during which switching mapping $\sigma(t)$ of the communication topologies is shown in Fig. 2. The duration of globally unreachable communication topology is 5 s in total and their total number of occurrences is 4. Then, we can obtain $K_1 = [2.1124, 5.6705, 5.1231]$, $r \in C_m$, $K_2 = [0.0940, -0.5396, 2.2431]$, $r \in C_p$ and

$$\Gamma_1 = \begin{bmatrix} 4.4621 & 11.9781 & 10.8219 \\ 11.9781 & 32.1540 & 29.0503 \\ 10.8219 & 29.0503 & 26.2461 \end{bmatrix}, \quad r \in C_m$$

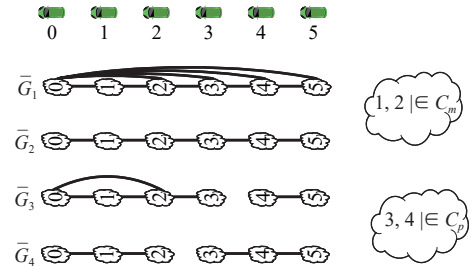

Fig. 1. Switching communication topologies caused by DoS attacks.

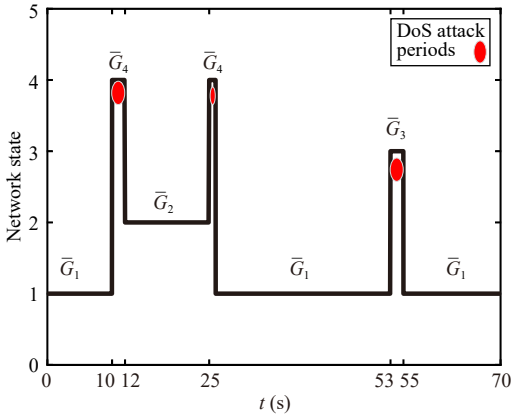

Fig. 2. Switching mapping $\sigma(t)$ of communication topology.

$$\Gamma_2 = \begin{bmatrix} 0.0088 & -0.0507 & 0.2108 \\ -0.0507 & 0.2911 & -1.2103 \\ 0.2108 & -1.2103 & 5.0317 \end{bmatrix}, \quad r \in C_p.$$

Set $\beta = 0.46$, $\alpha = 1.5$, $\varrho = 15.0677$ and $\gamma = 3.48$. Choosing $\zeta^* = 0.311$ and $\zeta = 0.01$, it is easy to obtain $T_p(0,70) = 5 \le 5.3214$ and $N_p(0,70) = 3 \le 3.8838$, which ensure that the conditions (8) are satisfied.

With the provided parameters, the followers' position trajectories, velocity and spacing error trajectories are depicted in Figs. 3−5, respectively. It is shown in Fig. 3 that each follower vehicle can achieve the leader tracking during the whole simulation. From Figs. 4 and 5, it is demonstrated that all follower vehicles is capable of tracking the leader's velocity while maintaining a desired distance from its front and behind vehicles, although their velocities and distance errors suffer from a large deviation under cyber attacks. Fig. 6 shows vehicles' accelerations, from which it is clear that they are convergent to zero. Fig. 7 depicts the adaptive gain values of six followers. It can be seen that the adaptive gain values converge to some finite values. Hence, the proposed control design has been

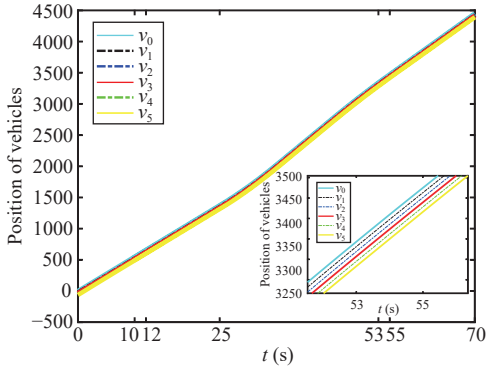

Fig. 3. Vehicles' positions under DoS attacks.

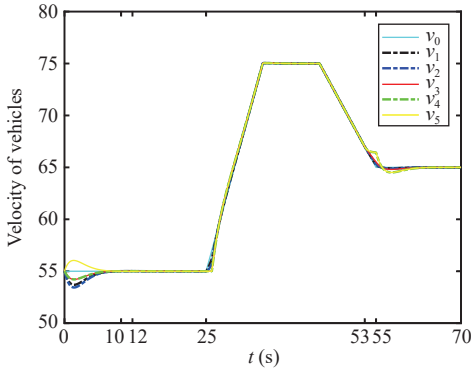

Fig. 4. Vehicles' velocities under DoS attacks.

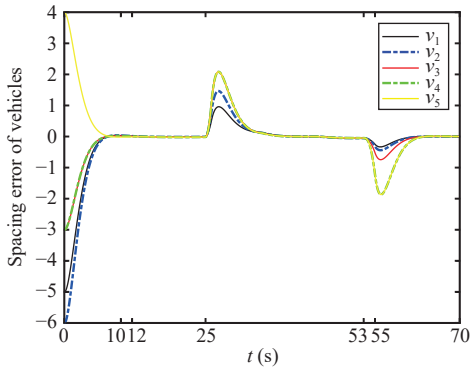

Fig. 5. Vehicles' spacing errors under DoS attacks.

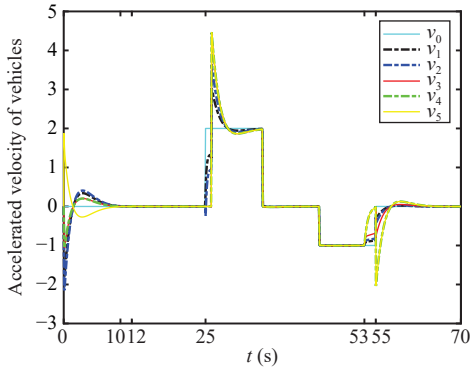

Fig. 6. Vehicles' accelerations under DoS attacks.

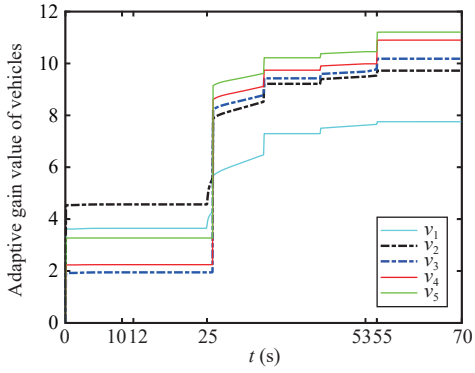

Fig. 7. Adaptive gains $c_i^r(t)$ of vehicles under DoS attacks.

numerically verified.

Conclusions: In this letter, vehicular platoon control under DoS attacks has been investigated. A fully distributed control scheme has been presented for ensuring the stability of vehicular platoon systems. By adaptively adjusting the parameter of the control scheme, global information does not need to be calculated. Then, a sufficient condition has been derived to achieve the controller gain design. In the future, co-existence of multiple cyber attacks and communication channels with limited capacities will be considered.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (NSFC) (62073171, 62173181), the Natural Science Foundation of Jiangsu Province (BK20200744, BK20180455), Jiangsu Specially-Appointed Professor (RK043 STP19001), 1311 Talent Plan of Nanjing University of Posts and Telecommunications, the Fundamental Research Funds for the Central Universities (30920032203), the Natural Science Foundation of Tianjin (20JCQNJC00390), and Graduate Scientific Research Innovation Project of Tianjin (2021YJSO2S31).

References

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

[2] G. Guo and W. Yue, "Sampled-data cooperative adaptive cruise control of vehicles with sensor failures," *IEEE Trans. Intel. Transp. Syst.*, vol. 15, no. 6, pp. 2404–2418, 2014.

[3] S. E. Li, Y. Zheng, K. Li, Y. Wu, J. K. Hedrick, F. Gao, and H. Zhang, "Dynamical modeling and distributed control of connected and automated vehicles: Challenges and opportunities," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 3, pp. 46–58, 2017.

[4] F. Gao, X. Hu, S. E. Li, K. Li, and Q. Sun, "Distributed adaptive sliding mode control of vehicular platoon with uncertain interaction topology," *IEEE Trans. Ind. Electron.*, vol. 65, no. 8, pp. 6352–6361, 2018.

[5] F. Ma, J. Wang, S. Zhu, S. Y. Gelbal, Y. Yang, B. Aksun-Guvenc, and L. Guvenc, "Distributed control of cooperative vehicular platoon with nonideal communication condition," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8207–8220, 2020.

[6] X. Ge, S. Xiao, Q.-L. Han, X.-M. Zhang, and D. Ding, "Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks," *IEEE/CAA J. Autom. Sinica*, vol. 9, no. 1, pp. 31–46, 2022.

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

[8] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, pp. 46–65, 2015.

[9] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomput.*, vol. 275, pp. 1674–1683, 2018.

[10] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, 2017.

[11] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, 2015.

[12] R. Merco, F. Ferrante, and Pisu, "A hybrid controller for DoS-resilient string-stable vehicle platoons," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1697–1707, 2020.

[13] Z. A. Biron, S. Dey, and 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, 2018.

[14] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Trans. Cybern.*, 2021. DOI: 10.1109/TCYB.2021.3074318.

[15] Y. Zhao, Z. Liu, and W. S. Wong, "Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances," *IEEE Trans. Intell. Transp. Syst.*, 2021. DOI: 10.1109/TITS.2021.3097356.