Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Resilient Distributed Event-Triggered Control of Vehicle Platooning Under DoS Attacks ⋆

Shunyuan Xiao [*,**], **Xiaohua Ge** [*], **Qing-Long Han** [†,*], **Zhenwei Cao** [*], **Yijun Zhang** [**], **Honghai Wang** [***]

[*] *School of Software and Electrical Engineering, Swinburne University of Technology, Melbourne, VIC 3122, Australia*
[**] *School of Automation, Nanjing University of Science and Technology, Nanjing, 210094, P. R. China*
[***] *College of Information Science and Engineering, State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, 110819, P. R. China*
[†] *The corresponding author: qhan@swin.edu.au*

Abstract: This paper deals with the resilient distributed control of a platoon of automated vehicles under DoS attacks. First, an event-triggered transmission mechanism resilient to energy-limited DoS attacks is proposed to save the possible bandwidth of vehicle-to-vehicle communication channels. A consensus-based distributed control strategy, which is implemented on each vehicle, is developed to account for the information interaction of leading and following vehicles under the proposed resilient event-triggered data transmission mechanism. Second, an attack-tolerant performance index with certain resilience level is put forward in such a way to achieve resilience evaluation of the vehicular platoon system. Third, sufficient conditions are derived for ensuring the consensus of the resulting vehicular platoon system while preserving the prescribed resilience performance requirement. Furthermore, a co-design criterion for determining the distributed platoon controller and triggering condition is presented. Finally, simulation under a predecessor-leader following topology is presented for validation of the obtained results.

Keywords: Resilient event-triggered mechanism, vehicle platooning, DoS attacks, predecessor-leader following topology

1. INTRODUCTION

Over the past decades, the rapidly developing freight transportation has brought heavy burden on traffic infrastructure and caused much congestion on highway network. As one of prominent technologies of intelligent transportation systems, vehicular platoon control aims at maintaining autonomous vehicles as a platoon with specified spacing and the same driving speed, which potentially leads to more reliability and safety, improvement on traffic throughput, and reduction on fuel consumption. Due to its promising application in modern society, several results on vehicular platooning have been reported, e.g., stability and string stability (Dunbar and Caveney, 2012; Besselink and Johansson, 2017), scalability (Knorn et al., 2015; Zheng et al., 2016), attack detection (Lu et al., 2019; Mousavinejad et al., 2019), and control synthesis (Ploeg et al., 2014; Guo et al., 2016; Wen and Guo, 2019).

In a vehicular platoon system, each vehicle is capable of sensing and sampling its information including position, direction, velocity and acceleration, and transmitting such information to its potential neighboring vehicles. In general, there are six commonly used communication topologies for vehicle interaction: predecessor following communication, predecessor-leader following communication, bidirectional communication, bidirectional-leader communication, two-predecessors following communication, and two-predecessor-leader following communication (Zheng et al., 2016). These communication topologies determine the information flows and exchanges, based on which the platoon controllers deployed on the vehicles can be implemented in a distributed manner.

Due to a large quantity of data exchange in vehicular ad hoc networks (VANETs), conventional periodic data transmission may cause excessive and unnecessary burden to the communication channel (Guo and Wen, 2016), especially when the fluctuation of sampled vehicle information is very small. In practical platoon control, the VANET-based communication bandwidth is often restricted, and the embedded modules on vehicles, such as microprocessors and onboard signal transmitters and receivers, are sometimes energy-constrained. Therefore, an alternative resource-efficient mechanism, i.e., event-triggered intermittent transmission, has been extensively adopted in vehicle platoon control to “filter out” some data packets of less importance (Ding et al., 2018; Ge et al., 2020; Wei et al., 2017; Wen et al., 2018; Zhang et al., 2020). For example, a dynamic event-triggered

⋆ This work was supported in part by the Australian Research Council Discovery Project under Grant DP190101557, and National Natural Science Foundation of China Under Grant 61973166 and 61703086.

scheme with adjustable threshold was designed in Wen et al. (2018) to save the communication bandwidth of VANETs. With a suitable event-triggered mechanism deployed on vehicles, the updates of inter-vehicle information exchanges in VANETs can be effectively reduced, which has great potential to save constrained communication and computation resources.

The communication network allows information sharing among nodes (vehicles) and enables more nodes (vehicles) to access the network medium, meanwhile, causes high risks of being attacked by malicious adversaries (Ge et al., 2019). Naturally, how to preserve desired safety and security requirements in an automated vehicle platoon has drawn increasing attention over the past decade (Amoozadeh et al., 2015; Hu et al., 2017; Biron et al., 2018; Cui et al., 2019; Sheehan et al., 2019). To mention a few, in Hu et al. (2017), a trust-based suggestion mechanism was proposed for distinguishing the misbehaved vehicles through an established reputation system. Sliding mode observers were constructed in Biron et al. (2018) to not only detect the occurrence of DoS attacks but also evaluate the impact of the attacks on the platoon control performance. Note that DoS attacks represent a typical class of data availability attacks that prevent the data transmission among interacting nodes (agents or system components) over some communication network (Guan and Ge, 2017, 2018; Zhang et al., 2019), and thus severely affect the cooperation among automated vehicles for achieving distributed platoon control. Although several results on modeling and analyzing DoS attacks have been available in the literature of networked control systems and cyber-physical systems, there are few studies that explore resiliency of automated vehicle platoon systems against DoS attacks through distributed event-triggered control strategy, which motivates this study.

In this paper, the problem of resilient event-triggered platoon control under energy-limited DoS attacks will be investigated. The main contribution lies in that a new distributed event-triggered strategy resilient to DoS is delicately developed for platooning of a team of controlled vehicles over some shared communication medium. Specifically, the transmitted data packets among the vehicles, organized by the developed event-triggered mechanism, will be intercepted by adversaries through launching DoS attacks into VANETs. A resilient event-triggered scheme will be proposed for attack-tolerant platoon control by intentionally discarding a few data packets to attenuate the adverse effects of DoS attacks. The stability of the platoon error system will be analyzed through Lyapunov functional method and a co-design approach to distributed platoon control and triggering condition will be derived.

The rest of the paper is arranged as follows. In Section 2, the main problem is formulated. In Section 3, main results of prescribed resilience performance analysis and co-design of platoon controller and event-triggered condition are derived. Section 4 presents a simulation study for verification. Section 5 concludes the paper.

2. PROBLEM FORMULATION

2.1 The Model of Vehicle Dynamics

With the parameter notations of a vehicle given in Table 1, the nonlinear dynamics of a vehicle, indexed by i, $i = 0, 1, ..., N$, are described as follows (Zheng et al., 2016)

Table 1. Notations of Vehicle Parameters

Notation	Description
m_i	Vehicle mass
g	Gravity acceleration
ς	Inertial delay
T_i	Driving/breaking torque
T_{di}	Desired driving/breaking torque
D_i	Drag coefficient
f	Rolling resistance coefficient
R_i	Tire radius
ϖ_i	Mechanical efficiency

$$\begin{cases} \dot{q}_i(t) = v_i(t) \\ \dot{v}_i(t) = \dfrac{\varpi_i T_i(t)}{m_i R_i} - \dfrac{D_i v_i^2(t)}{m_i} - gf \\ \varsigma \dot{T}_i(t) + T_i(t) = T_{di}(t) \end{cases} \tag{1}$$

where $q_i(t)$ denotes the vehicle i's position and $v_i(t)$ is vehicle i's velocity. For linearization purpose, the desired driving/braking torque is constructed as

$$T_{di}(t) = \frac{R_i}{\varpi_i}\Big(D_i v_i(t)(2\varsigma a_i(t) + v_i(t)) + m_i g f + m_i u_i(t)\Big)$$

where $a_i(t)$ and $u_i(t)$ are the acceleration and the designed control input of vehicle i, respectively. Substituting the torque into (1), the vehicle dynamic can be written as

$$\begin{cases} \dot{q}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = -\dfrac{1}{\varsigma} a_i(t) + \dfrac{1}{\varsigma} u_i(t). \end{cases} \tag{2}$$

2.2 Inter-Vehicle Communication

In this paper, we consider that $N + 1$ automated and communicated vehicles, consisting of one leading vehicle, labeled as 0, and N following vehicles, indexed $i \in \mathcal{V} = \{1, 2, ..., N\}$, move along a lane one after another and form a straight line. Each vehicle is embedded with inertial sensors and GPS units to monitor the information of its motion. Transmitter and receiver antenna units are also equipped for VANET-based vehicle-to-vehicle communication. The leading vehicle gives the referenced moving information under prescribed spacing policy. The communication topology among N following vehicles is described by a directed and connected graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ denoting the set of information links among the following vehicles. Let $\mathcal{A} = [a_{ij}]_{N\times N}$ be the corresponding adjacency matrix with $a_{ij} = 1 \Leftrightarrow (i, j) \in \mathcal{E}$, $i, j \in \mathcal{V}$, which implies that vehicle i is able to receive information from vehicle j. Note that $a_{ii} = 0$ for $\forall i \in \mathcal{V}$. The neighboring set of vehicle i is indicated as $\mathbf{N}_i = \{j \in \mathcal{V} | a_{ij} = 1\}$. Then the corresponding Laplacian matrix $\mathcal{G}$ is denoted as $\mathcal{L} = [l_{ij}]_{N\times N}$ where $l_{ij} = -a_{ij}$ when $i \neq j$ and $l_{ij} = \sum_{s\in \mathbb{N}_i} a_{is}$ when $i = j$, $\forall i, j \in \mathcal{V}$.

To further describe the information flow from leading vehicle to following vehicles, an augmented and directed graph is defined as $\mathcal{G}_* = \{\mathcal{V}_*, \mathcal{E}_*\}$ where $\mathcal{V}_* = \{0\} \bigcup \mathcal{V}$ and $\mathcal{E}_* \subseteq \mathcal{V}_* \times \mathcal{V}_*$. Obviously, one has $\mathcal{E} \subseteq \mathcal{E}_*$. A pinning matrix $\mathcal{P} = \mathrm{diag}\{p_1, p_2, ..., p_N\}$ is defined to indicate the information flow from vehicle 0 to vehicle $i \in \mathcal{V}$, where $p_i = 1$ indicates following vehicle i is able to receive the leading vehicle 0's information, i.e., $(i, 0) \in \mathcal{E}_*$, otherwise, no information link exists from vehicle 0 to vehicle i. The access set of vehicle i to vehicle 0 can be defined as $\mathbf{P}_i = \{0\}$ when $p_i = 1$ and $\mathbf{P}_i = \varnothing$ when $p_i = 0$. Then it is easy to have that all the vehicles feeding information to vehicle i belong to the set $\mathbf{I}_i = \mathbf{N}_i \cup \mathbf{P}_i$.

Assumption 1. There exists at least one spanning tree rooting from leading vehicle 0 in graph $\mathcal{G}_*$.

2.3 Consensus-Based Distributed Platoon Control Law

The consensus-based distributed control law on vehicle i is constructed as follows

$$u_i(t) = \sum_{j\in\mathbf{I}_i}\Big(k_q(q_i(t)-q_j(t)-d_{i,j}) + k_v(v_i(t)-v_j(t)) + k_a(a_i(t)-a_j(t))\Big) \quad (3)$$

where $d_{i,j} = q_i - q_j$ is the desired distance between vehicle i and j; k_q, k_v and k_a are controller gains to be determined. Note that $u_0(t) = 0$. We consider hereafter the constant vehicle spacing policy, i.e., $d_{i-1,i} = d_0$, with $d_0 > 0$.

To facilitate the sequent analysis, we define

$$\begin{cases} \delta_i^q(t) = q_i(t) - q_0(t) - d_{i,0} \\ \delta_i^v(t) = v_i(t) - v_0(t) \\ \delta_i^a(t) = a_i(t) - a_0(t). \end{cases} \quad (4)$$

Further setting $x_i(t) = [\delta_i^q(t),\ \delta_i^v(t),\ \delta_i^a(t)]^{\mathrm{T}}$, we have

$$u_i(t) = K\sum_{j\in\mathbf{I}_i}(x_i(t) - x_j(t)) \quad (5)$$

where $K = [k_q,\ k_v,\ k_a]$ is the gain matrix of the controller.

2.4 Resilient Event-Triggered Transmission Mechanism

In vehicle platoon, vehicle i is capable of transmitting signal $x_i(t)$, which includes the error information of position, velocity and acceleration, to its neighbors. Due to the wireless vehicle-to-vehicle communication nature, two problems associated with the platoon control are worthy of special attention: *limited network bandwidth* and *malicious DoS attacks*. To save the limited bandwidth as well as alleviate the adverse effects of DoS attacks, a resilient event-triggered mechanism similar to Sun et al. (2019) is adopted in the vehicle platoon process. The sensor deployed on each vehicle samples the vehicle information periodically with the sampling period $h > 0$. The sampling instants of all sensors are synchronous and take values in set $\{0, h, 2h, ..., kh\}$, $k \in \mathbb{N}$. The event-triggered transmission instants of vehicle i belong to set $\{0, t_1^i h, t_2^i h, ..., t_k^i h\}$, $k \in \mathbb{N}$. However, a few data packets transmitted by the event generator may be intercepted by attackers and thus lost. As a result, given a successfully triggered instant $t_k^i h$, the next update triggered time $t_{k+1}^i h$ may be prolonged to $t_{k+1}^{i,dos} h$. Denote by ϑh the current time instant and define $e_i(\vartheta h) = x_i(t_k^i h) - x_i(\vartheta h)$, $e_i^{dos}(\vartheta h) = x_i(\vartheta h) - x_i(t_{k+1}^i h)$. Then a resilient triggering condition is designed as

$$e_i^{\mathrm{T}}(\vartheta h)\Phi e_i(\vartheta h) > \sigma x_i^{\mathrm{T}}(t_k h)\Phi x_i(t_k h) + \xi(\vartheta h)\Gamma_i^{dos}(\vartheta h) \quad (6)$$

where $\sigma > 0$ is a prescribed *threshold* constant; $\Phi > 0$ is a *weighting matrix* to be determined; $\xi(\vartheta h)$ is an *indicating function* of the occurrence of DoS attacks, i.e., $\xi(\vartheta h) = 1$ indicates the occurrence of DoS attacks, otherwise, the transmission is secure; and $\Gamma_i^{dos}(\vartheta h) = e_i^{dos\,\mathrm{T}}(\vartheta h)\Phi e_i^{dos}(\vartheta h)$. Due to the finite energy budget of real-world adversaries, the duration of DoS attacks could be restricted and it is thus natural to assume a bound $\bar{\Gamma} > 0$ such that

$$\Gamma_i^{dos}(\vartheta h) \le \bar{\Gamma}, \forall i \in \mathcal{V}. \quad (7)$$

Once condition (6) is satisfied, the resilient event-triggered mechanism will be activated for scheduling each vehicle's sampled data and the next triggering instant of vehicle i can be recursively determined by

$$t_{k+1}^i h = t_k^i h + \min_{\vartheta}\{\vartheta h | e_i^{\mathrm{T}}(\vartheta h)\Phi e_i(\vartheta h) > \Lambda_i(\vartheta h)\} \quad (8)$$

where $\Lambda_i(\vartheta h) = \sigma x_i^{\mathrm{T}}(t_k h)\Phi x_i(t_k h) + \xi(\vartheta h)\Gamma_i^{dos}(\vartheta h)$.

Under the event-triggered mechanism (8), the distributed control law (5) for vehicle i becomes

$$u_i(t) = K\sum_{j\in\mathbf{I}_i}(x_i(t_k^i h) - x_j(t_{\tilde{k}_j}^j h)),\ t \in [t_k^i h, t_{k+1}^i h) \quad (9)$$

where $x_i(t_k^i h)$ is the latest transmitted data of vehicle i, $x_j(t_{\tilde{k}_j}^j h)$ denotes the latest transmitted data of vehicle j which is wirelessly connected to vehicle i, and $\tilde{k}_j \triangleq \mathrm{argmin}_{\tilde{k}}\{\vartheta - t_{\tilde{k}}^j | \vartheta > t_{\tilde{k}}^j, \tilde{k} \in \mathbb{N}\}$. Divide the triggering interval into $[t_k^i h, t_{k+1}^i h) = \sum_{\vartheta=t_k^i}^{t_{k+1}^i - 1}[\vartheta h, (\vartheta+1)h)$. Then define $\tau(t) = t - \vartheta h$, $t \in [\vartheta h, (\vartheta+1)h)$, we have

$$\begin{aligned} u_i(t) =& K\sum_{j\in\mathbf{I}_i}(x_i(t-\tau(t)) - x_j(t-\tau(t)) + e_i(t-\tau(t)) \\ & - e_j(t-\tau(t))),\ t \in [\vartheta h, (\vartheta+1)h) \end{aligned} \quad (10)$$

Defining $x(t) = \mathrm{col}_N^i\{x_i(t)\}$, we can further rewrite (2) with (10) in a compact form

$$\begin{cases} \dot{x}(t) = (I_N \otimes A)x(t) + (\mathcal{H} \otimes BK)x(t-\tau(t)) \\ \qquad + (\mathcal{H} \otimes BK)e(t-\tau(t)) \\ x(s) = \phi(s),\ s \in [-h, 0] \end{cases} \quad (11)$$

where $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\varsigma} \end{bmatrix}$, $B = \begin{bmatrix} 0 \\ 0 \\ -\frac{1}{\varsigma} \end{bmatrix}$, $\mathcal{H} = \mathcal{L} + \mathcal{P}$, and $\phi(s)$, $s \in [-h, 0]$ is the initial condition.

2.5 The Problem to Be Addressed

The problem to be addressed is thus to design a suitable consensus-based distributed platoon controller in the form of (3) under the resilient event-triggered mechanism (8) for a vehicular platoon with each vehicle's model in the form of (2) such that ***1)*** *in the absence of attacks*, the accelerations as well as velocities of following vehicles reach the same values as those of leading vehicle 0, while the distance between vehicles i and j, $\forall i, j \in \mathcal{V}_*$ is kept as a desired distance $d_{i,j}$, i. e., $\lim_{t\to\infty}|a_i(t) - a_0(t)| = 0$, $\lim_{t\to\infty}|v_i(t) - v_0(t)| = 0$, and $\lim_{t\to\infty}|q_i(t) - q_j(t) - d_{i,j}| = 0$; and ***2)*** *in the presence of energy-limited DoS attacks*, system (11) satisfies certain resilience performance $\|x(t)\| \le \eta$, where $\eta > 0$.

Remark 2. The performance index $\|x(t)\| \le \eta$ is presented to evaluate the resilience of the vehicular platoon control system to energy-limited DoS attacks. The resilience level η can be determined to ensure the spacing, velocity as well as acceleration errors of vehicle platooning to be always constrained under the corrupted vehicle-to-vehicle communication.

3. MAIN RESULTS

This section presents the sufficient conditions for the resilient distributed platoonning control of the connected vehicles which can be also regarded as the asymptotic stability of the resulting closed-loop system (11). Furthermore, a co-design criterion for the controller gain as well as the parameter of resilient event triggering condition is also presented.

Theorem 3. Under Assumption 1, for given positive scalars σ, h, ρ, and given matrices K, Φ, system (11) is asymptotically stable satisfying constrained resilience performance if there exist matrix S and positive definite real matrices P, Q, R such that

$$\begin{bmatrix} \Upsilon & \Xi \\ * & -R \end{bmatrix} < 0, \ \begin{bmatrix} R & S \\ * & R \end{bmatrix} \geq 0 \tag{12}$$

where $\Upsilon = [\Upsilon_{pq}]_{4\times 4}$ is a symmetric matrix with nonzero blocks given as $\Upsilon_{11} = I_N \otimes (PA + A^{\mathrm{T}}P) + Q - R$, $\Upsilon_{12} = \mathcal{H} \otimes PBK + R + S$, $\Upsilon_{13} = -S$, $\Upsilon_{14} = \mathcal{H} \otimes PBK$, $\Upsilon_{22} = -2R - S - S^{\mathrm{T}} + I_N \otimes \sigma\Phi$, $\Upsilon_{23} = R + S$, $\Upsilon_{24} = I_N \otimes \sigma\Phi$, $\Upsilon_{33} = -Q - R$, $\Upsilon_{44} = I_N \otimes (\sigma - 1)\Phi$, and $\Xi = [hR(I_N \otimes A),\ hR(\mathcal{H} \otimes BK),\ 0,\ hR(\mathcal{H} \otimes BK)]^{\mathrm{T}}$.

Proof. Construct a Lyapunov function

$$V(t) = V_1(t) + V_2(t) + V_3(t) \tag{13}$$

where $V_1(t) = x^{\mathrm{T}}(t)(I_N \otimes P)x(t)$, $V_2(t) = \int_{t-h}^{t} x^{\mathrm{T}}(s)Qx(s)\mathrm{d}s$, and $V_3(t) = h\int_{-h}^{0}\int_{t+\theta}^{t} \dot{x}^{\mathrm{T}}(s)R\dot{x}(s)\mathrm{d}s\mathrm{d}\theta$.

Taking the derivative of (13) along the trajectory of (11), we have

$$\begin{aligned} \dot{V}_1(t) &= 2x^{\mathrm{T}}(t)(I_N \otimes P)\Big((I_N \otimes A)x(t) + (\mathcal{H} \otimes BK)x(t-\tau(t)) \\ &\quad + (\mathcal{H} \otimes BK)e(t-\tau(t))\Big) \\ \dot{V}_2(t) &= x^{\mathrm{T}}(t)Qx(t) - x^{\mathrm{T}}(t-h)Qx(t-h) \\ \dot{V}_3(t) &= h^2\dot{x}^{\mathrm{T}}(t)R\dot{x}(t) - h\int_{t-h}^{t} \dot{x}^{\mathrm{T}}(s)R\dot{x}(s)\mathrm{d}s. \end{aligned} \tag{14}$$

Applying Lemma 1 in Ge and Han (2015), we have

$$\begin{aligned} &-h\int_{t-h}^{t} \dot{x}^{\mathrm{T}}(s)R\dot{x}(s)\mathrm{d}s \\ &\leq -(x(t-\tau(t)) - x(t))^{\mathrm{T}}R(x(t-\tau(t)) - x(t)) \\ &\quad - (x(t-h) - x(t-\tau(t)))^{\mathrm{T}}R(x(t-h) - x(t-\tau(t))) \\ &\quad + 2(x(t-\tau(t)) - x(t))^{\mathrm{T}}S(x(t-h) - x(t-\tau(t))) \end{aligned} \tag{15}$$

where S is a real matrix satisfying the second inequality in (12).

Further from (6), we have

$$\begin{bmatrix} x(t-\tau(t)) \\ e(t-\tau(t)) \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} I_N \otimes \sigma\Phi & I_N \otimes \sigma\Phi \\ I_N \otimes \sigma\Phi & I_N \otimes (\sigma-1)\Phi \end{bmatrix} \begin{bmatrix} x(t-\tau(t)) \\ e(t-\tau(t)) \end{bmatrix} + N\bar{\Gamma} \geq 0. \tag{16}$$

Defining vector $\xi(t) = [x^{\mathrm{T}}(t), x^{\mathrm{T}}(t-\tau(t)), x^{\mathrm{T}}(t-h), e^{\mathrm{T}}(t-\tau(t))]^{\mathrm{T}}$ and combining (14)-(16), one obtains

$$\dot{V}(t) = \xi^{\mathrm{T}}(t)(\Upsilon + \Xi R^{-1}\Xi^{\mathrm{T}})\xi(t) + N\bar{\Gamma}.$$

By Schur complement and (12), we have that $\Upsilon + \Xi R^{-1}\Xi^{\mathrm{T}} < 0$, which indicates that there exists a positive scalar ρ such that $\xi^{\mathrm{T}}(t)(\Upsilon + \Xi R^{-1}\Xi^{\mathrm{T}})\xi(t) \leq -\rho V(t)$. Then we have

$$\dot{V}(t) \leq -\rho V(t) + N\bar{\Gamma}. \tag{17}$$

Multiplying $\mathrm{e}^{\rho t}$ and calculating the integral from 0 to T on both sides of (17), we have

$$V(T) \leq \mathrm{e}^{-\rho T}V(0) + \frac{N\bar{\Gamma}}{\rho}(1 - \mathrm{e}^{-\rho T}). \tag{18}$$

Note that T can be any time instant, and then we have

$$x^{\mathrm{T}}(t)Px(t) \leq V(t) \leq V(0) + \frac{N\bar{\Gamma}}{\rho} \tag{19}$$

which leads to

$$\|x\| \leq \sqrt{\frac{V(0) + \frac{N\bar{\Gamma}}{\rho}}{\lambda(P)}} \tag{20}$$

where $\lambda(P)$ denotes the minimum eigenvalue of matrix P. Letting $\eta = \sqrt{\frac{V(0)+\frac{N\bar{\Gamma}}{\rho}}{\lambda(P)}}$, one has the proof is completed.

Remark 4. From (20), one has that a lager $\bar{\Gamma}$ leads to a larger upper bound of resilience level to the concerned DoS attacks. In other words, the longer the attack duration, the more control performance loss. In addition, the larger values of $\lambda(P)$ and ρ also cause more resilience of the platoon control. Thus, stability of the resulting closed-loop system (11) together with the optimization of Trace(P) deserves further study.

Now we are in a position to provide a co-design approach to determining the platoon controller as well as the event triggering condition.

Theorem 5. In a vehicular platoon control system under Assumption 1, for given positive scalars σ, h, ρ, α, the following vehicles can track vehicle 0's position, velocity and acceleration with prescribed spacing policy and satisfy constrained resilience performance if there exist matrices $\tilde{K}$ and $\tilde{S}$, and positive definite real matrices U, $\tilde{Q}$, $\tilde{R}$ such that

$$\begin{bmatrix} \tilde{\Upsilon} & \tilde{\Xi} \\ * & \alpha^2\tilde{R} - 2\alpha(I_N \otimes U) \end{bmatrix} < 0, \ \begin{bmatrix} \tilde{R} & \tilde{S} \\ * & \tilde{R} \end{bmatrix} \geq 0 \tag{21}$$

where $\tilde{\Upsilon} = [\tilde{\Upsilon}_{pq}]_{4\times 4}$ is a symmetric matrix with nonzero blocks $\tilde{\Upsilon}_{11} = I_N \otimes (AU + UA^{\mathrm{T}}) + \tilde{Q} - \tilde{R}$, $\tilde{\Upsilon}_{12} = \mathcal{H} \otimes B\tilde{K} + \tilde{R} + \tilde{S}$, $\tilde{\Upsilon}_{13} = -\tilde{S}$, $\tilde{\Upsilon}_{14} = \mathcal{H} \otimes B\tilde{K}$, $\tilde{\Upsilon}_{22} = -2\tilde{R} - \tilde{S} - \tilde{S}^{\mathrm{T}} + I_N \otimes \sigma\tilde{\Phi}$, $\tilde{\Upsilon}_{23} = \tilde{R} + \tilde{S}$, $\tilde{\Upsilon}_{24} = I_N \otimes \sigma\tilde{\Phi}$, $\tilde{\Upsilon}_{33} = -\tilde{Q} - \tilde{R}$, $\tilde{\Upsilon}_{34} = I_N \otimes (\sigma - 1)\tilde{\Phi}$, and $\tilde{\Xi} = [h(I_N \otimes AU),\ h(\mathcal{H} \otimes B\tilde{K}),\ 0,\ h(\mathcal{H} \otimes B\tilde{K})]^{\mathrm{T}}$. Furthermore, the controller gain and the event-triggered weighting matrix can be calculated as

$$K = \tilde{K}U^{-1},\ \Phi = U^{-1}\tilde{\Phi}U^{-1}. \tag{22}$$

Proof. Denote $U = P^{-1}$, $\tilde{Q} = (I_N \otimes U)Q(I_N \otimes U)$, $\tilde{R} = (I_N \otimes U)R(I_N \otimes U)$, $\tilde{S} = (I_N \otimes U)S(I_N \otimes U)$, $\tilde{\Phi} = U\Phi U$ and $\tilde{K} = KU$. Then pre- and post-multiplying the both sides of the two inequalities in (12) with diag$\{I_N \otimes U, I_N \otimes U, I_N \otimes U, I_N \otimes U, R^{-1}\}$ and diag$\{I_N \otimes U, I_N \otimes U\}$, respectively, one can easily derive inequalities in (21) together with $-(I_N \otimes U)\tilde{R}^{-1}(I_N \otimes U) \leq \alpha^2\tilde{R} - 2\alpha(I_N \otimes U)$. Thus the proof has been completed.

4. AN ILLUSTRATIVE EXAMPLE

A simulation study on vehicle platoon control is given in this section to demonstrate the derived resilient event-triggered vehicle platoon control strategy. The predecessor-leader following topology (Zheng et al., 2016) is adopted here for describing inter-vehicle information exchanges, as also shown in Fig. 1.

All the vehicles are homogeneous, which indicates the corresponding parameters of all vehicles are the same. We further let $C_{A,i} = 0.492$, $g = 9.8m/s^2$, $f_i = 0.01$, $\varpi_{T,i} = 0.9$, $m_i = 2.9 \times 10^3 kg$, $R_i = 0.3m$, $\varsigma = 0.25s$, desired spacing $d_{i-1,i} = 30m$, $i = 0, 1, 2, ..., 5$ $h = 0.1s$, $\sigma = 0.03$ and $\rho = 1$. Through the design approach proposed in Theorem 5, one can compute the controller gain matrix and event-triggered weighting matrix as

$$K = [0.0912\ 0.4941\ 0.1790]$$
$$\Phi = \begin{bmatrix} 1.0961 & 5.4035 & 2.0645 \\ 5.4035 & 32.0073 & 11.0849 \\ 2.0645 & 11.0849 & 6.2801 \end{bmatrix}.$$

Moreover, choose the acceleration of the leading vehicle as

$$a_0(t) = \begin{cases} 1m/s^2, & 0s \leq t \leq 20s \\ -1m/s^2, & 20s < t \leq 30s \\ 0m/s^2, & t > 30s. \end{cases} \tag{23}$$

Applying the designed distributed event-triggered control strategy into the platoon of vehicles, the motion trajectories of the controlled vehicle platoon are given in Figs. 2-5. Specifically, the position trajectories of leading and following vehicles are provided in Fig. 2, which clearly demonstrates that under the proposed resilient event-triggered platoon control strategy, the following vehicles can successfully track the leading vehicle with desired spacing distance regardless of the simulated DoS attacks. Figs. 3 and 4 indicates that the following vehicles 1-5 can eventually preserve the same velocity and acceleration as those of the leading vehicle 0, respectively, in the presence of DoS attacks. Note that the occurrences and durations of DoS attacks are both illustrated in Figs. 2-4.

Finally, the event release instants and holding intervals according to the designed resilient event-triggered conditions are depicted in Fig. 5, from which one can obviously see that the total number of actually transmitted data has been effectively reduced. Thus, the proposed resilient distributed event-triggered platoon control method provides a potential benefit for being applied in some resource-constrained scenarios in networked and automated vehicular platoons.

5. CONCLUSION

The resilient distributed event-triggered platoon control strategy under DoS attacks for automated vehicles has been studied. The adverse effects of passive packet dropouts caused by the DoS attacks have been carefully tackled under the proposed resilient event-triggered transmission mechanism. An effective co-design approach for determining the desired distributed platoon controller as well as the resilient event-triggered condition on each vehicle has been provided, through which vehicles are able to maintain the prescribed spacing with each other and the same velocity and acceleration as the leading vehicle. In our future work, the potential tradeoff between the platoon control effectiveness and the system resilience will be further examined.

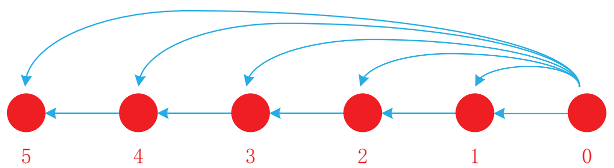

Fig. 1. The prescribed predecessor-leader following communication topology of a vehicle platoon system consisting 1 leading vehicle and 5 following vehicles moving along a lane

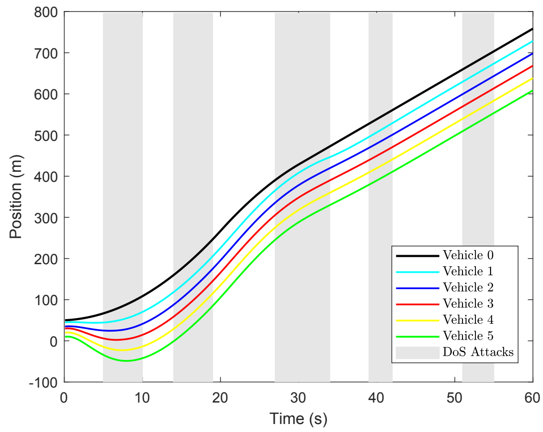

Fig. 2. Positions of the leading vehicle 0 and following vehicles $i = 1, 2, \cdots, 5$ during DoS attacks

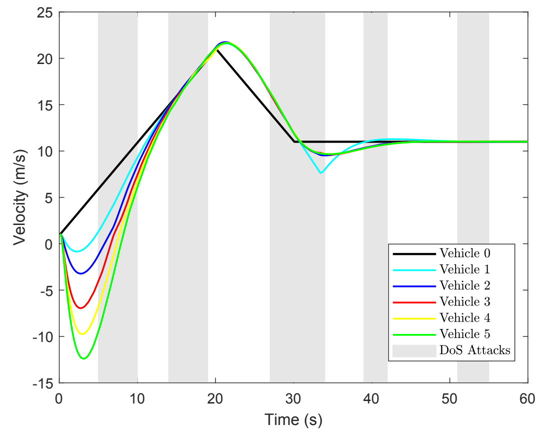

Fig. 3. Velocities of the leading vehicle 0 and following vehicles $i = 1, 2, \cdots, 5$ during DoS attacks

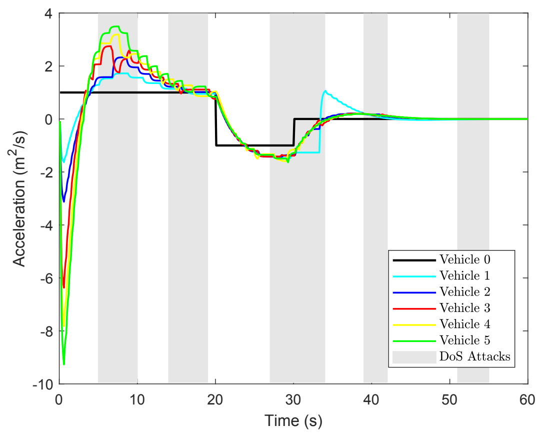

Fig. 4. Accelerations of the leading vehicle 0 and following vehicles $i = 1, 2, \cdots, 5$ during DoS attacks

REFERENCES

Amoozadeh, M., Raghuramu, A., Chuah, C.-N., Ghosal, D., Zhang, H. M., Rowe, J., and Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, 53(6), 126–132.

Besselink, B., and Johansson, K. H. (2017). String stability and a delay-based spacing policy for vehicle platoons subject to disturbances. *IEEE Transactions on Automatic Control*, 62(9), 4376–4391.

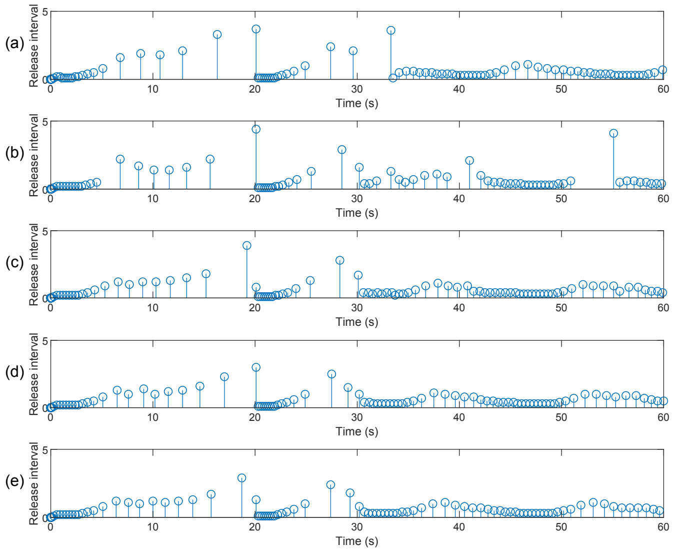

Fig. 5. Release instants and intervals on the 5 following vehicles: (a) Vehicle 1; (b) Vehicle 2; (c) Vehicle 3; (d) Vehicle 4; (e) Vehicle 5

Biron, Z. A., Dey, S., and Pisu, P. (2018). Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, 19(12), 3893–3902.

Cui, J., Liew, L. S., Sabaliauskaite, G., and Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks*, 90, 101823.

Ding, L., Han, Q.-L., Ge, X., and Zhang, X.-M. (2018). An overview of recent advances in event-triggered consensus of multi-agent systems. *IEEE Transactions on Cybernetics*, 48(4), 1110–1123.

Dunbar, W. B., and Caveney, D. S. (2012). Distributed receding horizon control of vehicle platoons: Stability and string stability. *IEEE Transactions on Automatic Control*, 57(3), 620–633.

Ge, X., and Han, Q.-L. (2015). Distributed event-triggered H_∞ filtering over sensor networks with communication delays. *Information Sciences*, 291, 128–142.

Ge, X., Han, Q.-L., Zhang, X.-M., Ding, L., and Yang, F. (2020). Distributed event-triggered estimation over sensor networks: A survey. *IEEE Transactions on Cybernetics*, 50(3), 1306–1320.

Ge, X., Han, Q.-L., Zhong, M., and Zhang, X.-M. (2019). Distributed Krein space-based attack detection over sensor networks under deception attacks. *Automatica*, 109, 108557.

Guan, Y., and Ge, X. (2017). Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks. *IEEE Access*, 5, 10858–10870.

Guan, Y., and Ge, X. (2018). Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Transactions on Signal and Information Processing over Networks*, 18(1), 48–59.

Guo, G., and Wen, S. (2016). Communication scheduling and control of a platoon of vehicles in VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 17(6), 1551–1563.

Guo, X., Wang, J., Liao, F., and Teo, R. S. H. (2016). Distributed adaptive integrated-sliding-mode controller synthesis for string stability of vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 17(9), 2419–2429.

Hu, H. A., Lu, R., Zhang, Z., and Shao, J. (2017). REPLACE: A reliable trust-based platoon service recommendation scheme in VANET. *IEEE Transactions On Vehicular Technology*, 66(2), 1786–1797.

Knorn, S., Donaire, A., Aguero, J. C., and Middleton, R. H. (2015). Scalability of bidirectional vehicle strings with static and dynamic measurement errors. *Automatica*, 62, 208–212.

Lu, Z., Qu, G. and Liu, Z. (2019). A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, 20(2), 760–776.

Mousavinejad, E., Yang, F., Han, Q.-L., Ge, X., and Vlacic, L. (2019). Distributed cyber attack detection and recovery mechanism for vehicle platooning. *IEEE Transactions on Intelligent Transportation Systems*, to be published, DOI: 10.1109/TITS.2019.2934481.

Ploeg, J., Shukla, D. P., Wouw, N., and Nijmeijer, H. (2014). Controller synthesis for string stability of vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 15(2), 854–865.

Sheehan, B., Murphy, F., Mullins, M., and Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A*, 124, 523–536.

Sun, H., Peng, C., Wang, Y., Cao, D., and Tian, Y. (2019). Output-based resilient event-triggered control for networked control systems under denial of service attacks. *IET Control Theory and Applications*, 13(16), 2521–2528.

Wen, S., and Guo, G. (2019). Sampled-data control for connected vehicles with Markovian switching topologies and communication delay. *IEEE Transactions on Intelligent Transportation Systems*, to be published, DOI: 10.1109/TITS.2019.2921781.

Wen, S., Guo, G., Chen, B., and Gao, X. (2018). Event-triggered cooperative control of vehicle platoons in vehicular ad hoc networks. *Information Sciences*, 459, 341–353.

Wei, Y., Wang, L., and Guo, G. (2017). Event-triggered platoon control of vehicles with time-varying delay and probabilistic faults. *Mechanical Systems and Signal Processing*, 87, 96–117.

Zhang, X.-M., Han, Q.-L., Ge, X., and Ding, L. (2020). Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. *IEEE Transactions on Cybernetics*, to be published, DOI: 10.1109/TCYB.2019.2956137.

Zhang, X.-M., Han, Q.-L., Ge, X., Ding, D., Ding, L., Yue, D., and Peng, C. (2020). Networked control systems: A survey of trends and techniques. *IEEE/CAA Journal of Automatica Sinica*, 7(1), 1–17.

Zheng, Y., Li, S. E., Wang, J., Cao, D., and Li, K. (2016). Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies. *IEEE Transactions on Intelligent Transportation Systems*, 17(1), 14–26.