Design and Analysis of Secure Distributed Estimator for Vehicular Platooning in Adversarial Environment

Raj Gautam Dutta, *Member, IEEE*, Yaodan Hu, *Student Member, IEEE*, Feng Yu, Teng Zhang, and Yier Jin, *Senior Member, IEEE*

***Abstract*— Platooning of connected vehicles is a solution geared toward improving traffic throughput, highway safety, driving comfort, and fuel efficiency. These vehicles are equipped with Cooperative Adaptive Cruise Controller (CACC) that integrates information from dedicated short-range communication (DSRC) radio and sensors for safe navigation. The possibility of malicious attacks such as Denial of Service (DoS) or False Data Injection (FDI) on sensor data or control inputs tends to affect reliability, and jeopardize the safety of connected vehicles. Thus, securing sensor data of these vehicles from DoS or FDI attacks is essential to avoid unwanted consequences. To withstand sensor attacks, resilient state estimators have been developed for networked cyber-physical systems (CPS). However, such estimators do not perform well as the number of compromised sensors of the system increases. As such, we propose a novel convex optimization based Resilient Distributed State Estimator (RDSE) that bounds the state estimation error, irrespective of the magnitude of the attack and the number of compromised sensors. We theoretically prove that the proposed estimator has similar performance compared to the state-of-the-art Distributed Kalman Filter (DKF) under attack free and noise free scenarios. While under attack, our RDSE outperforms the DKF and we provide a theoretical bound on state estimation error generated by RDSE during an attack. We also demonstrate the effectiveness of RDSE against FDI attacks in a platoon with five vehicles and compare its performance during attack against the DKF and the Resilient Distributed Kalman Filter (RDKF).**

***Index Terms*— Vehicle Platoon, denial of service, false data injection, convex optimization, distributed estimation.**

I. Introduction

INCREASING population and economic activities has gradually raised the need for road freight transportation around the world. Despite its importance, road freight transportation is facing serious challenges posed by increasing fuel price and greenhouse gas emission. Consequently, advancements were made in the areas of information and communication technologies that led to the development of cooperative methods such as *platooning*. Such a solution tends to enhance safety, traffic throughput, fuel efficiency of transportation networks, and reduces carbon emissions. A group of vehicles moving at the same speed and maintaining close intervehicular distance is known as a *platoon*. Its safe operation can be ensured by using a feedback control system that uses measurements from onboard sensors and state information of neighboring vehicles through Dedicated Short Range Communication (DSRC) radios to control velocity and intervehicular distance between platoon vehicles. Such a system obtained by integrating existing cruise controller architecture with communication capabilities is called *cooperative adaptive cruise control* (CACC). Unlike adaptive cruise controller (ACC) or cruise controller (CC), the control inputs in CACC are coordinated among several vehicles to achieve stable platoon behavior.

Vehicles of the platoon follow an information flow topology to exchange information among each other. Early-stage platoons were radar-based, where each vehicle only obtained information from its preceding car and the following car [1], [2]. Information flow topology representative of the radar-based platoon were predecessor following and bidirectional [1]–[3]. With the addition of vehicular communication, topology such as predecessor-leader following, bidirectional-leader, two predecessors following, and two predecessor-leader following, have become possible in platooning [4]. Investigation was done to understand the relationship between communication topology and formation stability in [5]. By using the eigenvalues of the Laplacian matrix of the communication graph such as complete, acyclic directed, single directed, and two-cyclic undirected, they were able to relate individual vehicle's stability with stability of N identical (with the same dynamics) vehicles of the network.

Over the last decade, research on design and analysis of string stable controllers for vehicle platoon has matured significantly [6]–[8]. As such, current research efforts have been focused on making such controllers robust/resilient to environmental uncertainties as well as adversarial attacks [9]–[23]. In the case of attacks, an adversary either modify the controller to destabilize or take control of the platoon or make the communication channel unavailable to degrade the Quality of Service (QoS) of the network. For the network attack

Manuscript received December 19, 2018; revised August 29, 2019, April 21, 2020, and July 15, 2020; accepted October 30, 2020. This work was supported in part by the National Science Foundation under Grant CNS-1818500 and in part by the CyberFlorida Collaborative Seed Award Program. The Associate Editor for this article was E. Kaisar. *(Corresponding author: Yier Jin.)*

Raj Gautam Dutta, Yaodan Hu, and Yier Jin are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: r.dutta@ufl.edu; cindy.hu@ufl.edu; yier.jin@ece.ufl.edu).

Feng Yu and Teng Zhang are with the Department of Mathematics, University of Central Florida, Orlando, FL 32816 USA (e-mail: feng.yu@ucf.edu; teng.zhang@ucf.edu).

Digital Object Identifier 10.1109/TITS.2020.3036376

scenario, [9], [12]–[15] analyzed the impact of different attacks such as DoS and False data injection (FDI) on the DSRC protocol stack and designed detection and/or prevention methods. There are also works that targeted attack design, security analysis, and development of mitigation strategies for controllers of vehicle platoon [10], [11], [16]–[20], [23]. Such attacks compromise integrity of the system by altering control inputs, control laws, or sensor measurements. Repercussions include vehicle pileup or increase in fuel consumption.

Various approaches have been proposed to address integrity attacks on platoon control systems [11], [16], [19], [23]. In [16] and [19], sliding mode controller and switching controller frameworks were developed respectively as countermeasures. For detection of integrity attacks, [19] proposed a model-based scheme whereas [11] combined system identification techniques with machine learning. Barrier approach, where artificial bounds were imposed on control inputs to limit attackers influence, was proposed by [23]. Another direction, which is relevant to our work is the design of attack resilient estimators for distributed systems such as platoon [22], [24]–[28]. Preliminary resilient estimators were either centralized or decentralized i.e. they required aggregation of information of all the agents of the distributed system at a particular location (centralized) or required all the agents to have information of all the other agents of the system (decentralized) [22], [24], [25]. Aggregation of data in a centralized or decentralized fashion made these estimators computationally inefficient. Consequently, resilient distributed state estimators, that required information of only an agent's neighbors were developed [26]–[28]. However, these methods either did not provide performance analysis results of their algorithm or made several assumptions on the network topology.

In this paper, we model the platoon as a linear time-invariant system. A malicious attack corrupts the sensor measurements of some vehicles of the platoon. We design and analyze a novel Resilient Distributed State Estimator (RDSE) to mitigate the affect of attacks on platoon vehicles. Our estimator is inspired from the Distributed Kalman Filter (DKF). We show the asymptotic convergence of estimation error to zero for both DKF and RDSE when there is no attack and no noise. Furthermore, our resiliency analysis shows that RDSE bounds the disturbance on the state estimate caused by an attack. Compared to [28], our RDSE and its analysis does not make assumptions of the structure of the graph (except being connected), the number of corrupted nodes, and the eigenvalues of system matrix A.

Our paper makes the following novel contributions:

- We design Resilient Distributed State Estimator (RDSE) as countermeasure for data integrity attacks on sensor measurements of a platoon vehicle and analyze its performance. Two unique features of RDSE are as follows: (i) It does not restrict the number of neighbors of an agent that can be compromised and (ii) The estimator's performance does not get degraded (beyond an upper bound) with the magnitude of the attack.
- We provide the convergence result of DKF and RDSE for a no-noise and no-attack scenario. To the best of our knowledge, we are the first to provide analytical results for DKF.

The rest of the paper is organized as follows: In Section II, we present works related to ours and in section III, we describe the model of platoon with CACC, the measurement attack model, and formulate the problem. DKF, RDSE, their performance analysis, and discussions are in Section IV. The effectiveness of RDSE is demonstrated on a five vehicle platoon scenario in Section V. Final conclusions are drawn in Section VI and additional materials are given in Appendix A and B.

II. Literature Review

Several security measures have been proposed to mitigate the effect of integrity attacks on sensors, controllers, and network of distributed system such as platoon [11], [16], [19], [23], [26]–[28]. Dadras *et al.* [11] proposed a detection algorithm that combined system identification approach with the thresholding/clustering method to detect gain modification and destabilizing attack on the vehicle of a platoon. Their method requires input-output data of each vehicle to identify the system matrix, but does not require any information on number of attackers or system parameters. Sajjad *et al.* [16] designed an insider attack aware sliding mode control scheme that used only local sensor data and a decentralized attack detector to reduce the severity of collision in a platoon. In their case, the attacker modifies the control law of a vehicle to induce an oscillatory behavior in the platoon. While designing their solution, they assumed that the bidirectional platoon was homogeneous with all cars sharing the same control law. DeBruhl *et al.* [19] considered an insider attack on platoon's vehicular network that could manipulate the control law of a vehicle or misreport information with the intention of either reducing headway speed, joining platoon without having necessary distancing equipment, collision induction, or misinforming follower vehicle. They developed an error calculation and threshold based mechanism, which compared the expected behavior of the preceding vehicle with observed behavior to detect the attack. Whenever an attack was found, they switched the control mode from CACC to non-cooperative ACC so that the vehicle could use only radar or LIDAR data for navigation. Kafash *et al.* [23] proposed an approach that reduced the capabilities of an attacker by imposing artificial bounds on the control inputs that drive the system. Whether the attack was caused by manipulation of the control inputs or sensors, these actuator bounds would restrict the system from reaching unsafe states.

The attack resilient distributed state estimators were developed as an alternative to mitigate the impact of attack on the system [26]–[28]. Khan and Stankovic [26] proposed attack detection and single message exchange state estimation methods for a compromised communication scenario. Their estimator relied on statistical consistency of nodal and local data sets and physical-layer feedback. Matei *et al.* [27] designed a multi-agent filtering scheme in conjunction with a trust-based mechanism to secure the state estimates of power grid under false data injection attack. In their approach, an agent of the grid computes local state estimates based

on their own measurement and of their trusted neighbors. However, [26], [27] did not provide any theoretical guarantees of their methods. Mitra and Sundaram [28] developed a secure distributed observer for the Byzantine adversary model, where some nodes of the network were compromised by an adversary. Prior to state estimation, they decomposed the linear system model using Kalman's observability decomposition method. Then, Luenberger observer [29] was used at each node to estimate the states corresponding to detectable eigenvalues. The undetectable portions of the states at each node were estimated using secure consensus algorithm, which used measurements of well-behaving neighboring nodes. However, their method required the network to be highly connected to mitigate the effect of a small number of adversarial nodes. Furthermore, all these methods [26]–[28] were proposed for a general distributed system and have not been applied to a platoon. In this paper, we design an attack resilient distributed estimator which overcome the limitations of the above filters for the vehicle platoon.

III. Preliminaries and Problem Description

In this section, the model of CACC equipped vehicles of the platoon, model of the communication network, the platoon dynamics, and the problem definition are introduced.

A. System Model

We consider a homogeneous predecessor-leader following platoon of n cooperative adaptive cruise control (CACC) equipped vehicles without attacks. In Figure 1, $c^{(i)}$ is the position of i-th vehicle in the traffic, where $(i = 0, \cdots, n)$ and $d^{(i)} = (c^{(i-1)}(t) - c^{(i)}(t))$ is the actual distance between vehicle $i-1$ and its follower i. The active sensors and the vehicle-to-vehicle (V2V) communication devices on the cars are responsible for gathering these measurements. We assume that the leader car of the platoon has index $i = 0$, and followers of the platoon have index $i = 1, \ldots, n$. These vehicles should maintain a desired distance $d^{r,(i)}$ to its preceding vehicle, which in our case is proportional to the time headway ($\tau_h = 0.9$ sec [30]) between the vehicles, minimum stopping distance ($d^r = 10$ m), and the speed of the follower vehicle ($v^{(i)}$).

$$d^{r,(i)}(t) = d_r + \tau_h v^{(i)}(t), \quad 1 \le i \le m \tag{1}$$

According to [31], the spacing-policy in Equation (1) improves road efficiency, safety, and attenuates disturbance. Now, the objective of the local control law is to regulate the following distance and velocity errors to zero in the platoon.

$$e^{(i)}(t) = d^{(i)}(t) - d^{r,(i)}(t) \tag{2}$$

$$\dot{e}^{(i)}(t) = v^{(i-1)}(t) - v^{(i)}(t) - \tau_h^{(i)} a^{(i)}(t) \tag{3}$$

Subsequently, a platoon of homogeneous vehicles (the dynamics and the controller governing all the vehicles are identical) is considered and longitudinal dynamics of the i-th follower vehicle is described by the following set of linear equations based on [4]:

$$\begin{aligned} \dot{d}^{(i)} &= v^{(i)} \\ \dot{v}^{(i)} &= a^{(i)} \\ \dot{a}^{(i)} &= -\frac{1}{\tau} a^{(i)} + \frac{1}{\tau} u^{(i)} \end{aligned} \tag{4}$$

$d^{(i)}(t)$, $v^{(i)}(t)$, $a^{(i)}(t)$ are distance, velocity, and acceleration of the i-th vehicle and $\tau = 1.008$ is a constant that represent inertial delay of vehicles longitudinal dynamics and is assumed to be identical for all vehicle.

B. Communication Network Modeling

We model the V2V communication topology of the platoon with the help of a graph. We assume that the platoon includes n follower vehicles and one leader (0), $\mathrm{X} \triangleq \{0\} \cup \{1, 2, \ldots, n\}$. The information flow among followers and leader is given by a directed graph $G = (\mathcal{V}, \mathcal{E})$. In the graph, nodes represent the leader and followers, $\mathcal{V} = \mathrm{X}$, whose dynamics are given by (4) and edges, $\mathcal{E} = \mathcal{V} \times \mathcal{V}$, represent communication between them. Here, $(i, j) \in \mathcal{E}$ is a unidirectional edge between i and j, that enables i to send messages to j. Neighborhood of $i \in X \setminus \{0\}$ is defined as the set of nodes that are adjacent to it, i.e., $N^{(i)} = \{i\} \cup \{j \in \mathcal{V} : (i, j) \in \mathcal{E}\}$ and with whom it can communicate. In our case, we consider predecessor-leader following communication topology where the preceding car of a follower and the leader of the platoon are its neighbor. To describe the information exchange among followers, we use an adjacency matrix, $M = [m^{(i)(j)}] \in \mathbb{R}^{n \times n}$, where

$$m^{(i)(j)} = \begin{cases} 1 & : (i, j) \in \mathcal{E} \\ 0 & : (i, j) \notin \mathcal{E} \end{cases}$$

Furthermore, we model the communication between the leader and its followers as a directed graph G. As such, there exists a directed edge via which leader exchanges its information with every follower. In this paper, we use the words vehicle and node interchangeably.

C. Closed-Loop Platoon Dynamics

To compute the desired acceleration, the CACC controller of the platoon vehicle, i, relies on the information of neighbors, j, which can be represented as $N^{(i)} = \{j | j \neq i \text{ and } (j, i) \in \mathcal{E}\}$. The controller uses a combination of DSRC based feed forward input, $u_{ff}^{(i)}$, and sensor measurement based feedback input, $u_{fb}^{(i)}$, to obtain the following control input of the plant: $u^{(i)} = u_{fb}^{(i)} + u_{ff}^{(i)}$.

The radar and internal sensors of the CACC unit measures the preceding vehicles distance and velocity, which are used to calculate inter-vehicular errors, $e^{(i)}$, $\dot{e}^{(i)}$. Subsequently, a proportional and derivative (PD) feedback controller operates on the errors to generate the following input:

$$u_{fb}^{(i)} = k_p e^{(i)} + k_d \dot{e}^{(i)} \tag{5}$$

where, k_p is the proportional gain and k_d is the derivative gain of the linear controller.

The feed forward controller uses acceleration data of the directly preceding vehicle $\hat{a}^{(i-1)}$ and the leader $\hat{a}^{(0)}$ (obtained by DSRC) to improve vehicle following and string stability performance. The feed forward control input is given by the following equation:

$$\dot{u}_{ff}^{(i)} = -\frac{1}{\tau_h^{(i)}} u_{ff}^{(i)} + \frac{1}{\tau_h^{(i)}} (\hat{a}^{(i-1)}) + \frac{1}{\tau_h^{(i)}} (\hat{a}^{(0)}) \tag{6}$$

In the case where the vehicles are behaving correctly then $\hat{a}^{(i-1)} = a^{(i-1)}$ and $\hat{a}^{(0)} = a^{(0)}$ during the update periods. We make this assumption as we consider the DSRC communication to be secure.

The closed-loop dynamics of CACC equipped vehicle is obtained by combining the longitudinal dynamics model (Equation 4) with the feedback control law (Equation 5) and the feed forward control law (Equation 6). By choosing the state variable as $x^{(i)T} = [d^{(i)}\ v^{(i)}\ a^{(i)}\ u_{ff}^{(i)}] \in \mathbb{R}^4$, the state space representation of the i-th CACC equipped vehicle in an $n-$ vehicle string is given by the following time-invariant linear equations

$$\begin{aligned} \dot{x}^{(i)} &= A^{(i)}x^{(i)} + B^{(i)}u^{(i)} \\ &= (A^{(i)} + B^{(i)}K^{(i)T})x^{(i)} \end{aligned} \tag{7}$$

$$y^{(i)} = C^{(i)}x^{(i)} \tag{8}$$

where, $A^{(i)}$ is the homogeneous system matrix of the ith vehicle, $B^{(i)}$ is the homogeneous transformation vector corresponding to the control input $u^{(i)}$ of the ith vehicle, $K^{(i)}$ is the homogeneous linear controller gain matrix, $y^{(i)} \in \mathbb{R}^4$ ($i = 0, \cdots, n$), is the output vector, and $C^{(i)}$ is the heterogeneous output transformation matrix of the ith vehicle. The matrices of the above equations are given in Appendix A. The leader, i.e., car 0 has a unique control law, which is $u^{(0)} = u_r$, where u_r is the reference desired acceleration of the platoon. It is assumed that the leader receives u_r in real-time and no prediction is made on its value.

For the closed loop dynamics of the homogeneous platoon, we aggregate the state vector of all the vehicles as: $X = \{x^{(0)T}, x^{(1)T}, x^{(2)T}, \ldots, x^{(n)T}\}$

The homogeneous platoon of cars interconnected by a given information topology can be represented in the following compact form:

$$\dot{X} = \mathbf{A}X \tag{9}$$

$$y^{(i)} = \mathbf{C}^{(i)}X \tag{10}$$

where, $\mathbf{A}$, $\mathbf{C}^{(i)}$ are matrices of the distributed system.

From Equation (7) and Equation (9), we observe that platoon dynamics are functions of each vehicle's longitudinal dynamics A, the network topology M, the distributed feedback and feed-forward control laws, $(u_{fb}^{(i)}, u_{ff}^{(i)})$ and the spacing policy $d_r^{(n)}$. We also discretize Equation (9) and Equation (10) with sampling period of 0.01 second to get the following,

$$X_{k+1} = \mathbf{A}X_k \tag{11}$$

$$y_k^{(i)} = \mathbf{C}^{(i)}X_k \tag{12}$$

D. Attack Strategies

We consider two variants of sensor data manipulation attack and assume that the attacks do not corrupt measurements of all the follower vehicles. In the first type, we assume that the adversary has control over followers of the platoon and it transmits wrong sensor data to the vehicle's controller via its internal network. We define such an attack as False Data Injection (FDI), whose goal is to make the vehicle behave incorrectly. Consequently, such an attack can lead to destabilization of the platoon. The impact of such an attack on the output equation of the system can be described by:

$$y_k^{(i),a} = y_k^{(i)} + \Gamma_k\, \mathbf{a}_k^{(i)} \tag{13}$$

where, $\mathbf{a}_k^{(i)}$ is the malicious injected data vector. The attack scenario can be analyzed with the given Bernoulli model: $\mathbb{P}([\Gamma_k]^{(i)(i)} = 1) = 0, \forall i = 1, 2, \ldots, n,\ k < k_f$ and $\mathbb{P}([\Gamma_k]^{(i)(i)} = 1) = p_{af}, \forall i = 1, 2, \ldots, n,\ k \geq k_f$, where p_{af} is the probability of successfully injecting false data after time k_f.

In the second variant, we consider the attacker is present outside the target vehicle. As such the adversary uses tools such as Jammer to blind the sensors of the targeted follower. We define such an attack as Denial of Service (DoS), whose impact on the system can be captured by the following attacked output signal, $y_k^{(i),a}$:

$$y_k^{(i),a} = y_k^{(i)} - \Gamma_k(y_k^{(i)} - y_\tau^{(i)}) \tag{14}$$

where, τ is the time at which the last good measurement, $y_\tau^{(i)}$, was obtained and $\Gamma_k \in \mathbb{B}^{q\times q}$ is a Binary diagonal matrix whose ith diagonal entry when $[\Gamma_k]^{(i)(i)} = 1$, indicates the DoS attack on vehicle $i \in n$ and $[\Gamma_k]^{(i)(i)} = 0$, shows its absence. Such an attack on vehicles can be represented using the following Bernoulli model: $\mathbb{P}([\Gamma_k]^{(i)(i)} = 1) = 0, \forall i = 1, 2, \ldots, n,\ k \leq \tau$, and $\mathbb{P}([\Gamma_k]^{(i)(i)} = 1) = p_{aj}, \forall i = 1, 2, \ldots, n,\ k > \tau$, where p_{aj} is the probability of successfully jamming the sensor data after time τ. An adversary can carry out any one of these attacks, but not simultaneously. In this paper, we evaluate the vehicle platoon under FDI attack and present the results in Section V. Our experiments can be easily extended to the case of DoS attack.

E. Problem Description

Given a homogeneous platoon of n follower vehicles and a leader represented by linear time-invariant system model, linear measurement model, and directed communication graph G, our goal is to design a filter that can estimate system states such that $\lim_{k\to\infty} \|\hat{X}_k^{(i)} - X_k\| \to 0,\ \forall i \in \mathbb{R}^n$ when there is no attack and the estimation errors are bounded when measurements of all sensors of a subset of vehicles of the platoon $\mathcal{V}_a \subset \mathcal{V}$ are compromised by an attack.

To build such an estimator, we make the following assumptions.

- Matrix $(\mathbf{A}, \mathbf{C}^{(i)})$ are detectable of the system. This assumption is in line with the assumption in [28], [32], where it was stated as necessary condition for solving the distributed estimation problem with asymptotic guarantees.
- Each vehicle receives estimated state information from the vehicle in front and the leader via a secure communication channel. Thus, we do not consider any attack on the network.
- We assume that the vehicles cannot detect the attack on the sensor measurements and thus accepts the corrupted state estimates from its neighbors.

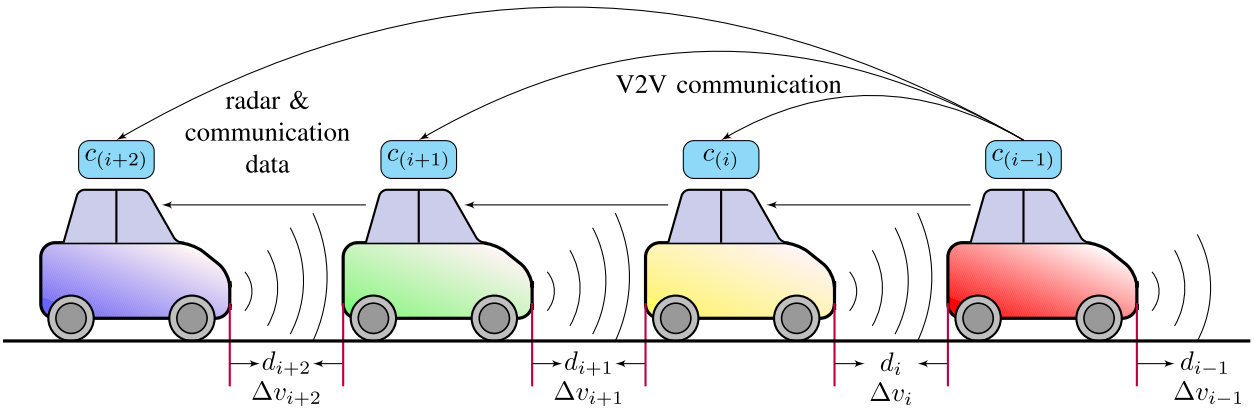


Fig. 1. Homogeneous CACC vehicle platoon with predecessor-leader following communication topology.

IV. Design & Analysis of Distributed Estimator

In this section, we first analyze the performance of the Distributed Kalman Filter (DKF) in attack-free and noise-free scenarios. The motivations behind this analysis are two-fold: (i) to the best of our knowledge, this is the first convergence result on DKF for noise-free and attack-free scenarios; and (ii) it forms the basis for the analysis of our attack resilient estimator.

A. Distributed Estimation Without Attack

Based on the Bayesian interpretation of the Kalman filter that consider local measurements from vehicle i, state estimates of the neighbors of i, output equation, $y_k^{(i)} = \mathbf{C}^{(i)}X + v_k^{(i)}$ with $v_k^{(i)} \sim N(0, \Sigma_v^{(i)})$, and state equation, $X_{k+1} = \mathbf{A}X_k + w_k^{(i)}$ with $w_k^{(i)} \sim N(0, \Sigma_w^{(i)})$, the state estimator can be described as: $\mathbf{P}_{k|k-1}^{(i)} = A\mathbf{P}_{k-1}^{(i)}A^T + \Sigma_w^{(i)}$; $\mathbf{P}_k^{(i)} = \left(\frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_{k|k-1}^{(j)\,-1} + C_i^T \Sigma_v^{(i)\,-1} C_i\right)^{-1}$; $\hat{X}_k^{(i)} = \mathbf{P}_k^{(i)}\left(\frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_{k|k-1}^{(j)\,-1} A\hat{X}_{k-1}^{(j)} + C^{(i)\,T}\Sigma_v^{(i)\,-1} y_k^{(i)}\right)$; where $\mathbf{P}_k^{(i)}$ is the estimation error covariance matrix and $\hat{X}_k^{(i)}$ is the state estimate.

First, we investigate the attack-free and noise-free case for the following discrete time linear-time invariant (LTI) model

$$X_{k+1} = \mathbf{A}X_k,\ \ y_k^{(i)} = \mathbf{C}^{(i)}X_k \tag{15}$$

We assume that $\mathbf{P}^{(i)}$ is chosen according to the following equation,

$$\mathbf{P}^{(i)} = \left(\frac{1}{d_i}\sum_{j\in N^{(i)}} (\mathbf{A}\mathbf{P}^{(j)}\mathbf{A}^T + \Sigma_w^{(j)})^{-1} + \mathbf{C}^{(i)\,T}\Sigma_v^{(i)\,-1}\mathbf{C}^{(i)}\right)^{-1} \tag{16}$$

where, $N^{(i)} = \{i\} \cup \{\text{neighbors of } i \text{ in } G\}$ and $d_i = |N^{(i)}|$ is the total number of neighbors of node i. While in Kalman filter, $\Sigma_v^{(i)}$ and $\Sigma_w^{(i)}$ are commonly used to denote the covariance of the noise in the system, they can also be treated as parameters for developing the algorithm in the noise-free setting (Kalman filter application in the noise-free setting is discussed in [33]). In principle, they can be chosen to be any positive definite matrices. The impact of the values of $\Sigma_v^{(i)}$ and $\Sigma_w^{(i)}$ on the estimate are discussed in Section IV-B. The distributed estimator then has the following prediction rules,

$$\begin{aligned}\mathbf{P}_{|}^{(i)} &= \mathbf{A}\mathbf{P}^{(i)}\mathbf{A}^T + \Sigma_w^{(i)}\\ \hat{X}_k^{(i)} &= \mathbf{P}_k^{(i)}\left(\frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_{|}^{(j)-1}\mathbf{A}\hat{X}_{k-1}^{(j)} + \mathbf{C}^{(i)T}\Sigma_v^{(i)-1}y_k^{(i)}\right)\end{aligned} \tag{17}$$

where, $\mathbf{P}_{|}^{(i)}$ is *a priori* estimate covariace of vehicle i. This estimator is motivated from the Distributed Kalman Filter studied of [34]–[37].

Before applying this estimator, we need to ensure that a solution to (16) exist. Thus, we give the following theoretical guarantee on the existence of solution.

Theorem 4.1: If the graph G is connected, $\mathbf{A}$ is full-rank, $(\mathbf{A}, \mathbf{C}^{(i)})$ is observable, and $\Sigma_v^{(i)}$ is full rank for all $1 \le i \le n$, then there exist $\{\mathbf{P}^{(i)}\}_{i=1}^n$ that satisfy Equation (16).

This proof of Theorem 4.1 in Appendix B shows that the covariance matrices of the estimator converges when they are initialized as zero matrices. In comparison, there exist work on convergence of the covariance matrices of DKF: The authors in [38] prove the convergence of the covariance using probability theory and the authors in [35] perform convergence analysis on a modified DKF which has one prediction/update step at each time point. We remark that the convergence analysis in the standard Kalman filter uses observability assumption and as such it is the optimal assumption we could make as well.

The following theorem states the main result of distributed estimation without attack and noise and its proof is in the Appendix B. This theorem states that the estimation error converges to zero in the attack-and noise-free scenario. There exist work on convergence of estimation error of DKF. For the noise-free case, Li *et al.* [39] prove that estimation error converges to a unique value. However, we are not aware of any work that has convergence result for the attack-and noise-free scenario as considered by us. Our proof is based on the observation that the estimation error do not increase over time and as a result, the estimation error converges.

Theorem 4.2: (*Convergence of DKF*) Under the assumptions of Theorem 4.1, the estimator Equation (17) converges to the correct solution in the sense that for all $1 \le i \le n$, $\lim_{k\to\infty} \|\hat{X}_k^{(i)} - X_k\| \to 0$.

The result described here is called the "omniscience property" [28], [32], which is proved under the same system setting as Theorem 4.2, but for a different estimation algorithm. We remark that while the condition "$(\mathbf{A}, \mathbf{C}^{(i)})$ is observable" is more restrictive than the condition "$(\mathbf{A}, \mathbf{C}^{(i)})$ is detectable" of [32], in practice the difference could be addressed using the idea of decomposing the system $(\mathbf{A}, \mathbf{C}^{(i)}, X)$ into two parts corresponding to stable and unstable eigenvalues of $\mathbf{A}$. Note that for X, the stable part converges to zero, thus it is sufficient to investigate the subsystem of $(\mathbf{A}, \mathbf{C}^{(i)}, X)$ that is associated with unstable eigenvalues of $\mathbf{A}$. More specifically, let $\mathbf{A} = \mathbf{U}\text{diag}(\mathbf{S}_1, \mathbf{S}_2)\mathbf{U}^{-1}$ be the Jordan transformation of $\mathbf{A}$, where $\mathbf{U}$ is the similarity transformation matrix, $\mathbf{S}_1$ is a square matrix that contains all Jordan blocks with stable eigenvalues and $\mathbf{S}_2$ consists of all Jordan blocks with unstable eigenvalues. Then, with $\tilde{X}_k = \mathbf{U}^{-1}X_k$ and $\tilde{X}_k = [\tilde{X}_{1,k}, \tilde{X}_{2,k}]$, the state evolution of (15) is equivalent to the equations: $\tilde{X}_{k+1,1} = \mathbf{S}_1\tilde{X}_{k,1}$, $\tilde{X}_{k+1,2} = \mathbf{S}_2\tilde{X}_{k,2}$. We have $\|\tilde{X}_{k,1}\| \to 0$ as $k \to \infty$. Thus, it is sufficient to estimate $\tilde{X}_{k,2}$. To have the "omniscience property" of the estimation of $\tilde{X}_{k,2}$ from $\mathbf{y}_k^{(i)} = \mathbf{C}^{(i)}\mathbf{U}\tilde{X}_k \approx \mathbf{C}^{(i)}\mathbf{U}_2\tilde{X}_{k,2}$ ($\mathbf{U}_2$ is a submatrix of $\mathbf{U}$ corresponding to the component $\mathbf{S}_2$), Theorem 4.2 implies that it is sufficient to have the observability of $(\mathbf{S}_2, \mathbf{C}^{(i)}\mathbf{U}_2)$. By applying the "Eigenvalue assignment" of [40, Table 15.1], it can be shown that the observability of $(\mathbf{S}_2, \mathbf{C}^{(i)}\mathbf{U}_2)$ is equivalent to the detectability of $(\mathbf{A}, \mathbf{C}^{(i)})$.

B. Resilient Distributed State Estimator

We discuss the design of our optimization based estimator, RDSE, which is resilient to sensor attacks. We also analyze its performance and prove that when there is no attack, the estimation error converges to zero and in the presence of attack, the estimation error is bounded.

We investigate the case with attack, which is given by the following model: $X_{k+1} = \mathbf{A}X_k$, $y_k^{(i),a} = \mathbf{C}^{(i)}X_k + \mathbf{a}_k^{(i)}$ where $\mathbf{a}_k^{(i)}$ is the attacker input and following is our RDSE based on optimization:

$$\begin{aligned}\hat{X}_k^{(i)} = \arg\min_{X_k, a_k^{(i)}} &(y_k^{(i),a} - \mathbf{C}^{(i)}X_k - \mathbf{a}_k^{(i)})^T \Sigma_v^{(i)\,-1} \\ &\times (y_k^{(i),a} - \mathbf{C}^{(i)}X_k - \mathbf{a}_k^{(i)}) + \lambda \left\|\mathbf{a}_k^{(i)}\right\|_1 \\ &+ \frac{1}{d_i}\sum_{j\in N^{(i)}} (X_k - \mathbf{A}\hat{X}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)-1}(X_k - \mathbf{A}\hat{X}_{k-1}^{(j)}) \quad (18)\end{aligned}$$

This method is motivated from the DKF in Equation (17) as follows: Equation (17) can be considered as the following optimization problem:

$$\begin{aligned}\hat{X}_k^{(i)} = \arg\min_{X_k} &(y_k^{(i),a} - \mathbf{C}^{(i)}X_k)^T \Sigma_v^{(i)\,-1}(y_k^{(i),a} - \mathbf{C}^{(i)}X_k) \\ &+ \frac{1}{d_i}\sum_{j\in N^{(i)}} (X_k - \mathbf{A}\hat{X}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)-1}(X_k - \mathbf{A}\hat{X}_{k-1}^{(j)}) \quad (19)\end{aligned}$$

To make an optimization-based estimator more resilient to attacks, a commonly used strategy is to use optimization with ℓ_1 norm on the terms affected by attack [24]. We apply a similar strategy, where we apply a penalty, λ, on the attacked values, $\mathbf{a}_k^{(i)}$ and subtract the attack value from the attacked measurement $y_k^{(i),a}$. This procedure makes our algorithm more resilient to attacks. The optimization problem in Equation (18) does not have an explicit solution, but it can be solved efficiently as it is a convex optimization problem.

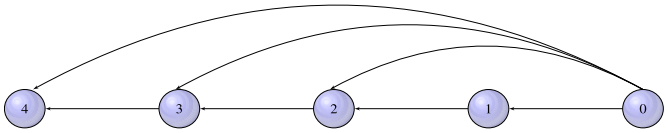


Fig. 2. Directed graph of homogeneous predecessor-leader following topology of five vehicle platoon. (0)-(4) represents numbering of vehicles (nodes), with (0) being the leader of the platoon. The edges represents sensor and V2V communication between vehicles.

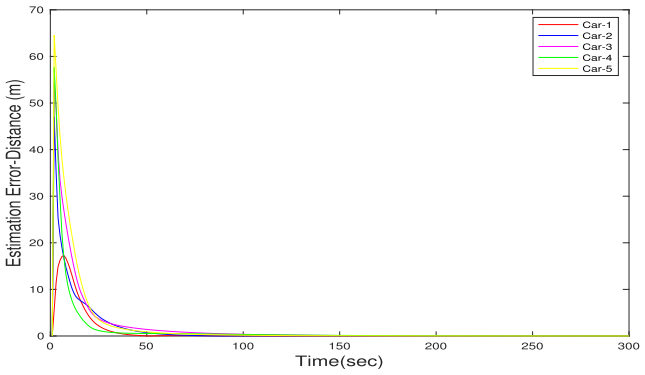


Fig. 3. Performance of our resilient distributed estimator, (18), in the attack free case. ($\lambda = 2$, $\Sigma_v = 10\mathbf{I}$, $\Sigma_w = \mathbf{I}$).

The choice of λ is critical in our approach and it gives a balance between the terms, $\mathbf{a}_k^{(i)}$ and $\sum_{j\in N^{(i)}}(X_k - \mathbf{A}\hat{X}_{k-1}^{(j)})^T\mathbf{P}_{|}^{(j)\,-1}(X_k - \mathbf{A}\hat{X}_{k-1}^{(j)})$. A large value of λ implies more weight is placed on attacked values, $\mathbf{a}_k^{(i)}$. Although, such a choice of λ makes the estimation error converge quickly to a small value, it will give less stable performance in the presence of an attack. On the contrary, when λ is small, it will take longer for the estimation error to converge to a small value, but the method will be stable against attack.

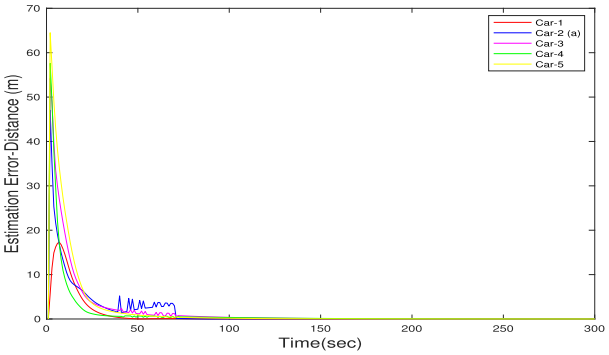
As $\Sigma_v^{(i)\,-1}$ appears in the term $(y_k^{(i),a} - \mathbf{C}^{(i)}X_k)^T\Sigma_v^{(i)\,-1}(y_k^{(i),a} - \mathbf{C}^{(i)}X_k)$, it will have an impact opposite to that of λ on state estimate i.e. when Σ_v is large, it will take longer for the estimation error to converge to a small value, but it will make the method stable against attack. In contrast, large value of Σ_w will result in large $\mathbf{P}_{|}$ and it will have an impact similar to λ on state estimates. Furthermore, experimental results in Section V demonstrate the impact of these parameters on state estimation error.

To analyze this estimator, we consider two scenarios:

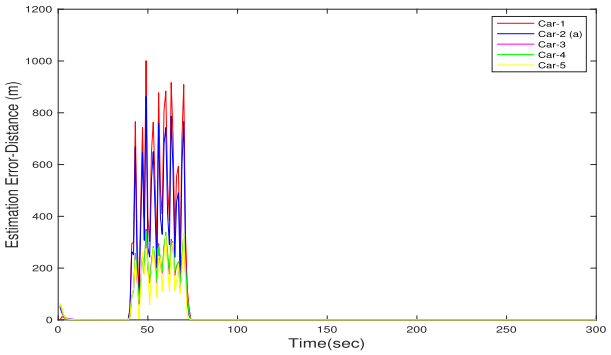
1) Sensors of all vehicles are benign and the platoon operates normally.

2) Sensors of some vehicles are compromised.

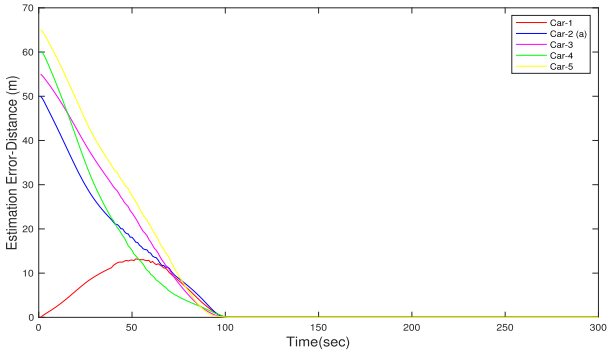
We provide the following theoretical guarantee (proof is in Appendix B) for the first scenario. It suggests that when the initial estimation error $\hat{\mathbf{e}}_0^{(i)}$ is not too large, the algorithm follow the "omniscience property" and the estimation error converges to zero. Now, the proof of this theorem is based on the structure of the proof of Theorem 4.2, i.e., we first show that the estimation error does not increase over time and then,



(a) Performance of our RDSE, (18), during FDI attack. Car under attack is marked with (a). Distance estimation error is bounded and small. ($\lambda = 2, \Sigma_v = 10\mathbf{I}, \Sigma_w = \mathbf{I}$)



(b) Performance of Distributed Kalman Filter (DKF), (19), during FDI attack. Car under attack is marked with (a). Distance estimation error is large. ($\lambda = 2, \Sigma_v = 10\mathbf{I}, \Sigma_w = \mathbf{I}$)



(c) Performance of Resilient Distributed Kalman Filter (RDKF), of [47], during FDI attack. Car under attack is marked with (a). Convergence time is longer compared to RDSE. ($\lambda = 2, \Sigma_v = 10\mathbf{I}, \Sigma_w = \mathbf{I}$)

Fig. 4. FDI attack: (a, b, c) comparison of estimated distance error of RDSE against DKF and RDKF.

with some additional arguments, we show that the estimation error converges to zero.

Theorem 4.3: (*Convergence of RDSE*) Let c_0 be a number such that if $\mathbf{e}^{(i)}$ satisfies $\mathbf{e}^{(i)\,T}\mathbf{P}_{|}^{(i)\,-1}\mathbf{e}^{(i)} \leq c_0$ for all $1 \leq i \leq n$, then for all $1 \leq i \leq n$,

$$\left\| \Sigma_v^{(i)\,-1}\mathbf{C}^{(i)}\mathbf{P}_{|}^{(i)} \left(\frac{1}{d_i} \sum_{j \in N^{(i)}} \mathbf{P}_{|}^{(j)\,-1} A\mathbf{e}^{(j)} \right) \right\|_{\infty} \leq \lambda/2. \quad (20)$$

Under the assumptions of Theorem 4.1, if the initial estimation error $\hat{\mathbf{e}}_0^{(i)}$ is small in the sense that $\hat{\mathbf{e}}_0^{(i)\,T}\mathbf{P}_{|}^{(i)\,-1}\hat{\mathbf{e}}_0^{(i)} \leq c_0$ for all $1 \leq i \leq n$, then for the first scenario without attack, the estimation of $\mathbf{a}_k^{(i)}$ in (18) is consistently zero and the sequence produced by (18) converges to the correct solution i.e. for all $1 \leq i \leq n$, $\lim_{k\to\infty} \|\hat{X}_k^{(i)} - X_k\| \to 0$.

We remark that, while this theorem makes the assumption that the initial estimation error $\{\hat{\mathbf{e}}_0^{(i)}\}_{i=1}^n$ is not very large, in practice we notice that our algorithm converges even when initial estimations of $X_0^{(i)}$ are bad.

For the second scenario, the following resiliency theorem (proof in the Appendix B) states that no matter how large the magnitude of the attack, the deviation of the state estimate of RDSE is bounded. Consequently, even during a worst-case attack scenario, the error of the state estimate is upper bounded. Compared to Theorem 4.3, which states that the estimation error converge to zero when there is no attack, this result suggests that the estimation error is bounded during attack. This result separates RDSE from the traditional DKF of Section IV-A, where an unbounded attack could result in an unbounded estimation error. Furthermore, our analysis and results are different from the theoretical guarantees given for the resilient distributed estimator of [28]. We have made fewer assumptions on the eigenvalues of $\mathbf{A}$ and graph structure of the network. We only show that the estimation error is bounded (rather than convergence to zero result shown in [28]).

Theorem 4.4: (*Resiliency of RDSE*) Consider the optimization problem (18). For different values of $y_k^{(i),a}$, the norm of the difference of the estimated value $\hat{X}_k^{(i)}$ is at most

$$\lambda\|\mathbf{K}\|\|[(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K})^T \Sigma_v^{(i)\,-1}(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K}) + \mathbf{K}^T\mathbf{Q}\mathbf{K}]^{-1}\|, \quad (21)$$

where $\mathbf{K} = (\mathbf{Q} + \mathbf{C}^{(i)T}\Sigma_v^{(i)\,-1}\mathbf{C}^{(i)})^{-1}\mathbf{C}^{(i)T}\Sigma_v^{(i)\,-1}$ and $\mathbf{Q} = \frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_{|}^{(j)\,-1}$.

This theorem implies that the disturbance on the state estimate caused by an arbitrary attack on $y_k^{(i),a}$ is bounded. It also partially explains the observations that large $\Sigma_v^{(i)}$ corresponds to more stable performance of the estimator during an attack. According to Equation (21) (represents the maximum additional estimation error that can be caused by an attack), large $\Sigma_v^{(i)}$ will make the upper bound on estimation error smaller.

C. Discussions

Recently, researchers have demonstrated successful attacks on sensors such as LIDAR, GPS, ultrasonic, camera, and radar [41]–[45]. As such, autonomous vehicles that rely heavily on

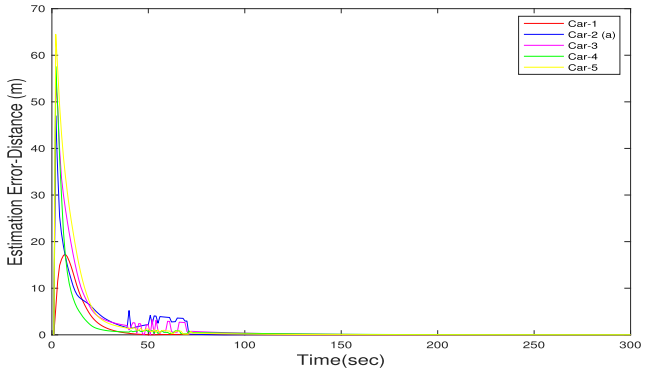


Fig. 5. Performance of our RDSE, (18), during FDI attack on multiple cars-2, 3. ($\lambda = 2$, $\Sigma_v = 10\mathbf{I}$, $\Sigma_w = \mathbf{I}$).

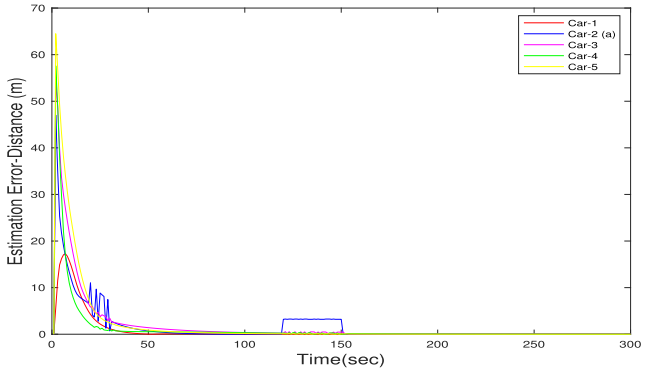


Fig. 6. Performance of our RDSE, (18), during multiple FDI attack on cars-2. ($\lambda = 2$, $\Sigma_v = 10\mathbf{I}$, $\Sigma_w = \mathbf{I}$).

these sensors for decision making remains vulnerable to attack. Our estimator, RDSE, is a countermeasure against jamming and false data injection attack on vehicle sensors. Our system-level solution will ensure that the vehicle gracefully degrades to a less optimal, but safe operational mode during attack and return to optimal operational mode after attack. As such, our estimator when combined with the CACC controller will ensure the safety and the mobility of the platoon. However, certain properties of vehicle platoon such as cost and emission benefits will not be preserved during an attack. In future, we will present quantitative analysis to show the impact of combining CACC controller with our RDSE on safety, mobility, emission, and cost.

We remark that the Theorem 4.4 only captures the impact of sporadic attack (an attack which does not occur continuously for a long time) on the estimation of $\hat{X}_k^{(i)}$. Following this theorem, if the estimation error is small enough to satisfy the condition of Theorem 4.3 after an attack, then we can consider such an estimation error as the "initial estimation error" in Theorem 4.3 and use it to show that despite the attack, the estimation error of our estimator still converge to zero, provided we have attack-free measurements after the sporadic attack. The long-term impact of persistent attack is not considered and we leave it as possible future work.

V. Experimental Results

In this section, we consider a platoon of five vehicles to demonstrate the effectiveness of the RDSE approach against sensor attacks. We represent the dynamics of vehicles of the platoon using a linear time-invariant model given by (7). The sensor measurement equations of a car with and without attacks are given by Equations (8), (13) and (14), respectively. The system matrix $\mathbf{A}$, the input transformation matrix B, the controller gain matrix K, and the output matrix $\mathbf{C}^{(i)}$, of the homogeneous platoon are given in Appendix A. The dimension of the state, x, of each vehicle is four and each follower is equipped with four sensors. Also, the leader vehicle has information of all the follower vehicles of the platoon.

The directed communication graph of the platoon, as shown in Figure 2, consists of five nodes (representing homogeneous vehicles) and eight edges (representing radar and V2V communication). We simulate vehicle dynamics of the platoon, communication graph, and the sensor attack in MATLAB.

• *Case 1: Attack-free scenario*

We first evaluate our algorithm over the attack-free scenario. Figure 3 compares estimation error of five vehicles over a time frame of 300 seconds. Y-axis represents normalized distance estimation error of all the cars in meters (m). We observe that the state estimation error is less than 70m for all the cars and they converge to a small value (< 1m) within 50 seconds.

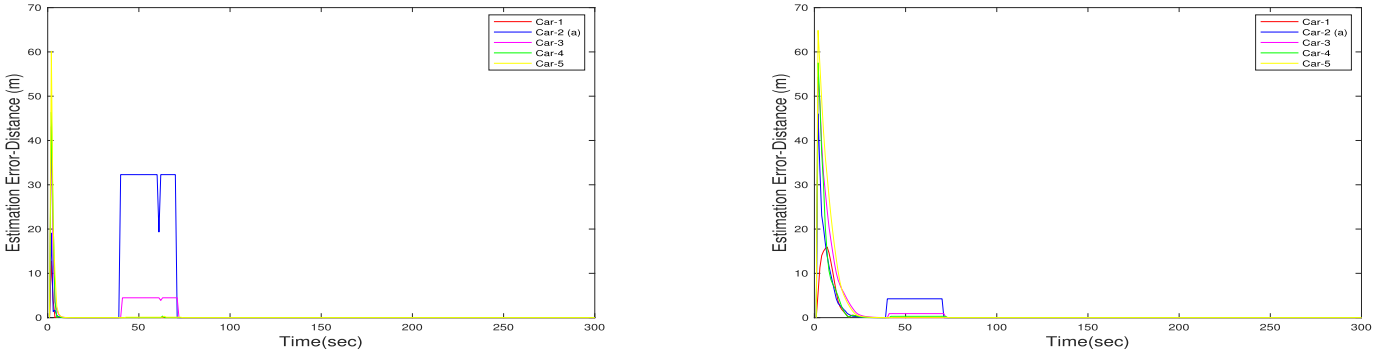
• *Case 2: False Data Injection (FDI) attack*

We consider a scenario where an adversary corrupts measurements of internal sensors of a vehicle after a certain time point. In case of a FDI attack on our experimental system, malicious data of random value are added to all sensor outputs of car-2, 3 at random time points of variable duration.

Case 2-a: Resiliency Comparison

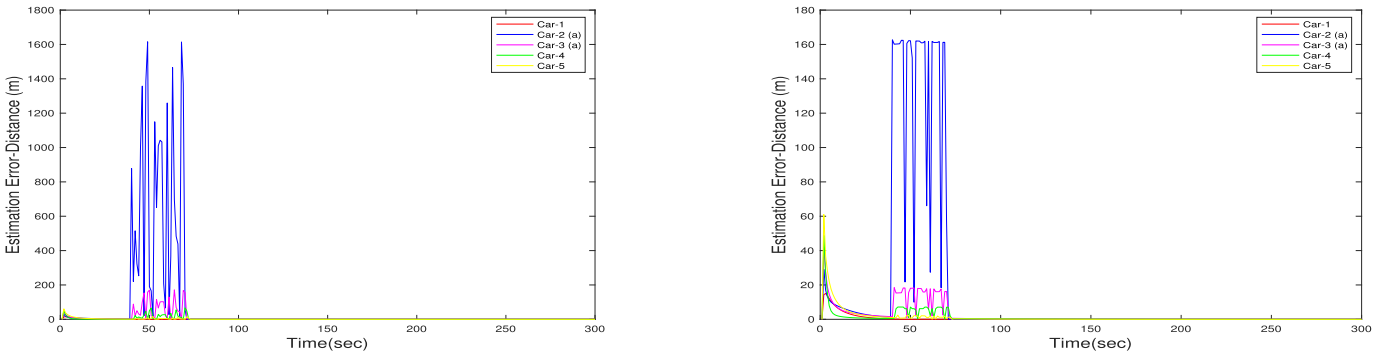
In this case, we compare the performance of RDSE against the Distributed Kalman Filter (DKF) and Resilient Distributed Kalman Filter (RDKF) of [46] during FDI attack. For the experimental setup, we assume that the attacked signal $\{\mathbf{a}_k^{(i)}\}_{i=2,3}$ is injected into the output sensor data of the attacked cars at different time points, but the attack does not corrupt all the measurements after its initiation. The probability of occurrence of the FDI attack at any time after its initiation on a vehicle is $p_a = 0.99$, i.e. probability of an attack being successful is high during the attack duration. For instance, in our experiment, the attack on car-2 of Figure 4a is successful at most of the time points from $41 - 70$ seconds. In our simulation, we set the parameters $(\lambda, \Sigma_v, \Sigma_w) = (2, 10\mathbf{I}, \mathbf{I})$, where $\mathbf{I}$ is the identity matrix. Figure 4 compares the performance of our proposed algorithm against DKF and RDKF [46]. We observe that the FDI attack affects distance estimation of the neighbor (car-3) of the compromised car-2. Note that the estimated distance error of our filter, shown in Figure 4a, are small and the system is stable, while the error in DKF goes up to 1000m and the error takes longer to converge to a small value in case of RDKF. When there is no attack, our method perform as well as an optimal estimator for distributed systems. As perturbation in estimation error caused by the attack is small in our algorithm, the likelihood of preventing collision is high, as it keeps the distance error (< 6 m) between cars-$(2, 3)$ less than the minimum stopping distance of $d_r = 10$m.

The vast difference in performance between RDKF of [46] and RDSE can be attributed to the design of the estimators. In RDSE, the parameter λ directly affect the sensitivity of



(a) $(\lambda = 2, \Sigma_v = \mathbf{I}, \Sigma_w = 10\mathbf{I})$ (b) $(\lambda = 2, \Sigma_v = \mathbf{I}, \Sigma_w = \mathbf{I})$

Fig. 7. Performance of our RDSE for fixed $\lambda = 2$ and different values of parameters Σ_w, during FDI attack on car-2.



(a) $(\lambda = 1000)$ (b) $(\lambda = 100)$

Fig. 8. Performance of our RDSE for fixed $\Sigma_v = 10\mathbf{I}$, $\Sigma_w = \mathbf{I}$ and different values of $\lambda = 1000, 100$, during FDI attack on car-2.

the estimator to attack. As such, small value of λ makes the estimator more resilient to attack, whereas large value make the estimator more sensitive to attack. It should be noted that λ does not affect the convergence of RDSE. On the contrary, in RDKF of [46], λ affects the local information of the agent and the information of its neighbors. Large value of λ implies more weight is placed on local information and neighbors information. Although such a choice of λ makes the estimation error converge to zero quickly in the absence of attack, it will make the system less resilient to attack. When λ is small, it will take longer for the estimation errors to converge to zero in RDKF, but the method will be more resilient to attack. Thus, the value of $\lambda = 2$ chosen in our current setting is suitable to increase resiliency of RDKF, but it takes more time to converge than the RDSE. In longer simulation run, the performance of RDKF and RDSE are comparable.

Case 2-b: Attack on Multiple Cars and Attacks with Multiple Time Duration

We further considered attack on multiple cars-2, 3 between time duration $40 - 70$ seconds and with parameter values, $(\lambda, \Sigma_v, \Sigma_w) = (2, 10\mathbf{I}, \mathbf{I})$. From Figure 5 we observe that the distance estimation errors for all the cars are less than safety distance of $d_r = 10$m. Furthermore, we consider attack on car-2 with same parameter values at multiple time duration's, $20-30$ seconds and $120-150$ seconds. We observe from Figure 6, that the estimation error is within the safe distance. Also, after the first attack (from $20 - 30$ seconds), the filter takes 18 seconds to recover and reduce the distance estimation error to $<$ 2m. After the second attack (from $120 - 150$ seconds), it takes 1 second to recover and reduce the distance estimation error to $<$ 1m. This is because as the filter stabilizes, it takes less time to converge when subsequent attack occurs.

Case 2-c: Parameter Tuning

We also tried various values of parameters λ and Σ_w. In particular, we follow the setup of Figure 4a i.e. fix $\lambda = 2$ and replace Σ_w by $10\mathbf{I}$ and $\mathbf{I}$. The results obtained are shown in Figure 7. We also fix the value of parameters $(\Sigma_v = 10\mathbf{I}, \Sigma_w = \mathbf{I})$ and vary $\lambda = 1000, 100$ and the results are shown in Figure 8. As stated in Section IV-B, smaller λ or larger Σ_v gives slower convergence at the beginning, but more stable performance during attacks, and larger Σ_w gives faster convergence at the beginning, but less stable performance during attacks.

VI. Conclusion

In this paper, we have proposed a novel attack-resilient distributed state estimation algorithm, RDSE, that can recursively estimate states and it bounds the error on state estimates during attack on sensors of a platoon vehicle. We consider a homogeneous platoon of five vehicles and demonstrate that the estimation error of our method asymptotically converges to zero when there is no attack and has an upper bound during False Data Injection (FDI) attack. Our results show that after proper tuning of the parameters of the estimator, the distance estimation error is always below the safe distance even in the presence of an attack. In the future, we plan to improve our current analysis to stochastic systems and also intend to develop new attack-detection procedures.

APPENDIX A - MATRICES

$$A^{(i)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -\tau^{-1} & \tau^{-1} \\ 0 & 0 & \tau_h^{-1} & -\tau_h^{-1} \end{bmatrix}$$

$$B^{(i)} = \begin{bmatrix} 0 \\ 0 \\ \tau^{-1} \\ 0 \end{bmatrix} \quad K^{(i)} = \begin{bmatrix} k_p \\ -(k_p\tau_h + k_d) \\ -(1 + k_d\tau_h) \\ 0 \end{bmatrix}$$

$C^{(i)}$ is heterogeneous binary random 4×4 matrix, for all $i = 0, 1, \ldots, n$.

$\mathbf{A}$ is $4(n+1) \times 4(n+1)$ matrix obtained by combining $(A^{(i)} + B^{(i)}K^{(i)T})$ matrix of all $i = 0, \ldots, n$ according to the adjacency matrix M.

$\mathbf{C}^{(i)}$ is heterogeneous binary random $4 \times 4(n+1)$ matrix.

APPENDIX B - PROOF OF THEOREMS

Proof of Theorem 4.1

In the proof, both $\mathbf{A} \succcurlyeq \mathbf{B}$ and $\mathbf{B} \preccurlyeq \mathbf{A}$ mean that $\mathbf{A} - \mathbf{B}$ is positive semidefinite.

Here, we let $\mathbf{P}_0^{(i)} = \mathbf{0}$ for all $1 \le i \le n$ and show that for the sequence $\mathbf{P}_k^{(i)}$ generated by

$$\mathbf{P}_{k|k-1}^{(i)} = \mathbf{A}\mathbf{P}_{k-1}^{(i)}\mathbf{A}^T + \Sigma_w^{(i)}$$

$$\mathbf{P}_k^{(i)} = \left(\frac{1}{d_i} \sum_{j \in N^{(i)}} \mathbf{P}_{k|k-1}^{(j)\,-1} + \mathbf{C}^{(i)\,T} \Sigma_v^{(i)\,-1} \mathbf{C}^{(i)} \right)^{-1}$$

the limit, $\lim_{k\to\infty} \mathbf{P}_k^{(i)}$, exists and it is a positive definite matrix for all $1 \le i \le n$. If this is true, then $\mathbf{P}^{(i)} = \lim_{k\to\infty} \mathbf{P}_k^{(i)}$ is a solution to (16).

We will first show that $\mathbf{P}_1^{(i)\,-1}$ is bounded below by a positive definite matrix. For $k = 1$, we have

$$\mathbf{P}_1^{(i)\,-1} \succcurlyeq \mathbf{C}^{(i)T} \Sigma_v^{(i)\,-1} \mathbf{C}^{(i)},$$

which is positive semidefinite with range being the row space of $\mathbf{C}^{(i)}$, i.e., $\{\mathbf{C}^{(i)\,T}\mathbf{z} : \mathbf{z} \in \mathbb{R}^q\}$.

If $j \in N^{(i)}$ (and by definition $i \in N^{(i)}$), then

$$\mathbf{P}_2^{(i)\,-1} \succcurlyeq \frac{1}{d_i}(\mathbf{A}\mathbf{P}_1^{(j)}\mathbf{A}^T + \Sigma_w^{(j)})^{-1} + \mathbf{C}^{(i)T} \Sigma_v^{(i)\,-1} \mathbf{C}^{(i)} + \frac{1}{d_i}(\mathbf{A}\mathbf{P}_1^{(i)}\mathbf{A}^T + \Sigma_w^{(i)})^{-1},$$

which is a positive semidefinite matrix of range $\{\mathbf{C}^{(i)\,T}\mathbf{z}_1 + \mathbf{A}\mathbf{C}^{(i)\,T}\mathbf{z}_2 + \mathbf{A}\mathbf{C}^{(i)\,T}\mathbf{z}_3 : \mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3 \in \mathbb{R}^q\}$. By applying the same procedure to time $k = 3, 4, \cdots$, we verify that for sufficiently large k, the range of $\mathbf{P}_k^{(i)\,-1}$ can be given by the linear combination of $\oplus_j \{\mathbf{A}^{l(j)}\mathbf{C}^{(j)T}\mathbf{z}\}\ \forall j$ such that there exists a path from j to i of length $l(j)$. It can be shown that for sufficiently large k, the set contains the range of $\mathbf{A}^r\mathbf{C}^T, \mathbf{A}^{r+1}\mathbf{C}^T, \mathbf{A}^{r+2}\mathbf{C}^T, \cdots$ for some positive integer r. When $\mathbf{A}$ is full-rank and $(\mathbf{A}, \mathbf{C}^{(i)})$ is observable, this range is $\mathbb{R}^n$ and as a result, $\mathbf{P}_k^{(i)\,-1}$ is larger than a positive definite matrix with full rank. This suggests that $\mathbf{P}_k^{(i)}$ is bounded by a positive definite matrix from above.

In addition, by induction it can be shown that $\mathbf{P}_k^{(i)}$ is strictly increasing in the sense that

$$\mathbf{P}_0^{(i)} \preccurlyeq \mathbf{P}_1^{(i)} \preccurlyeq \mathbf{P}_2^{(i)} \preccurlyeq \cdots.$$

Since, the sequence is bounded above, its limit exist. In addition,

$$\mathbf{P}_k^{(i)} \succcurlyeq \left(\frac{1}{d_i} \sum_{j \in N^{(i)}} \Sigma_w^{(j)\,-1} + \mathbf{C}^{(i)T} \Sigma_v^{(i)\,-1} \mathbf{C}^{(i)} \right)^{-1}$$

Thus, its limit is positive definite.

■ *Proof of Theorem 4.2* We specify the estimation error as $\mathbf{e}_k^{(i)} = \hat{X}_k^{(i)} - X_k$ and show that,

$$\mathbf{e}_k^{(i)\,T} \mathbf{P}^{(i)\,-1} \mathbf{e}_k^{(i)} \le \frac{1}{d_i} \sum_{j \in N^{(i)}} \mathbf{e}_{k-1}^{(j)\,T} \mathbf{P}^{(j)\,-1} \mathbf{e}_{k-1}^{(i)}. \tag{22}$$

Applying (19), we have $\mathbf{e}_k^{(i)} = \arg\min_{\mathbf{e}_k} f(\mathbf{e}_k)$, where

$$f(\mathbf{e}_k) = (\mathbf{C}^{(i)}\mathbf{e}_k)^T \Sigma_v^{(i)\,-1} (\mathbf{C}^{(i)}\mathbf{e}_k) + \frac{1}{d_i} \sum_{j \in N^{(i)}} (\mathbf{e}_k - \mathbf{A}\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)-1} (\mathbf{e}_k - \mathbf{A}\mathbf{e}_{k-1}^{(j)}) \tag{23}$$

Using the fact that $\nabla f(\mathbf{e}_k)|_{\mathbf{e}_k = \mathbf{e}_k^{(i)}} = 0$, we have

$$(\mathbf{C}^{(i)}\mathbf{e}_k^{(i)})^T \Sigma_v^{(i)\,-1} (\mathbf{C}^{(i)}\mathbf{e}_k^{(i)}) + \frac{1}{d_i} \sum_{j \in N^{(i)}} (\mathbf{e}_k^{(i)} - A\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)\,-1} \mathbf{e}_k^{(i)} = 0. \tag{24}$$

Combining (24) with $f(\mathbf{e}_k^{(i)}) \ge 0$ gives,

$$\frac{1}{d_i} \sum_{j \in N^{(i)}} (\mathbf{A}\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)\,-1} \mathbf{A}\mathbf{e}_{k-1}^{(j)} \ge (\mathbf{C}^{(i)}\mathbf{e}_k^{(i)})^T \Sigma_v^{(i)\,-1} (\mathbf{C}^{(i)}\mathbf{e}_k^{(i)}) + \frac{1}{d_i} \sum_{j \in N^{(i)}} \mathbf{e}_k^{(i)\,T} \mathbf{P}_{|}^{(j)\,-1} \mathbf{e}_k^{(i)} = \mathbf{e}_k^{(i)\,T} \mathbf{P}^{(i)\,-1} \mathbf{e}_k^{(i)}. \tag{25}$$

Since, $\mathbf{P}^{(i)\,-1} - \mathbf{A}^T\mathbf{P}_{|}^{(j)\,-1}\mathbf{A} = \mathbf{P}^{(i)\,-1} - \mathbf{A}^T(\mathbf{A}\mathbf{P}^{(i)}\mathbf{A}^T + \Sigma_w^{(i)})^{-1}\mathbf{A} = \mathbf{P}^{(i)\,-1} - (\mathbf{P}^{(i)} + \mathbf{A}^{-1}\Sigma_w^{(i)}\mathbf{A}^{-1\,T})^{-1}$ is positive semidefinite, (25) implies (22), and (22) implies that

$$\max_{1 \le i \le n} \mathbf{e}_k^{(i)} \mathbf{P}^{(i)\,-1} \mathbf{e}_i^{(k)}$$

does not increase as a function of k and thus, it converges. However, it remains to be proven that it converges to zero. If this is not the case, then (25) achieves the equality $(\mathbf{A}\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)\,-1} \mathbf{A}\mathbf{e}_{k-1}^{(j)} = \mathbf{e}_k^{(j)\,T} \mathbf{P}^{(j)\,-1} \mathbf{e}_k^{(j)}$ and it implies that $\mathbf{e}_{k-1}^{(j)} = 0$ for all $j \in N^{(i)}$. Combining it with $\mathbf{A}\mathbf{e}_{k-1}^{(j)} = \mathbf{e}_k^{(i)}$ (which follows from the equality $f(\mathbf{e}_k^{(i)}) = 0$), we get $\mathbf{e}_k^{(i)} = 0$. ■

Proof of Theorem 4.3 Similar to the proof of (23), we have $(\mathbf{e}_k^{(i)}, \mathbf{a}_k^{(i)}) = \arg\min_{\mathbf{e}_k, \mathbf{a}_k} f(\mathbf{e}_k)$, where

$$f(\mathbf{e}_k) = (\mathbf{C}^{(i)}\mathbf{e}_k + \mathbf{a}_k)^T \Sigma_v^{(i)\,-1} (\mathbf{C}^{(i)}\mathbf{e}_k + \mathbf{a}_k) + \lambda \|\mathbf{a}_k\|_1 + \frac{1}{d_i} \sum_{j \in N^{(i)}} (\mathbf{e}_k - \mathbf{A}\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_{|}^{(j)\,-1} (\mathbf{e}_k - \mathbf{A}\mathbf{e}_{k-1}^{(j)}) \tag{26}$$

By differentiation with respect to $\mathbf{a}_k$ and $\mathbf{e}_k$, $\mathbf{e}_k^{(i)}$ and $\mathbf{a}_k^{(i)}$ are the solutions that satisfy

$$(\mathbf{C}^{(i)}\mathbf{e}_k^{(i)} + \mathbf{a}_k^{(i)})^T \Sigma_v^{(i)-1}\mathbf{C}^{(i)} + \frac{1}{d_i}\sum_{j\in N^{(i)}} (\mathbf{e}_k^{(i)} - A\mathbf{e}_{k-1}^{(j)})^T \mathbf{P}_|^{(j)-1} = 0 \tag{27}$$

and

$$\|(\mathbf{C}^{(i)}\mathbf{e}_k^{(i)} + \mathbf{a}_k^{(i)})^T \Sigma_v^{(i)-1}\|_\infty \le \lambda/2. \tag{28}$$

As a result, if the solution to (27) when $\mathbf{a}_k^{(i)} = 0$, i.e.,

$$\mathbf{P}_|^{(i)}\left(\frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_|^{(j)-1} A\mathbf{e}_{k-1}^{(j)}\right) \tag{29}$$

satisfies (28) with $\mathbf{a}_k^{(i)} = 0$, i.e.,

$$\left\| \left(\mathbf{C}^{(i)}\mathbf{P}_|^{(i)}\left(\frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_|^{(j)-1} A\mathbf{e}_{k-1}^{(j)}\right)\right)^T \Sigma_v^{(i)-1} \right\|_\infty \le \lambda/2,$$

then $\mathbf{e}_k^{(i)}$ is given by (29) and $\mathbf{a}_k^{(i)} = 0$.

Applying the assumption (20), this condition is satisfied for $k = 1$, so $\mathbf{a}_1^{(i)} = 0$ for all $1 \le i \le n$. Then using the proof of Theorem IV.2 and induction (note that $\max_{1\le i\le n} \mathbf{e}_k^{(i)}\mathbf{P}^{(i)-1}\mathbf{e}_i^{(k)}$ is monotone), one can show that $\mathbf{a}_k^{(i)} = 0$ for all $k \ge 1$ and the errors $\mathbf{a}_k^{(i)}$ converges to zero.

Proof of Theorem 4.4

Let $\mathbf{Q} = \frac{1}{d_i}\sum_{j\in N^{(i)}} \mathbf{P}_|^{(j)-1}$, then (18) can be rewritten as

$$\begin{aligned}\hat{X}_k^{(i)} = \arg\min_{X_k, \mathbf{a}_k^{(i)}} &(y_k^{(i),a} - \mathbf{C}^{(i)}X_k - \mathbf{a}_k^{(i)})^T \Sigma_v^{(i)-1} \\ &\times (y_k^{(i),a} - \mathbf{C}^{(i)}X_k - \mathbf{a}_k^{(i)}) + \lambda \left\|\mathbf{a}_k^{(i)}\right\|_1 \\ &+ (X_k - d)^T\mathbf{Q}(X_k - d),\end{aligned} \tag{30}$$

where, d is a vector depending on $\mathbf{A}\hat{X}_{k-1}^{(j)}$ and $\mathbf{P}_|^{(j)}$. WLOG we may also assume that $d = 0$. Fixing $\mathbf{a}_k^{(i)}$, the solution of (30) is given by

$$\hat{X}_k^{(i)} = \mathbf{K}(y_k^{(i),a} - \mathbf{a}_k^{(i)}), \tag{31}$$

$$\mathbf{K} = (\mathbf{Q} + \mathbf{C}^{(i)T}\Sigma_v^{(i)-1}\mathbf{C}^{(i)})^{-1}\mathbf{C}^{(i)T}\Sigma_v^{(i)-1} \tag{32}$$

Plugging it into (30) and differentiate with respect to $\mathbf{a}_k^{(i)}$, we have

$$\|[(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K})^T\Sigma_v^{(i)-1}(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K}) + \mathbf{K}^T\mathbf{Q}\mathbf{K}](\mathbf{a}_k^{(i)} - y_k^{(i),a})\|_\infty \le \lambda/2.$$

Combining it with (31), we have an upper bound on

$$\|y_k^{(i),a} - \mathbf{a}_k^{(i)}\| \le \|[(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K})^T\Sigma_v^{(i)-1}(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K}) + \mathbf{K}^T\mathbf{Q}\mathbf{K}]^{-1}\|\lambda/2$$

as well as

$$\|\hat{X}_k^{(i)}\| \le \|\mathbf{K}\|\|[(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K})^T\Sigma_v^{(i)-1}(\mathbf{I} - \mathbf{C}^{(i)}\mathbf{K}) + \mathbf{K}^T\mathbf{Q}\mathbf{K}]^{-1}\|\lambda/2.$$

■

REFERENCES

[1] S. S. Stankovic, M. J. Stanojevic, and D. D. Siljak, "Decentralized overlapping control of a platoon of vehicles," *IEEE Trans. Control Syst. Technol.*, vol. 8, no. 5, pp. 816–832, 2000.

[2] Y. Zhang, B. Kosmatopoulos, P. A. Ioannou, and C. C. Chien, "Using front and back information for tight vehicle following maneuvers," *IEEE Trans. Veh. Technol.*, vol. 48, no. 1, pp. 319–328, 1999.

[3] P. Seiler, A. Pant, and K. Hedrick, "Disturbance propagation in vehicle strings," *IEEE Trans. Autom. Control*, vol. 49, no. 10, pp. 1835–1842, Oct. 2004.

[4] Y. Zheng, S. E. Li, J. Wang, L. Y. Wang, and K. Li, "Influence of information flow topology on closed-loop stability of vehicle platoon with rigid formation," in *Proc. 17th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2014, pp. 2094–2100.

[5] J. A. Fax and R. M. Murray, "Information flow and cooperative control of vehicle formations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1465–1476, Sep. 2004.

[6] J. Ploeg, N. van de Wouw, and H. Nijmeijer, "Lp string stability of cascaded systems: Application to vehicle platooning," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 2, pp. 786–793, Mar. 2014.

[7] S. E. Li, Y. Zheng, K. Li, and J. Wang, "An overview of vehicular platoon control under the four-component framework," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2015, pp. 286–291.

[8] B. van Arem, C. J. G. van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristics," *IEEE Trans. Intell. Transp. Syst.*, vol. 7, no. 4, pp. 429–436, Dec. 2006.

[9] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[10] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proc. 10th ACM Symp. Inf., Comput. Commun. Secur.*, 2015, pp. 167–178.

[11] S. Dadras, S. Dadras, and C. Winstead, "Identification of the attacker in cyber-physical systems with an application to vehicular platooning in adversarial environment," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 5560–5567.

[12] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.

[13] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6475–6488, Jul. 2017.

[14] A. Alipour-Fanid, M. Dabaghchian, H. Zhang, and K. Zeng, "String stability analysis of cooperative adaptive cruise control under jamming attacks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 157–162.

[15] Z. Cao, J. Kong, U. Lee, M. Gerla, and Z. Chen, "Proof-of-relevance: Filtering false data via authentic consensus in vehicle ad-hoc networks," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Apr. 2008, pp. 1–6.

[16] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *Proc. 1st ACM Workshop Cyber-Phys. Syst.-Secur. PrivaCy*, 2015, pp. 43–53.

[17] D. D. Dunn, S. A. Mitchell, I. Sajjad, R. M. Gerdes, R. Sharma, and M. Li, "Regular: Attacker-induced traffic flow instability in a stream of semi-automated vehicles," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 499–510.

[18] I. Sajjad, R. Sharma, and R. Gerdes, "A game-theoretic approach and evaluation of adversarial vehicular platooning," in *Proc. 1st Int. Workshop Safe Control Connected Auto. Vehicles*, New York, NY, USA, 2017, pp. 35–41.

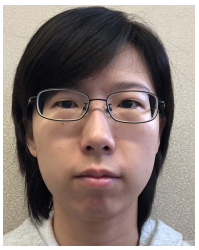
[19] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, New York, NY, USA, 2015, p. 22.

[20] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: An efficiency-motivated attack against autonomous vehicular transportation," in *Proc. 29th Annu. Comput. Secur. Appl. Conf.*, New York, NY, USA, 2013, pp. 99–108.

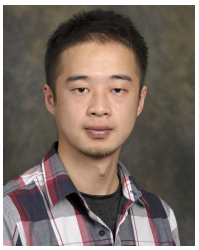
[21] R. G. Dutta, F. Yu, T. Zhang, Y. Hu, and Y. Jin, "Security for safety: A path toward building trusted autonomous vehicles," in *Proc. Int. Conf. Comput.-Aided Des.*, New York, NY, USA, Nov. 2018, p. 92.

[22] R. G. Dutta *et al.*, "Estimation of safe sensor measurements of autonomous system under attack," in *Proc. 54th Annu. Des. Autom. Conf.*, Jun. 2017, p. 46.
[23] S. H. Kafash, J. Giraldo, C. Murguia, A. A. Cárdenas, and J. Ruths, "Constraining attacker capabilities through actuator saturation," *CoRR*, vol. abs/1710.02576, pp. 1–5, Dec. 2017.
[24] Y. Mo and E. Garone, "Secure dynamic state estimation via local estimators," in *Proc. IEEE 55th Conf. Decision Control (CDC)*, Dec. 2016, pp. 5073–5078.
[25] M. Pajic, J. Weimer, and N. Bezzo, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," *IEEE Control Syst.*, vol. 37, no. 2, pp. 66–81, Apr. 2017.
[26] U. A. Khan and A. M. Stankovic, "Secure distributed estimation in cyber-physical systems," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2013, pp. 5209–5213.
[27] I. Matei, J. S. Baras, and V. Srinivasan, "Trust-based multi-agent filtering for increased smart grid security," in *Proc. 20th Medit. Conf. Control Autom. (MED)*, Jul. 2012, pp. 716–721.
[28] A. Mitra and S. Sundaram, "Secure distributed observers for a class of linear time invariant systems in the presence of byzantine adversaries," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 2709–2714.
[29] G. Ellis, *Observers Control Systems: A Practical Guide*. Amsterdam, The Netherlands: Elsevier, 2002.
[30] V. Vegamoor, S. Yan, S. Rathinam, and S. Darbha, "Mobility and safety benefits of connectivity in CACC vehicle strings," 2020, *arXiv:2003.04511*. [Online]. Available: http://arxiv.org/abs/2003.04511
[31] R. Rajamani and C. Zhu, "Semi-autonomous adaptive cruise control systems," *IEEE Trans. Veh. Technol.*, vol. 51, no. 5, pp. 1186–1192, Sep. 2002.
[32] S. Park and N. C. Martins, "Design of distributed LTI observers for state omniscience," *IEEE Trans. Autom. Control*, vol. 62, no. 2, pp. 561–576, Feb. 2017.
[33] K. Rapp and P.-O. Nyman, "Stability properties of the discrete-time extended Kalman filter," *IFAC Proc. Volumes*, vol. 37, no. 13, pp. 1377–1382, Sep. 2004.
[34] R. Olfati-Saber, "Distributed Kalman filtering for sensor networks," in *Proc. 46th IEEE Conf. Decis. Control*, 2007, pp. 5492–5498.
[35] D. Marelli, M. Zamani, and M. Fu, "Distributed Kalman filter in a network of linear dynamical systems," 2017, *arXiv:1711.07625*. [Online]. Available: https://arxiv.org/abs/1711.07625
[36] A. Abdelgawad, "Distributed Kalman filter with fast consensus for wireless sensor networks," *Int. J. Wireless Inf. Netw.*, vol. 23, no. 1, pp. 82–88, Mar. 2016.
[37] R. Carli, A. Chiuso, L. Schenato, and S. Zampieri, "Distributed Kalman filtering based on consensus strategies," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 4, pp. 622–633, May 2008.
[38] S. Kar, S. Cui, H. V. Poor, and J. M. F. Moura, "Convergence results in distributed Kalman filtering," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 2500–2503.
[39] D. Li, S. Kar, J. M. F. Moura, H. V. Poor, and S. Cui, "Distributed Kalman filtering over massive data sets: Analysis through large deviations of random Riccati equations," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1351–1372, Mar. 2015.
[40] J. Hespanha, *Linear Systems Theory*, 2nd Ed. Princeton, NJ, USA: Princeton Univ. Press, 2018.
[41] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Eur.*, Nov. 2015, pp. 1–13.
[42] K. C. Zeng *et al.*, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 1527–1544.
[43] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against Lidar for automotive applications," in *Int. Conf. Cryptograph. Hardw. Embedded Syst.*, 2017, pp. 445–467.
[44] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018.
[45] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Defcon*, vol. 24, no. 8, p. 109, 2016.
[46] R. G. Dutta, T. Zhang, and Y. Jin, "Resilient distributed filter for state estimation of cyber-physical systems under attack," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2019, pp. 5141–5147.

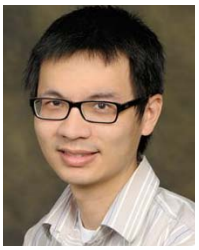
Raj Gautam Dutta (Member, IEEE) received the B.Tech. degree in electronics and communication from Visvesvaraya Technological University, India, in 2007, and the M.S. degree in electrical engineering with an emphasis on control systems and the Ph.D. degree in computer engineering from the University of Central Florida, USA, in 2011 and 2018, respectively. He is currently a Post-Doctoral Associate with the Department of Electrical and Computer Engineering (ECE), University of Florida. His current research interests include design of attack detection and resilient algorithms for autonomous CPS. In the past, he developed security solutions for semiconductor soft IP cores by using formal verification.



Yaodan Hu (Student Member, IEEE) received the B.Sc. degree in applied physics from the University of Science and Technology of China (USTC), China, in 2015. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Florida (UF). Her research interest includes attack and defense mechanism design in cyber-physical systems.



Feng Yu received the B.S. degree in mathematics and the B.E. degree in economics from the Southwestern University of Finance and Economics, China, in 2016, and the M.S. degree in mathematics from the University of Central Florida (UCF), in 2018, where he is currently pursuing the Ph.D. degree with the Department of Mathematics. His research focuses on PDE, optimization. He is currently on the areas of cyber-physical system and optimization. He received the ORC fellowship from the UCF in 2016.



Teng Zhang received the B.S. degree in mathematics from Fudan University, China, in 2006, and the Ph.D. degree in mathematics from the University of Minnesota, Minneapolis, MN, USA, in 2011. From September 2011 to August 2015, he was a Post-Doctoral Fellow with the Institute for Mathematics and its Applications (IMA), Minneapolis, and the Program in Applied and Computational Mathematics, Princeton University, Princeton, NJ, USA. He is currently a faculty member with the Department of Mathematics, University of Central Florida, Orlando, FL. His research interests include robust statistics, high-dimensional data analysis, matrix analysis/random matrix analysis, convex programming, and their applications to computer vision and data mining.

Yier Jin (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Zhejiang University, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from Yale University, in 2012. He is currently an Associate Professor and the IoT Term Professor with the Department of Electrical and Computer Engineering (ECE), University of Florida (UF). His research focuses on the areas of hardware security, embedded systems design and security, trusted hardware intellectual property (IP) cores, and hardware-software co-design for modern computing systems. He is also interested in the security analysis on the Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era. He was a recipient of the DoE Early CAREER Award in 2016 and ONR Young Investigator Award in 2019. He received Best Paper Award at DAC'15, ASP-DAC'16, HOST'17, ACM TODAES'18, GLSVLSI'18, and DATE'19. He is also the IEEE Council on Electronic Design Automation (CEDA) Distinguished Lecturer.