Secure platooning control of automated vehicles under cyber attacks

Author

Mousavinejad, E, Vlacic, L

Published

2022

Journal Title

ISA Transactions

Version

Accepted Manuscript (AM)

DOI

10.1016/j.isatra.2022.02.046

Rights statement

Downloaded from

Funder(s)

ARC

Grant identifier(s)

LE0233830

Griffith Research Online

Secure Platooning Control of Automated Vehicles Under Cyber Attacks

Eman Mousavinejad[a,*], Ljubo Vlacic[a]

[a]*School of Engineering and Built Environment, Griffith University*

Abstract

This paper studies the problem of secure control of automated vehicles in a platoon-based driving pattern over a vehicular ad-hoc network (VANET) subject to various cyber attacks. The platoon under consideration is a convoy of a leader vehicle whose control input is unknown to its following vehicles and some follower vehicles with uncertain heterogeneous engine time constants, bounded disturbance and noise. First, a local estimator is developed for each follower vehicle so as to construct some confidence ellipsoidal estimation region always enclosing vehicular true state regardless of uncertain heterogenous engine time constants, bounded disturbance and noise. A convex optimization algorithm is proposed to find some optimal ellipsoidal sets and recursively solve out gain matrices of the local estimators. Then, a scalable control protocol employing the state estimates from its local and underlying neighboring estimators is designed to accomplish secure platooning control. Under the derived design technique, the resulting closed-loop platooning tracking errors are proven to remain in the vicinity of zero. Comparative studies are conducted to validate the efficacy of the proposed control method on achieving the satisfactory platooning performance by handling different attack strategies.

Keywords: Vehicle platooning, cyber attacks, secure control, set-membership estimation, vehicular ad-hoc networks (VANETs).

1. Introduction

The ever-growing demand in mobility of human and freight in modern societies has stimulated significant increase in the number of vehicles on the road and hence, exerted mounting pressure on the existing transportation infrastructure. As a consequence, global concern has escalated over current transportation systems due to road congestion and accidents, environmental pollution, and energy waste. As an effective intelligent transportation system (ITS) technology, vehicle platooning has been deemed as a promising

*Corresponding author
Email address: `eman.mousavinejad@griffith.edu.au` (Eman Mousavinejad)

means for enhancing the efficiency, safety, and reliability of road transportation. The central aim of vehicle platooning is to cooperatively regulate a convoy of automated vehicles to generate and maintain desired spacing policies and the same velocities (and/or accelerations) [1]. Modification of driving pattern into a platoon-based scheme allows more vehicles to share the capacity of a road with less accelerating or decelerating which further results in improving the traffic throughput and driving comfort [2–5]. Besides, due to the reduction of air resistance between successive vehicles, the vehicle platooning leads to a significant reduction in energy consumption and exhaust emissions [6–9].

The advent of a specific subset of mobile ad-hoc network for vehicle-to-vehicle (V2V) communication, namely vehicular-ad-hoc network (VANET), enables vehicles with wireless transceivers to exchange their key motion information including position, velocity, and acceleration with other vehicles in the platoon via various inter-vehicle communication topologies such as the bidirectional topology [11, 12], leader bidirectional topology [13], leader predecessor-following topology [10], and so on. Despite offering convenience of adopting different V2V communication topologies, the VANET technology faces security challenges as it may be vulnerable to malicious attacks due to its open access environment. Failure to preserve security of data transmitted over VANETs may lead to poor performance of vehicle platooning or even cause fatal accidents [14].

An adversary can deteriorate the performance of a communication network by compromising the security properties of data via generally two main attack strategies [15]: 1) denial-of-service (DoS) and 2) deception. Over the past decade, numerous studies have investigated the security of vehicle platoon systems subject to different cyber attack strategies. For instance, a distributed attack detection algorithm and a recovery mechanism based on a set-membership estimation approach are proposed in [16] to secure the vehicle platoon system against DoS and deception attacks. In [17], a real-time protocol is developed to detect and further estimate the effect of DoS attacks on V2V communication channels. To detect radio jamming DoS attacks on VANETs, a data-mining-based detection technique is developed in [18]. A secure distributed adaptive control algorithm for a platoon of vehicles connected via directed V2V communication subject to intermittent DoS attacks is presented in [19]. Various secure distributed estimation and control approaches are proposed in [20–26] to cope with deception attacks on sensory data transmitted over V2V communication channels. For example, in [21], a residual signal is generated by a distributed adaptive sliding mode observer so as to detect false data injection (FDI) attacks and further estimate the attack magnitude.

Although fruitful results are available in the literature for secure platooning control of vehicular systems, some challenging issues still remain open. The *first* one is that a large proportion of existing results concentrate on a specific type of attack due to the scarcity of a unified attack framework for simultaneously modeling different attack strategies, while demanding less prior knowledge of attacks. Typically, two attack models that have been explored in the multi-vehicle system literature include: 1) stochastic models [27, 28] requiring specific statistical properties of attack signals; and 2) switching system models [29] where the attack occurrence frequency is often constrained. To ensure a certain level of security over unsafe VANETs, the priori assumptions on modeling of attacks need to be satisfied so that the developed secure platooning control approaches guarantee a safe driving condition. Therefore, how can one develop a secure platooning control protocol which delivers a sufficient level of safe performance under different attack strategies with less modeling knowledge of attack signals? The *second* issue is that a multitude of studies focus on designing a platoon control protocol with direct use of full and accurate vehicular state [10, 13, 29, 30]. However, acquiring the complete and exact state information of a vehicle moving in a realistic driving scenario is quite difficult and may even be impossible [31]. Thus, it is not uncommon to access partial vehicular state information which necessitates the requirement of a state estimation technique. It is noteworthy that the design of a suitable state estimation technique generally pertains to available knowledge of the actual system model, the noise/distrubance type and assumption [32]. For example, probabilistic state estimation strategies, particularly Kalman filtering and its variants [33–37], are only accurate in a practical scenario where statistical properties of noise/distrubance are well known and there exist small amount of dynamical uncertainties. On the other hand, deterministic state estimation strategies such as H_∞ estimation [38–40] only preserve the worse-case performance of the resulting estimation error system. In vehicle platooning, however, a platoon may consists of nonidentical vehicles with different parameters and their driving conditions can be complex and varying. Hence, the vehicular uncertainties and empirically pre-specified statistical properties of noise/disturbance jeopardize the state estimation performance and the results may not be always reliable. Thus, how can one develop an effective platoon control protocol employing the vehicular state estimates enclosed by a confidence region so as to ensure the inclusion of the vehicular true states while there exist exogenous disturbance, parameter uncertainties, and measurement noise?

In this study, we aim to address the questions mentioned above. More specifically, we study the problem of secure platooning control of vehicular systems with uncertain dynamics due to the coexistence of heterogenous engine time constants, an unknown leader control input, unknown-but-bounded (UBB) measurement noise, and UBB exogenous disturbance. The novelty of this study lies on a unified set-membership state estimator design and secure platooning controller design against various cyber attack strategies. The proposed secure platooning control is capable of handling various V2V communication topologies which are unsafe and may be compromised by different attack strategies. The main contributions of this paper are threefold.

1. *A general model of vehicle longitudinal dynamics* is considered to incorporate the simultaneous presence of heterogenous engine time constants, an unknown leader control input, UBB exogenous disturbance inputs on each follower vehicle whose sensory outputs suffer from UBB measurement noise.
2. *A local set-membership estimator* is developed for each follower vehicle to provide some reliable confidence region bounded by an ellipsoid. The confidence region contains all possible state estimates while always guaranteing to enclose vehicular true states subject to bounded uncertainties resulting from heterogenous engine time constants, UBB exogenous disturbance and measurement noise. The only requirement is to gain knowledge of some hard bounds on the uncertain signals.
3. *A scalable secure platooning control protocol* is designed to combat a class of amplitude-bounded attacks. Specifically, different attack strategies can be incorporated in a unified framework since only the hard bounds of the attack signals are needed for the stability analysis of the proposed secure control system rather than its design procedure. Furthermore, each follower vehicle only requires the state estimates provided by its local estimator and those of its underlying neighbors so as to compute control design parameters. Thus, the control design criterion is free of platoon scale. Under the theoretical stability analysis of the proposed control protocol, it is proven that the closed-loop platoon tracking errors are uniformly ultimately bounded.

Notations: The n-dimensional Euclidean space is denoted by $\mathbb{R}^n$. $\mathbb{N}$ represents the set of nonnegative integers. $\|\cdot\|$ and $\|\cdot\|_F$ stand for the Euclidean norm and the Frobenius norm, respectively. The column vector $[x_1^T, x_2^T, \ldots, x_n^T]^T$ is represented by $\mathrm{col}_n\{x_i\}$. For a matrix $M \in \mathbb{R}^{m\times n}$, $\underline{\sigma}(M)$ and $\bar{\sigma}(M)$ denote its minimum and maximum singular values, respectively. $\otimes$ denotes the Kronecker product. Dimensions of matrices, if not specified, are assumed to be compatible.

2. Problem formulation

2.1. Vehicle longitudinal dynamics

Consider a vehicular platooning system including one leader numbered by 0 and N followers numbered by $i \in \mathcal{V}_N = \{1, 2, \ldots, N\}$, where vehicles are traveling on a straight and flat road. The longitudinal dynamics of vehicle i can be described by the widely employed linearized third-order model [12, 13, 41, 42] as

$$\tau_i \dddot{p}_i(t) + \ddot{p}_i(t) = u_i(t) + w_i(t), \tag{1}$$

where the vehicle i's position, velocity, and acceleration are denoted by $p_i(t) \in \mathbb{R}$, $\dot{p}_i(t) = v_i(t) \in \mathbb{R}$, and $\ddot{p}_i(t) = a_i(t) \in \mathbb{R}$, respectively; τ_i is the vehicle i's engine time constant; and $w_i(t) \in \mathbb{R}^{n_w}$ denotes the UBB exogenous disturbance input on vehicle i.

To deal with the heterogenous parameter τ_i in (1), we estimate the vehicle i's engine time constant with a fixed nominal value τ_0, which is identical for all vehicle $i \in \mathcal{V}_{N+1}$, and an estimation error $\Delta\tau_i$ as $\tau_i = \tau_0 + \Delta\tau_i$. Thus, (1) can be written as

$$\tau_0 \dot{a}_i(t) = -a_i(t) + u_i(t) + w_i(t) - \phi_i(t), \tag{2}$$

where $\phi_i(t) = \Delta\tau_i \dot{a}_i(t)$, which is unknown but assumed to be bounded with a known bound as $\|\phi_i(t)\| \leq \phi_M$, $\phi_M > 0$. Such an assumption is mild as the real-time jerk $\dot{a}_i(t)$ of each vehicle during practical platooning should not exceed certain limit in order to guarantee driving comfort.

Recalling (1) and (2), and denoting the stacked state vector of vehicle i as $x_i(t) = [p_i(t), v_i(t), a_i(t)]^T$, the continuous-time state-space dynamic model of vehicle i can be written as $\dot{x}_i(t) = A_c x_i(t) + B_c(u_i(t) - \phi_i(t) + w_i(t))$, where $A_c = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & \frac{-1}{\tau_0} \end{bmatrix}$ and $B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau_0} \end{bmatrix}$. In this study, the sampled vehicular data are considered for the analysis and design procedures. Thus, considering the sampling period as $h > 0$ along with a zero-order hold mechanism, the discrete-time longitudinal dynamic model for each vehicle $i \in \mathcal{V}_{N+1}$ is given by

$$x_i(k+1) = Ax_i(k) + B(u_i(k) - \phi_i(k) + w_i(k)), \tag{3}$$

where $x_i(k) = [p_i(k), v_i(k), a_i(k)]^T \in \mathbb{R}^{n_x}$, with $n_x = 3$, $A = e^{A_c h} = \begin{bmatrix} 1 & h & 0 \\ 0 & 1 & h \\ 0 & 0 & e^{-\frac{h}{\tau_0}} \end{bmatrix}$, $B = \int_0^h e^{A_c s} ds\ B_c = \begin{bmatrix} 0 \\ 0 \\ 1 - e^{-\frac{h}{\tau_0}} \end{bmatrix}$, and $w_i(k)$ belongs to the specified ellipsoid as

$$\mathcal{W}_k^i \triangleq \{w_i(k) : w_i^T(k) W_{i,k}^{-1} w_i(k) \leq 1\}. \tag{4}$$

where $W_{i,k} = W_{i,k}^T > 0$ is a time-varying matrix of compatible dimension.

Without loss of generality, we suppose $w_0(k) = 0$ on the leader vehicle and its engine time constant τ_0 takes the nominal value as $\tau_0 = \tau_0$, and hence $\phi_0(k) = 0$. However, the leading vehicle can take a time-varying input $u_0(k)$, which is not accessible to any follower vehicle in the fleet. Furthermore, it is assumed that $\|u_0(k)\| \leq u_M$ with $u_M \geq 0$, which is an unknown constant.

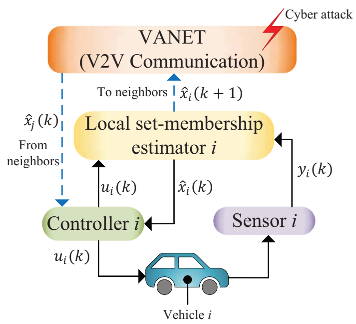


Figure 1: Schematic of set-membership-estimator-based platooning control for vehicle $i \in \mathcal{V}_N$ over a VANET under cyber attacks.

2.2. V2V communication modeling

Considering each vehicle as a node, the information exchange among the follower vehicles is considered to be bidirectional and hence, its corresponding V2V communication topology can be depicted by an undirected graph $\mathcal{G} = \{\mathcal{V}_N, \mathcal{E}, \mathcal{A}\}$, where $\mathcal{V}_N$ is an index set of N nodes specifying the follower set, $\mathcal{E} \subseteq \mathcal{V}_N \times \mathcal{V}_N$ describes the edge set, and $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$ is the weighted adjacency matrix. An edge $(i, j) \in \mathcal{E}$ indicates that there exists a bidirectional link between the follower vehicles i and j, which means vehicle i can both receive and send information from and to vehicle j. The adjacency element a_{ij} denotes the coupling gain of the V2V information link, which satisfies $(i, j) \in \mathcal{E} \Leftrightarrow a_{ij} > 0$ and otherwise $a_{ij} = 0$. Self-loops are excluded, i.e., $a_{ii} = 0$ for all $i \in \mathcal{V}_N$. Graph $\mathcal{G}$ is connected if, for any $i, j \in \mathcal{V}_N$, there exists a path from node i to node j, where a path from node i to node j is a sequence of edges (i, i_1), (i_1, i_2), $\ldots$, (i_p, j). The Laplacian matrix of graph $\mathcal{G}$ is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A} \in \mathbb{R}^{N\times N}$, where $\mathcal{D} = \mathrm{diag}\{d_1, \ldots, d_N\}$ is the degree matrix of $\mathcal{G}$ with $d_i = \sum_{j=1}^{N} a_{ij}$. $N_i = \{j \in \mathcal{V}_N : (i, j) \in \mathcal{E}\}$ defines a set of nodes which are vehicle i's neighbors.

The leader vehicle indexed by 0 receives no information from the follower vehicles and it can only send its information to a subset of the follower vehicles. Let $a_{i0} > 0$, $i \in \mathcal{V}_N$ imply that vehicle i is pinned to the leader, that is, it can directly receive information from the leader vehicle otherwise $a_{i0} = 0$. Denote $\mathcal{A}_0 = \mathrm{diag}\{a_{10}, a_{20}, \ldots, a_{N0}\}$ and $\mathcal{H} = \mathcal{L} + \mathcal{A}_0$.

Assumption 1. Graph $\mathcal{G}$ is connected and at least one of the follower vehicles is pinned to the leader.

Lemma 1. If Assumption 1 is satisfied, then $\mathrm{trace}(\mathcal{A}_0) > 0$ and $\mathcal{H}$ is a positive definite matrix.

The follower vehicle $i \in \mathcal{V}_N$ in the platoon is equipped with onboard sensors which first collect the real-time motion information of vehicle i and then transmit it to the local set-membership estimator i so as to estimate the complete vehicle i's state vector as depicted in Fig. 1. The vehicle i's state estimates are then shared via VANET with their associated neighboring vehicles defined by a prescribed topology. The measurement output from the onboard sensor on the ith follower vehicle is given as

$$y_i(k) = Cx_i(k) + D\vartheta_i(k), \tag{5}$$

where $y_i(k) \in \mathbb{R}^{n_y}$, $C \in \mathbb{R}$ and $D \in \mathbb{R}$ are known matrices with compatible dimensions, and $\vartheta_i(k)$ is the UBB measurement noise enclosed by the following ellipsoid:

$$\mathcal{V}_k^i \triangleq \{\vartheta_i(k) : \vartheta_i^T(k)V_{i,k}^{-1}\vartheta_i(k) \leq 1\}, \tag{6}$$

where $V_{i,k} = V_{i,k}^T > 0$ represents a time-varying matrix of compatible dimension.

2.3. Local set-membership estimator

In the following, set-membership estimators are constructed for each vehicle in the platoon so as to estimate their state vector information, i.e., position, velocity, and acceleration components. Specifically, our interest is to design the local set-membership estimator $i \in \mathcal{V}_N$ of the form

$$\hat{x}_i(k+1) = A\hat{x}_i(k) + Bu_i(k) + L_{i,k}(y_i(k) - \hat{y}_i(k)) \tag{7}$$

for all $k \in \mathbb{N}$, where $\hat{x}_i(k) \in \mathbb{R}^{n_x}$ is the estimate of vehicle i's true state $x_i(k)$; $\hat{y}_i(k) = C\hat{x}_i(k)$ is the output of the local estimator i; and $L_{i,k}$ is the time-varying gain matrix to be determined. Let $\hat{x}_i(0) = \hat{x}_{i,0}$ be the given initial condition of estimator i. The initial state of vehicle i, $x_i(0) = x_{i,0}$, is assumed to belong to a given ellipsoid

$$\mathcal{X}_0^i \triangleq \{x_{i,0} : (x_{i,0} - \hat{x}_{i,0})^T P_{i,0}^{-1}(x_{i,0} - \hat{x}_{i,0}) \leq 1\} \tag{8}$$

for all $i \in \mathcal{V}_N$, where $P_{i,0} = P_{i,0}^T > 0$ is a known matrix representing the ellipsoid's initial shape matrix.

Now, the concerned local set-membership state estimation problem can be defined as follows.

Definition 1. For vehicle i expressed by (3) and (5) in the presence of bounded parameter uncertainty $\phi_i(k)$, UBB exogenous disturbance $w_i(k)$, and UBB measurement noise $\vartheta_i(k)$, the set-membership state estimation is said to be achievable if there exists a gain sequence $L_{i,k}$ in such a way as to confine the vehicle i's state $x_i(k+1)$ $\forall i \in \mathcal{V}_N$, in a state estimation ellipsoid obtained by estimator i as [43–45]

$$\mathcal{X}_{k+1}^i \triangleq \{x_i(k+1) : e_i^T(k+1)P_{i,k+1}^{-1}e_i(k+1) \leq 1\}, \tag{9}$$

which always encloses the vehicle i's true state for all $k \in \mathbb{N}$. $e_i(k+1) = x_i(k+1) - \hat{x}_i(k+1)$ denotes the local state estimation error at time $k+1$, $\hat{x}_i(k+1)$ is the center of the state estimation ellipsoid $\mathcal{X}_{k+1}^i$ calculated by estimator i in (7), and $P_{i,k+1} = P_{i,k+1}^T > 0$ is its time-varying shape matrix.

2.4. A set-membership-estimator-based distributed platooning control law

Let $\hat{p}_i(k)$, $\hat{v}_i(k)$, $\hat{a}_i(k)$ be the estimates of vehicle i's true state components $p_i(k)$, $v_i(k)$, and $a_i(k)$, respectively, computed by the local set-membership estimator i. Further, denote $\hat{p}_0(k) = p_0(k)$, $\hat{v}_0(k) = v_0(k)$, and $\hat{a}_0(k) = a_0(k)$. Using the state estimates of neighboring vehicles $j \in \mathcal{N}_i$, which are fed into the local estimator i, we are interested in the control protocol for each vehicle $i \in \mathcal{V}_N$ as

$$u_i(k) = K \sum_{j \in \mathcal{N}_i} a_{ij}(\hat{x}_i(k) - \tilde{x}_j(k) - d_{i,j}) + a_{i0}(\hat{x}_i(k) - \tilde{x}_0(k) - d_i), \tag{10}$$

where K is the control gain matrix to be designed; $d_i = [d_{i,0}, 0, 0]^T$ with $d_{i,0}$ denoting the desired distance between vehicle i and the leader; $d_{i,j} = d_i - d_j$ is a vector with its first component representing the desired distance between vehicle i and vehicle j; by setting $d_{i,0} = i \cdot d$, we consider a constant spacing policy, that is $d_{i+1,i} = d > 0$; $\tilde{x}_j(k)$ and $\tilde{x}_0(k)$ are the state estimates of vehicle i's underlying neighbors and the leading vehicle specified by $\mathcal{N}_i$ and $\mathcal{A}_0$, respectively, which may be tampered by an adversary.

2.5. Cyber attacks models

Given that a distinguished feature of the vehicular platooning system defines as the cooperative tasks among vehicles, a crafty adversary may derive a benefit from such a fact to capture a subset of vehicles in the platoon and manipulate their state estimates prior to being transmitted into their neighboring vehicles over the VANET. For example, the VANET's normal functioning may be violated by an adversary by performing DoS attacks which render vehicular data unavailable. Typically, this can be accomplished by flooding the VANET with unnecessary information which results in channel congestion and hence, jamming the network. Furthermore, an adversary may decide to compromise the confidentiality and integrality of vehicular data through some deception attacks in an effort to manipulate the platooning system in to his/her desired behavior. To perform such an attack, the adversary must also be capable of launching a disclosure attack so as to accumulate necessary knowledge of vehicular data in a timely fashion. Two typical deception attacks on VANETs that have attracted much attention are FDI attacks and replay attacks. In FDI attacks, an adversary launches the disclosure attack and simultaneously adds the bogus information into the content of the data transmitted over the VANET. Replay attacks, however, are implemented in two phases, where the adversary first records the exchanged data through the disclosure attack and then replays the recorded data in such a way as to mislead the platoon with the outdated vehicular information.

To present a unified model of these various attack strategies tampering with the transmitted vehicular state estimates over the wireless V2V communication, let $\mathcal{V}_a = \{i_1, \ldots, i_p\} \subseteq \mathcal{V}_{N+1}$ be the set of vehicles captured by the adversary and $\mathcal{V}_a^c$ be the complement of that set, i.e., $\mathcal{V}_a^c = \mathcal{V}_{N+1} - \mathcal{V}_a$. The state estimates of the vehicles in the sets $\mathcal{V}_a$ and $\mathcal{V}_a^c$ can be modeled as

$$\tilde{x}_i(k) = \begin{cases} \hat{x}_i(k) + \varpi_i(k), & i \in \mathcal{V}_a \\ \hat{x}_i(k), & i \in \mathcal{V}_a^c \end{cases} \tag{11}$$

where $\varpi_i(k) \in \mathbb{R}^{n_x}$ is an attack signal delicately designed by the adversary and assumed to be bounded as $\|\varpi_i(k)\| < \varpi_M$, where $\varpi_M \geq 0$ is an unknown constant. This is a mild assumption since a realistic adversary has limited budget and energy to construct an attack signal. Note that the attack signal $\varpi_i(k)$ incorporates different attack strategies, namely, DoS, replay, and FDI attacks, as its special cases, which will be exemplified in Section 5.

2.6. Problem to be addressed

Define the platoon tracking error of each follower vehicle $i \in \mathcal{V}_N$ as $\delta_i(k) \triangleq [\delta_{pi}(k), \delta_{vi}(k), \delta_{ai}(k)]^T = x_i(k) - x_0(k) - \bar{d}_{i,0}$, where $\delta_{pi}(k) = p_i(k) - p_0(k) - d_{i,0}$, $\delta_{vi}(k) = v_i(k) - v_0(k)$, and $\delta_{ai}(k) = a_i(k) - a_0(k)$ represent the position, velocity, and acceleration tracking errors, respectively. From the local set-membership state estimation error at time k, it is easy to confirm that $\hat{x}_i(k) = x_i(k) - e_i(k)$. Then, recalling (3) and (10), we have

$$\delta_i(k+1) = A\delta_i(k) + BK \sum_{j \in \mathcal{N}_i} a_{ij}((\delta_i(k) - \delta_j(k)) - (e_i(k) - e_j(k))) + a_{i0}\delta_i(k) - \Omega_i(k), \tag{12}$$

where $\Omega_i(k) = \sum_{j \in \mathcal{N}_i} a_{ij}\varpi_j(k) + a_{i0}\varpi_0(k)$, which is bounded as $\|\Omega_i(k)\| \leq \Omega_M$ with an unknown constant $\Omega_M > 0$ since $\|\varpi_i(k)\| < \varpi_M$, $\forall i \in \mathcal{V}_{N+1}$.

The problem to be tackled in this paper can now be stated as: For a platooning system of $N+1$ vehicles with their dynamics described by (3) over a bidirectional V2V communication topology satisfying Assumption 1, the objectives are 1) to design a local set-membership estimator (7) for each follower vehicle i through computing an appropriate matrix sequence $P_{i,k+1}$ and the state estimate $\hat{x}_i(k+1)$ so as to find a confidence state estimation ellipsoid, $\mathcal{X}_{k+1}^i$, which always encloses the true state of vehicle i; and 2) to design a distributed platooning control protocol (10) such that the platoon tracking error in (12) is uniformly ultimately bounded in the coexistence of heterogeneous engine time constant τ_i, UBB exogenous disturbance $w_i(k) \in \mathcal{W}_k^i$, UBB measurement noise $\vartheta_i(k) \in \mathcal{V}_k^i$, unknown leader control input $u_0(k)$, and cyber attacks in the form of (11).

3. Local set-membership estimator design

For each follower vehicle i in the platoon, our interest lies in designing a local set-membership estimation technique which computes some confidence ellipsoidal estimation sets enclosing the vehicular state based on the measurement of the vehicle i's onboard sensor. Thus, we next present Theorem 1 which outlines the sufficient condition on the existence of the desired local estimator in the form of (7) such that (9) holds.

Theorem 1. *For the vehicle i's dynamic model in the form of (3) and (5) subject to $\|\phi_i(k)\| \le \phi_M$, $w_i(k) \in \mathcal{W}_k^i$, and $\vartheta_i(k) \in \mathcal{V}_k^i$, suppose that the vehicle i's true state at time k is enclosed by its state estimation ellipsoid $\mathcal{X}_k^i$. Then, the current state of vehicle i, $x_i(k+1)$, is guaranteed to reside in the state estimation ellipsoid $\mathcal{X}_{k+1}^i$ if there exist matrix sequences $P_{i,k+1}$, $L_{i,k}$, and scalar sequences $\mu_m^i(k) > 0$, $m = 1, \ldots, 4$, such that the convex optimization problem*

$$\min_{P_{i,k+1}, L_{i,k}, \mu_m^i(k)} \operatorname{trace}(P_{i,k+1}) \quad \textit{subject to} \begin{bmatrix} -P_{i,k+1} & \Pi_{i,k} \\ * & \Psi_{i,k} \end{bmatrix} \le 0 \tag{13}$$

is solvable for all $k \in \mathbb{N}$ and $\forall i \in \mathcal{V}_N$, where

$$\Pi_{i,k} = \begin{bmatrix} 0 & (A - L_{i,k}C)E_{i,k} & B & -L_{i,k}D & -B \end{bmatrix},$$

$$\Psi_{i,k} = diag\{-1 + \sum_{m=1}^{3} \mu_m^i(k) + \mu_4^i(k)\phi_M^2, -\mu_1^i(k)I_{n_x}, -\mu_2^i(k)W_{i,k}^{-1}, -\mu_3^i(k)V_{i,k}^{-1}, -\mu_4^i(k)I_{n_u}\}.$$

Proof. Suppose that the follower vehicle i's true state at time k, $x_i(k)$, is confined in $\mathcal{X}_k^i$ and satisfies $(x_i(k) - \hat{x}_i(k))^T P_{i,k}^{-1}(x_i(k) - \hat{x}_i(k)) \le 1$. Applying a Cholesky factorization, one can obtain $P_{i,k} = E_{i,k}E_{i,k}^T$. Defining $\alpha_i(k) = E_{i,k}^{-1}(x_i(k) - \hat{x}_i(k))$, it is easy to verify that

$$\alpha_i^T(k)\alpha_i(k) = (x_i(k) - \hat{x}_i(k))^T P_{i,k}^{-1}(x_i(k) - \hat{x}_i(k)) \le 1. \tag{14}$$

Thus there exists a vector $\alpha_i(k)$ satisfying $\|\alpha_i(k)\| \leq 1$ such that

$$x_i(k) = \hat{x}_i(k) + E_{i,k}\alpha_i(k). \tag{15}$$

From (3), (5), and (15), the follower vehicle i's state estimation error at time $k+1$ can be calculated as

$$\begin{aligned} e_i(k+1) &= A(x_i(k) - \hat{x}_i(k)) - B\phi_i(k) + Bw_i(k) - L_{i,k}(C(x_i(k) - \hat{x}_i(k)) + D\vartheta_i(k)) \\ &= (A - L_{i,k}C)E_{i,k}\alpha_i(k) - B\phi_i(k) + Bw_i(k) - L_{i,k}D\vartheta_i(k) \end{aligned} \tag{16}$$

Denoting $\zeta_i(k) = [1,\ \alpha_i^T(k),\ w_i^T(k),\ \vartheta_i^T(k),\ \phi_i^T(k)]^T$, from (16), one has $e_i(k+1) = \Pi_{i,k}\zeta_i(k)$. Thus, the quadratic estimation error $e_i^T(k+1)P_{i,k+1}^{-1}e_i(k+1)$ in (9) can be restated as

$$\zeta_i^T(k)\left(\Pi_{i,k}^T P_{i,k+1}^{-1}\Pi_{i,k} + \Phi\right)\zeta_i(k) \leq 0, \tag{17}$$

where $\Phi = \mathrm{diag}\{-1, 0, 0, 0, 0\}$.

From (14), (4), (6), and $\|\phi_i(k)\| \leq \phi_M$, we have the following constraints that $\zeta_i^T(k)\Upsilon_{1,k}\zeta_i(k) \geq 0$, $\zeta_i^T(k)\Upsilon_{2,k}\zeta_i(k) \geq 0$, $\zeta_i^T(k)\Upsilon_{3,k}\zeta_i(k) \geq 0$, $\zeta_i^T(k)\Upsilon_{4,k}\zeta_i(k) \geq 0$, where $\Upsilon_{1,k} = \mathrm{diag}\{1, -I_{n_x}, 0, 0, 0\}$, $\Upsilon_{2,k} = \mathrm{diag}\{1, 0, -W_{i,k}^{-1}, 0, 0\}$, $\Upsilon_{3,k} = \mathrm{diag}\{1, 0, 0, -V_{i,k}^{-1}, 0\}$, $\Upsilon_{4,k} = \mathrm{diag}\{\phi_M^2, 0, 0, 0, -I_{n_u}\}$.

Applying $\mathcal{S}$-procedure, (17) holds if there exist positive scalar sequences $\mu_m^i(k)$, $m = 1, \ldots, 4$, such that

$$\Pi_{i,k}^T P_{i,k+1}^{-1}\Pi_{i,k} + \Phi + \mu_1^i(k)\Upsilon_{1,k} + \mu_2^i(k)\Upsilon_{2,k} + \mu_3^i(k)\Upsilon_{3,k} + \mu_4^i(k)\Upsilon_{4,k} \leq 0. \tag{18}$$

Applying the Schur Complement, the inequality in (18) is equivalent to the inequality in (13), which does not guarantee an optimal ellipsoid. To obtain some optimal ellipsoids, an optimization problem is introduced in (13). This completes the proof. □

Remark 1. By Theorem 1, the proposed local set-membership estimation problem can be converted into the feasibility problem of a group of recursive linear matrix inequalities (RLMIs) in (13). By virtue of Theorem 1, the gain matrix of estimator i, $L_{i,k}$, can be recursively solved out and the optimal state estimation ellipsoids $\mathcal{X}_{k+1}^i$ in (9) can be determined so as to enclose the true state of vehicle i in the presence of bounded parameter uncertainty, UBB exogenous disturbance and measurement noise. Hence, Theorem 1 establishes a design criterion for the desired local set-membership state estimator in (7) and confidence state estimation ellipsoids in (9). Due to the linearity of the inequality in (13) regarding the variables P_{k+1}^i, $L_{i,k}$, and $\mu_m^i(k)$,

$m = 1, \ldots, 4$, the optimization problem (13) can be solved by some existing semidefinite programming at each time step k. The interior-point algorithm usually has a polynomial-time complexity $\mathcal{O}(\mathcal{R}\mathcal{M}^3)$, where $\mathcal{R}$ is the total row size of the RLMI (13) and $\mathcal{M}$ is the total number of scalar decision variables of the RLMI. Therefore, the computational complexity of the developed RLMI (13) depends polynomially on the dimensions of vehicles' parameter variables including the number of states n_x, the number of control inputs n_u, the number of exogenous disturbance inputs n_w, and the number of measurement outputs and noises n_y, and n_ϑ, respectively.

4. Stability analysis and control design

To facilitate the following analysis, let $\delta(k) = \mathrm{col}_N^i\{\delta_i(k)\}$, $\varepsilon(k) = \mathrm{col}_N^i\{\varepsilon_i(k)\}$, $e(k) = \mathrm{col}_N^i\{e_i(k)\}$, $\Omega(k) = \mathrm{col}_N^i\{\Omega_i(k)\}$, $\xi_i(k) = w_i(k) - u_0(k) - \phi_i(k)$, and $\xi(k) = \mathrm{col}_N^i\{\xi_i(k)\}$. The compact form of the platoon tracking error system can be obtained as

$$\delta(k+1) = (I_N \otimes A + \mathcal{H} \otimes BK)\delta(k) - (\mathcal{H} \otimes BK)e(k) - (I_N \otimes BK)\Omega(k) + (I_N \otimes B)\xi(k). \tag{19}$$

According to Lemma 1, matrix $\mathcal{H} \in \mathbb{R}^{N\times N}$ has N positive eigenvalues denoted by λ_i, $i = 1, \ldots, N$, which can be formed in sequence as $0 < \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_N$. Also, a unitary matrix U can be found such that $U^{-1}\mathcal{H}U = \mathrm{diag}\{\lambda_1, \lambda_2, \ldots, \lambda_N\} \triangleq J_{\mathcal{H}}$. Letting $\bar{\delta}(k) = (U^{-1} \otimes I_{n_x})\delta(k)$, $\bar{e}(k) = (U^{-1} \otimes I_{n_x})e(k)$, $\bar{\Omega}(k) = (U^{-1} \otimes I_{n_x})\Omega(k)$, $\bar{\xi}(k) = (U^{-1} \otimes I_{n_x})\xi(k)$, one can restate (19) as

$$\bar{\delta}(k+1) = (I_N \otimes A + J_{\mathcal{H}} \otimes BK)\bar{\delta}(k) - (J_{\mathcal{H}} \otimes BK)\bar{e}(k) - (I_N \otimes BK)\bar{\Omega}(k) + (I_N \otimes B)\bar{\xi}(k). \tag{20}$$

According to [46], the stability analysis of the compact error system of N vehicles in (20) is equivalent to the stability analysis of the error system of single vehicle $i \in \mathcal{V}_N$ in the form of

$$\bar{\delta}_i(k+1) = (A + \lambda_i BK)\bar{\delta}_i(k) - \lambda_i BK\bar{e}_i(k) - BK\bar{\Omega}_i(k) + B\bar{\xi}_i(k) \tag{21}$$

where $\|\bar{e}_i(k)\| \leq \bar{e}_M$, $\|\bar{\Omega}_i(k)\| \leq \bar{\Omega}_m$, and $\|\bar{\xi}_i(k)\| \leq \bar{\xi}_M$ with unknown constants $\bar{e}_M > 0$, $\bar{\Omega}_m > 0$, and $\bar{\xi}_M > 0$.

Theorem 2. *Suppose the vehicular platoon in (3) over a VANET communication topology satisfies Assumption 1. For a given matrix K and a positive constant η, if there exist matrices $P_\delta > 0$ and Q such that*

$$\Lambda_i < 0, \quad i \in \mathcal{V}_N \tag{22}$$

holds, where Λ_i is a 2×2 symmetric block matrix with $\Lambda_{i(1,1)} = Q^T(A - I_{n_x}) + (A^T - I_{n_x})Q + \lambda_i(Q^T BK + K^T B^T Q)$, $\Lambda_{i(2,1)} = P_\delta - Q + \eta Q^T(A - I_{n_x}) + \eta\lambda_i Q^T BK$, and $\Lambda_{i(2,2)} = P_\delta - \eta(Q + Q^T)$, then the tracking error signal $\bar{\delta}_i(k)$ is uniformly ultimately bounded.

Proof. Considering the Lyapunov function candidate as $V_i(\bar{\delta}_i(k), k) = \bar{\delta}_i^T(k) P_\delta \bar{\delta}_i(k)$ and denoting $\Delta\bar{\delta}_i(k) = \bar{\delta}_i(k+1) - \bar{\delta}_i(k)$, then one has that

$$\Delta V_i(\bar{\delta}_i(k), k) = \bar{\delta}_i^T(k+1) P_\delta \bar{\delta}_i(k+1) - \bar{\delta}_i^T(k) P_\delta \bar{\delta}_i(k) = 2\bar{\delta}_i^T(k) P_\delta \Delta\bar{\delta}_i(k) + \Delta\bar{\delta}_i^T(k) P_\delta \Delta\bar{\delta}_i(k). \tag{23}$$

From (21), one can easily verify that there exist a constant $\eta > 0$ and a matrix Q such that

$$2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T \big[(A - I_{n_x})\bar{\delta}_i(k) - \Delta\bar{\delta}_i(k) + \lambda_i BK\bar{\delta}_i(k) - \lambda_i BK\bar{e}_i(k) - BK\bar{\Omega}_i(k) + B\bar{\xi}_i(k)\big] = 0. \tag{24}$$

Adding the left-hand side of (24) into the right-hand side of (23) yields

$$\begin{aligned}\Delta V_i(\bar{\delta}_i(k), k) =& 2\bar{\delta}_i^T(k) P_\delta \Delta\bar{\delta}_i(k) + \Delta\bar{\delta}_i^T(k) P_\delta \Delta\bar{\delta}_i(k) + 2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T \big[(A - I_{n_x})\bar{\delta}_i(k) - \Delta\bar{\delta}_i(k) + \\ & \lambda_i BK\bar{\delta}_i(k)\big] - 2\lambda_i\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T BK\bar{e}_i(k) - 2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T BK\bar{\Omega}_i(k) + \\ & 2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T B\bar{\xi}_i(k).\end{aligned} \tag{25}$$

Suppose that the true state of vehicle i is confined in its state estimation ellipsoid at time k, i.e., $x_i(k) \in \mathcal{X}_k^i$, which implies that $x_i(k) = \hat{x}_i(k) + E_{i,k}\alpha_i(k)$. Hence, one can conclude that $e_i(k) = E_{i,k}\alpha_i(k)$. Further, we have $\|e_i(k)\| = \|E_{i,k}\alpha_i(k)\| \le \|E_{i,k}\|\|\alpha_i(k)\|$. Since $\|\alpha_i\| \le 1$, $\|E_{i,k}\| \le \|E_{i,k}\|_F$, and $\|E_{i,k}\|_F = \sqrt{\mathrm{trace}(E_{i,k}E_{i,k}^T)} = \sqrt{\mathrm{trace}(P_{i,k})} = e_M$, one can conclude that $\|e_i(k)\| \le e_M$. Thus, $\|\bar{e}_i(k)\| \le \bar{e}_M$.

Denoting $\theta_i(k) = [\bar{\delta}_i^T(k), \Delta\bar{\delta}_i^T(k)]^T$ and $\bar{\lambda} \triangleq \max_{i\in\mathcal{V}_N}\{\lambda_i\}$, for the last three terms in (25) we have

$$\begin{aligned} &- 2\lambda_i\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T BK\bar{e}_i(k) \le 2\bar{\lambda}\sqrt{1+\eta^2}\|\theta_i(k)\|\bar{\sigma}(Q^T BK)\bar{e}_M \\ &- 2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T BK\bar{\Omega}_i(k) \le 2\sqrt{1+\eta^2}\|\theta_i(k)\|\bar{\sigma}(Q^T BK)\bar{\Omega}_M \\ &2\big[\bar{\delta}_i^T(k) + \eta\Delta\bar{\delta}_i^T(k)\big] Q^T B\bar{\xi}_i(k) \le 2\sqrt{1+\eta^2}\|\theta_i(k)\|\bar{\sigma}(Q^T B)\bar{\xi}_M.\end{aligned} \tag{26}$$

Thus, we have

$$\Delta V_i(\bar{\delta}_i(k),k) \leq \theta_i^T(k)\Lambda_i\theta_i(k) + 2\sqrt{1+\eta^2}\|\theta_i(k)\|\Big(\bar{\sigma}(Q^TBK)(\bar{\lambda}\bar{e}_M + \bar{\Omega}_M) + \bar{\sigma}(Q^TB)\bar{\xi}_M\Big). \tag{27}$$

Denoting $\varrho_i = \underline{\sigma}(-\Lambda_i)$, we further have

$$\Delta V_i(\bar{\delta}_i(k),k) \leq -\varrho_i\|\theta_i(k)\|^2 + 2\sqrt{1+\eta^2}\|\theta_i(k)\|\Big(\bar{\sigma}(Q^TBK)(\bar{\lambda}\bar{e}_M + \bar{\Omega}_M) + \bar{\sigma}(Q^TB)\bar{\xi}_M\Big). \tag{28}$$

Then, $\Delta V_i(\bar{\delta}_i(k),k)$ is negative as long as

$$\|\theta_i(k)\| > \frac{2\sqrt{1+\eta^2}\Big(\bar{\sigma}(Q^TBK)(\bar{\lambda}\bar{e}_M + \bar{\Omega}_M) + \bar{\sigma}(Q^TB)\bar{\xi}_M\Big)}{\varrho_i}. \tag{29}$$

Therefore, one has that $\Delta V_i(\bar{\delta}_i(k),k)$ is negative outside the region defined by the bounds and hence, $\|\theta_i\|$ is uniformly ultimately bounded. Thus, the tracking error signal $\bar{\delta}_i$ in the closed-loop dynamics remains uniformly ultimately bounded. This completes the proof. □

Remark 2. In light of Theorem 2, a sufficient condition is established so as to guarantee that the closed-loop tracking error signal $\bar{\delta}_i(k)$ is uniformly ultimately bounded. However, this theorem cannot be straightforwardly employed to find out a solution for the control gain K since there exist the coupling terms Q^TBK and its transpose in (22). Moreover, the LMI in (22) depends on the eigenvalues of the graph matrix $\mathcal{H}$, which has a dimension of $N \times N$. Hence, the computational complexity of solving such an LMI considerably increases as the number of follower vehicles N in the platoon grows. In what follows, Theorem 3 is presented to deal with the above-mentioned issues and provide a simple criterion for designing a distributed platoon control protocol in the form of (10).

Theorem 3. *For a given positive constant η, the tracking error signal $\bar{\delta}_i(k)$ in the closed-loop error system (21) is uniformly ultimately bounded if there exist matrices $\tilde{Q}$ and $\tilde{P}_\delta > 0$ such that*

$$\tilde{\Lambda}_i|_{\lambda_i=\underline{\lambda}} < 0 \quad \textit{and} \quad \tilde{\Lambda}_i|_{\lambda_i=\bar{\lambda}} < 0 \tag{30}$$

holds, where $\underline{\lambda} \triangleq \min_{i\in\mathcal{V}_N}\{\lambda_i\}$ and $\tilde{\Lambda}_i$ is a 2×2 symmetric block matrix with $\tilde{\Lambda}_{i(1,1)} = (A-I_{n_x})\tilde{Q}+\tilde{Q}^T(A^T - I_{n_x}) + \lambda_i(B\tilde{K}+\tilde{K}^TB^T)$, $\tilde{\Lambda}_{i(2,1)} = \tilde{P}_\delta - \tilde{Q} + \eta(A-I_{n_x})\tilde{Q} + \eta\lambda_iB\tilde{K}$, and $\tilde{\Lambda}_{i(2,2)} = \tilde{P}_\delta - \eta\tilde{Q} - \eta\tilde{Q}^T$. Moreover, the control gain matrix K can be computed as $K = \tilde{K}\tilde{Q}^{-1}$.

Proof. From $\Lambda_{i(2,2)}$ in the inequality (22), it is clear that $P_\delta - \eta(Q+Q^T) < 0$, which indicates that the matrix Q is nonsingular. Set $\tilde{Q} = Q^{-1}$, $\tilde{P}_\delta = \tilde{Q}^T P_\delta \tilde{Q}$, and $\tilde{K} = K\tilde{Q}$. Premultiplying and postmultiplying the inequality in (22) by $\mathrm{diag}\{Q^{-T}, Q^{-T}\}$ and $\mathrm{diag}\{Q^{-1}, Q^{-1}\}$, respectively, one can obtain $\tilde{\Lambda}_i < 0$ as shown in (30). Since $\tilde{\Lambda}_i < 0$ is convex with respect to λ_i, it is sufficient to verify $\tilde{\Lambda}_i < 0$ for $\lambda_i = \underline{\lambda}$ and $\lambda_i = \bar{\lambda}$. This completes the proof. □

Before closing this section, by virtue of Theorems 1 and 3, Algorithm 1 is proposed to accomplish the simultaneous platoon tracking control over the VANET communication subject to attacks and set-membership estimation of the follower vehicles $i \in \mathcal{V}_N$'s true states with heterogenous engine time constant and in the presence of UBB exogenous disturbance and measurement noise.

Algorithm 1 State Estimation and Platoon Control Design

1: Given initial conditions $x_{i,0}$ and $\hat{x}_{i,0}$. Choose suitable $W_{i,k}$, $V_{i,k}$, and $P_{i,0}$ such that (4), (6), and (8) hold. Calculate $E_{i,0}$ by $P_{i,0} = E_{i,0}E_{i,0}^T$. Set $k = 0$, $x_i(k) = x_{i,0}$, $\hat{x}_i(k) = \hat{x}_{i,0}$, and $E_{i,k} = E_{i,0}$
2: For the considered V2V communication topology, compute the maximum and minimum eigenvalues of the graph matrix $\mathcal{H}$ as $\underline{\lambda}$, $\bar{\lambda}$
3: For a given constant $\eta > 0$, solve Theorem 3 to obtain a control matrix gain (K). If Theorem 3 fails to be feasible then `modify` η and `redo` Step 3; otherwise `continue`
4: Determine the simulation time t_{sim} seconds for all $i \in \mathcal{V}_{N+1}$
5: **for** $k = 0 : t_{sim}/h - 1$ **do**
6:     **for** $i = 1 : N$ **do**
7:         **for** $j = 1 : N$ **do**
8:             Collect $\tilde{x}_j(k)$ from each neighbor of vehicle i as prescribed in $\mathcal{N}_i$
9:         **end for**
10:         Collect $x_0(k)$ from the leader vehicle over $\mathcal{A}_0$
11:         Calculate $u_i(k)$ in (20) under K, $\hat{x}_i(k)$, $\tilde{x}_j(k)$ from its neighbors, and $\tilde{x}_0(k)$ from the leader vehicle
12:         Solve the OP (13) in Theorem 1 to obtain $P_{i,k+1}$ and $L_{i,k}$. From $P_{i,k+1} = E_{i,k+1}E_{i,k+1}^T$, compute $E_{i,k+1}$
13:         Compute the state estimation $\hat{x}_i(k+1)$ by (7) and denote it as the center of the estimation ellipsoid $\mathcal{X}_{k+1}^i$. Form the estimation set as $X_{i,k+1} = \hat{x}_i(k+1) + E_{i,k+1}\alpha_i$
14:         Output $\{P_{i,k+1}\}$ and $\{L_{i,k}\}$, vehicle i's state estimate $\hat{x}_i(k)$ and the state estimation ellipsoidal set $\{X_{i,k+1}\}$
15:     **end for**
16: **end for**

5. Simulation results

To verify the effectiveness of the developed theoretical results for vehicle platooning, in this section, we present various case studies to comprehensively conduct comparative analysis considering several V2V communication topologies under different attack strategies. Specifically, we consider a platoon of one leader and six follower vehicles with their heterogeneous engine time constants are taken as $\tau_i = \tau_0 + (-1)^i(0.05i^2/(N+$

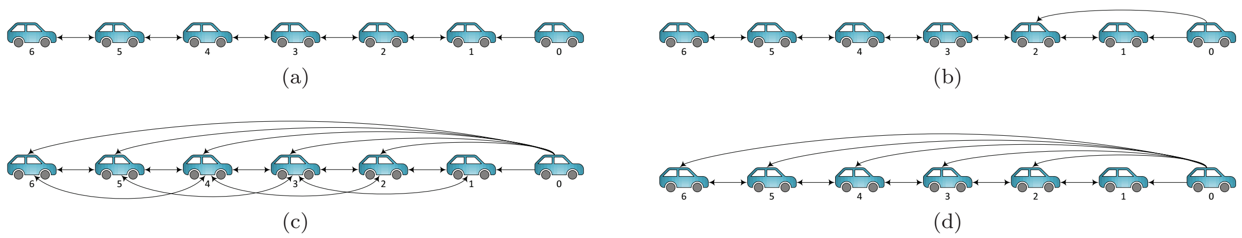


Figure 2: Various V2V communication topologies. (a) Bidirectional (BD); (b) Leader-two-bidirectional (LTBD); (c) Leader-two-predecessor-bidirectional (LPBD); (d) Leader-bidirectional (LBD).

i^2)), $i \in \mathcal{V}_N$, where $\tau_0 = 0.5$ s. The vehicular platoon is set to have a desired spacing of $d_{i-1,i} = 15$ m and other parameters are chosen as $\eta = 1.05$, $\phi_M = 0.15$, $C = [1, 0, 0]$, and $D = 0.2$. The driving scenario starts with $p_0 = 100$ m, $v_0 = 5$ m/s, $a_0 = 0$ m/s^2 for the leader vehicle and zero initial tracking errors for all followers. In subsequent simulation, we examine four different V2V communication topologies depicted in Fig. 2. The graph $\mathcal{G}$'s adjacency elements are chosen as $a_{ij} = 1$ for $(i, j) \in \mathcal{E}$. Also, $a_{i0} = 1$ if vehicle i is pinned to the leader. Given a sampling period of $h = 8$ ms, the simulation will be run for $t_{sim} = 35$ s or 4375 time steps.

Each follower vehicle in the platoon is subject to the UBB exogenous disturbance input derived from $w_i(k) = 1.75(i^2/(1 + i^2)) \sin(0.08k)$, $i \in \mathcal{V}_N$ and the UBB measurement noises as $\vartheta_1(k) = 0.2 \sin(0.0476k)$, $\vartheta_2(k) = 0.13 \sin(0.0467k)$, $\vartheta_3(k) = 0.12 \sin(0.0474k)$, $\vartheta_4(k) = 0.16 \sin(0.0469k)$, $\vartheta_5(k) = 0.15 \sin(0.0478k)$, $\vartheta_6(k) = 0.11 \sin(0.0472k)$. Choosing $W_{i,k} = 3.5$ and $V_{i,k} = 0.5$, one can easily confirm that $w_i(k)$ and $\vartheta_i(k)$ are enclosed in the ellipsoidal sets (4) and (6), respectively. The initial state estimates of vehicles $i \in \mathcal{V}_N$ in the platoon are chosen as $\hat{x}_{1,0} = [86.6, 5.2, 0]^T$, $\hat{x}_{2,0} = [71.7, 4.81, 0]^T$, $\hat{x}_{3,0} = [56.4, 4.89, 0]^T$, $\hat{x}_{4,0} = [41.8, 4.45, 0]^T$, $\hat{x}_{5,0} = [25.1, 4.93, 0]^T$, $\hat{x}_{6,0} = [10.5, 4.12, 0]^T$, which also represent the initial centers of their state estimation ellipsoidal sets $\mathcal{X}_0^i$ with their initial shape matrices are given by $P_{i,0} = \text{diag}\{5, 2, 1\}$. Furthermore, the leader control input is given by $u_0(k) = 0.2h(k - 125)$ for $125 \leq k < 500$; $u_0(k) = 0.6$ for $k \geq 500$ and $k < 1000$; $u_0(k) = -0.2h(k - 1000) + 0.6$ for $1000 \leq k < 1375$; and $u_0(k) = 0$ otherwise.

We consider that a malicious adversary chooses a set of vehicles as $\mathcal{V}_a = \{0, 2, 4\}$ so as to launch different attack strategies as follows. 1) A DoS attack which blocks 20% of the exchanged state estimates of vehicle $i \in \mathcal{V}_a$ over the VANET can be represented as $\varpi_i(k) = -\gamma \hat{x}_i(k)$ with $\gamma = 0.2$ during different time intervals τ_a^{DoS}. 2) A replay attack tampering with 70% of the transmitted state estimates of vehicle $i \in \mathcal{V}_a$ can be modeled as $\varpi_i(k) = \gamma(\hat{x}_i(k - \tau_a^{\text{Rep}}) - \hat{x}_i(k))$, where $\gamma = 0.7$ and $\tau_a^{\text{Rep}} > 0$ represents different time windows of recoding sequence of data from the state estimate $\hat{x}_i(k)$ starting from k_r. Then the adversary replays the collected data through VANET from k_f over the same time window size. 3) To model an FDI attack,

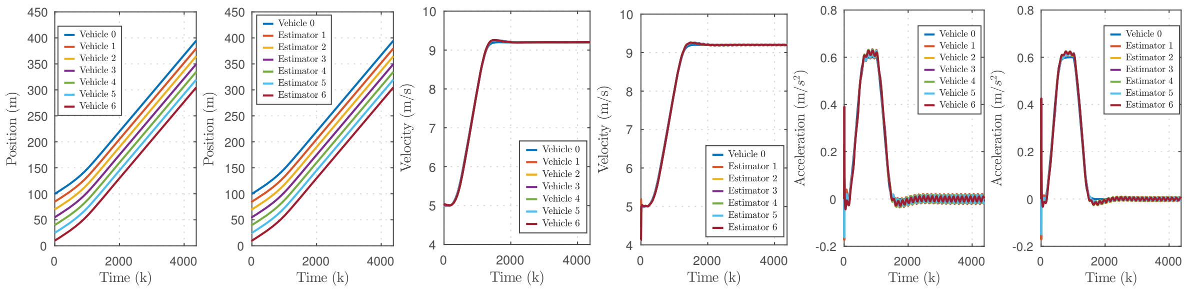


Figure 3: Vehicle i's state trajectories and estimator i's response over LBD-based V2V communication with no attack.

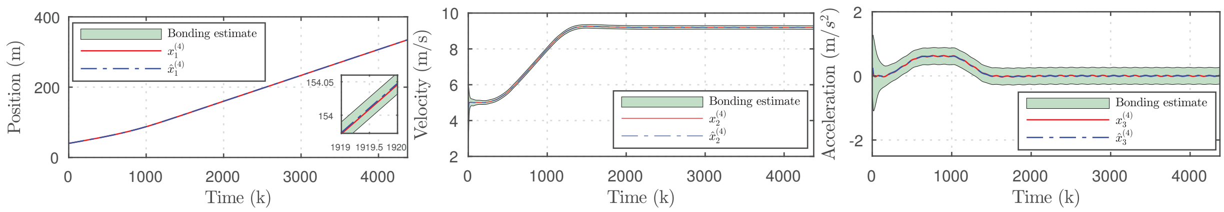


Figure 4: Vehicle 4's guaranteed state estimates with no attack.

an arbitrary bounded attack signal can be chosen as $\varpi_i(k) = \gamma[-1.8; -0.78; 0]^T \|\sin(0.5k+2)\|$, where γ describes different amplitudes of the FDI attack signal prescribed by the adversary.

5.1. *Local set-membership estimator performance*

First, we investigate the guaranteed state estimation performance of the local set-membership estimators against the bounded uncertainties in follower vehicles' engine time constants, UBB exogenous disturbances, and UBB measurement noises. The V2V communication topology is considered as LBD as illustrated in Fig. 2. When the VANET is free of attack, i.e., $\varpi_i(k) = 0$, running Algorithm 1, we have the trajectories of vehicle true state components and their estimates as illustrated in Fig. 3, which also demonstrates that the expected platooning objectives are well satisfied. To verify the guaranteed state estimation performance, we take vehicle 4 as an example. From Fig. 4, one can clearly observe that the true state components of vehicle 4 are guaranteed to be confined in the derived bounding state estimation ellipsoid $\mathcal{X}^4_{k+1}$ at each time step k. To quantitatively assess the performance of the local set-membership estimators for all follower vehicles, we introduce a quadratic estimation error (QEE) on each estimator i as an ellipsoidal estimation performance index by $\mathscr{E}^i_k = e_i^T(k)P^{-1}_{i,k}e_i(k)$. From Fig. 5a, it can be easily verified that $\mathscr{E}^i_k \le 1$ for all follower vehicles $i = 1, 2, \dots, 6$, which further indicates that the true states of these vehicles always reside in their bounding ellipsoidal state estimation sets $\mathcal{X}^i_{k+1}$ at each time step k.

We next consider the three following cases where there exist the DoS attacks with $\tau_a^{DoS} = 50$ steps (400 ms) from $k = 750$, replay attacks with $\tau_a^{\text{Rep}} = 375$ steps (3 s), $k_r = 250$, $k_f = 750$, and FDI attacks with

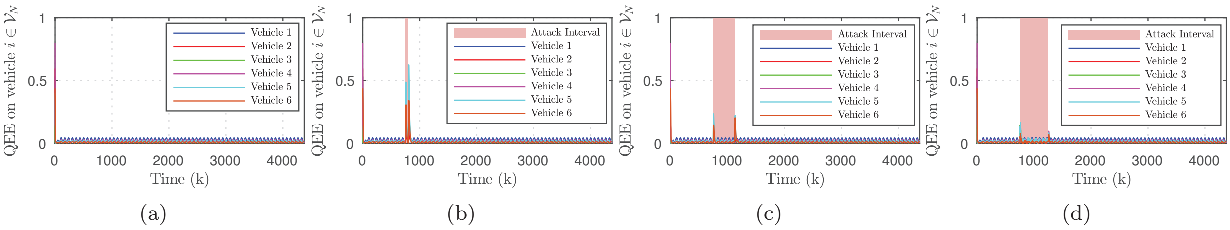


Figure 5: QEEs over different attack strategies; (a) no attack. (b) DoS attack. (c) Replay attack. (d) FDI attack.

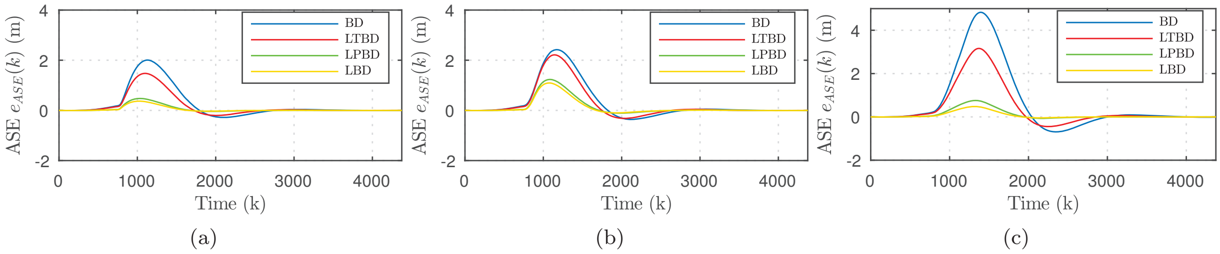


Figure 6: Trajectories of $e_{ASE}(k)$ for different V2V communication topologies compromised by different attack strategies; (a) DoS attack. (b) Replay attack. (c) FDI attack.

Table I: Bounds of ASE under various V2V communication topologies compromised by different attack strategies.

Topologies	BD	LTBD	LPBD	LBD
DoS - ASE bound (m)	2.0030	1.4754	0.4751	0.3688
Replay - ASE bound (m)	2.4286	2.2134	1.2340	1.0947
FDI - ASE bound (m)	4.8384	3.1605	0.7599	0.4817

$\gamma = 5$ for 500 steps (4 s) from $k = 750$ on the exchanged state estimates of the vehicles in $\mathcal{V}_a$. Under these three attack strategies, Figs. 5b, 5c, 5d verify that the true states of follower vehicles are confined in their corresponding state estimation ellipsoids $\mathcal{X}^i_{k+1}$ since the QEEs remain in their specified bounds as $\mathscr{E}^i_k \leq 1$. It should be noted that, however, the local state estimators provide larger QEEs due to the impacts of these attacks. In other words, the resilience of the local set-membership state estimators can be preserved under the considered attack strategies, however, the performance of the local estimators are degraded compared with Fig. 5a without attacks.

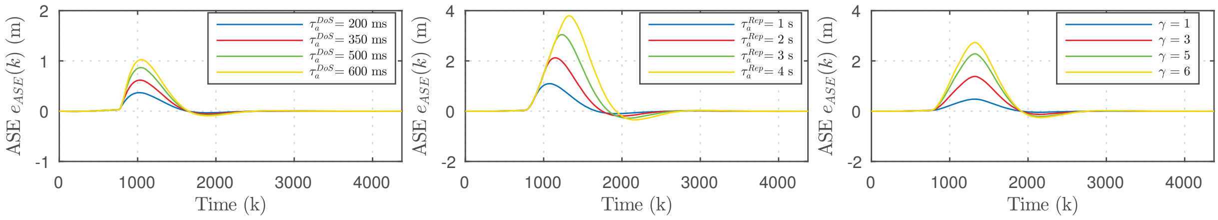
5.2. Various V2V communication topologies

In this section, we aim to test the developed platooning control approach over four various communication topologies depicted in Fig. 2 subject to the various attack strategies as DoS attacks with $\tau_a^{DoS} = 25$ steps (200 ms) and $\gamma = 0.2$, replay attacks with $\tau_a^{\mathrm{Rep}} = 125$ steps (1 s) and $\gamma = 0.7$, and FDI attacks with $\gamma = 1$ and their other parameters are given the same as those in Section 5.1. To facilitate this, we define an average spacing error (ASE) as $e_{\mathrm{ASE}}(k) = (1/N)\sum_{i=1}^{N}(p_{i-1}(k) - p_i(k) - d_{i-1,i})$. Applying the design procedure in Algorithm 1, ASEs over different topologies subject to the considered attack strategies are gathered in Fig. 6. Furthermore, Table I summarizes the maximum bounds on ASEs. From the comparative results in Fig. 6 and Table I, one can conclude that the platooning performance over the LBD topology is superior to the others, while the BD topology turns in the worst platooning performance. Specifically, under the presence of the attacks on the exchanged data from the leader vehicle $i = 0$, and the follower vehicles $i = 2$ and 4, the LBD topology enables all platoon members to be informed by the leader and hence, more information is propagated among neighboring vehicles. However, this is not the case for the BD and LTBD topologies where, at most, the first two vehicles can access the leader information, while the other members are only dependent on their neighbors which may be tampered or not completely available due to the attacks. Comparing the results between the LPBD and LBD topologies under the same attack strategies, one can observe that the platoon performance over LPBD is slightly degraded. Such marginal degradation can be due to the fact that the LPBD-based platoon allows transmission of more data among neighboring vehicles and hence, more platoon members require data from vehicles 2 and 4, which may contain bogus information or not be fully available under the presence of attacks.

5.3. Different attack settings

In this section, we study the impact of the three attack strategies with their different settings prescribed by an adversary. This can be specified by various attack intervals for DoS and replay attacks, i.e., τ_a^{DoS} and τ_a^{Rep}, and different amplitudes for FDI attacks, that is, γ. The V2V communication topology is chosen as LBD. The proposed set-membership-based platooning control approach is tested through calculation of the platoon's ASEs considering the different settings for each attack, as demonstrated in Fig. 7. The maximum bounds on ASEs under these scenarios are given in Table II. Unsurprisingly, smaller DoS and replay attacks intervals and less FDI attack amplitude result in a faster convergence of ASE with a lower bound in all of these scenarios, which also indicates better platooning performance.

Now, with the same attacks' settings provided in Section 5.1, the platooning performance of the developed secure set-membership-based control approach is assessed over the LBD topology. The true values of vehicular state components and the spacing errors over time steps are depicted in Fig. 8. During the period of these attack strategies, it is clearly evident that the vehicle spacing grows comparatively large. Furthermore, reaching the desired consensus among velocities and accelerations require a much longer time. However, under the proposed secure set-membership-based control approach, the vehicle platoon over an unsafe V2V communication topology can tolerate a certain level of unfavorable impacts of different attack strategies with various settings, while delivering satisfactory platooning performance.



(a) (b) (c)

Figure 7: Trajectories of $e_{ASE}(k)$ for different settings of (a) DoS attack; (b) Replay attack; and (c) FDI attack over LBD communication topology.

Table II: ASE bounds for different settings of (a) DoS attack; (b) Replay attack; and (c) FDI attack over LBD communication topology.

(a)

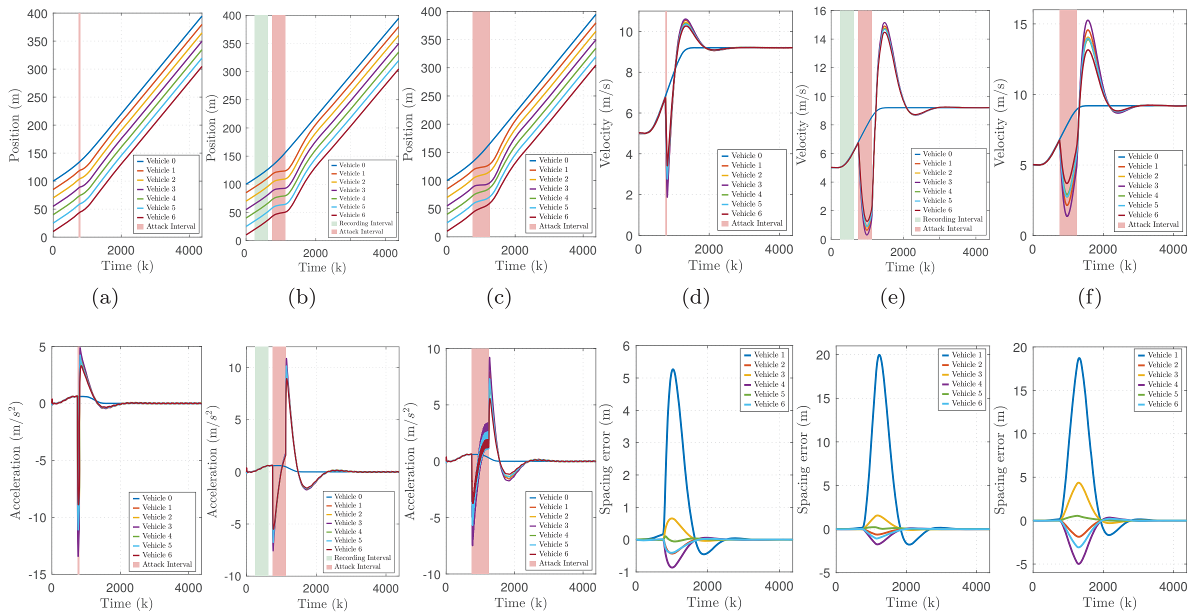
τ_a^{DoS}	600 ms	500 ms	350 ms	200 ms
ASE bound (m)	1.0247	0.8669	0.6174	0.3688

(b)

τ_a^{Rep}	4 s	3 s	2 s	1 s
ASE bound (m)	3.7940	3.0456	2.1231	1.0947

(c)

γ	6	5	3	1
ASE bound (m)	2.7311	2.2812	1.3814	0.4817



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

Figure 8: Vehicles' state $p_i(k)$, $v_i(k)$, $a_i(k)$ and spacing error $p_{i-1}(k) - p_i(k) - d_{i-1,i}$ trajectories over LBD communication topology under different attacks; (a), (d), (g), (j) DoS attack. (b), (e), (h), (k) Replay attack. (c), (f), (i), (l) FDI attack.

6. Conclusion

The secure platooning control problem has been addressed for a fleet of automated vehicles over VANET under different attack strategies. A local set-membership estimator has been developed to construct the complete state estimates of each follower vehicle in the presence of uncertain heterogenous engine time constants, UBB exogenous disturbance and measurement noise. The distributed control protocol of each platoon member utilizes the vehicular state estimates computed by its local estimator and those of its specified neighboring vehicles. Then, under different attack strategies, the vehicle platooning performance over different bidirectional V2V communication topologies has been analyzed in the sense of uniformly ultimately boundedness. Finally, the effectiveness of the proposed theoretical results has been evaluated over several comprehensive case studies.

References

[1] X. Ge, Q.-L. Han, L. Ding, Y.-L. Wang, and X.-M. Zhang, Dynamic event-triggered distributed coordination control and its applications: A survey of trends and techniques, IEEE Trans. Syst. Man Cybern. Syst. 50 (9) (2020) 3112–3125.

[2] D. Jia, K. Lu, J. Wang, X. Zhang, X. Shen, A survey on platoon-based vehicular cyber-physical systems, IEEE Commun. Surveys Tuts. 18 (1) (2016) 263–284.

[3] Y. Zu, C. liu, R. Dai, Distributed traffic speed control for improving vehicle throughput, IEEE Intell. Transp. Syst. Mag. 11 (3) (2019) 56–68.

[4] H. Yu, R. Jiang, Z. He, Z. Zheng, L. Li, R. Liu, X. Chen, Automated vehicle-involved traffic flow studies: A survey of assumptions, models, speculations, and perspectives, Transportation Research Part C 127 (2021) 103101.

[5] D. Zhao, H. Wang, Longitudinal influence of autonomous vehicles and vehicular communication on post-accident traffic, IEEE Intell. Transp. Syst. Mag. 13 (4) (2019) 1646–178.

[6] B. Van Arem, C. J. G. van Driel, R. Visser, The impact of cooperative adaptive cruise control on traffic-flow characteristics, IEEE Trans. Intell. Transp. Syst. 7 (4) (2006) 429–436.

[7] K.-Y. Liang, J. Mårtensson, K. Johansson, Heavy-duty vehicle platoon formation for fuel efficiency, IEEE Trans. Intell. Transp. Syst. 17 (4) (2016) 1051–1061.

[8] C. Zhai, F. Luo, Y. Liu, Z. Chen, Ecological cooperative look-ahead control for automated vehicles travelling on freeways with varying slopes, IEEE Trans. Veh. Technol. 68 (2) (2019) 1208–1221.

[9] Y. Ma, J. Wang, Predictive control for NO_x emission reductions in diesel engine vehicle platoon application, IEEE Trans. Veh. Technol. 68 (7) (2019) 6429–6440.

[10] A. A. Peters, R. H. Middleton, O. Mason, Leader tracking in homogeneous vehicle platoons with broadcast delays, Automatica 50 (1) (2014) 64–74.

[11] P. Barooah, P. G. Mehta, J. P. Hespanha, Mistuning-based control design to improve closed-loop stability margin of vehicular platoons, IEEE Trans. Autom. Control 54 (9) (2009) 2100–2113.

[12] X. Ge, S. Xiao, Q.-L. Han, X.-M. Zhang, D. Ding, Dynamic event-triggered scheduling and platooning control co-design for automated vehicles over vehicular ad-hoc networks, IEEE/CAA J. Automatica Sinica 9 (1) (2022) 31–46.

[13] Y. Zheng, S. Eben Li, J. Wang, D. Cao, K. Li, Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies, IEEE Trans. Intell. Transp. Syst. 17 (1) (2016) 14–26.

[14] R. G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13.

[15] D. Ding, Q.-L. Han, X. Ge, and J. Wang, Secure state estimation and control of cyber-physical systems: A survey, IEEE Trans. Syst. Man Cybern. Syst., 51 (1) (2021) 176–190.

[16] E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, L. Vlacic, Distributed cyber attacks detection and recovery mechanism for vehicle platooning, IEEE Trans. Intell. Transp. Syst. 21 (9) (2020) 3821–3834.

[17] Z. Abdollahi Biron, S. Dey, P. Pisu, Real-time detection and estimation of denial of service attack in connected vehicle systems, IEEE Trans. Intell. Transp. Syst. 19 (12) (2018) 3893–3902.

[18] N. Lyamin, D. Kleyko, Q. Delooz, A. Vinel, Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining, IEEE Commun. Lett. 23 (3) (2019) 442–445.

[19] S. Xiao, X. Ge, Q.-L. Han, Y. Zahng, Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks, IEEE Trans. Cybern. (Early access). doi:10.1109/TCYB.2021.3074318.

[20] R. G. Dutta, Y. Hu, F. Yu, T. Zhang, Y. Jin, Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment, IEEE Trans. Intell. Transp. Syst. (Early access). doi:10.1109/TITS.2020.3036376.

[21] N. Jahanshahi, R. M. Ferrari, Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach, IFAC-PapersOnLine 51 (23) (2018) 212–217.

[22] Z. Ju, H. Zhang, Y. Tan, Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator, IEEE Internet Things J. 7 (5) (2020) 3693–3705.

[23] X. He, E. Hashemi, K. H. Johansson, Distributed control under compromised measurements: Resilient estimation, attack detection, and vehicle platooning, Automatica 134 (2021) 109953.

[24] A. Petrillo, A. Pescapé, 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. 51 (3) (2021) 1134–1149.

[25] R. A. Biroon, Z. A. Biron, P. Pisu, False data injection attack in a platoon of CACC: Real-time detection and isolation with a PDE approach, IEEE Trans. Intell. Transp. Syst. (Early access). doi:10.1109/TITS.2021.3085196.

[26] R. Merco, Z. A. Biron, P. Pisu, Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control, in: 2018 Annual American Control Conference (ACC), 2018, pp. 5582–5587.

[27] A. Alipour-Fanid, M. Dabaghchian, K. Zeng, Impact of jamming attacks on vehicular cooperative adaptive cruise control systems, IEEE Trans. Veh. Technol. 69 (11) (2020) 12679–12693.

[28] Z. Ju, H. Zhang, Y. Tan, Distributed deception attack detection in platoon-based connected vehicle systems, IEEE Trans. Veh. Technol. 69 (5) (2020) 4609–4620.

[29] D. Zhang, Y. Shen, S. Zhou, Distributed secure platoon control of connected vehicles subject to DoS attack: Theory and application, IEEE Trans. Syst. Man Cybern. Syst. 51 (11) (2021) 7269–7278.

[30] J. Ploeg, D. P. Shukla, N. van de Wouw, H. Nijmeijer, Controller synthesis for string stability of vehicle platoons, IEEE Trans. Intell. Transp. Syst. 15 (2) (2014) 854–865.

[31] A. Eskandarian, C. Wu, C. Sun, Research advances and challenges of autonomous and connected ground vehicles, IEEE Trans. Intell. Transp. Syst. 22 (2) (2021) 683–711.

[32] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang, Distributed event-triggered estimation over sensor networks: A survey, IEEE Trans. Cybern. 50 (3) (2020) 1306–1320.

[33] R. Olfati-Saber, Distributed Kalman filtering for sensor networks, in: the 46th IEEE Conference on Decision and Control, 2007, pp. 5492—5498.

[34] L. Xie, Y. Soh, C. de Souza, Robust Kalman filtering for uncertain discrete-time systems, IEEE Trans. Autom. Control 39 (6) (1994) 1310—1314.

[35] S. Antonov, A. Fehn, A. Kugi, Unscented kalman filter for vehicle state estimation, Veh. Syst. Dyn. 49 (9) (2011) 1497–1520.

[36] H. Suzuki, Dynamic state estimation in vehicle platoon system by applying particle filter and unscented kalman filter, Procedia Comput. Sci. 24 (2013) 30–41.

[37] X. Liu, H. Qu, J. Zhao, P. Yue, Maximum correntropy square-root cubature kalman filter with application to SINS/GPS integrated systems, ISA Trans. 80 (2018) 195–202.

[38] U. Shaked, N. Berman, H_∞ nonlinear filtering of discrete-time processes, IEEE Trans. Signal Process. 43 (9) (1995) 2205—2209.

[39] X. Ge, Q.-L. Han, Z. Wang, A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks, IEEE Trans. Cybern. 49 (4) (2019) 1148–1159.

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

[41] A. Ghasemi, R. Kazemi, S. Azadi, Stable decentralized control of a platoon of vehicles with heterogeneous information feedback, IEEE Trans. Veh. Technol. 62 (9) (2013) 4299–4308.

[42] Y. Zheng, S. E. Li, K. Li, W. Ren, Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed h-infinity controller synthesis, IEEE Trans. Intell. Transp. Syst. 19 (5) (2018) 1353–1364.

[43] X. Ge, Q.-L. Han, and F. Yang, Event-based set-membership leader-following consensus of networked multi-agent systems subject to limited communication resources and unknown-but-bounded noise, IEEE Trans. Ind. Electron. 64 (6) (2017) 5045–5054.

[44] D. Ding, Z. Wang, and Q.-L. Han, A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks, IEEE Trans. Autom. Control 65 (4) (2020) 1792–1799.

[45] X. Ge, Q.-L. Han, and Z. Wang, A dynamic event-triggered transmission scheme for distributed set-membership estimation over wireless sensor networks, IEEE Trans. Cybern. 49 (1) (2019) 171–183.

[46] S. Stankovic, M. Stanojevic, D. Siljak, Decentralized overlapping control of a platoon of vehicles, IEEE Trans. Control Syst. Technol. 8 (5) (2000) 816–832.