IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 February 2023, accepted 25 February 2023, date of publication 28 February 2023, date of current version 3 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3250398

THEORY

Observer-Based Secure Control for Vehicular Platooning Under DoS Attacks

SAKINEH KHODADADI, TOHID KARGAR TASOOJI, AND HORACIO J. MARQUEZ, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 1H9, Canada
Corresponding author: Sakineh Khodadadi (sakineh@ualberta.ca)

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

ABSTRACT This paper investigates an observer-based secure control problem for platooning of connected vehicles in the presence of Denial-of-Service (DoS) attacks. DoS attacks usually prevent the vehicle-to-vehicle data packets transmission which will lead to performance degradation of platooning system or vehicle collision. To deal with DoS attacks, we consider an observer-based mechanism to estimate the state of vehicles based on available sensor measurements which significantly improves the resilience and tolerance of platooning system during the attack interval. Then, we provide the optimization framework to maximize the duration of the DoS attack such that the platooning system can tolerate safe operation without performance degradation. The simulation results verify the effectiveness of the proposed method.

INDEX TERMS Platooning system, observer-based secure control, denial-of-service (DoS) attack.

I. INTRODUCTION

The the rapid development of intelligent transportation systems (ITS) has paved the way to consider vehicular platoons in which vehicles move in a coordinated manner, maintaining a minimal inter-vehicular distance. Compared with individual driving, platoon-based driving can significantly improve traffic efficiency and fuel economy while reducing traffic congestion and the risk of accidents [1]. Due to these potential benefits, cooperative platooning control has been extensively investigated over the past few years [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. Yue et al. [16] investigate the dynamic event-triggered fault-tolerant model-free adaptive platooning control problem of vehicle platoon systems under sensor faults. Deng et al. [17] address the resilient practical cooperative output regulation problem for heterogeneous linear multi-agent systems (MASs) with unknown switching exosystem dynamics under DoS attack. The safe operation of platoon systems can be guaranteed using cooperative control that employs measurements from onboard sensors and state packets of neighboring vehicles through Dedicated Short Range Communication (DSRC) radios to control the speed of the platoon system, as well as inter-vehicular distance [18].

In the future, it is expected that vehicles will receive basic safety information about roadway infrastructure warning the drivers about road crashes via Vehicle to Infrastructure (V2I) communication and exchange information between vehicles via Vehicle to Vehicle (V2V) communication. These communication systems can be implemented using DSRC networks. Such complex systems, including communications, computing, and control devices, can be viewed as vehicular cyber-physical systems (VCPSs), where all vehicles are coordinated in a platoon pattern based on information exchange. One potential vulnerability of VCPSs is that since these systems rely on network communications, they are vulnerable to cyber-attacks.

Cyber-attacks represent a serious hazard. An adversary may launch an attack in the form of an attack signal that either blocks or compromises the transmission of data packets over the network, thus leading to performance degradation and possible vehicle collisions. As a result, cyber-attacks are considered one of the main threats in VCPSs [1].

In general, cyber-attacks can be categorized a denial of service (DoS) attacks, relay attacks, and deception attacks [19]. DoS attacks are the easiest to implement by an adversary

The associate editor coordinating the review of this manuscript and approving it for publication was Eyuphan Bulut.

and are therefore commonly encountered in communication networks. In DoS attacks, an adversary aims to overload communication devices by propagating a random jamming signal that prevents the exchange the information with neighboring vehicles. Consequently, DoS attacks can cause instability in the platoon system which can result in multiple collisions.

In this paper, we focus on addressing control issues in the presence of DoS attacks. To the best of our knowledge, there have been very few results on resilient platoon control of VCPSs in the presence of DoS attacks [1]. In particular, the problem of designing a resilient platoon control mechanism that achieves asymptotic stability in the presence of DoS attacks remains an open problem.

A. RELATED WORKS

Up to date, there are few works in the literature addressing the impact of cyber-attacks on VCPSs. Zhao et al. [1] investigated the platoon control problem for VCPSs in the presence of DoS attacks with multiple disturbances. The authors propose a recovery mechanism to restrict the time duration rate and occurrence frequency of the adverse impact of DoS attacks on VCPSs. Mousavinejad et al. [20] develop distributed attack detection and recovery mechanisms in a vehicle platooning control system. Biron et al. [21] propose a real-time scheme to detect the occurrence of DoS attacks and estimate the impact of the attack on the connected vehicle system. The scheme relies on a set of observers that can detect the attack and estimate its effect on the platoon. Petrillo et al. [22] propose a secure adaptive cooperative control approach to solve the problem of tracking the time-varying motion of the leading vehicle under different types of cyber attacks as well as network-induced phenomena. The authors prove analytically the effectiveness of their approach using the Lyapunov–Krasovkii method under the assumption that the information provided by the leader vehicle cannot be falsified.

B. MAIN CONTRIBUTION

In this paper, we consider VCPSs and propose an observer-based control strategy that is resilient to DoS attacks. Our goal is to achieve asymptotic tracking of the leader while maintaining the desired intervehicular spacing despite the presence of DoS attacks. We cast our solution as an optimization problem that maximizes tolerance of the attack duration without degradation of performance.

Our main contribution can be summarized as follows:

1) Different from the existing work in resilient platoon control, [1], where the authors assume a recovery mechanism to deal with DoS attacks, we develop an observer-based secure control for the platooning system. The observer is employed to estimate the state of vehicles based on available measurements and the adverse impact caused by the DoS attacks can be weakened with the observer.
2) Unlike [1], [21] which consider periodic DoS attacks and unknown but constant delay, we consider a more practical attack scenario where a DoS attack occurs aperiodically. Our goal is to obtain an upper bound for the duration and frequency of attacks such that platooning system can achieve asymptotic tracking of the leader while maintain the desired intervehicular spacing.
3) We establish an optimization framework in order to maximize the duration of the attack such that the platooning system can tolerate safe operation without degradation of performance.

The remainder of this article is structured as follows. The problem statement and preliminaries are given in Section II. In Section III, we design a secure controller that stabilizes the platooning system in the presence of DoS attacks. In Section IV we present numerical simulations to verify the theoretical results. Finally, Section V contains the conclusions and final remarks.

TABLE 1. Notation.

Notation	Description
$\mathrm{diag}(.)$	block diagonal matrix
$\otimes$	Kronecker product
A^T	transpose of matrix A
A^{-1}	inverse of matrix A
I_N	identity matrix of appropriate dimensions
i and j	identity of vehicle i and vehicle j
$\mathcal{H}$	Laplacian matrix
$\lambda_{\min}(A)$	the minimum eigenvalue of the matrix A
$\lambda_{\max}(A)$	the maximum eigenvalue of the matrix A
$\mathcal{N}_i$	communication neighboring set of the vehicle i
$p_i(t)$	the position of vehicle i
$v_i(t)$	the speed of vehicle i
$a_i(t)$	the acceleration of vehicle i
$x_i(t)$	the state of vehicle i
$x_0(t)$	the state of the leader vehicle
$d_{i,i-1}$	the desired space between vehicle i and $i-1$
$\hat{x}_i(t)$	the estimated state of vehicle i
$\tilde{x}_i(t)$	the estimation error of vehicle i
G_{ob}	the observer gain of vehicle i
K	the control gain of vehicle i

II. PROBLEM FORMULATION AND PRELIMINARIES

A. GRAPH THEORY

We consider a platoon-based vehicular system with $N+1$ vehicles including a leader vehicle and N following vehicles. An directed communication graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ is used to describe the interaction among vehicles. Here $\mathcal{V} = \{v_1, \ldots, v_N\}$ is the set of follower vehicles in the graph, $\mathcal{E}$ is a set of edges and $\mathcal{A} = \lfloor a_{ij} \rfloor \in \mathbb{R}^{N\times N}$ represents the adjacency matrix. The identifier "i" denotes the ith follower vehicle in the platoon. If $(i, j) \in \mathcal{E}$, then the two follower vehicles i and j are adjacents with $a_{ij} = 1$. In this case, vehicles i and j can exchange information with each other, otherwise $a_{ij} = 0$. $\mathcal{N}_i$ represents the communications neighbouring set of vehicle i. The matrix $\mathcal{L} = [l_{ij}] \in \mathbb{R}^{n_i\times n_i}$ represents the Laplacian matrix of the graph with $l_{ij} = \sum_{i\neq j, j\in\mathcal{N}_i} a_{ij}$ and $l_{ij} = -a_{ij}$ where $i \neq j$.

We also consider a graph $\bar{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}}, \bar{\mathcal{A}})$ to describe a communication graph between a leader and the followers where $\bar{\mathcal{V}} = \mathcal{V} \cup \{0\}$. Note that node 0 denotes a leader vehicle and $\mathcal{V} = \{1, 2, \ldots, N\}$ denote the index of all other follower vehicles. If a follower vehicle i receives information from the leader, then $a_{i0} > 0$, otherwise $a_{i0} = 0$. Also, the leader does not receive information from the follower vehicles. Therefore, the communication interaction between a leader and followers is directed. We define $\mathcal{H} = \mathcal{L} + \Delta$ where $\Delta = \text{diag}(a_{10}, \ldots, a_{N0})$.

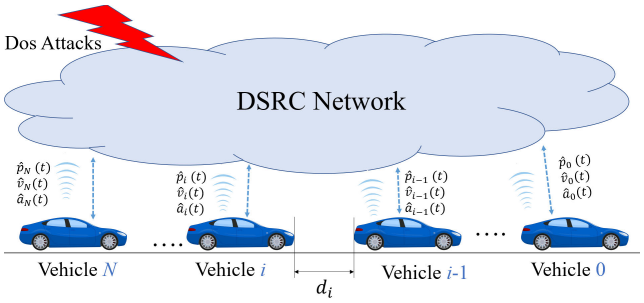


FIGURE 1. A platoon of connected vehicles under DoS attacks.

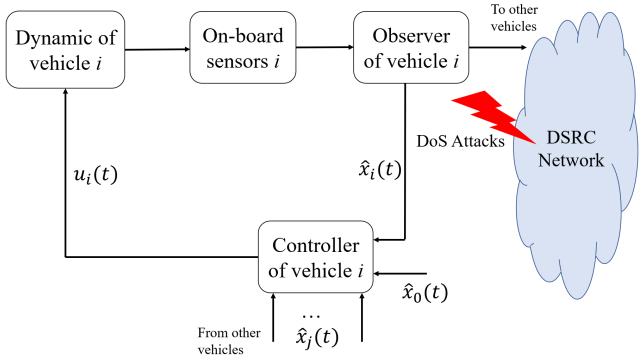


FIGURE 2. Block diagram of observer-based secure control for a platoon of connected vehicles under DoS attacks.

B. PROBLEM STATEMENT

Consider a platoon-based vehicular system with a group of autonomous vehicles including a leader vehicle and N following vehicles (see Fig. 1). Specifically, we use an observer for each vehicle i equipped with onboard sensors to reconstruct the state based on available measurements. Then, each vehicle exchanges the estimated states with other vehicles through a Dedicated Short Range Communication (DSRC) network. As Fig. 2 shows, each vehicle i can transmit the estimated position $\hat{p}_i(t)$, estimated velocity $\hat{v}_i(t)$, and estimated acceleration $\hat{a}_i(t)$ with neighboring vehicles through an unreliable communication network susceptible to DoS attacks. In this paper, we consider a scenario in which the attacker can launch a DoS attack on the communication channels between vehicles for a period of time so that the transmission of information among vehicles is not possible. Our goal is to design a resilient controller for each vehicle i with the observer scheme and investigate under what sufficient conditions the platooning system achieves asymptotic tracking of the leader and maintains a safe inter-vehicular distance.

C. VEHICLE DYNAMICS

The longitudinal dynamic of each vehicle $i \in \mathcal{V}$ can be represented as follows [1]:

$$\begin{cases} \dot{p}_i(t) = v_i(t) \\ \dot{v}_i(t) = a_i(t) \\ \dot{a}_i(t) = -\frac{1}{\tau} a_i(t) + \frac{1}{\tau} u_i(t), \end{cases} \tag{1}$$

where τ denotes the inertial time constant of a vehicle and $u_i(t)$ is the control signal of each vehicle i. Note that we assume that the external disturbance caused by wind gusts, ground frictions, and rolling resistance is negligible. The main goal of the platoon control is to ensure that each follower vehicle tracks the velocity $v_0(t)$ of the leader while maintaining a desired inter-vehicular distance $d_{i,i-1}$ with its predecessor vehicle $i-1$. In other words, each follower vehicle i is expected to achieve the following:

$$\begin{cases} p_i(t) - p_{i-1}(t) \to d_{i,i-1} \\ v_i(t) \to v_0(t). \end{cases} \tag{2}$$

D. DoS ATTACK MODEL

DoS attacks are one of the most commonly encountered cyber attacks in communication networks. DoS attacks in VCPSs impose illegitimate requests in order to change the average service time in the communication network. Therefore, DoS attacks induce extra service time which leads to interruptions of the transmission of information over the network. An attacker uses an attack signal to flood the communication channels, jamming the network nodes so that information packets transmitted by legitimate users have to queue up for the duration of the attack. There are several ways of mathematically representing DoS attacks, including (i) treating the attack as packet losses [24], [25], or (ii) as a time-delay [4], [26], [27]. In the first case, the model assumes that the attack causes network congestion ultimately leading to the loss of useful communication packets between vehicles.

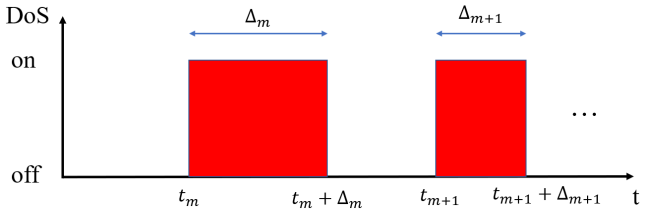


FIGURE 3. Illustration of DoS attack strategy.

In the second, the network congestion produces a delay such that vehicles in the platoon cannot access to the DSRC on time and receive information from other vehicles with a time delay.

In this paper, we consider the first type of the DoS attack model. Fig. 3 represents the DoS attack strategy. The attacker launches an attack signal of variable duration. We assume that the attacker signal consists of the variable on and off periods. This situation is typical in DoS attacks, primarily to avoid detection, and also due to limited energy resources by a non-sophisticated attacker. Accordingly, we assume that the total time sequence is divided into two parts: (i) normal period without DoS attacks and (ii) intervals where a DoS attack blocks the transmission of information between vehicles. The mth attack period is denoted as $D_m = [t_m, t_m + \Delta_m)$ where t_m is the time instant that the DoS attack starts and Δ_m is the duration of attack. For given $t \geq \tau$, the set of intervals such that the communication between vehicles is denied is defined as $\Xi_a(\tau, t) = \bigcup D_m \bigcap [\tau, t]$, the set of time intervals where communication between vehicles is allowed is $\Xi_s(\tau, t) = \Xi_a(\tau, t) \backslash [\tau, t]$. We also make the following assumptions with respect to the duration and frequency of the DoS attacks (see reference [28]):

Assumption 1: ([28]) For any $T_2 > T_1 \geq t_0$, $N_a(T_1, T_2)$ represents the total number of Dos attacks over the interval $[T_1, T_2)$. The frequency of DoS attacks over the interval $T_a(T_1, T_2)$ is defined as follows:

$$F_a(T_1, T_2) = \frac{N_a(T_1, T_2)}{T_2 - T_1}. \tag{3}$$

Assumption 2: ([28]) For any $T_2 > T_1 \geq t_0$, let $T_a(T_1, T_2)$ represent the total time interval of DoS attacks over the interval $[T_1, T_2)$. The attack duration over $[T_1, T_2)$ is described as follows: there exists scalars $T_0 \geq 0$ and $\tau_a > 1$ satisfying

$$T_a(T_1, T_2) \leq T_0 + \frac{T_2 - T_1}{\tau_a}. \tag{4}$$

III. OBSERVER-BASED SECURE CONTROL SCHEME DESIGN FOR PLATOONING SYSTEM

A. CLOSED-LOOP SYSTEM MODEL

The dynamical equations of vehicle (1), can be written in the following form:

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad i = 1, 2, \ldots, N, \tag{5}$$

where $x_i(t) = [p_i(t), v_i(t), a_i(t)]^T$, represents the state vector of vehicle i, and the matrices A and B are given by:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ -\frac{1}{\tau} \end{bmatrix}.$$

where we assume a homogeneous platoon of vehicles. The observer for each vehicle i is designed to estimate the state of vehicle i based on available sensor measurements with the following structure:

$$\dot{\hat{x}}_i(t) = A\hat{x}_i(t) + Bu_i(t) + G_{ob}\Big(y_i(t) - \hat{y}_i(t)\Big), \ i = 1, \ldots, N \tag{6}$$

where $\hat{x}_i(t) = [\hat{p}_i(t), \hat{v}_i(t), \hat{a}_i(t)]^T$ is the estimate of vehicle state $x_i(t)$, $u_i(t)$ is the control input to be designed, $y_i(t)$ is measured onboard sensors in vehicle i, $\hat{y}_i(t) = C\hat{x}_i(t)$ is the observer output, and G_{ob} is the observer gain matrix to be determined.

The control law to achieve the platoon control objective (2) is defined as follows:

$$u_i(t) = K\Bigg[\sum_{j=1}^{N} a_{ij}\Big(\hat{x}_i(t) - \hat{x}_j(t) - D_{ij}\Big) + a_{i0}\Big(\hat{x}_i(t) - \hat{x}_0(t) - D_{i0}\Big)\Bigg], \tag{7}$$

where $D_{ij} = [d_{ij}, 0, 0]^T$ with $d_{ij} = \sum_{l=j}^{i-1} d_{l,l+1}$ being the desired space between the vehicle i and vehicle j; $K = [k^p, k^v, k^a]$ is the controller gain to be designed and a_{ij} is the element of the adjacency matrix and indicate the interaction between vehicle i and vehicle j. The parameter a_{i0} indicates the communication interaction between the leader and follower. Note that each vehicle i needs to know its interaction with other vehicles which can be detected by roadside infrastructures and transmitted to all vehicles through Vehicle to Infrastructure (V2I) communication [1].

Assumption 3: Each vehicle needs to know the interaction topology of the platooning system, which can be detected by roadway infrastructures and transmit to each vehicle via V2I communications which is free of DoS attacks.

Remark 1: Assumption 3 reflects the fact that current approaches in cyber-attack detection and network recovery mechanisms [29], [30], [31], [32] all rely on dedicated trustworthy roadside units (RSUs) to ensure high-quality V2I communications, which can be guaranteed by large-scale deployment of roadside units (RSUs) or by employing visible light as communication links [29]. Therefore, in this work we consider secured V2I communications to broadcast the interaction topology of the platooning system while designing an observer-based secure control for each vehicle to handle DoS attacks on the V2V network.

Consider now vehicle i in (5) and the objective of the platooning system (2). The tracking error between the leader and vehicle i can be defined as follows:

$$e_i(t) = x_i(t) - x_0(t) - D_{i0}, \tag{8}$$

where $x_0(t) = [p_0(t), v_0(t), 0]$. Using Eqs. (5)-(8) and considering the observer error $\tilde{x}_i(t) = x_i(t) - \hat{x}_i(t)$, we obtain the following expression for the tracking error:

$$\dot{e}_i(t) = Ae_i(t) + BK\Bigg[\sum_{j=1}^{N} a_{ij}\Big(e_i(t) - e_j(t) - \tilde{x}_i(t) + \tilde{x}_j(t)\Big) + a_{i0}\Big(e_i(t) - \tilde{x}_i(t)\Big)\Bigg]. \tag{9}$$

Let the extended vectors $e(t)$ and $\hat{x}(t)$ be defined as follows: $e(t) = [e_1^T(t), e_2^T(t), \ldots, e_N^T(t)]^T$ and $\hat{x}(t) = [\hat{x}_1^T(t), \hat{x}_2^T(t), \ldots, \hat{x}_N^T(t)]^T$. We can write:

$$\dot{e}(t) = \Big(I_N \otimes A + \mathcal{H} \otimes BK\Big)e(t) - \Big(\mathcal{H} \otimes BK\Big)\tilde{x}(t) \tag{10}$$

$$\dot{\tilde{x}}(t) = \Big[I_N \otimes A - I_N \otimes G_{ob}C\Big]\tilde{x}(t), \tag{11}$$

where $\mathcal{H} = \mathcal{L} + \Delta$. Then, we say that the platooning system is stable provided that:

$$\lim_{t\to\infty} e_i(t) = 0. \tag{12}$$

Therefore, our objective is to design the feedback controller gain K and the observer to gain G_{ob} for each follower vehicle i and derive sufficient conditions for the duration $T_a(T_1, T_2)$ and frequency $F_a(T_1, T_2)$ of the DoS attacks such that stability of all follower vehicles in the platooning system is guaranteed.

Remark 2: In this paper, the observer plays an important role during the DoS attack interval. We consider a scenario in which each vehicle i in the platooning system is equipped with onboard sensors to measure, directly or indirectly, relative distance, velocity, and acceleration, with respect to the preceding and follower vehicles. This task can be accomplished by fusing LiDAR data and image-based object detection, and estimating the state of vehicle j in order to design the controller of vehicle i during the attack interval. In other words, by using exteroceptive sensors in vehicle i and the state estimate of neighboring vehicles we obtain the control input during DoS attack intervals. However, a DoS attack does not affect the measurement $y_i(t)$ received from the onboard sensors used in the observer. Therefore, the observer is used to mitigate the adverse effects caused by Dos attacks and to improve the resilience and tolerance of the platooning system against DoS attacks. We emphasize the difference between this approach with previous work. Indeed, some references (see for example [23], [28]) set the control input to be either zero or constant during the attacked period.

Remark 3: We consider a platoon of vehicles with the vehicle model described in continuous time. We chose this formulation because vehicles respond to continuous-time commands and therefore a continuous-time representation is the most natural model for these systems. Implicit in our formulation is the assumption that sensors communicate with their neighbors at a sampling rate much higher than the vehicle dynamics. Thus, communications between sensors can be considered virtually continuous. Communication constraints can, of course, be addressed using the event-triggering framework. We have not made use of the event-triggering approach explicitly to simplify our presentation.

B. STABILITY ANALYSIS

In this section, we develop sufficient conditions for the duration and frequency of the DoS attacks for the platooning system to achieve asymptotic tracking of the leader and maintain the desired inter-vehicular spacing. We then propose an optimization framework to improve the resiliency and tolerance of the platooning system against DoS attacks by simultaneously designing the controller gain and observer gain.

Theorem 1: Consider the system dynamics described in (5) with the observer structure (6). If Assumptions 1-3 are satisfied, then stability of the platooning system is guaranteed if the following conditions are satisfied:

1) *There exist a constant ξ^* such that the frequency of DoS attacks $F_a(t_0, t)$ satisfies the following inequality*:

$$F_a(t_0, t) = \frac{N_a(t_0, t)}{t - t_0} \le \frac{\xi^*}{\ln(\mu) + (\gamma_s + \gamma_a)\Delta^*}. \tag{13}$$

2) *There exists a positive constant τ_a in the duration of DoS attack with an arbitrary constant $T_0 \ge 0$ such that*

$$\tau_a > \frac{\gamma_s + \gamma_a}{\gamma_s + \xi^*}. \tag{14}$$

The parameters γ_s and γ_a can be obtained from the following linear matrix inequality (LMI) conditions:

$$\begin{bmatrix} QA + A^TQ + \gamma_1 I & QC & \mathcal{H}\otimes BK \\ C^TQ & R & 0 \\ (\mathcal{H}\otimes BK)^T & 0 & P \end{bmatrix} < 0, \tag{15}$$

$$\begin{bmatrix} A^TP^{-1} + P^{-1}A + \gamma_2 I + \epsilon^{-1}P^{-1} & P^{-1}B \\ B^TP^{-1} & -T \end{bmatrix} < 0, \tag{16}$$

$$\begin{bmatrix} QA + A^TQ - \gamma_3 I & QC & \mathcal{H}^{\delta(t)}\otimes BK \\ C^TQ & R & 0 \\ (\mathcal{H}^{\delta(t)}\otimes BK)^T & 0 & S \end{bmatrix} < 0, \tag{17}$$

$$\begin{bmatrix} A^TS^{-1} + S^{-1}A - \gamma_4 I + \epsilon^{-1}S^{-1} & S^{-1}B \\ B^TS^{-1} & -T \end{bmatrix} < 0, \tag{18}$$

where convergence rate γ_s during normal periods and convergence rate γ_a during attack intervals are given by

$$\gamma_s = \max\{\gamma_1, \gamma_2\},$$
$$\gamma_a = \min\{\gamma_1, \gamma_2\}.$$

Proof: Step 1 (Two Intervals Classification):
We define the interval of time where the communications are free of DoS attack and also the interval of time with DoS attack. The mth time interval of DoS attack is as follows:

$$\Upsilon_m = [t_m, t_m + \Delta_m + \Delta^*),$$

where t_m is the time instant that the DoS attack starts, Δ_m is the duration of attack and Δ^* represent the uncertainty in the mth time interval of DoS attack. Therefore the time interval $[\tau, t)$ consists of the following union of subintervals: $[\tau, t) = \bar{\Xi}_s(\tau, t) \cup \bar{\Xi}_a(\tau, t)$ with

$$\bar{\Xi}_a(\tau, t) = \cup\Upsilon_m \cap [\tau, t], \quad \bar{\Xi}_s(\tau, t) = [\tau, t] \setminus \bar{\Xi}_a(\tau, t).$$

Step 2 (Lyapunov Stability Analysis):
1) We consider the time interval $\bar{\Xi}_s(\tau, t)$ where vehicles communicate with each other without DoS attack and choose the following Lyapunov function:

$$V_1(t) = \tilde{x}^T(t)(\Phi \otimes Q)\tilde{x}(t) + e^T(t)(\Phi \otimes P^{-1})e(t). \tag{19}$$

Using Eqs. (10)-(11), the time derivative of (19) is given by:

$$\begin{aligned}\dot{V}_1(t) &= \tilde{x}^T(t)\Big[\Phi \otimes \Big(QA + A^TQ\Big)\Big]\tilde{x}(t) \\ &\quad - \tilde{x}^T(t)\Big(\Phi \otimes QCR^{-1}C^TQ\Big)\tilde{x}(t) \\ &\quad + e^T(t)\Big[\Phi \otimes \Big(A^TP^{-1} + P^{-1}A\Big) \\ &\quad + \Big(\mathcal{H}^T\Phi + \mathcal{H}\Phi\Big) \otimes P^{-1}BT^{-1}B^TP^{-1}\Big]e(t) + M,\end{aligned} \tag{20}$$

where

$$\begin{aligned}M &= \tilde{x}^T(t)\Big(\Phi\mathcal{H} \otimes BK\Big)^T P^{-1}e(t) \\ &\quad + e^T(t)\Big(\Phi\mathcal{H} \otimes P^{-1}BK\Big)\tilde{x}(t).\end{aligned} \tag{21}$$

Using Young's inequality $2a^Tb \le \varepsilon a^Ta + \varepsilon^{-1}b^Tb$ for any ε and $a, b \in \mathbb{R}^n$ we can write:

$$\begin{aligned}\dot{V}_1(t) &\le \tilde{x}^T(t)\Big[\Phi \otimes \Big(QA + A^TQ\Big) - \Big(\Phi \otimes QCR^{-1}C^TQ\Big) \\ &\quad - \varepsilon\Big(\Phi\mathcal{H} \otimes BK\Big)^T P^{-1}\Big(\Phi\mathcal{H} \otimes BK\Big)\Big]\tilde{x}(t) \\ &\quad + e^T(t)\Big[\Phi \otimes \Big(A^TP^{-1} + P^{-1}A\Big) + \Big(\mathcal{H}^T\Phi + \mathcal{H}\Phi\Big) \\ &\quad \otimes P^{-1}BT^{-1}B^TP^{-1} - \varepsilon^{-1}P^{-1}\Big]e(t) \\ &= \begin{bmatrix}\tilde{x}(t) \\ e(t)\end{bmatrix}^T \begin{bmatrix}\Pi_1 & 0 \\ 0 & \Pi_2\end{bmatrix}\begin{bmatrix}\tilde{x}(t) \\ e(t)\end{bmatrix}.\end{aligned} \tag{22}$$

Therefore, the condition for stability of the platooning system in a period of normal operation without attack is:

$$\begin{aligned}\Pi_1 &= \Phi \otimes \Big(QA + A^TQ\Big) - \Big(\Phi \otimes QCR^{-1}C^TQ\Big) \\ &\quad - \varepsilon\Big(\Phi\mathcal{H} \otimes BK\Big)^T P^{-1}\Big(\Phi\mathcal{H} \otimes BK\Big) + \gamma_1 I < 0,\end{aligned} \tag{23}$$

$$\begin{aligned}\Pi_2 &= \Phi \otimes \Big(A^TP^{-1} + P^{-1}A\Big) + \Big(\mathcal{H}^T\Phi + \mathcal{H}\Phi\Big) \\ &\quad \otimes P^{-1}BT^{-1}B^TP^{-1} - \varepsilon^{-1}P^{-1} + \gamma_2 I < 0.\end{aligned} \tag{24}$$

Using the Schur complement lemma, inequalities (23)-(24) can be transformed into the following LMI conditions:

$$\begin{bmatrix}QA + A^TQ + \gamma_1 I & QC & \mathcal{H} \otimes BK \\ C^TQ & R & 0 \\ (\mathcal{H} \otimes BK)^T & 0 & P\end{bmatrix} < 0, \tag{25}$$

$$\begin{bmatrix}A^TP^{-1} + P^{-1}A + \gamma_2 I + \epsilon^{-1}P^{-1} & P^{-1}B \\ B^TP^{-1} & -T\end{bmatrix} < 0. \tag{26}$$

2) We now consider the DoS attack periods. During attack intervals, malicious attacks affect the communication channels between vehicles and the interaction topology becomes $\mathcal{H}^{\delta(t)}$. We consider the Lyapunov function V_2 for observer error dynamic and tracking error dynamics:

$$V_2(t) = \tilde{x}^T(t)(\Phi \otimes Q)\tilde{x}(t) + e^T(t)(\Phi \otimes S^{-1})e(t). \tag{27}$$

Taking the derivative of $V_2(t)$ along the trajectories (10)-(11) we have:

$$\begin{aligned}&\dot{V}_2(t) \\ &\le \tilde{x}^T(t)\Big[\Phi \otimes \Big(QA + A^TQ\Big) - \Big(\Phi \otimes QCR^{-1}C^TQ\Big) \\ &\quad - \varepsilon\Big(\Phi\mathcal{H}^{\delta(t)} \otimes BK\Big)^T S^{-1}\Big(\Phi\mathcal{H}^{\delta(t)} \otimes BK\Big)\Big]\tilde{x}(t) \\ &\quad + e^T(t)\Big[\Phi \otimes \Big(A^TS^{-1} + S^{-1}A\Big) + \Big(\mathcal{H}^{\delta(t)^T}\Phi + \mathcal{H}^{\delta(t)}\Phi\Big) \\ &\otimes S^{-1}BT^{-1}B^TS^{-1} - \varepsilon^{-1}S^{-1}\Big]e(t) \\ &= \begin{bmatrix}\tilde{x}(t) \\ e(t)\end{bmatrix}^T \begin{bmatrix}\Pi_3 & 0 \\ 0 & \Pi_4\end{bmatrix}\begin{bmatrix}\tilde{x}(t) \\ e(t)\end{bmatrix}.\end{aligned} \tag{28}$$

Therefore, the condition for stability of the platooning system during attack intervals is:

$$\begin{aligned}\Pi_3 &= \Phi \otimes \Big(QA + A^TQ\Big) - \Big(\Phi \otimes QCR^{-1}C^TQ\Big) \\ &\quad - \varepsilon\Big(\Phi\mathcal{H} \otimes BK\Big)^T P^{-1}\Big(\Phi\mathcal{H} \otimes BK\Big) - \gamma_3 I < 0,\end{aligned} \tag{29}$$

$$\begin{aligned}\Pi_4 &= \Phi \otimes \Big(A^TP^{-1} + P^{-1}A\Big) + \Big(\mathcal{H}^T\Phi + \mathcal{H}\Phi\Big) \\ &\quad \otimes P^{-1}BT^{-1}B^TP^{-1} - \varepsilon^{-1}P^{-1} - \gamma_4 I < 0.\end{aligned} \tag{30}$$

Then, we obtain the following LMI conditions:

$$\begin{bmatrix}QA + A^TQ - \gamma_3 I & QC & \mathcal{H}^{\delta(t)} \otimes BK \\ C^TQ & R & 0 \\ (\mathcal{H}^{\delta(t)} \otimes BK)^T & 0 & S\end{bmatrix} < 0 \tag{31}$$

$$\begin{bmatrix}A^TS^{-1} + S^{-1}A - \gamma_4 I + \epsilon^{-1}S^{-1} & S^{-1}B \\ B^TS^{-1} & -T\end{bmatrix} < 0 \tag{32}$$

Based on above analysis, we can combine both scenarios for the platooning system with/without DoS attacks to obtain the following relationship:

$$V(t) = \begin{cases} e^{-\gamma_s(t-t_{m-1}-\Delta_{m-1})}V(t_{m-1} + \Delta_{m-1}), & t \in \Xi_s(\tau, t) \\ e^{\gamma_a(t-t_m)}V(t_m), & t \in \Xi_a(\tau, t). \end{cases} \tag{33}$$

Our goal is to find an upper bound on the DoS attacks frequency and duration. The solution of the Lyapunov function can be written as follows:

$$\begin{aligned}V(t) &\le e^{\gamma_a(t-t_m)}V(t_m) \le e^{\gamma_a(t-t_m)}V(t_m^-) \\ &\le \mu e^{\gamma_a(t-t_{m-1})}[e^{-\gamma_s(t-t_{m-1}-\Delta_{m-1})}V(t_{m-1} + \Delta_{m-1})] \\ &\le \mu^2 e^{\gamma_a(t-t_{m-1})}[e^{-\gamma_s(t-t_{m-1}-\Delta_{m-1})}V(t_{m-1}^-)] \\ &\le \mu^2 e^{\gamma_a(t-t_{m-2})}[e^{-\gamma_s(t-t_{m-2}-\Delta_{m-2})}V(t_{m-2} + \Delta_{m-2})] \\ &\le \cdots \\ &\le \mu^{m+1}e^{-\gamma_s|\bar{\Xi}_s(t_0,t)|}e^{\gamma_a|\bar{\Xi}_a(t_0,t)|}V(t_0),\end{aligned} \tag{34}$$

where $N_a(t_0, t) = m + 1$ is the number of activation attacks. Also, γ_a represents the convergence rate of the error system in (9) during the attacked interval, and γ_s is the convergence

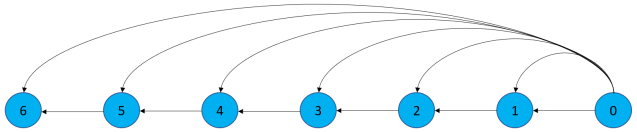


FIGURE 4. Communication topology of vehicles.

rate of the error system in (9) during normal intervals. Note that $|\bar{\Xi}_s(t_0,t)| = t - t_0 - |\bar{\Xi}_a(t_0,t)|$ and due to uncertainty of duration attack $|\bar{\Xi}_s(t_0,t)| \leq |\bar{\Xi}_s(t_0,t)| + \Big(1 + N_a(t_0,t)\Big)\Delta^*$. Then,

$$\begin{aligned} &-\gamma_s\Big(t - t_0 - |\bar{\Xi}_a(t_0,t)|\Big) + \gamma_a|\bar{\Xi}_s(t_0,t)| \\ &= -\gamma_s(t-t_0) + (\gamma_s+\gamma_a)|\bar{\Xi}_s(t_0,t)| \\ &\leq -\gamma_s(t-t_0) + (\gamma_s+\gamma_a) \\ &\quad \times \left[T_0 + \frac{t-t_0}{\tau_a} + \Big(1 + N_a(t_0,t)\Big)\Delta^*\right] \end{aligned} \tag{35}$$

We can write:

$$\begin{aligned} V(t) \leq\ & e^{(\gamma_s+\gamma_a)(T_0+\Delta^*)} e^{-\gamma_s(t-t_0)} e^{\frac{(\gamma_s+\gamma_a)}{\tau_a}(t-t_0)} \\ & \times e^{[\ln(\mu)+(\gamma_s+\gamma_a)\Delta^*]N_a(t_0,t)} V(t_0). \end{aligned} \tag{36}$$

Considering Eqs. (13)-(14) and $\xi = \gamma_s + \frac{(\gamma_s+\gamma_a)}{\tau_a} - \xi^* > 0$ we obtain:

$$V(t) \leq e^{(\gamma_s+\gamma_a)(T_0+\Delta^*)} e^{-\xi(t-t_0)} V(t_0), \tag{37}$$

which completes the proof.

Remark 4: Notice that even though P and P^{-1}, S, and S^{-1} appear in the LMIs, each LMI is only a function of one of those variables, thus resulting in a well-defined LMI. □

Remark 5: According to the result of Theorem 1, stability of the platooning system can be guaranteed provided that conditions (13) and (14) are satisfied. Notice that, according to the assumptions and practical considerations, DoS attacks have limited duration and frequency. The system tolerance to DoS attacks, however, is proportional to the maximum convergence rate γ_s during the normal period and minimum convergence rate γ_a during attacked intervals. Therefore, by maximizing the γ_s and minimizing the γ_a, our solution can improve the tolerance of platooning system against DoS attacks. Theorem 1 provides conditions for the upper bound of the attack duration to achieve the platooning objectives (2). Therefore, asymptotic tracking of the leader and maintaining the desired safety distance of platooning system can be achieved provided that the attack duration is smaller than a certain value. This is accomplished provided that $\tau_a > \frac{\gamma_s+\gamma_a}{\gamma_s+\xi^*}$. We consider a practical case where the DoS attacks occur aperiodically. This is contrary to [1], [33] which assume periodic DoS attacks. To this end, we added the uncertainty term Δ^* in Eq. (35) to model the aperiodic DoS attack scenario. In this equation the value of the parameter Δ^* is unknown and can take a different value for each attack,

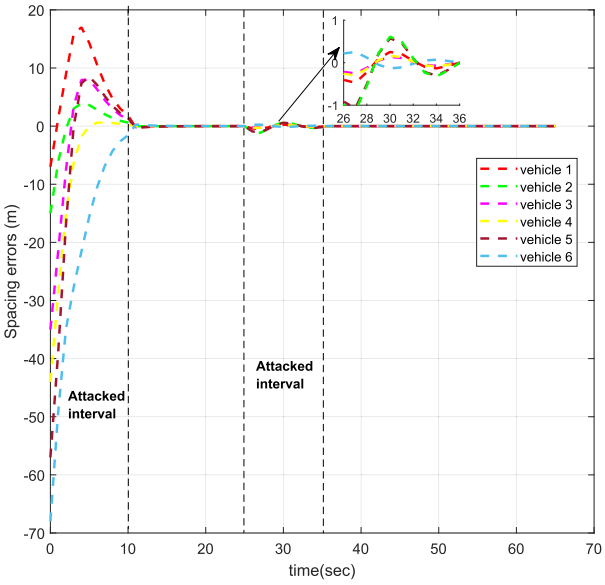


FIGURE 5. Spacing errors of vehicles under DoS attacks [1].

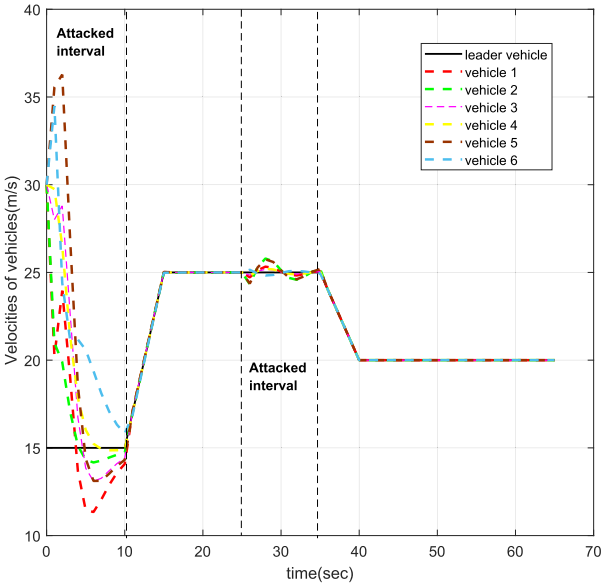


FIGURE 6. Velocities of vehicles under DoS attacks [1].

thus resulting in aperiodic behavior. Our goal is to design the control gain and observer gain such that tolerance to the duration of DoS attacks is maximized as much as possible to ensure the robustness of the platooning system against DoS attacks. To this end, we establish the following optimization problem:

$$\begin{aligned} \min_{K, G_{ob}, \gamma_s, \gamma_a} \quad & \frac{\gamma_s+\gamma_a}{\gamma_s+\xi^*} \\ s.t. \quad & \text{LMI conditions (15)} - \text{(18)}. \end{aligned} \tag{38}$$

Remark 6: As mentioned in the optimization problem (38), the control gain $K = [k^p, k^v, k^a]$ is designed to reduce the impact of DoS attack in control performance and achieve

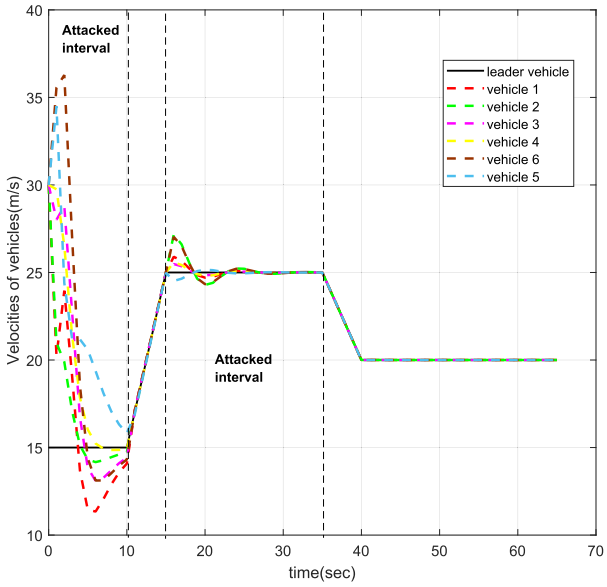


FIGURE 7. Spacing errors of vehicles under DoS attacks.

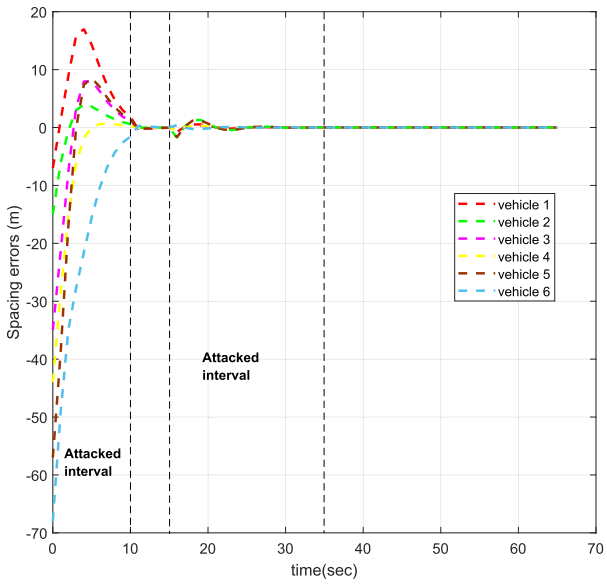


FIGURE 8. Velocities of vehicles under DoS attacks.

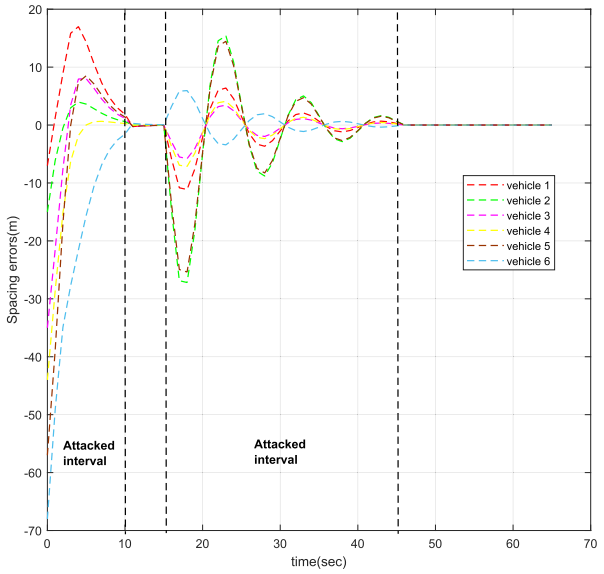


FIGURE 9. Spacing errors of vehicles under DoS attacks [1].

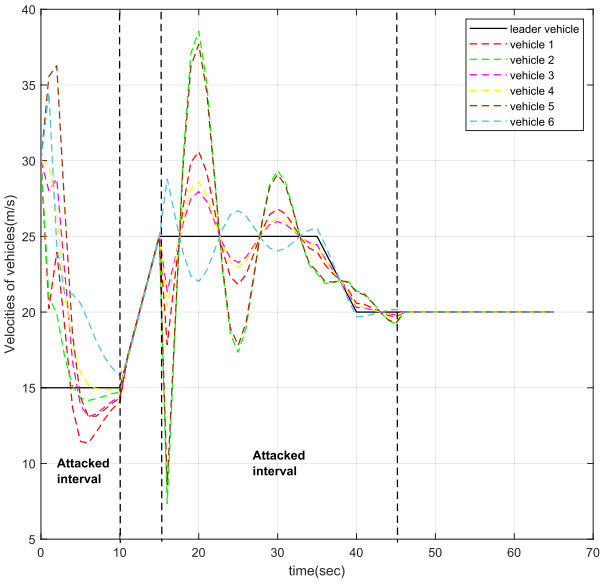


FIGURE 10. Velocities of vehicles under DoS attacks [1].

the desired tracking performance for the platoon of vehicle system. In other words, the optimal control gain is designed based on the worst-case attack duration (maximal attack duration) that the system can tolerate.

Remark 7: Since the DoS attack duration is typically unknown to the defender and is not periodic, the defender might consider a worst-case attack scenario. This can be done by a suitably small τ_a and regard it as the maximum-allowable attack duration bound to account for a worst-case attack scenario during the design procedure. Therefore, we choose τ_a according to the optimization problem (38) in a way that the tolerance to the duration of DoS attacks (proportion of $\frac{1}{\tau_a}$) is maximized to ensure the robustness of the platooning system against DoS attacks. It is worth noting, however, that in either case the design procedure inevitably introduces certain conservatism since the actual/real-time attack duration may be smaller than the worst-case attack scenario.

IV. SIMULATION RESULTS

In this section, we provide simulation results to illustrate the effectiveness of the proposed method. We consider a team of seven vehicles, consisting of one leader and six follower vehicles. The vehicle state is defined as follows:

$$x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix},$$

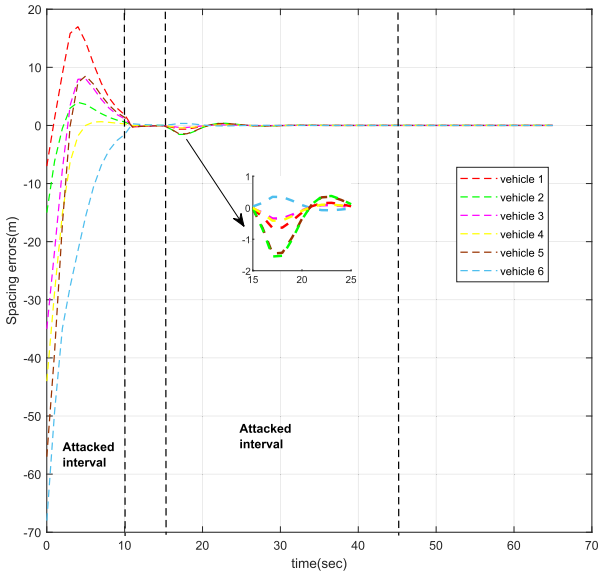


FIGURE 11. Spacing errors of vehicles under DoS attacks.

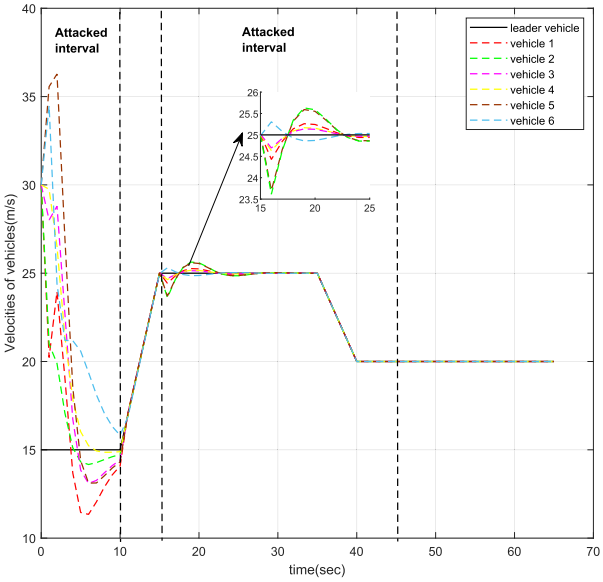


FIGURE 12. Velocities of vehicles under DoS attacks.

where x_1 represents position, x_2 velocity, and x_3 acceleration of the respective vehicle. The communication topology of vehicles is shown in Fig. 4. The inertial time constant of each vehicle is assumed as $\tau_a = 0.54$. We consider the system (5) with

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -1.8519 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ -1.8519 \end{bmatrix}$$
$$C = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}.$$

Considering the directed communication topology of the six follower vehicles, the associated adjacency matrix can be selected as follows:

$$\mathcal{L} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \end{bmatrix}$$
$$\Delta = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We consider the optimization framework (38) to design the controller and observer gains that maximize the duration of attack. Using the MATLAB software and selecting $T = 0.5$, $R = 0.1$, we obtaine the set of feasible solutions for the Lyapunov matrices P, and S, as well as the control gain K and observer gain G:

$$K = \begin{bmatrix} -2.7386 & -5.3068 & -2.7725 \end{bmatrix},$$
$$G = \begin{bmatrix} -1.2247 & -2.6814 & -1.3229 \end{bmatrix}^T,$$
$$P = \begin{bmatrix} 1.4533 & 1.0331 & 0.1479 \\ 1.0331 & 1.8541 & 0.2866 \\ 0.1479 & 0.2866 & 0.1497 \end{bmatrix},$$
$$Q = \begin{bmatrix} 1.6420 & 1.4225 & 0.3307 \\ 1.4225 & 2.7837 & 0.7240 \\ 0.3307 & 0.7240 & 0.3572 \end{bmatrix}.$$

In our simulation, we assume that the initial state of the leader vehicle is $x_0(0) = [0, 15, 0]^T$. The initial state of the followers is as follows: $x_1(0) = [-7, 15, 0]^T$, $x_2(0) = [-15, 15, 0]^T$, $x_3(0) = [-35, 15, 0]^T$, $x_4(0) = [-44, 15, 0]^T$, $x_5(0) = [-57, 15, 0]^T$, $x_6(0) = [-68, 15, 0]^T$. Also, the desired trajectory of the leader vehicle is as follows:

$$v_0(t) = \begin{cases} 15, & 0 \le t < 10 \\ 15 + 2t, & 10 \le t < 15 \\ 25, & 15 \le t < 35 \\ 25 - t, & 35 \le t < 40 \\ 20, & 40 \le t < 65 \end{cases}. \tag{39}$$

The simulation results in Fig. 5-8 show a comparison between the approach proposed in this article and the traditional method in [1] considering the effect of DoS attacks. As can be seen from Fig. 7 and Fig. 8 that using the proposed approach (observer-based resilient controller) the platooning system can tolerate safety distance and velocity tracking longer than using a traditional approach proposed in [1] (Fig. 5 and Fig.6). In other words, using a traditional control scheme where the control signal is maintained zero or constant during the DoS attack interval, the time to tolerate safety distance and velocity tracking is shorter than using our proposed method. Therefore, using our proposed approach (see Fig. 7-8) the follower vehicles can tolerate the DoS attacks at $[0s, 10s]$ and $[16s, 35s]$ and continue to track both the velocity and

trajectory of the leader while maintaining the desired safety distance with slight performance degradation.

Figures 9-12 expand the previous case by extending the duration of the DoS attack. Considering the same system, we now simulate DoS attacks over the intervals $[0s, 10s]$ and $[16s, 45s]$), with the same initial conditions. Figures 11 and Fig 12 shows the system performance using our controller whereas figures 9 and 10 show the same system response using the controller of [1]. As can be seen from the figures, our proposed controller show significantly improved tracking, thus illustrating the advantage of the proposed approach.

V. CONCLUSION

In this paper, we investigated the problem of observer-based secure control for platooning systems suffering from aperiodic DoS attacks. We consider the design of a resilient control that preserves the stability of the platooning system under DoS attacks. We obtain sufficient conditions on the duration and frequency of DoS attacks such that the platooning system achieves asymptotic tracking of the leader and maintains the desired safety distance. We also provide an optimization approach to maximize the duration of the DoS attacks without performance degradation.

REFERENCES

[1] 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.*, vol. 23, no. 8, pp. 10945–10956, Aug. 2022.

[2] P. Liu, A. Kurt, and U. Ozguner, "Distributed model predictive control for cooperative and flexible vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 27, no. 3, pp. 1115–1128, May 2019.

[3] J. Zhan, Z.-P. Jiang, Y. Wang, and X. Li, "Distributed model predictive consensus with self-triggered mechanism in general linear multiagent systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 3987–3997, Jul. 2019.

[4] Y. Feng, B. Hu, H. Hao, Y. Gao, Z. Li, and J. Tan, "Design of distributed cyber–physical systems for connected and automated vehicles with implementing methodologies," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4200–4211, Sep. 2018.

[5] Y. Lu, R. Su, C. Zhang, and L. Qiao, "Event-triggered adaptive formation keeping and interception scheme for autonomous surface vehicles under malicious attacks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 3947–3957, Jun. 2022, doi: 10.1109/TII.2021.3111219.

[6] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 3595–3608, Jun. 2022, doi: 10.1109/TII.2021.3126644.

[7] Z. Huang, D. Chu, C. Wu, and Y. He, "Path planning and cooperative control for automated vehicle platoon using hybrid automata," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 3, pp. 959–974, Mar. 2019.

[8] V. S. Dolk, J. Ploeg, and W. P. M. H. Heemels, "Event-triggered control for string-stable vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 12, pp. 3486–3500, Dec. 2017.

[9] P. Wang, H. Deng, J. Zhang, L. Wang, M. Zhang, and Y. Li, "Model predictive control for connected vehicle platoon under switching communication topology," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 7817–7830, Jul. 2022.

[10] 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, Aug. 2020.

[11] Y. Li, C. Tang, K. Li, X. He, S. Peeta, and Y. Wang, "Consensus-based cooperative control for multi-platoon under the connected vehicles environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 6, pp. 2220–2229, Jun. 2019.

[12] M. R. Hidayatullah and J.-C. Juang, "Centralized and distributed control framework under homogeneous and heterogeneous platoon," *IEEE Access*, vol. 9, pp. 49629–49648, 2021, doi: 10.1109/ACCESS.2021.3068968.

[13] H. Min, Y. Yang, Y. Fang, P. Sun, and X. Zhao, "Constrained optimization and distributed model predictive control-based merging strategies for adjacent connected autonomous vehicle platoons," *IEEE Access*, vol. 7, pp. 163085–163096, 2019, doi: 10.1109/ACCESS.2019.2952049.

[14] H. Ma, L. Chu, J. Guo, J. Wang, and C. Guo, "Cooperative adaptive cruise control strategy optimization for electric vehicles based on SA-PSO with model predictive control," *IEEE Access*, vol. 8, pp. 225745–225756, 2020, doi: 10.1109/ACCESS.2020.3043370.

[15] J. Wu, F. Yan, and J. Liu, "Effectiveness proving and control of platoon-based vehicular cyber-physical systems," *IEEE Access*, vol. 6, pp. 21140–21151, 2018, doi: 10.1109/ACCESS.2018.2800404.

[16] B.-F. Yue and W.-W. Che, "Data-driven dynamic event-triggered fault-tolerant platooning control," *IEEE Trans. Ind. Informat.*, early access, Oct. 31, 2022, doi: 10.1109/TII.2022.3217470.

[17] C. Deng, D. Zhang, and G. Feng, "Resilient practical cooperative output regulation for MASs with unknown switching exosystem dynamics under DoS attacks," *Automatica*, vol. 139, May 2022, Art. no. 110172.

[18] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, and Y. Jin, "Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 4, pp. 3418–3429, Apr. 2022.

[19] T. K. Tasooji and H. J. Marquez, "A secure decentralized event-triggered cooperative localization in multi-robot systems under cyber attack," *IEEE Access*, vol. 10, pp. 128101–128121, 2022, doi: 10.1109/ACCESS.2022.3227076.

[20] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 9, pp. 3821–3834, Sep. 2019.

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

[22] A. Petrillo, A. Pescapé, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, vol. 51, no. 3, pp. 1134–1149, Jan. 2021.

[23] C. De Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.

[24] B. Niemoczynski, S. Biswas, and J. Kollmer, "Stability of discrete-time networked control systems under denial of service attacks," in *Proc. Resilience Week (RWS)*, Aug. 2016, pp. 119–124.

[25] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack policy against remote state estimation," in *Proc. IEEE 52nd Annu. Conf. Decis. Control*, Dec. 2013, pp. 5444–5449.

[26] Z.-H. Pang, G. P. Liu, and Z. Dong, "Secure networked control systems under denial of service attacks," *IFAC Proc.*, vol. 44, no. 1, pp. 8908–8913, 2011.

[27] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Basar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Proc. 6th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2013, pp. 54–59.

[28] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

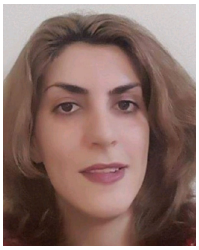
[29] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[30] C. A. Kerrache, N. Lagraa, C. T. Calafate, J. C. Cano, and P. Manzoni, "T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS," *Comput. Commun.*, vol. 93, pp. 68–83, Nov. 2016.

[31] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil attacks in urban vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[32] K. Varma, H. Hasbullah, and A. Kumar, "Prevention DoS attacks in VANET," *Wireless Pers. Commun., Int. J.*, vol. 73, no. 1, pp. 95–126, 2013.

[33] Y. Xu, M. Fang, P. Shi, and Z.-G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3468–3476, Aug. 2020.
[34] T. K. Tasooji and H. J. Marquez, "Event-triggered consensus control for multirobot systems with cooperative localization," *IEEE Trans. Ind. Electron.*, vol. 70, no. 6, pp. 5982–5993, Jun. 2023, doi: 10.1109/TIE.2022.3192673.



SAKINEH KHODADADI received the M.Sc. degree from the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. Her research interests include connected and automated vehicles, platoon control, autonomous driving, intelligent transportation systems, and cyber-physical systems.

TOHID KARGAR TASOOJI received the B.Sc. degree from the Urmia University of Technology, Urmia, Iran, in 2015, and the M.Sc. degree from Özyeğin University, Istanbul, Turkey, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada. His research interests include networked control and filtering, multi-agent systems with applications to robotics, and cyber-physical systems.

HORACIO J. MARQUEZ (Senior Member, IEEE) received the B.Sc. degree from the Instituto Tecnologico de Buenos Aires, Argentina, in 1987, and the M.Sc.E. and Ph.D. degrees in electrical engineering from the University of New Brunswick, Fredericton, Canada, in 1990 and 1993, respectively. Since 1996, he has been with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, Canada, where he is currently a Professor. His current research interests include nonlinear dynamical systems and control, nonlinear observer design, sampled-data systems, and control of cyber-physical systems. He was a recipient of the 2003–2004 McCalla Research Professorship awarded by the University of Alberta. He is currently a licensed professional engineer (P.Eng.) in the Province of Alberta. He is also a fellow of IET, Canadian Academy of Engineering, and Engineering Institute of Canada. He is also an Area Editor of the *International Journal of Robust and Nonlinear Control* and an Associate Editor of *IET-Control Theory & Applications*. He is the author of the book *Nonlinear Control Systems: Analysis and Design* (Wiley, 2003).