Resilient Platooning Control of Connected Automated Vehicles in the Presence of Cyber-attacks

Azwirman Gusrialdi*, Muhammad Iqbal* and Zhihua Qu

Abstract— **This paper considers the problem of platooning control of connected automated vehicles under cyber-attacks. Specifically, the attacker aims to prevent the follower vehicle from maintaining a pre-defined safe distance from its immediate predecessor by manipulating the measurement of the on-board radar and inserting bounded injections into the communication links and actuators of the follower vehicles. A novel distributed resilient control is proposed which does not require any assumptions on the number of attacks. It is shown that by appropriately designing the information being exchanged between the vehicles, the resilient control ensures that the follower vehicles converge to the leader vehicle's velocity and constant distance between the vehicles in presence of any number of attacks. Furthermore, the proposed resilient control also enables attack detection and identification in real-time and distributed manner. A Numerical example demonstrates the effectiveness of the proposed strategy.**

I. Introduction

The ever increasing demand of mobility has posed many challenges for the current infrastructures in terms of safety and efficiency. One way to deal with these challenges is to provide maximum autonomy to a network of vehicles. To that end, one needs to have a cooperative control strategies for a multiple vehicles system using vehicle-to-vehicle (V2V) communication to have higher efficiency in terms of fuel consumption and safety [1]. Nonetheless, V2V communication brings challenges in controlling a platoon systems [2].

A canonical problem in a platoon system is to enable follower vehicles to agree on a common velocity dictated by the leader vehicle, and a desired separation between all vehicles. This problem is solved in [3] by deriving distributed control law for each vehicle using position and velocity information from the neighboring vehicles. However, with the V2V communication infrastructure, the platoon systems are vulnerable to cyber-attacks as states information are shared via the communication network. In addition, the actuators and on-board sensors of the vehicles are also vulnerable to cyber-attacks due to the vehicle's digitalization. In particular, an attacker could inject malicious signals into the individual vehicle's local computation, communication channel, and on-board sensors to prevent the platooning from maintaining a desired spacing. This type of attacks is also known as false data injection (FDI) attacks which is the focus of this paper. Therefore, it is crucial to ensure resilient operation of the platoon in the presence of cyber-attacks.

Resilient distributed platooning control in the presence of FDI attacks has received significant attention in the last decade. A variety of strategies have been proposed to ensure resilient platooning against attack on the communication network, for example the removal of extreme values that a vehicle receives from the neighboring vehicles [4], the adoption of the competitive interaction method [5], [6], and the use of multiple V2V networks and data fusion algorithm to create redundancy at the receiver side and estimate the true information and further isolate the attacked channels [7]. However, those strategies require high network connectivity and impose restrictions on the number of attacked channels. Another line of work is by detecting the attacks, e.g., using a machine learning technique [8], followed by its mitigation. However, no guarantees are given on both the detection accuracy and stability of the platoon during the process. Finally, the work [9] proposes distributed robust platooning control against attacks on the communication network and sensors. However, the controller depends on the existence of a solution to linear matrix inequalities (LMIs).

This paper introduces a novel unified resilient distributed control which ensures a platoon of multiple vehicles to have a constant distancing between each other and moving with a desired constant velocity dictated by the leader vehicle in the presence of bounded cyber-attack on communication network, on-board sensors (radar), and actuators (local computation). To achieve this, virtual states are introduced which also enable each follower vehicle to identify the compromised radar sensor and/or communication links in a real-time and distributed manner. The main contributions of the proposed resilient distributed control are listed as follows:

- Even though this work considers a double integrator dynamics of the individual vehicle, the proposed distributed control is able to ensure resilient platoon under simultaneous attacks on communication network (including the communication link from the leader vehicle), on-board sensor (radar), and actuator (local computation) of the follower vehicles.
- In contrast to the strategy in [4], the proposed strategy imposes no restrictions on the maximum allowable number of attacks. However, it is assumed that the attacks have a bounded magnitude, which is reasonable

* Equal contributions.

The work of Azwirman Gusrialdi is supported by the Research Council of Finland under the Academy Project decision number 330073. The work of Zhihua Qu was supported in part by the U.S. Department of Energy's under Award DE-EE0007998, Award DE-EE0009028, Award DE-EE0009152, Award DE-EE0009339, and Award DE-AC05-76RL01830.

Azwirman Gusrialdi is with the Automation and Mechanical Engineering unit Tampere University, Finland. Muhammad Iqbal is with Department of Electrical Engineering and Automation, Aalto University, Finland. Zhihua Qu is with the Department of Electrical and Computer Engineering, University of Central Florida, USA. (e-mail: azwirman.gusrialdi@tuni.fi; muhammad.iqbal@aalto.fi; qu@ucf.edu).

as will be discussed later in the paper. Moreover, unlike the strategies in [4], [6], the proposed distributed control does not require high network connectivity.

- Unlike the strategy based on robust control in [9], the proposed resilient control does not depend on the existence of a solution to LMIs.
- In contrast to the related work in [8], the stability of the platoon is ensured during the attack detection and identification.

II. Preliminaries and Problem Formulation

First, we present some notations and preliminaries of induced matrix logarithmic norm at the outset.

A. Notations and Preliminaries

The Euclidean norm of a column vector $x \in \mathbb{R}^n$ is denoted by $\| x \|$, and $x^\top$ is the transpose of a vector x. The ith eigenvalue of a square matrix, say A, can be written as $\lambda_i(A) = a_i + \iota b_i$, where $a_i = \Re\{\lambda_i(A)\}$ is the real-part of $\lambda_i(A)$, $b_i = \Im\{\lambda_i(A)\}$ is the imaginary-part of $\lambda_i(A)$, and $\iota = \sqrt{-1}$. We denote $\mathbb{I}_n$ and $\mathbb{O}_n$ to represent $n \times n$ identity matrix and a zero matrix, respectively. A column vector with n entries, all equal to 1 is denoted by 1_n, and a column vector with zero entries is denoted by o_n. The time-derivative of a function $f : t \mapsto \mathbb{R}$ is denoted by $\dot{f}$. An *induced matrix logarithmic norm* of $A \in \mathbb{C}^{n\times n}$ is defined as [10]:

$$\mu(A) \triangleq \lim_{\theta\to 0_+} \frac{\|\mathbb{I}_n + \theta A\| - 1}{\theta}.$$

We will use $\mu_2(A) = \max_i \lambda_i(\frac{A+A^\top}{2})$, and the property $\mu(A+B) \le \mu(A) + \mu(B)$ [10] in our analysis.

B. Problem Statement

Consider a connected vehicle system (CVS), which consists of a leader vehicle 0 and n followers as shown in Fig. 1. The dynamics of each follower is given below:

$$\begin{aligned} \dot{p}_i &= v_i, \\ \dot{v}_i &= u_i, \end{aligned} \tag{1}$$

where $i \in \{1, 2, \cdots, n\}$, $p_i \in \mathbb{R}$ is the position of vehicle i, $v_i \in \mathbb{R}$ is its velocity, and u_i is a control input. It is assumed that the leader vehicle moves with a constant velocity v_0. Furthermore, it is assumed that each vehicle is equipped with: 1) an on-board radar or Lidar which measures the distance between vehicle i and its predecessor (i.e., vehicle $i-1$); 2) a wireless communication for sharing information between the vehicles. Without loss of generality, we assume that the communication network topology is given by the predecessor following (PF) topology, see Fig. 1. The objective of designing u_i is such that the followers maintain a desired velocity v_0 dictated by the leader and a desired spacing d between successive vehicles, i.e.,

$$\begin{aligned} &\lim_{t\to\infty} p^*_{i-1}(t) - p^*_i(t) = d, \\ &\lim_{t\to\infty} v^*_i(t) = v_0 \text{ for all } i \in \{1, 2, \cdots, n\} \end{aligned}$$

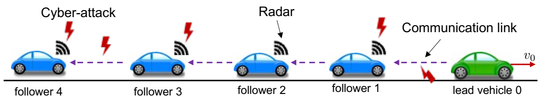


Fig. 1. A platoon of multiple vehicles with cyber-attacks on the sensors, actuators and communication networks.

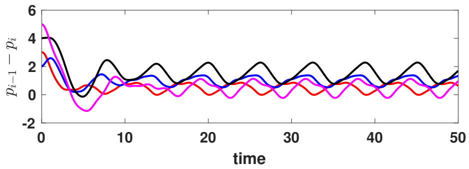


Fig. 2. An illustration of an attacker who is able to prevent the platoon from achieving equal successive vehicles' spacing $d = 1$ by inserting bounded injections into the sensors, actuators and communication links. The follower vehicles implement the standard control law given in (2).

where p^*_i, v^*_i denote the steady state. To this end, the current state-of-the-art considers the following distributed control law for the followers:

$$u_i = (p_{i-1} - p_i - d) + \gamma(v_{i-1} - v_i) \tag{2}$$

with $\gamma > 0$. In order to implement (2), the distance information $(p_{i-1} - p_i)$ is obtained from the radar measurement while the velocity v_{i-1} can be obtained via the communication network. Velocity v_{i-1} can also be obtained using radar, nonetheless, we use communication network to transmit a scaled v_{i-1} and to implement the resilient platooning control presented in the next section.

CVS is an example of cyber-physical systems (CPS), which in practice is vulnerable to cyber-attacks. Specifically, in this paper it is assumed that the adversary can inject bounded injections $\delta^u_i, \delta^s_i, \delta^c_i$ into the actuator of the follower vehicle i [11], the measurement of the radar of vehicle i, and the information received from vehicle i, including the leader vehicle, via the communication network. Furthermore, we assume that the injections are bounded, i.e.,

$$\|\delta^u_i(t)\| \le \overline{\delta}^u_i, \ \ \|\delta^s_i(t)\| \le \overline{\delta}^s_i, \ \ \|\delta^c_i(t)\| \le \overline{\delta}^c_i. \tag{3}$$

Note that the assumption on the bounded injections (3) is a reasonable precaution for intelligent attackers to avoid detection as the case of unbounded injections can be easily detected. This assumption has also been commonly imposed in the related work, see e.g., [12]. Specifically, the adversary aims to make the follower vehicles deviate from the desired spacing d and the leader velocity v_0, for example to disrupt the traffic flow or reduce the capacity of the traffic network as illustrated in Fig. 2. It is well known that control (2) is not robust to measurement error (or attack) [13].

The objective of this paper is twofold:

1) design a resilient platooning control u_i so that in the presence of unknown but bounded attacks (3), we have

$$|p^*_{i-1} - p^*_i - d| \le \epsilon_1, \text{ and } |v^*_i - v^*_0| \le \epsilon_2 \tag{4}$$

for small values of $\epsilon_1 > 0, \epsilon_2 > 0$.

2) design distributed algorithm for each vehicle to detect and identify in real-time attacks on radar sensor and/or communication link.

III. Main Results

In this section, we present a novel distributed resilient control strategy that enables agents to follow a leader with a constant velocity and maintain a desired spacing between vehicles in the presence of cyber-attacks. Furthermore, we also present distributed algorithms to detect and identify attacks on sensors and/or communication links.

A. Distributed Resilient Control Strategy for CVS

We propose the following platooning control for the i-th follower vehicle

$$\begin{aligned} u_i &= (p_{i-1} - p_i - d) + \gamma(v_{i-1} - v_i) + \\ &\quad \beta(q_i - q_{i-1} - d) + \beta(w_i - w_{i-1}), \\ \dot{q}_i &= w_i \\ \dot{w}_i &= (q_{i-1} - q_i - d) + \gamma(w_{i-1} - w_i) + \\ &\quad \beta(p_{i-1} - p_i - d) + \beta(v_{i-1} - v_i). \end{aligned} \tag{5}$$

Here, $\beta > 0$ is scalar gain and q_i, w_i are the composite signals/internal states that encompass position and velocity information from all preceding vehicles. Note that in contrast to the physical states p_i, v_i, the internal states do not have any physical meaning and thus are also called as *virtual* states. For the ith follower vehicle to implement the control law (5), it receives the distance information $p_{i-1,i} = p_{i-1} - p_i$ from its radar and the following information via the communication network:

$$\begin{aligned} &I_{i-1,1} = -\beta q_{i-1},\ I_{i-1,2} = \beta p_{i-1} + q_{i-1}, \\ &I_{i-1,3} = \beta w_{i-1},\ I_{i-1,4} = \gamma v_{i-1} - 2\beta w_{i-1}, \\ &I_{i-1,5} = \gamma w_{i-1} + \beta v_{i-1}. \end{aligned} \tag{6}$$

Note that the communication network topology for transmitting the information in (6) is similar to the one in Fig. 1, thus the sparsity of the network topology is preserved. As can be observed from (6), the virtual states are used not only to ensure resiliency of the platooning but also to mask the physical state information p_{i-1}, v_{i-1} to increase its privacy against external eavesdropper who does not know the structure of (6) as it is a local information to the vehicle. In addition, the information being transmitted in (6) is chosen to facilitate attack detection and identification as will be discussed in Section III-D. Next, the compromised information obtained via the sensor and communication network are then given by

$$\begin{aligned} &p^a_{i-1,i} = p_{i-1} - p_i + \delta^s_i \\ &I^a_{i-1,\theta} = I_{i-1,\theta} + \delta^c_{i-1},\ \theta = \{1, \cdots, 5\}. \end{aligned} \tag{7}$$

The overall follower vehicle dynamics (1) under the distributed control (5) in presence of cyber-attacks on actuators, sensors, and communication network can then be written as

$$\begin{aligned} \dot{p}_i &= v_i, \\ \dot{v}_i &= \{(p_{i-1} - p_i - d) + \gamma(v_{i-1} - v_i)\} + \\ &\quad \{\beta(q_i - q_{i-1} - d) + \beta(w_i - w_{i-1})\} + \delta_i, \\ \dot{q}_i &= w_i \\ \dot{w}_i &= \{(q_{i-1} - q_i - d) + \gamma(w_{i-1} - w_i)\} + \\ &\quad \{\beta(p_{i-1} - p_i - d) + \beta(v_{i-1} - v_i)\} + \tilde{\delta}_i. \end{aligned} \tag{8}$$

where the attacks introduced in (3) on actuator, communication and sensing affecting vehicle i are lumped into δ_i and the injection on communication network is combined into $\tilde{\delta}_i$. Next, we show the convergence results of the CVS system. To that aim, we introduce the following transformation:

$$\begin{aligned} \bar{p}_i &= p_i - p^*_i,\ \bar{v}_i = v_i - v^*_i, \\ \bar{q}_i &= q_i - q^*_i,\ \bar{w}_i = w_i - w^*_i, \end{aligned} \tag{9}$$

where $p^*_i = q^*_i$ and $v^*_i = w^*_i$.

Taking the time-derivative of (9), and using (8), we get

$$\begin{aligned} \dot{\bar{p}}_i &= \bar{v}_i, \\ \dot{\bar{v}}_i &= \{(\bar{p}_{i-1} - \bar{p}_i) + \gamma(\bar{v}_{i-1} - \bar{v}_i)\} + \\ &\quad \{\beta(\bar{q}_i - \bar{q}_{i-1}) + \beta(\bar{w}_i - \bar{w}_{i-1})\} + \delta_i, \\ \dot{\bar{q}}_i &= \bar{w}_i \\ \dot{\bar{w}}_i &= \{(\bar{q}_{i-1} - \bar{q}_i) + \gamma(\bar{w}_{i-1} - \bar{w}_i)\} + \\ &\quad \{\beta(\bar{p}_{i-1} - \bar{p}_i) + \beta(\bar{v}_{i-1} - \bar{v}_i)\} + \tilde{\delta}_i. \end{aligned} \tag{10}$$

where the bounded attacks δ_i and $\tilde{\delta}_i$ could be different from each other.

Next, writing (10) in a compact vector form:

$$\begin{aligned} \dot{\bar{p}} &= \bar{v}, \\ \dot{\bar{v}} &= -\bar{\mathcal{L}}\bar{p} - \gamma\bar{\mathcal{L}}\bar{v} + \beta\bar{\mathcal{L}}\bar{q} + \beta\bar{\mathcal{L}}\bar{w} + \delta, \\ \dot{\bar{q}} &= \bar{w} \\ \dot{\bar{w}} &= -\beta\bar{\mathcal{L}}\bar{p} - \beta\bar{\mathcal{L}}\bar{v} - \bar{\mathcal{L}}\bar{q} - \gamma\bar{\mathcal{L}}\bar{w} + \tilde{\delta}, \end{aligned} \tag{11}$$

where

$$\bar{\mathcal{L}} = \begin{bmatrix} 1 & & & \\ -1 & 1 & & \\ & \ddots & \ddots & \\ & & -1 & 1 \end{bmatrix}. \tag{12}$$

Note that $[\bar{\mathcal{L}}]_{11} = 1$ because $\dot{\bar{v}}_1 = -\bar{p}_1 - \gamma\bar{v}_1$. Let $\xi = [\bar{p}^\top, \bar{v}^\top, \bar{q}^\top, \bar{w}^\top]^\top$, then (11) can be written in the following compact form:

$$\dot{\xi} = M\xi + \Delta, \tag{13}$$

where

$$M = \begin{bmatrix} \mathbb{O}_n & \mathbb{I}_n & \mathbb{O}_n & \mathbb{O}_n \\ -\bar{\mathcal{L}} & -\gamma\bar{\mathcal{L}} & \beta\bar{\mathcal{L}} & \beta\bar{\mathcal{L}} \\ \mathbb{O}_n & \mathbb{O}_n & \mathbb{O}_n & \mathbb{I}_n \\ -\beta\bar{\mathcal{L}} & -\beta\bar{\mathcal{L}} & -\bar{\mathcal{L}} & -\gamma\bar{\mathcal{L}} \end{bmatrix}, \text{ and } \Delta = \begin{bmatrix} o_n \\ \delta \\ o_n \\ \tilde{\delta} \end{bmatrix}.$$

In the following, we show that all vehicles converge to a desired spacing while moving with a desired velocity without considering the attack.

B. Convergence of the CVS without Cyber-attacks

In this subsection, we derive conditions on β and γ given in (5) that ensure the asymptotic stability of (13) for a CVS with a directed path communication topology in the absence of cyber-attack, that is $\Delta = [o_n^\top, o_n^\top, o_n^\top, o_n^\top]^\top$.

Theorem 1. *Consider the error dynamics of the CVS given in* (13)*. Let $\Delta = [o_n^\top, o_n^\top, o_n^\top, o_n^\top]^\top$. Let the digraph of the CVS be directed path where the root node be the leader of the network. Let the velocity of the leader v_o be the desired velocity. If $\gamma > 0$ and $\beta \geq 0$ with $\gamma^2 \geq \beta^2 + 4$,* *then* $\lim_{t\to\infty} v_i = {v_i}^* = v_o$*,* $\lim_{t\to\infty} p_{i-1} - p_i = d$*,* $\lim_{t\to\infty} w_i = {w_i}^* = v_o$*, and* $\lim_{t\to\infty} q_{i-1} - q_i = d$*.*

Proof. Consider the following transformation:

$$\tilde{\xi} = P\xi \tag{14}$$

where

$$P = \begin{bmatrix} \mathbb{O}_n & \mathbb{I}_n & \mathbb{O}_n & \mathbb{O}_n \\ \mathbb{O}_n & \mathbb{O}_n & \mathbb{O}_n & \mathbb{I}_n \\ \mathbb{I}_n & \mathbb{O}_n & \mathbb{O}_n & \mathbb{O}_n \\ \mathbb{O}_n & \mathbb{O}_n & \mathbb{I}_n & \mathbb{O}_n \end{bmatrix} \tag{15}$$

is a permutation matrix with $PP^\top = \mathbb{I}$. The time-derivative of (14) yields

$$\dot{\tilde{\xi}} = \tilde{M}\tilde{\xi},\ \tilde{M} = \begin{bmatrix} M_1 & M_2 \\ \mathbb{I}_{2n} & \mathbb{O}_{2n} \end{bmatrix} \tag{16}$$

where $M_1 = \Omega_1 \otimes \bar{\mathcal{L}},\ M_2 = \Omega_2 \otimes \bar{\mathcal{L}}$ and

$$\Omega_1 = \begin{bmatrix} -\gamma & \beta \\ -\beta & -\gamma \end{bmatrix},\ \Omega_2 = \begin{bmatrix} -1 & \beta \\ -\beta & -1 \end{bmatrix}.$$

To show the stability (16), we find the eigenvalues of $\tilde{M}$ given in (16). To that aim, we find the roots of

$$\det(\lambda\mathbb{I} - \tilde{M}) = \det(\lambda^2\mathbb{I} - \lambda M_1 - M_2) = 0.$$

The set of right-eigenvectors associated with the eigenvalues of Ω_1 and Ω_2 are the same. Therefore, using the results [14, Theorem 4.2.12], we conclude that the right-eigenvectors associated with the eigenvalues of M_1 and M_2 are the same. Using $\det(A) = \Pi_{i=1}^n \lambda_i(A)$, and the fact that the set of eigenvectors associated with the eigenvalues of M_1 and M_2 are the same, we have:

$$\det(\lambda\mathbb{I} - \tilde{M}) = \Pi_{i=1}^n(\lambda^2 - \lambda\lambda_i(M_1) - \lambda_i(M_2)) = 0. \tag{17}$$

The closed form of the eigenvalues $\tilde{M}$ is

$$\lambda_i \pm = \frac{\lambda_i(M_1) \pm \sqrt{(\lambda_i(M_1))^2 + 4\lambda_i(M_2)}}{2}. \tag{18}$$

Next, we find the eigenvalues of M_1 and M_2. The eigenvalues of M_1 are elements in the set $S_1 = \{\lambda(\Omega_1)\lambda_i(\bar{\mathcal{L}}) | i = 1, \cdots, n\}$ and the eigenvalues of M_2 are elements in the set $S_2 = \{\lambda(\Omega_2)\lambda_i(\bar{\mathcal{L}}) | i = 1, \cdots, n\}$. We see that $\lambda(\Omega_1) = -\gamma \pm \iota\beta$ and $\lambda(\Omega_2) = -1 \pm \iota\beta$. The eigenvalues of $\bar{\mathcal{L}}$ are all 1; that is $\lambda_i(\bar{\mathcal{L}}) = 1$ for all $i \in \{1, 2, \cdots, n\}$. For $\tilde{M}$ to be Hurwitz, we see from (18) that $\gamma > 0$. In addition, the real-part of the square-root term in (18) must be less than $\frac{\gamma}{2}$, which can be ensured by satisfying the condition $\gamma^2 \geq \beta^2 + 4$. Therefore, for any $\gamma > 0$ and $\beta \geq 0$ with $\gamma^2 \geq \beta^2 + 4$, the eigenvalues of $\tilde{M}$ are in the open left-half plane. Thus, the results follows. □

C. Convergence in the presence of cyber-attacks

In this subsection, we consider attacks on the sensors, actuators, and communication network of the CVS as shown in Fig. 1. Subsequently, we show that the distributed resilient control strategy given in (5) mitigates the effects of cyber-attacks. To show that this is indeed the case, we include the bounded attack in the error dynamics of CVS given in (13) with $\delta \neq o_n$, and $\tilde{\delta} \neq o_n$.

Again considering the transformation given in (14), and its time-derivative, we have

$$\dot{\tilde{\xi}} = \tilde{M}\tilde{\xi} + \tilde{\Delta}, \tag{19}$$

where $\tilde{\Delta} = P\Delta$, and P is given in (15). Next we show that by increasing β and γ, the effects of bounded attacks can be mitigated.

Theorem 2. *Consider a dynamical system given in* (19)*, where* $\tilde{M}$ *is given in* (16)*. Let* $\bar{\mathcal{L}}$ *be the matrix given in* (12)*. Then for sufficiently large and fixed* $\gamma > 0$*, as* $\beta > 0$ *increases while satisfying the condition* $\gamma^2 \geq \beta^2 + 4$*, the objective in* (4) *is achieved for any given* $\epsilon_1 > 0$ *and* $\epsilon_2 > 0$*.*

Proof. For sufficiently large $\gamma > 0$ and $\beta > 0$, with $\gamma^2 \geq \beta^2 + 4$, $\tilde{M}$ is Hurwitz, thus the solution of (19) can be written as

$$\tilde{\xi} = \underbrace{exp\left(t\tilde{M}\right)\tilde{\xi}(0)}_{\text{zero-input response}} + \int_0^t exp\left((t-\tau)\tilde{M}\right)\tilde{\Delta}\mathrm{d}\tau. \tag{20}$$

Next, using the inequality $\|exp\left(t\tilde{M}\right)\| \leq exp\left(\mu(\tilde{M})t\right)$ given in [10, Theorem 27], we estimate the solution of (20) by

$$\|\tilde{\xi}\| \leq exp\left(\mu(\tilde{M})t\right)\|\tilde{\xi(0)}\| + \int_0^t exp\left(\mu(\tilde{M})(t-\tau)\|\tilde{\Delta}\|\right)\mathrm{d}\tau.$$

Since $\tilde{M}$ is Hurwitz, thus, by [15, Lemma 2.3], we have $\mu(\tilde{M}) < 0$. Consequently the zero-input response in (20) goes to zero as $t \to \infty$. To make the role of β explicit in suppressing the effects of cyber-attacks, we design a *weighted logarithmic norm* of $\tilde{M}$ using a *scaled diagonal matrix* $H = \mathrm{diag}(\frac{1}{\beta}, \cdots, \frac{1}{\beta})$. Let $T \in \mathbb{C}^{4n\times 4n}$ be a nonsingular change of basis matrix such that $T\tilde{M}T^{-1} = \Lambda + U = J$ [16], where $U \in \{0, 1\}^{4n\times 4n}$ has off-diagonal entries equal to those of Jordan matrix J and diagonal entries are all zero.

Next, using [17, Lemma 2.7], we can write

$$\mu_H(\tilde{M}) = \mu(HT\tilde{M}T^{-1}H^{-1}) \leq \mu(\Lambda) + \frac{1}{\beta}\mu(U).$$

Specifying $\mu(\Lambda)$ by taking $\mu_2(\Lambda)$, and by increasing β, we get

$$\mu_H(\tilde{M}) \leq \Re\{\alpha(\tilde{M})\} + \epsilon, \tag{21}$$

where $\alpha(\tilde{M})$ is the largest eigenvalue of $\tilde{M}$, and $\epsilon > 0$ is any small positive number that the designer wish to fix.

Using (21), eq. (20) can be written as:

$$\left\|\tilde{\xi}(t)\right\| \leq \exp\left(-\underline{\lambda}t\right)\left\|\tilde{\xi}(0)\right\| + \frac{1}{\underline{\lambda}}\sup_{0\leq\tau\leq t}\left\|\tilde{\Delta}\right\|,\ \forall t \in \mathbb{R}_{\geq 0}, \tag{22}$$

where $\underline{\lambda} = \Re\{\alpha(\tilde{M})\} + \epsilon$, and $\Re\{\alpha(\tilde{M})\} = -\frac{\gamma}{2} + \frac{1}{2}\Re\{h_1(\gamma, \beta)\}$ with

$$h_1(\gamma, \beta) = \sqrt{\gamma^2 - \beta^2 - 4 + \iota(2\beta\gamma + 4\beta)}. \tag{23}$$

By increasing β such that $\gamma^2 \geq \beta^2 + 4$, $|\underline{\lambda}|$ increases. Thus the effects of cyber-attacks can be suppressed by increasing

β such that $\gamma^2 \geq \beta^2 + 4$. In fact, for any ϵ_1 and ϵ_2, we can choose γ and β such that $|p^*_{i-1} - p^*_i - d| \leq \epsilon_1,$ and $|v^*_i - v^*_0| \leq \epsilon_2$. This completes the proof. □

Remark 1. As shown in (22), one can use the knowledge/estimate of the worst case attack for choosing the value of gains γ, β.

D. Distributed attack detection and identification

In this subsection, inspired by the results in [18]–[20] we present distributed algorithms for the follower vehicle to detect and identify in real-time whether its sensor and/or the information that it received from its neighbor via the communication network is compromised. The idea is for follower vehicle i to estimate the $(i-1)$th vehicle's physical and virtual states using the (possibly compromised) redundant information received via the communication network, i.e., $I_{i-1,\theta}$ in (6) and the measurement of the radar $p_{i-1,i}$. Two detection tests will then be designed using those estimated states.

First, from the (possibly corrupted) information $I^a_{i-1,1}$ and $I^a_{i-1,2}$ defined in (7), (6), vehicle i estimates the value $\hat{p}_{i-1,i} = \hat{p}_{i-1} - p_i$ according to

$$\hat{p}_{i-1,i} = \frac{1}{\beta}\left[I^a_{i-1,2} + \frac{I^a_{i-1,1}}{\beta}\right] - p_i.$$

We then propose the first detector test which compares the estimated $\hat{p}_{i-1,i}$ using the information received from the communication network and the one obtained from the radar measurement.

$$\textbf{Detection test 1}: \quad \chi_{i,1} = p^a_{i-1,i} - \hat{p}_{i-1,i}. \tag{24}$$

Next, using the (possibly compromised) information $I_{i-1,4}$ and $I_{i-1,5}$, vehicle i estimates the virtual state w_{i-1} as follow

$$\hat{w}^1_{i-1} = \frac{1}{\gamma^2 + 2\beta^2}(\gamma I^a_{i-1,5} - \beta I^a_{i-1,4}).$$

Vehicle i can also estimate w_{i-1} from $I_{i-1,3}$ as follow

$$\hat{w}^2_{i-1} = \frac{1}{\beta} I^a_{i-1,3}.$$

We further propose the second detector test which compares the estimated $\hat{w}_{i-1}$ using the information received from the communication network.

$$\textbf{Detection test 2}: \quad \chi_{i,2} = \hat{w}^2_{i-1} - \hat{w}^1_{i-1}. \tag{25}$$

Vehicle i can then detect and identify attacks on its radar and information received from vehicle $i-1$ via the communication network using detection tests (24), (25) as summarized in the following proposition.

Proposition 1. *Using detection tests* (24), (25)*, vehicle i can detect and identify attacks on sensor and the communication link from vehicle* $i-1$ *as follows*

1) *If* $\chi_{i,1} \neq 0$ *and* $\chi_{i,2} = 0$*, then only the radar of vehicle i is being attacked*
2) *If* $\chi_{i,1} \neq 0$ *and* $\chi_{i,2} \neq 0$*, then the radar of vehicle* i *and/or the communication link from vehicle* $i-1$ *are being attacked*
3) *If* $\chi_{i,1} = 0$*, then either there is no attacks on both the sensor and communication link or the adversary launches a stealthy attack.*

Proof. We prove each statement as follows:

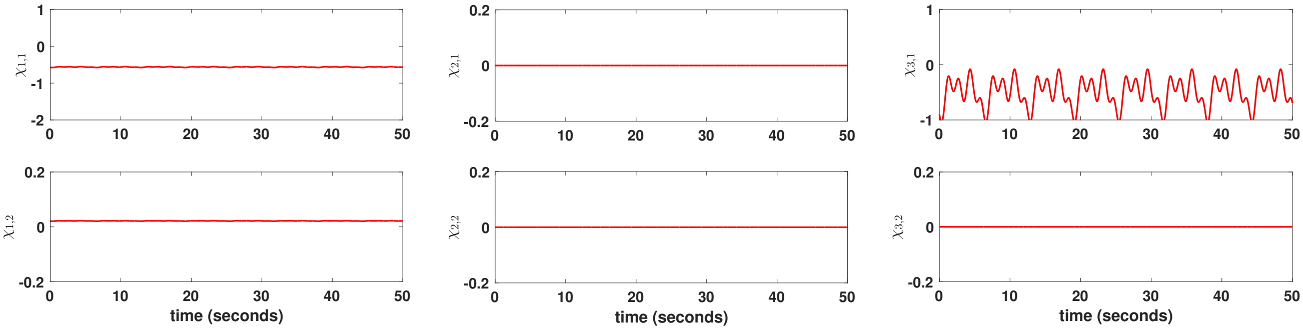
1) Since detection test $\chi_{i,1}$ compares the estimates using the information received from the communication network and the one measured by the radar, the mismatch between the two estimations alarms that either the radar or the communication or both of them are being attacked. Additionally, the detection test $\chi_{i,2}$ compares the estimations using the information transmitted via the communication network only. If these estimations match with each other, then we can conclude that the corresponding communication link is not compromised. Combining the results of detection test $\chi_{i,2}$ with $\chi_{i,1}$, it can then be concluded that only the radar is being attacked.
2) Similarly, $\chi_{i,2} \neq 0$ suggests that the communication link is being attacked. Hence, in combination with detection test $\chi_{i,1} \neq 0$, it can be concluded that the radar of vehicle i and/or the communication link from vehicle $i-1$ are being attacked.
3) $\chi_{i,1} = 0$ means that the estimation using information received via the communication network matches with the radar measurement. Hence, it can be concluded that either there is no attacks on both the sensor and communication link or the adversary launches a stealthy attack. However, it will be challenging for the adversary to launch stealthy attack as the structure of $I_{i-1,\theta}$ in (6) is a local information to each vehicle and unknown to the adversary.

□

IV. Simulations

Consider a network of five agents (one leader and four followers) connected with directed topology as given in Fig. 1. Each follower vehicle needs to maintain a desired spacing of $d = 1$ with its predecessor under attacks on the actuators, radars, and communication network as shown in Fig. 1. That is, the adversary inserts time-varying but bounded injections on the actuator of each follower vehicle, the radar sensor of follower vehicles $1, 3, 4$, and the communication links from the leader vehicle and from the follower vehicle 3. As shown in Fig. 2, the attacker is able to prevent the follower vehicles from maintaining a desired spacing.

Next, we implement the resilient distributed control in (5) for the follower vehicles with $\beta = 80$ and $\gamma = 100$. As depicted in Fig. 4, the resilient distributed control achieves the objective in (4) under unknown cyber-attacks. Finally, we demonstrate the performance of distributed attack detection and identification algorithm presented in Section III-D. Fig. 3 shows the detection tests $\chi_{i,1}, \chi_{i,2}$ of follower vehicles 1, 2, and 3 respectively. The follower vehicles are able to detect whether there are attacks on its radar and/or the communication link from their predecessor.



(a) Detection by follower vehicle 1

(b) Detection by follower vehicle 2

(c) Detection by follower vehicle 3

Fig. 3. Distributed attacked detection and identification using the strategies presented in Proposition 1. (a) the follower vehicle 1 can detect and identify that its radar and/or the communication link from the leader vehicle are being attacked since $\chi_{1,1} \neq 0, \chi_{1,2} \neq 0$; (b) the follower vehicle 2 can conclude that there is no attacks on both its radar and communication link from follower vehicle 1 since $\chi_{2,1} = 0$; (c) the follower vehicle 3 can detect and identify that only its radar is being attacked since $\chi_{3,1} \neq 0$ and $\chi_{3,2} = 0$.

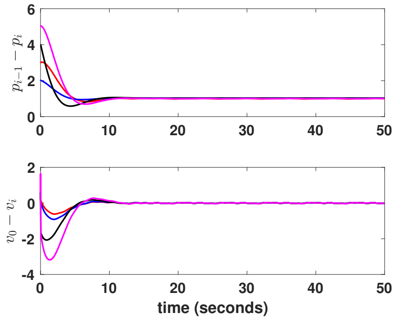


Fig. 4. Spacing between the follower vehicle and its predecessor (Top figure) and the error between the velocity of the leader vehicle and the follower vehicles (Bottom figure) under the proposed resilient distributed control (5) and in the presence of cyber-attacks. The spacings between successive vehicles are close to the desired spacing $d = 1$. Furthermore, the velocities of the follower vehicles converge close to the leader vehicle's constant velocity.

V. Conclusions and Future Works

The paper proposed a resilient platooning control for connected vehicles in the presence of adversaries. It is shown that the follower vehicles move at a desired velocity and keep a constant desired spacing between each others in the presence of attack on the communication network, actuators and the sensors of vehicles. The proposed resilient control also enables distributed and real-time attack detection and identification by the follower vehicles. Future works will consider higher-order individual vehicle's dynamics and leader vehicle with time varying velocity. Furthermore, we also aim to develop distributed control which ensures both resiliency and safety of the platoon.

References

[1] L. Xu, G. Yin, H. Zhang, *et al.*, "Communication information structures and contents for enhanced safety of highway vehicle platoons," *IEEE Transactions on vehicular Technology*, vol. 63, no. 9, pp. 4206–4220, 2014.

[2] Y. Bian, Y. Zheng, W. Ren, S. E. Li, J. Wang, and K. Li, "Reducing time headway for platooning of connected vehicles via v2v communication," *Transportation Research Part C: Emerging Technologies*, vol. 102, pp. 87–105, 2019.

[3] W. Ren and E. Atkins, "Distributed multi-vehicle coordinated control via local information exchange," *International Journal of Robust and Nonlinear Control*, vol. 17, no. 10-11, pp. 1002–1033, 2007.

[4] M. Safi, S. M. Dibaji, and M. Pirani, "Resilient coordinated movement of connected autonomous vehicles," *European Journal of Control*, vol. 64, p. 100613, 2022.

[5] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Transactions on Automatic Control*, vol. 63, no. 9, pp. 3159–3166, 2018.

[6] Y. Liu, Z. Li, and G. Guo, "Interaction network-based resilient consensus of connected vehicles against cyber-attacks," *IET Control Theory & Applications*, 2022.

[7] T. Yang, C. Murguia, D. Nešić, and C. Lv, "A robust cacc scheme against cyberattacks via multiple vehicle-to-vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 9, pp. 11184–11195, 2023.

[8] S. Boddupalli, A. S. Rao, and S. Ray, "Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15655–15672, 2022.

[9] Y. Liu, L. Xu, G. Cai, G. Yin, and F. Yan, "Distributed robust platooning control for heterogeneous vehicle group under parametric uncertainty and hybrid attacks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 5, pp. 5677–5689, 2023.

[10] C. A. Desoer and M. Vidyasagar, *Feedback systems: input-output properties*. SIAM, 2009.

[11] M. Iqbal, Z. Qu, and A. Gusrialdi, "Resilient dynamic average-consensus of multiagent systems," *IEEE Control Systems Letters*, vol. 6, pp. 3487–3492, 2022.

[12] P. Zhu, S. Jin, X. Bu, and Z. Hou, "Distributed data-driven control for a connected autonomous vehicle platoon subjected to false data injection attacks," *IEEE Trans. on Automation Science and Engineering*, 2023.

[13] B. Besselink and S. Knorn, "Scalable input-to-state stability for performance analysis of large-scale networks," *IEEE Control Systems Letters*, vol. 2, no. 3, pp. 507–512, 2018.

[14] R. A. Horn, R. A. Horn, and C. R. Johnson, *Topics in matrix analysis*. Cambridge university press, 1994.

[15] G.-D. Hu and M. Liu, "The weighted logarithmic matrix norm and bounds of the matrix exponential," *Linear algebra and its applications*, vol. 390, pp. 145–154, 2004.

[16] J. P. Hespanha, *Linear systems theory*. Princeton university press, 2018.

[17] F. Bullo, "Contraction theory for dynamical systems," *Kindle Direct Publishing*, vol. 1, pp. 979–8836646806, 2022.

[18] A. Gusrialdi and Z. Qu, "Cooperative systems in presence of cyber-attacks: a unified framework for resilient control and attack identification," in *American Control Conference*, pp. 330–335, 2022.

[19] A. Gusrialdi, M. Iqbal, and Z. Qu, "Towards resilient design of leader-following consensus with attack identification and privacy preservation capabilities," in *European Control Conference*, pp. 1–6, 2023.

[20] A. Gusrialdi and Z. Qu, "Resilient distributed optimization against cyber-attacks," *IEEE Control Systems Letters*, vol. 7, pp. 3956–3961, 2023.