Privacy-Preserving Collaborative Estimation for Networked Vehicles With Application to Collaborative Road Profile Estimation

Huan Gao, *Member, IEEE*, Zhaojian Li, *Senior Member, IEEE*, and Yongqiang Wang, *Senior Member, IEEE*

***Abstract*— Road information such as road profile has been widely used in intelligent vehicle systems to improve road safety, ride comfort, and fuel economy. However, practical challenges, such as vehicle heterogeneity, parameter uncertainty, and measurement reliability, make it extremely difficult for a single vehicle to accurately and reliably estimate such information. To overcome these limitations, we propose a new learning-based collaborative estimation approach by fusing information from a fleet of networked vehicles. However, information exchange among these vehicles necessary for collaborative estimation may disclose sensitive information such as individual vehicle's identity, which poses serious privacy threats. To address this issue, we propose a unified privacy-preserving collaborative estimation framework which allows connected vehicles to iteratively refine estimation results through exploiting sequential measurements made by multiple vehicles traversing the same road segment. The collaborative estimation approach systematically incorporates privacy-protection schemes into the estimation design and exploits estimation dynamics to obscure exchanged information. Different from patching conventional privacy mechanisms like differential privacy that will compromise algorithmic accuracy or homomorphic encryption that will incur heavy communication/computation overhead, the dynamics enabled privacy protection does not sacrifice accuracy or significantly increase communication/computation overhead. Numerical simulations confirm the effectiveness of our proposed approach.**

***Index Terms*— Collaborative estimation, privacy preservation, road profile estimation, networked vehicles.**

I. Introduction

WITH increasingly enhanced sensing capabilities on modern vehicles, there is a growing interest in employing road information in intelligent vehicle systems to enhance road safety, ride comfort, and fuel economy. For example, a comfort-based route planning system has been developed in [1] where road profile/roughness information is used to plan a route that balances travel time and ride comfort; road profile information has also been exploited in automotive suspension controls to achieve improved handling (hence road safety) and ride comfort [2] as well as energy harvesting [3]; and road profile information has been shown to be able to improve fuel economy when integrated in powertrain control to optimize vehicle speed [4]–[6], to name a few. Modern vehicles are equipped with a rich set of sensors that are readily available to be exploited to discover the aforementioned road information.

Vehicle interactions with road and traffic can be modeled as dynamical systems where road or traffic conditions such as grade, friction coefficient, road profile, and traffic density can be modeled as disturbances or system states. Therefore, input and state observers have been extensively used to estimate road and traffic information in automotive and transportation engineering in the past decades [7]–[13]. For example, the authors in [7] modeled road grade as a system state and constructed a state observer to estimate it. Some other papers such as [9] modeled roadway velocity disturbances as system inputs and employed an input observer to estimate them. Other approaches using accelerometers and gyroscope sensors embedded in cell phones were proposed for the qualitative detection of road anomalies such as potholes and speed bumps with the help of signal processing techniques [14], [15]. However, due to the limited precision of the accelerometers and gyroscope sensors equipped on cell phones, such cell-phone based approaches cannot offer sufficient resolution for accurate road profile estimation. Furthermore, the performance of cell-phone based estimation approaches is sensitive to the location, orientation, and placement/fixture of the cell phone used for detection.

It is worth noting that almost all existing road information estimation approaches are developed in a single-vehicle setting, which renders the estimation result susceptible to vehicle variability, parameter uncertainty, and measurement reliability. To overcome such limitations, we propose to exploit multiple (heterogeneous) vehicles to cooperatively estimate road information with model-induced learning signals, relayed from earlier participating vehicles to subsequent vehicles, for enhanced performance. It is worth noting that although centralized approaches such as traffic cloud center may be able to manage high-level information such as road grade and traffic density, they are not efficient approaches to handle low-level vehicle-specific measurements such as road profile.

Manuscript received 27 August 2020; revised 26 July 2021 and 6 January 2022; accepted 22 February 2022. Date of publication 8 March 2022; date of current version 11 October 2022. This work was supported in part by the National Science Foundation under Grant ECCS-1912702 and Grant CCF-2106293. The Associate Editor for this article was B. Ayalew. *(Corresponding author: Yongqiang Wang.)*

Huan Gao was with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA. He is now with the School of Automation, Northwestern Polytechnical University, Xi'an 710129, China (e-mail: huangao@nwpu.edu.cn).

Zhaojian Li is with the Department of Mechanical Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: lizhaoj1@egr.msu.edu).

Yongqiang Wang is with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA (e-mail: yongqiw@clemson.edu).

Digital Object Identifier 10.1109/TITS.2022.3154650

Built-in maps usually are able to provide grade information, but still cannot be used to provide these highly time-varying information (e.g., black ice, potholes), either. Therefore, the proposed collaborative estimation approach is more appropriate for the considered problem of estimating time-sensitive road-profile information since it is highly flexible and agile in implementation and tracking time-varying conditions. While the proposed collaborative estimation is expected to offer enhanced performance, the information exchange necessary for the implementation of the collaborative estimation may result in the disclosure of sensitive vehicle information and lead to privacy breaches.

In fact, privacy of networked vehicles is not a new problem [16]. In recent years, the fact that vehicle-to-vehicle communications can transmit a vehicle's position raises serious concerns about position and identity privacy [17] — an adversary can use vehicle-to-vehicle communications to track a car without being noticed [18], [19], leading to many potential malicious activities [20]. To address the urgent need for privacy, plenty of vehicle-to-vehicle privacy-preserving approaches have been proposed based on conventional information technology privacy mechanisms such as cryptography [21]–[23], k-anonymity [24], differential privacy [25], or information-theoretical privacy [26]. Recently results also emerged on the privacy preservation in vehicles based crowdsourcing [27], [28]. However, these approaches need a mighty trusted central authority having access to the identity of all participants and are inappropriate for the scenario considered in this work for two reasons. First, such a central authority may not exist, particularly in large-scale systems like swarm robots. Secondly, even a central server exists, it may not be fully trustable, i.e., it may be honest-but-curious which follows all communication/computation protocols correctly but is curious and uses received messages to infer other users' private information. In this case, privacy measures are still required by law to protect the privacy of individual vehicles when performing information collection [29], [30].

In this paper, we propose a unified framework for privacy-preserving collaborative estimation to cooperatively estimate road information from a fleet of networked vehicles without leaking individual vehicles' sensitive information. More specifically, by leveraging vehicle-to-vehicle and vehicle-to-infrastructure communications, we develop a decentralized collaborative estimation framework for multiple vehicles traveling on the same road segment to iteratively refine the estimation results. In particular, building upon our prior work on single-vehicle based optimal state estimation [9], we develop an iterative learning based estimation approach in which multiple vehicles sequentially relay their successive measurements of the same road information (e.g., road profile) to iteratively enhance collaborative estimation performance. Our framework emulates iterative learning control (ILC) that is frequently used to treat repetitive disturbances [31] and tune the feed-forward control signal iteratively based on the memory data from previous iterations. It is worth noting that conventional ILC assumes that the system plant and its operations remain the same over iterations. However, for road information estimation, vehicles are inherently heterogeneous and hence existing ILC theory cannot be applied. Different from [32], we explicitly integrate vehicle dynamics in the design of iterative learning to address the heterogeneity of vehicles. Therefore, our collaborative estimation approach nontrivially generalizes the conventional ILC theory to allow collaborative estimation among a sequence of heterogeneous vehicles. To enable privacy preservation between participating vehicles, we develop a new privacy-protection mechanism which is seamlessly integrated in the collaborative estimation framework. More specifically, by leveraging the inherent dynamical properties of collaborative estimation, we enable the obfuscation of exchanged messages in a completely decentralized manner without sacrificing algorithmic accuracy or incurring heavy communication/computation overhead, which is different from most of existing approaches.

The major contributions of our work are as follows: 1) We propose a learning-based collaborative estimation approach to fuse local road profile estimation from a fleet of networked vehicles, which overcomes the limitations of single-vehicle based estimation approaches, such as vehicle variability, parameter uncertainty, and measurement reliability; 2) To address the heterogeneity of vehicles, our learning-based collaborative estimation approach explicitly integrates vehicle dynamics in the design of iterative learning, which nontrivially generalizes the conventional ILC theory since ILC requires the system plant and its operations to remain the same over iterations; 3) To protect the privacy of participating vehicles, we directly incorporate a privacy-protection mechanism in the collaborative estimation approach, which is able to obfuscate exchanged information in a completely decentralized manner (no trusted central authority needed) without sacrificing algorithmic accuracy or incurring heavy communication/computation overhead. This is in significant difference from existing approaches based on differential privacy (which compromise algorithmic accuracy) and approaches based on homomorphic encryption (which incur heavy communication and computation overhead).

The remainder of this paper is organized as follows. Section II introduces the problem description and preliminary background on road information estimation in a single vehicle setting. A collaborative estimation framework for networked vehicles is proposed in Section III, which is followed by the dynamics-enabled privacy-preserving design in Section IV. Simulation experiments are presented in Section V. Finally we conclude this paper in Section VI.

II. Problem Description and Preliminaries

In this section, we present the problem description and review vehicle dynamics and our prior work on single vehicle-based estimation, which provides necessary context and the foundation for the proposed privacy-preserving collaborative estimation framework.

A. Problem Description

Road profile has been frequently proposed to be incorporated as a preview to enhance suspension controls for

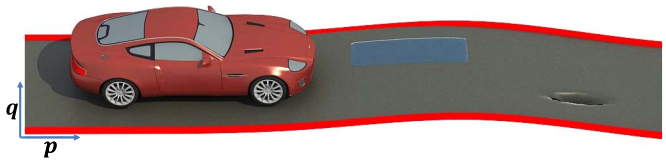

Fig. 1. Illustration of a road segment with one pothole.

improved safety and comfort [33]–[35]. Given a road segment (e.g., defined by two consecutive road mile markers [36]) as illustrated in Fig. 1, the objective of vehicle-based road profile estimation is to use existing onboard sensors (e.g., accelerometers, yaw rate, roll rate, GPS) to discover road profile information, which can be characterized by $w(p)$, a function of distance in the longitudinal direction (the p direction in Fig. 1). By scaling the distance p with the vehicle speed, the road information to be estimated can also be represented by $w(t)$, a function of time. Model-based road profile estimation approaches exploit onboard measurements along with the underlying dynamics to reconstruct w as well as to estimate vehicle states for feedback control [7], [11]. We next introduce the underlying vehicle dynamics and an estimation framework to discover road profile in a single-vehicle setting.

B. Vehicle Dynamical Model

Model-based road information discovery relies on a model that characterizes the underlying dynamics of vehicle-road interaction. In this work, we consider a fleet of heterogeneous vehicles. A reduced front half-car model of the j-th vehicle is shown in Fig. 2. The front half car body is modeled as a rigid body with mass m_j^b. I_j^x represents the moment of inertia about the longitudinal axis. The vertical displacement of the center of gravity (CG), left body tip, and right body tip, from equilibrium, are denoted by z_j, z_j^1, and z_j^2, respectively. L_j^1 and L_j^2 represent the left and right tip-to-CG distances, respectively. The parameters k_j^s and c_j^s represent the spring stiffness and damping coefficient of the suspension system, respectively. We further assume that the left and right sides have the same suspension parameters k_j^s and c_j^s. We denote the roll angle by θ_j. The variables q_j^1 and q_j^2 represent the left and right suspension deflections from equilibrium values, respectively. The signals w_j^l and w_j^r are the road velocity inputs to the left and right wheels, respectively. Since the wheels have high stiffness, we assume that w_j^l and w_j^r are directly applied to the left and right suspensions, respectively.

By defining $x_j^1 = q_j^1$, $x_j^2 = q_j^2$, $x_j^3 = \dot{z}_j$, and $x_j^4 = \dot{\theta}_j$ as the states, we have the following equations of motion

$$\begin{aligned}
\dot{x}_j^1 &= x_j^3 + L_j^1 x_j^4 - w_j^l \\
\dot{x}_j^2 &= x_j^3 - L_j^2 x_j^4 - w_j^r \\
m_j^b \dot{x}_j^3 &= -k_j^s x_j^1 - c_j^s \dot{x}_j^1 - k_j^s x_j^2 - c_j^s \dot{x}_j^2 \\
\frac{1}{2} I_j^x \dot{x}_j^4 &= -L_j^1 k_j^s x_j^1 - L_j^1 c_j^s \dot{x}_j^1 + L_j^2 k_j^s x_j^2 + L_j^2 c_j^s \dot{x}_j^2
\end{aligned} \quad (1)$$

Two sensor measurements, vertical accelerations of the left and right body tips, are used as outputs of vehicle j, which

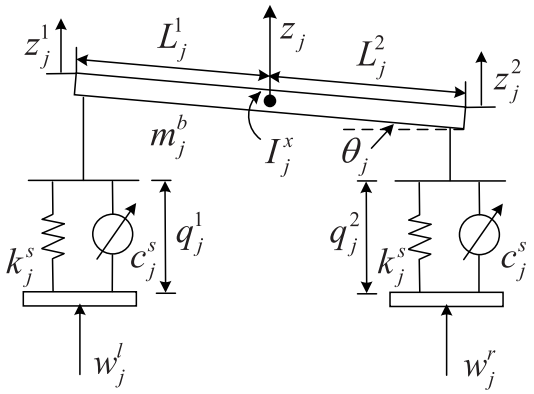

Fig. 2. A reduced front half-car model of vehicle j.

have the following form

$$\begin{aligned}
y_j^1 &= \ddot{z}_j^1 = \ddot{z}_j + L_j^1 \ddot{\theta}_j = \dot{x}_j^3 + L_j^1 \dot{x}_j^4 \\
y_j^2 &= \ddot{z}_j^2 = \ddot{z}_j - L_j^2 \ddot{\theta}_j = \dot{x}_j^3 - L_j^2 \dot{x}_j^4
\end{aligned} \quad (2)$$

Let $x_j = [x_j^1, x_j^2, x_j^3, x_j^4]^T$, $y_j = [\ddot{z}_j^1, \ddot{z}_j^2]^T$, $w_j = [w_j^l, w_j^r]^T$, and $v_j = [v_j^1, v_j^2]^T$ represent vehicle j's state vector, measurement vector, input vector, and measurement noise vector, respectively, we can rewrite (1) and (2) in a compact matrix form as follows

$$\begin{aligned}
\dot{x}_j &= A_j x_j + B_j w_j \\
y_j &= C_j x_j + D_j w_j + v_j
\end{aligned} \quad (3)$$

where A_j, B_j, C_j, and D_j are constant matrices of vehicle j derived from (1) and (2). Note that vehicle j's measurement noise vector v_j is assumed to satisfy $v_j = \sigma_\xi \dot{\xi}_j$ where ξ_j is a standard vector Wiener process representing sensor noises and the matrix $\sigma_\xi \sigma_\xi^T$ is positive-definite.

C. Road Information Estimation Based on a Single Vehicle

In this subsection, we take vehicle j as an example and introduce some preliminary results on road information estimation in a single vehicle setting, which includes an input observer [37] and a state estimator driven by JDP (jump-diffusion process) [9].

1) Input Observer: To estimate the road input w_j, vehicle j employs an input observer proposed by [37], which is given as follows

$$\begin{aligned}
\dot{\varepsilon}_j &= -\gamma S_j \varepsilon_j + \gamma_j S_j K_j A_j x_j + (\gamma_j S_j)^2 K_j x_j \\
\hat{w}_j &= -\varepsilon_j + \gamma_j S_j K_j x_j
\end{aligned} \quad (4)$$

where ε_j is the observer state, $\gamma_j > 0.5$ is a scalar gain, and $S_j = 0.5(1 + \gamma_j) I_2$, and $K_j = (B_j^T B_j)^{-1} B_j^T$.

2) Jump-Diffusion Process-Based Optimal State Estimator: Note that to employ the input observer in (4), vehicle j needs the state information x_j. Therefore, a state estimator is required to estimate x_j from measurements y_j in (3). Historically, diffusion (or Wiener) processes have been used to model stochastic disturbances in the development of state estimation methodologies, which have been applied in road information discovery such as road grade estimation [7] and

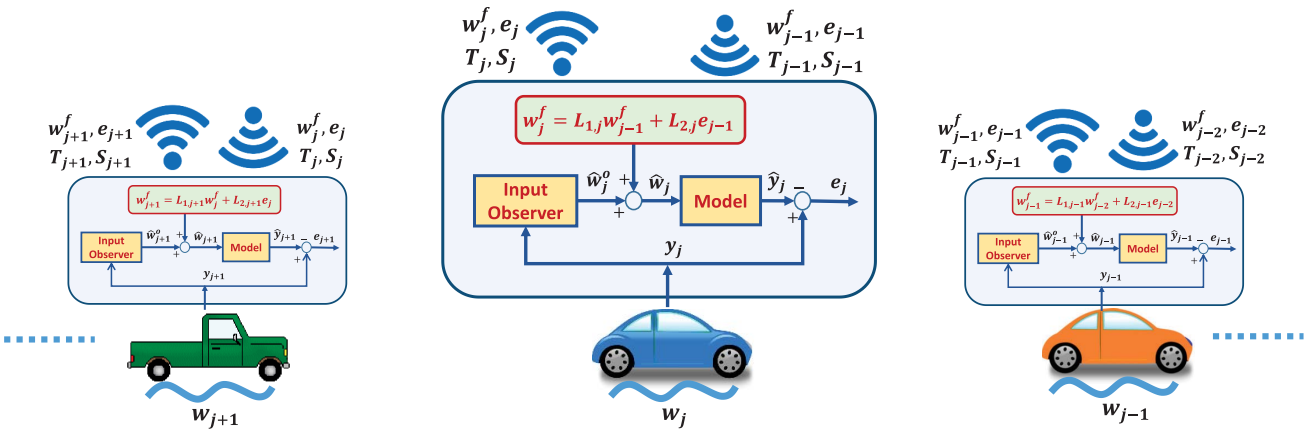

Fig. 3. Schematic diagram of iterative learning based collaborative estimation framework. A learning signal w_j^f is injected to vehicle j to relay estimation errors from heterogeneous vehicles.

tire-road friction estimation [8]. However, rare but pronounced events that can induce significant impact (such as a car hitting potholes or speed bumps) may be better modeled as jumps (Poisson processes). Therefore, jump-diffusion process (JDP), involving both jumps and diffusions, can be used to model road disturbances to vehicle j [9], [38]. More specifically, we denote vehicle j's road input w_j as $w_j = \dot{\eta}_j + \sigma_\zeta \dot{\zeta}_j$, where η_j is a vector jump process with each component having the same Poisson parameter λ and ζ_j is a standard vector Wiener process with $\sigma_\zeta \sigma_\zeta^T$ being positive-definite. The processes η_j and ζ_j are assumed to be independent. Furthermore, the jump size of each component of η_j is also a random variable. We denote the jump size mean and covariance by μ_η and Σ_η, respectively. A JDP-based state estimator of vehicle j was developed in our prior work in [9] as follows:

$$\dot{\hat{x}}_j = A_j \hat{x}_j + F_j(C_j \hat{x}_j - y_j) + (B_j + F_j D_j)\lambda_j \mu_\eta \tag{5}$$

where F_j is the estimator gain of vehicle j to be determined.

Lemma 1: (cf. Theorem 1 of [9]). Suppose the pair (A_j, C_j) is detectable, the pair (A_j, B_j) is stabilizable, and $S_j^T S_j > 0$. Then, the optimal gain F_j that minimizes

$$J_j = \lim_{t\to\infty} \frac{1}{t} E \int_0^t \big(x_j(\tau) - \hat{x}_j(\tau)\big)^T S_j^T S_j \big(x_j(\tau) - \hat{x}_j(\tau)\big) d\tau \tag{6}$$

in the open set of all gains F_j for which $(A_j + F_j C_j)$ is asymptotically stable (Hurwitz) is given by

$$F_j = -B_j \bar{\Sigma} D_j^T (V_j^2)^{-1} - Q_j C_j^T (V_j^2)^{-1} \tag{7}$$

where Q_j is the unique positive semi-definite solution to

$$\begin{aligned}\big(A_j - B_j \bar{\Sigma} D_j^T (V_j^2)^{-1} C_j\big) Q_j + V_j^1 - Q_j C_j^T (V_j^2)^{-1} C_j Q_j \\ + Q_j \big(A_j - B_j \bar{\Sigma} D_j^T (V_j^2)^{-1} C_j\big)^T = 0\end{aligned} \tag{8}$$

In (8), $\bar{\Sigma} = \sigma_\zeta \sigma_\zeta{}^T + \lambda \mu_\eta \mu_\eta^T + \lambda \Sigma_\eta$, $V_j^1 = B_j \bar{\Sigma} B_j^T - B_j \bar{\Sigma} D_j^T (V_j^2)^{-1} D_j \bar{\Sigma} B_j^T$, and $V_j^2 = \sigma_\zeta \sigma_\zeta{}^T + D_j \bar{\Sigma} D_j^T$.

III. Collaborative Estimation for Networked Vehicles

In this section, we extend the single vehicle-based estimator in Section II and develop a collaborative estimation framework by employing sequential measurements from multiple heterogeneous vehicles. Specifically, our collaborative estimation approach is inspired by iterative learning control (ILC). In particular, using sequential measurements taken from multiple vehicles traveling on the same road segment, we develop a completely decentralized iterative collaborative estimation approach by leveraging communication between vehicles which can be achieved using vehicle-to-vehicle or vehicle-to-infrastructure communications.

The proposed collaborative estimation framework is illustrated in Fig. 3. Consider a road segment (e.g., defined by road mileposts). Let j represent the sequence number of vehicles that drive over the road segment and participate in the collaborative estimation. The iterative learning framework exploits sequential estimation error e_j $(j = 1, 2, \cdots)$ and learning signal w_j^f $(j = 1, 2, \cdots)$ to iteratively refine the road information estimate. More specifically, let P_j represent the actual dynamics of vehicle j, and $\hat{P}_j$ represent the accessible mathematical representation used to model the actual dynamics. D_j represents the local input observer, y_j represents the vehicle's measurements, and $\hat{y}_j = \hat{P}\hat{w}_j$ represents the output by feeding the estimated input $\hat{w}_j$ to the plant model. Furthermore, T_j denotes the dynamics from the true road disturbance w_j (input) to the estimation error e_j (output), and S_j denotes the dynamics from the learning signal w_j^f (input) to the estimation error e_j (output). From Fig. 3, we have $T_j = P_j - \hat{P}_j D_j P_j$ and $S_j = -\hat{P}_j$. The proposed collaborative estimation framework is summarized in Algorithm 1.

From the proposed collaborative estimation framework we know that vehicle j receives the error signal e_{j-1} and learning signal w_{j-1}^f from an earlier participating vehicle $j-1$. So the inputs to the estimation system on vehicle j are the true road disturbance w_j and the learning signal w_j^f. The measurement-prediction mismatch e_j can be

Algorithm 1 Proposed Collaborative Estimation Framework

A fleet of networked vehicles travel on the same road segment and participate in the collaborative estimation of the road input w. For each vehicle j:

1: After traversing the considered road segment, vehicle j collects its measurements y_j.
2: Using the measurements y_j, vehicle j employs the JDP-based state estimator in (5) to estimate its state x. Based on the estimate of the state x, vehicle j uses the input observer in (4) to get an initial estimate of the road input w, which is denoted as $\hat{w}_j^o$.
3: After receiving information T_{j-1}, S_{j-1}, e_{j-1}, and w_{j-1}^f from vehicle $j-1$, vehicle j constructs its learning filters $L_{1,j}$ and $L_{2,j}$ (the way how to construct learning filters will be discussed below), and then obtains its learning signal $w_j^f = L_{1,j} w_{j-1}^f + L_{2,j} e_{j-1}$.
4: Using $\hat{w}_j = \hat{w}_j^o + w_j^f$, vehicle j obtains its estimate of the road input.
5: By feeding the estimated signal $\hat{w}_j$ to the plant model $\hat{P}_j$, vehicle j obtains the signal $\hat{y}_j$ and the error signal e_j using $e_j = y_j - \hat{y}_j$.
6: Vehicle j sends its information T_j, S_j, e_j, and w_j^f to vehicle $j+1$.

neatly described as

$$e_j = T_j w_j + S_j w_j^f \tag{9}$$

where T_j and S_j are transfer functions from w_j to e_j and from w_j^f to e_j, respectively, as defined above. Note that they can be represented in either time domain in the form of state space or frequency domain using transfer functions. We design the following iterative estimation mechanism for vehicle j

$$w_j^f = L_{1,j} w_{j-1}^f + L_{2,j} e_{j-1} \tag{10}$$

where $L_{1,j}$ and $L_{2,j}$ are the learning filters to be designed, w_{j-1}^f is the learning signal relayed from vehicle $j-1$, and e_{j-1} is the error signal from vehicle $j-1$. Plugging (10) into (9) leads to

$$\begin{aligned} e_j &= T_j w_j + S_j \left[L_{1,j} w_{j-1}^f + L_{2,j} e_{j-1} \right] \\ &= T_j w_j + S_j L_{2,j} e_{j-1} + S_j L_{1,j} S_{j-1}^{-1} \left[e_{j-1} - T_{j-1} w_{j-1} \right] \\ &= \left[S_j L_{2,j} + S_j L_{1,j} S_{j-1}^{-1} \right] e_{j-1} \\ &\quad + \left[T_j - S_j L_{1,j} S_{j-1}^{-1} T_{j-1} \right] w \end{aligned} \tag{11}$$

where we assumed $w_j = w_{j-1} = w, \forall j = 1, 2, \cdots$.

It is worth noting that (11) represents the dynamic estimation error from vehicle $j-1$ to vehicle j. Next we will design learning filters $L_{1,j}$ and $L_{2,j}$, such that $||S_j L_{2,j} + S_j L_{1,j} S_{j-1}^{-1}||$ and $||T_j - S_j L_{1,j} S_{j-1}^{-1} T_{j-1}||$ are minimized, i.e.,

$$\min_{L_{1,j},\, L_{2,j}} ||S_j L_{2,j} + S_j L_{1,j} S_{j-1}^{-1}|| + ||T_j - S_j L_{1,j} S_{j-1}^{-1} T_{j-1}|| \tag{12}$$

Noting that $||T_j - S_j L_{1,j} S_{j-1}^{-1} T_{j-1}||$ only depends on $L_{1,j}$, we can solve (12) in a sequential manner. By setting

$$L_{1,j}^* = S_j^{-1} T_j T_{j-1}^{-1} S_{j-1} \tag{13}$$

we have $||T_j - S_j L_{1,j}^* S_{j-1}^{-1} T_{j-1}|| = 0$. Given $L_{1,j}^* = S_j^{-1} T_j T_{j-1}^{-1} S_{j-1}$, setting

$$L_{2,j}^* = -S_j^{-1} T_j T_{j-1}^{-1} \tag{14}$$

leads to $||S_j L_{2,j}^* + S_j L_{1,j}^* S_{j-1}^{-1}|| = 0$.

Note that the proposed iterative collaborative estimation approach removes the fundamental assumption of homogeneous dynamics in traditional ILC via explicitly taking vehicle dynamics into account. More specifically, the dynamics of vehicle j is integrated in the design of learning filters $L_{1,j}$ and $L_{2,j}$. Therefore, the proposed approach is a highly nontrivial generalization to ILC since it overcomes the homogeneous assumption in ILC, which is extremely significant in practice because homogeneous vehicles rarely exist in practical transportation systems.

Remark 1: It is worth noting that our proposed approach is transparent to vehicle speed. Of course, vehicle speed may indirectly affect the quality of sensor measurements and hence affect final performance. But theoretically, as long as sensor measurements can be obtained, our collaborative estimation approach can iteratively improve the estimation performance.

Under the proposed collaborative estimation framework, vehicle j needs to send the error signal e_j, learning signal w_j^f, and its dynamics T_j and S_j to vehicle $j+1$ after driving through the road segment, so that vehicle $j+1$ can construct learning filters $L_{1,j+1}$ and $L_{2,j+1}$, and further get its learning signal w_{j+1}^f using (10). However, such information exchange necessary for the implementation of the collaborative estimation may result in the disclosure of sensitive vehicle information and lead to privacy breaches. In the next section, we will present a new privacy-preserving design to address such privacy concerns.

IV. Privacy Protection in the Collaborative Estimation Framework

As analyzed in Section III, the proposed collaborative estimation framework requires explicitly exchanging of T_j and S_j, which contain sensitive model and dynamics information of vehicle j. Such information could be used by a malicious party to infer sensitive information of vehicle j such as its type and even identity and hence poses serious privacy threats. In the considered collaborative estimation environment, the malicious party could be a vehicle participating in the collaborative estimation or it could be an external eavesdropper wiretapping communication channels. Therefore, before putting the sensitive information T_j and S_j out on the communication channel and sending them to vehicle $j+1$, vehicle j has to obfuscate and cover such information. It is worth noting that anonymity has been discussed to enable privacy of vehicle-to-vehicle communications by making the message sender indistinguishable. However, anonymity has its limitations such as increased computational latency/communication overhead and

reduced scalability [20]. Moreover, as indicated in [39], simple anonymization is usually not enough to guarantee privacy as privacy breaches generally arise from the possibility of linking anonymized data with public side information, as demonstrated in [40] and [41]. Furthermore, in existing anonymization based privacy-preserving approaches, it is assumed that a trusted server exists to manage the real identifies of all participants in order to track and isolate malicious participants [20], [42]. Such an assumption may not be valid in practice. It is also worth noting that other conventional privacy-preserving approaches like differential privacy or homomorphic encryption (as adopted in our prior work [43], [44]) are not desirable here since differential privacy unavoidably compromises the accuracy of computation and homomorphic encryption incurs heavy communication/computation overhead.

Given that the exchanged information T_j and S_j contain the sensitive model and dynamics information of vehicle j, we propose a new privacy design seamlessly integrated with our collaborative estimation framework. To this end, we first give our attack models and a precise definition of privacy.

- *Eavesdropping attacks* are attacks in which an external eavesdropper wiretaps communication channels to intercept exchanged messages in an attempt to learn the information about sending vehicles.
- *Honest-but-curious attacks* are attacks in which attackers follow all protocol steps correctly but are curious and collect all received intermediate data in an attempt to learn the information about other participating vehicles.

Definition 1: The privacy of vehicle j is preserved if an attacker cannot infer the dynamics T_j and S_j of vehicle j. More specifically, attackers cannot infer the exact zeros and poles of T_j and S_j.

We propose to exploit the inherent dynamical properties of collaborative estimation to obfuscate exchanged information. More specifically, instead of sending T_j, S_j, e_j, and w_j^f directly from vehicle j to vehicle $j+1$, we propose to let vehicle j send

$$\begin{aligned}\tilde{T}_j &= \Psi_j^{T1} T_j \Psi_j^{T2} \\ \tilde{S}_j &= \Psi_j^{S1} S_j \Psi_j^{S2} \\ \tilde{e}_j &= \Psi_j^{e} e_j \\ \tilde{w}_j^f &= \Psi_j^{w} w_j^f \end{aligned} \tag{15}$$

instead, where Ψ_j^{T1}, Ψ_j^{T2} Ψ_j^{S1}, Ψ_j^{S2}, Ψ_j^{e} and Ψ_j^{w} are obfuscating dynamical systems, i.e., $\Psi_j^{T1}(s)$, $\Psi_j^{T2}(s)$, $\Psi_j^{S1}(s)$, $\Psi_j^{S2}(s)$, $\Psi_j^{e}(s)$, and $\Psi_j^{w}(s)$ are generated by and only known to vehicle j. Note that since e_j and w_j^f are two-dimensional signals and T_j and S_j are MIMO transfer functions, the obfuscating dynamical systems should also be matrices of appropriate dimensions.

The difficulties in designing obfuscating dynamical systems lie in eliminating their influence on the accuracy of collaborative estimation, i.e., in guaranteeing the optimality of $L_{1,j+1}$ and $L_{2,j+1}$ for the update of w_{j+1}^f. We prove that if the obfuscating dynamics are designed according to Theorem 1, then the optimality of $L_{1,j+1}$ and $L_{2,j+1}$ will not be affected at all, i.e., the collaborative estimation accuracy will not be affected at all by the privacy design:

Theorem 1: The information obfuscation framework has no influence on the accuracy of collaborative estimation if the obfuscating dynamical systems satisfy the following relationships:

$$\begin{aligned}\Psi_j^{T1} &= \Psi_j^{e} = \Psi_j^{S1} \\ \Psi_j^{T2} &= I \\ \Psi_j^{w} &= (\Psi_j^{S2})^{-1} \end{aligned} \tag{16}$$

Proof: To prove that the information obfuscation framework has no influence on the accuracy of collaborative estimation, it is sufficient to prove that the information obfuscation framework does not affect vehicle $j+1$'s computing accuracy of w_{j+1}^f since the information from vehicle j only involves in the computation of w_{j+1}^f.

We first show how the obfuscating dynamical systems in (16) affect the design of $L_{1,j+1}$ and $L_{2,j+1}$ on vehicle $j+1$. Under the information obfuscation framework, vehicle $j+1$ designs $L_{1,j+1}$ in (13) and $L_{2,j+1}$ in (14) as follows

$$\begin{aligned}\tilde{L}_{1,j+1}^* &= S_{j+1}^{-1} T_{j+1} \tilde{T}_j^{-1} \tilde{S}_j \\ &= S_{j+1}^{-1} T_{j+1} (\Psi_j^{T1} T_j \Psi_j^{T2})^{-1} \Psi_j^{S1} S_j \Psi_j^{S2} \\ &= S_{j+1}^{-1} T_{j+1} T_j^{-1} S_j \Psi_j^{S2} \\ &= L_{1,j+1}^* \Psi_j^{S2} \end{aligned} \tag{17}$$

and

$$\begin{aligned}\tilde{L}_{2,j+1}^* &= -S_{j+1}^{-1} T_{j+1} \tilde{T}_j^{-1} \\ &= -S_{j+1}^{-1} T_{j+1} (\Psi_j^{T1} T_j \Psi_j^{T2})^{-1} \\ &= -S_{j+1}^{-1} T_{j+1} T_j^{-1} (\Psi_j^{T1})^{-1} \\ &= L_{2,j+1}^* (\Psi_j^{T1})^{-1} \end{aligned} \tag{18}$$

Note that in the above derivation, we used $\Psi_j^{T1} = \Psi_j^{S1}$ and $\Psi_j^{T2} = I$ in (16). It is also worth noting that $\tilde{L}_{1,j+1}^*$ and $\tilde{L}_{2,j+1}^*$ are the optimal solution to (12) under the information obfuscation framework since they lead to

$$||T_{j+1} - S_{j+1} \tilde{L}_{1,j+1}^* \tilde{S}_j^{-1} \tilde{T}_j|| = 0 \tag{19}$$

and

$$||S_{j+1} \tilde{L}_{2,j+1}^* + S_{j+1} \tilde{L}_{1,j+1}^* \tilde{S}_j^{-1}|| = 0 \tag{20}$$

Next we evaluate the influence of the information obfuscation on w_{j+1}^f:

$$\tilde{w}_{j+1}^f = \tilde{L}_{1,j+1}^* \tilde{w}_j^f + \tilde{L}_{2,j+1}^* \tilde{e}_j \tag{21}$$

Plugging (17) and (18) into (21) leads to

$$\begin{aligned}\tilde{w}_{j+1}^f &= L_{1,j+1}^* \Psi_j^{S2} \Psi_j^{w} w_j^f + L_{2,j+1}^* (\Psi_j^{T1})^{-1} \Psi_j^{e} e_j \\ &= L_{1,j+1}^* w_j^f + L_{2,j+1}^* e_j \\ &= w_{j+1}^f \end{aligned} \tag{22}$$

where we used $\Psi_j^{w} = (\Psi_j^{S2})^{-1}$ and $\Psi_j^{T1} = \Psi_j^{e}$ in (16).

Therefore, we can see that once the obfuscating dynamical systems satisfy the relationships in (16), the information obfuscation mechanism will not affect the computation of w_{j+1}^f and further $\hat{w}_{j+1}$ on vehicle $j+1$, meaning that the information obfuscation framework has no influence on the accuracy of collaborative estimation. ■

Combining (15) and (16) leads to

$$\begin{aligned}\tilde{T}_j &= \Psi_j^{S1} T_j \\ \tilde{S}_j &= \Psi_j^{S1} S_j \Psi_j^{S2} \\ \tilde{e}_j &= \Psi_j^{S1} e_j \\ \tilde{w}_j^f &= (\Psi_j^{S2})^{-1} w_j^f \end{aligned} \tag{23}$$

So vehicle j only needs to design Ψ_j^{S1} and Ψ_j^{S2} to obfuscate its private dynamics T_j and S_j. Incorporating (23) in the collaborative estimation framework, we propose the information obfuscation mechanism in Algorithm 2.

Algorithm 2 Privacy-Protection Mechanism

In Algorithm 1, vehicle j replaces Step 6 with the following steps:

1: Vehicle j randomly chooses two positive integers n_1 and n_2, and keeps them private to itself.
2: Vehicle j randomly selects n_1 poles (from the left-half of the s-plane) and four groups of zeros with each group having n_1 zeros. Using one group of zeros and n_1 poles, vehicle j can construct a transfer function. Therefore, using these four groups of zeros and n_1 poles, vehicle j constructs a 2-by-2 transfer function matrix as Ψ_j^{S1}. Ψ_j^{S1} will be private to vehicle j.
3: Vehicle j randomly selects n_2 poles (from the left-half of the s-plane) and four groups of zeros with each group having n_2 zeros. Using these four groups of zeros and n_2 poles, vehicle j constructs a 2-by-2 transfer function matrix as Ψ_j^{S2}. Ψ_j^{S2} will be private to vehicle j.
4: Using the obfuscating dynamical systems Ψ_j^{S1} and Ψ_j^{S2}, vehicle j obfuscates its T_j, S_j, e_j, and w_j^f according to (23), and then sends the obfuscated information $\tilde{T}_j$, $\tilde{S}_j$, $\tilde{e}_j$, and $\tilde{w}_j^f$ to vehicle $j+1$.

Next we show that our proposed information obfuscation mechanism can indeed achieve the defined privacy.

Theorem 2: Our privacy-preserving mechanism can protect the privacy of vehicle j's dynamics T_j and S_j using the obfuscating dynamical systems Ψ_j^{S1} and Ψ_j^{S2}.

Proof: To prove that the privacy of vehicle j can be protected, it is sufficient to prove that T_j and S_j cannot be inferred by an attacker. Our idea is to prove that neither honest-but-curious vehicle $j+1$ nor an eavesdrop attacker can distinguish whether the original dynamics of vehicle j is T_j (resp. S_j) or $\bar{T}_j$ (resp. $\bar{S}_j$) where $\bar{T}_j$ and $\bar{S}_j$ can be any stable dynamics that have different orders, zeros, and poles from T_j and S_j, respectively. Under the information obfuscation framework, no matter information exchange is implemented via vehicle-to-vehicle communication or vehicle-to-infrastructure communication, we can assume that any attacker has access to the obfuscated dynamics $\tilde{T}_j$ and $\tilde{S}_j$ sent by vehicle j. Therefore, if we can prove that under any stable dynamics $\bar{T}_j$ and $\bar{S}_j$, the obfuscated dynamics $\tilde{T}_j$ and $\tilde{S}_j$ could keep unchanged, then neither honest-but-curious vehicle $j+1$ nor an eavesdrop attacker can infer the original dynamics T_j and S_j (including their zeros and poles).

It can be proven that under any stable dynamics $\bar{T}_j$ and $\bar{S}_j$, there always exist obfuscating dynamical systems

$$\begin{aligned}\bar{\Psi}_j^{S1} &= \Psi_j^{S1} T_j \bar{T}_j^{-1} \\ \bar{\Psi}_j^{S2} &= \bar{S}_j^{-1} \bar{T}_j T_j^{-1} S_j \Psi_j^{S2} \end{aligned} \tag{24}$$

making the obfuscated dynamics $\tilde{T}_j$ and $\tilde{S}_j$ exactly the same as under the original dynamics T_j and S_j, i.e.,

$$\begin{aligned}\tilde{T}_j &= \Psi_j^{S1} T_j = \bar{\Psi}_j^{S1} \bar{T}_j \\ \tilde{S}_j &= \Psi_j^{S1} S_j \Psi_j^{S2} = \bar{\Psi}_j^{S1} \bar{S}_j \bar{\Psi}_j^{S2} \end{aligned} \tag{25}$$

Therefore, neither honest-but-curious vehicle $j+1$ nor an eavesdrop attacker can infer the original dynamics T_j and S_j, meaning that our privacy-preserving approach can protect the privacy of vehicle j's dynamics T_j and S_j using the obfuscating dynamical systems Ψ_j^{S1} and Ψ_j^{S2}. ■

Remark 2: Note that not only the dynamics T_j and S_j but also the signals e_j and w_j^f of each vehicle j need to be obfuscated by the obfuscating dynamical systems Ψ_j^{S1} and Ψ_j^{S2}. So the signals e_j and w_j^f will be completely reshaped and covered since different frequency components of e_j and w_j^f will be amplified/attenuated differently by Ψ_j^{S1} and Ψ_j^{S2}. Therefore, information of the original signals e_j and w_j^f will also be covered by the information obfuscation framework. After the obfuscation, vehicle j sends the obfuscated information $\tilde{T}_j$, $\tilde{S}_j$, $\tilde{e}_j$, and $\tilde{w}_j^f$ to vehicle $j+1$, so that vehicle $j+1$ can implement collaborative estimation.

Remark 3: The design of obfuscating dynamical systems Ψ_j^{S1} and Ψ_j^{S2} is subject to a trade-off between complexity and performance. Namely, to provide a stronger privacy protection, it is desirable to use higher-order transfer functions Ψ_j^{S1} and Ψ_j^{S2} having complicated dynamics (more zeros and poles) to cover the original models. However, a higher order of the dynamics Ψ_j^{S1} and Ψ_j^{S2} will slightly improve the computational complexity. In fact, as can be seen from our proof in Theorem 2, as long as Ψ_j^{S1} and Ψ_j^{S2} have one pole and zero (private to vehicle j), an attacker will be unable to infer the true dynamics of vehicle j. Overall, the obfuscating process in (23) has almost negligible effect on data transmission and delay on estimation. This is because the obfuscation only performs algebraic transformations on the transmitted messages, and it does not increase the communication overhead. Of course, the algebraic transformation may slightly improve the computational overhead, which is completely manageable for state-of-the-art vehicular processors.

Remark 4: Different from existing privacy-preserving approaches which rely on encryption or pseudonyms management, the proposed privacy-preserving approach employs self-generated obfuscating dynamical systems which are simple in computation, lightweight in communication, and completely scalable in implementation. Furthermore,

compared with differential privacy based approaches which add additive noise to exchanged signals and hence unavoidably affect algorithmic accuracy, our approach does not sacrifice the accuracy of estimation, which is crucial in safety-critical dynamical systems.

Remark 5: As stated in Algorithm 1 and Algorithm 2, our proposed approach does not require participating vehicles to perform measurements and estimation simultaneously. Given a road segment, each vehicle passes the road segment in a serial manner and only needs to collect its measurement when traveling on the road segment. After all vehicles passed and collected measurements, they perform iterative learning and obfuscation sequentially. More specifically, vehicle j first estimates the road profile $w(t)$ and gets an initial estimate $\hat{w}_j^o$ using JDP-based state estimator in (5), input observer in (4), and collected measurements y_j. Then by employing iterative learning results received from vehicle $j-1$ (if vehicle j is not the first vehicle), vehicle j obtains its estimate of the road input. After that, vehicle j obfuscates its information and sends the obfuscated information to vehicle $j+1$. Then the same process proceeds until the last vehicle.

Remark 6: It is worth noting that in our collaborative estimation approach, information exchange from vehicle j to vehicle $j+1$ can be implemented using vehicle-to-vehicle communications. It can also be realized indirectly using an intermediate infrastructure, i.e., vehicle j sends information to an infrastructure (e.g., a cloud), and then the infrastructure relays the information to vehicle $j+1$. As proven in Theorem 2, no matter which way is used, our proposed privacy-protection mechanism is able to protect the privacy of participating vehicles.

V. Simulation Results

Following our proposed collaborative estimation approach, a sequence of 10 heterogeneous vehicles were simulated to collaboratively improve the estimation performance. We assume that for each vehicle j, the exact values of its vehicle parameters such as m_j^b, k_j^s, c_j^s, and I_j^x are not available, and we can only access unbiased estimations of these parameters with ± 10 percentage error. The parameters of the JDP estimator were set as $\lambda = 0.01$, $\mu_\eta = [3.1,\ 1.5]^T$, $\Sigma_\eta = 3.3 \cdot I_2$, $\sigma_\zeta = 7.8 \cdot I_2$, and $\sigma_\xi = 0.011 \cdot I_2$, where I_2 represents a 2×2 identity matrix. We repeat the simulation for 100 times, and record the estimation errors in terms of mean square error for each simulation. The averaged estimation performance is shown in Fig. 4. Note that each vehicle j only sends its dynamics T_j and S_j, error signal e_j, and learning signal w_j^f to its subsequent vehicle $j+1$. So vehicle 1 did not receive any information from other vehicles, meaning that the estimation results of vehicle 1 are exactly the same as individual-vehicle based estimation results. To the contrary, the estimation on vehicle j ($j > 1$) incorporates information from vehicle $j-1$ (which further incorporates information from its preceding vehicles), and hence represents collaborative estimation results using j vehicles (from vehicle 1 to vehicle j). From the simulation results in Fig. 4, we can see that the estimation error of vehicle 1, i.e., individual-vehicle based estimation error, is much larger than other vehicles' estimation errors, which confirms that our proposed collaborative estimation approach can significantly improve the estimation performance over individual-vehicle based estimation.

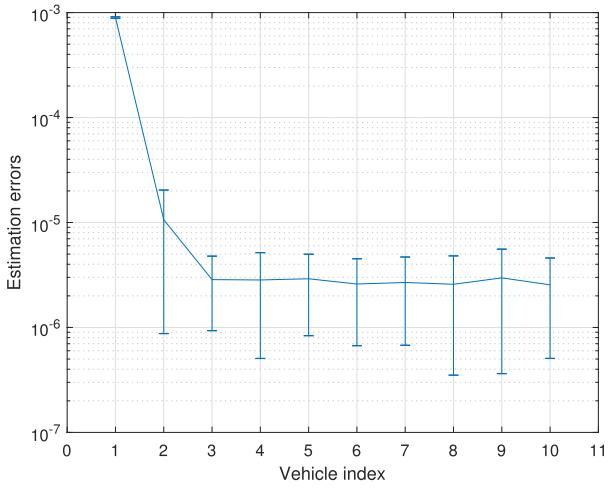

Fig. 4. Estimation performance of a sequence of 10 heterogeneous vehicles.

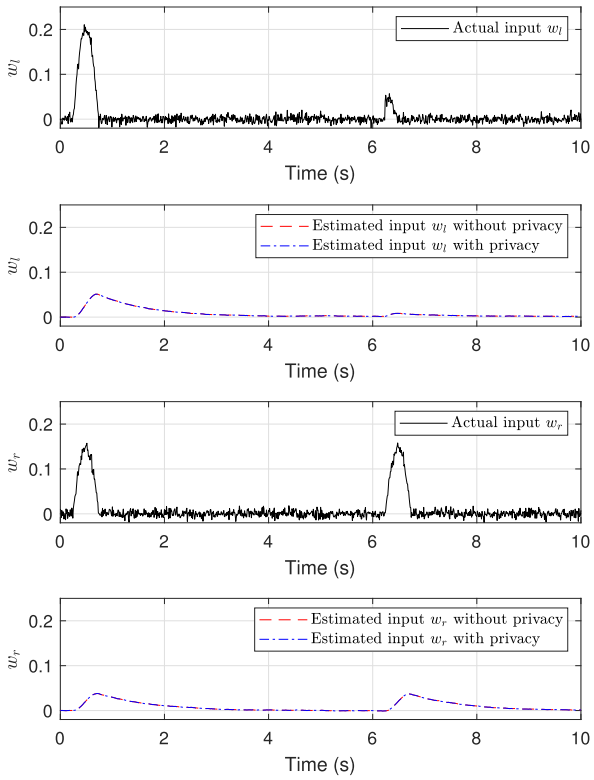

Fig. 5. Comparisons of the actual road input signals with the estimated signals using and not using our privacy-preserving design for vehicle 1.

It is clear from the simulation results in Fig. 4 that the number of vehicles does affect the estimation accuracy. It can be seen that the estimation accuracy improves as the number of vehicles increases. Due to the presence of measurement noises and vehicle parameter uncertainties, the estimation error can only be reduced to a certain level. On the other hand, the estimation error always converged at the third vehicle, meaning

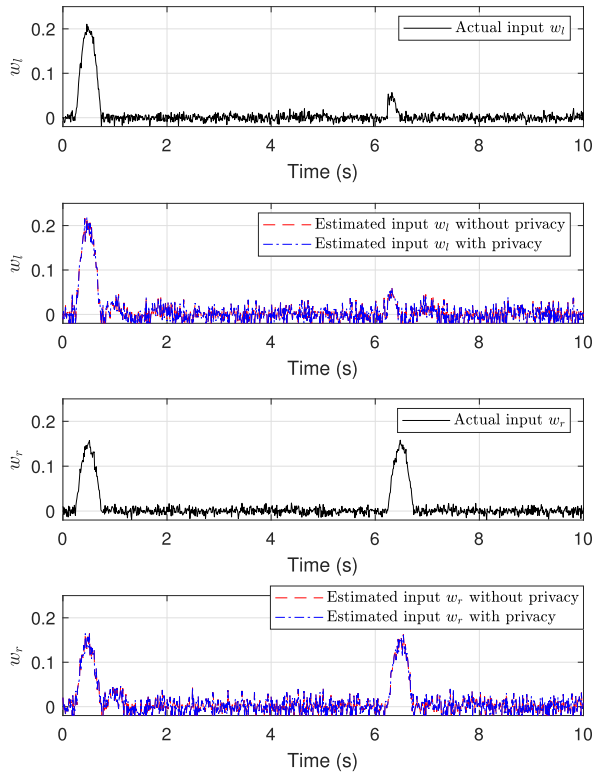

Fig. 6. Comparisons of the actual road input signals with the estimated signals using and not using our privacy-preserving design for vehicle 2.

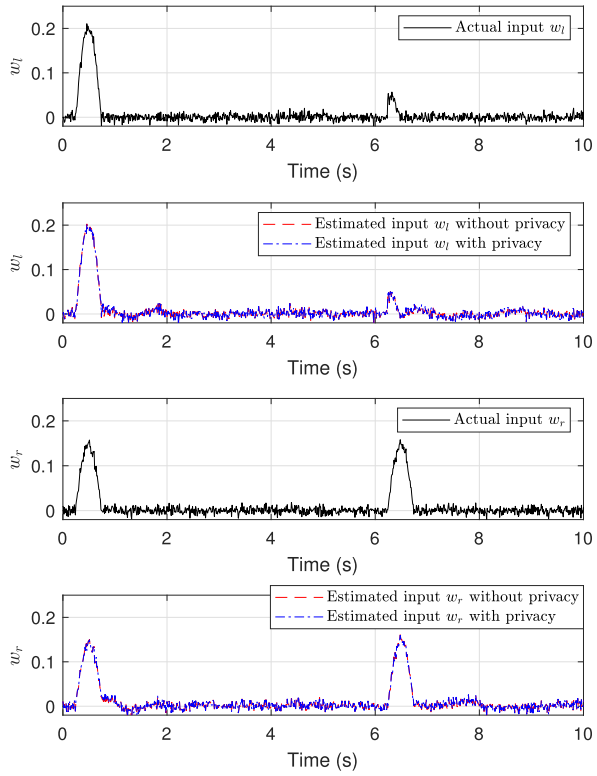

Fig. 7. Comparisons of the actual road input signals with the estimated signals using and not using our privacy-preserving design for vehicle 3.

that our approach achieves fast convergence after iteratively learning using only 3 vehicles.

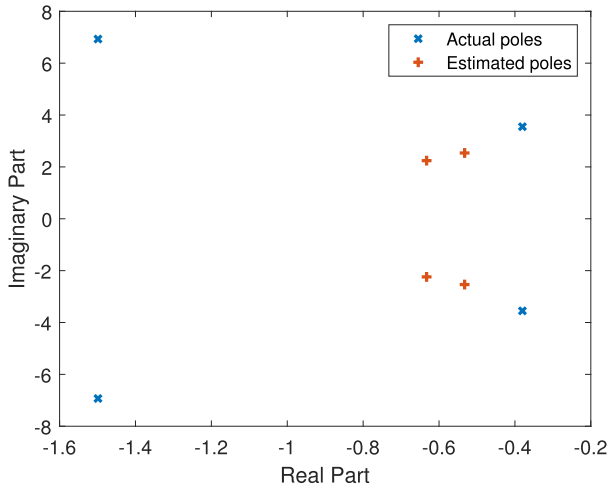

Fig. 8. Comparisons of the actual poles with the estimated poles of S_1 for vehicle 1.

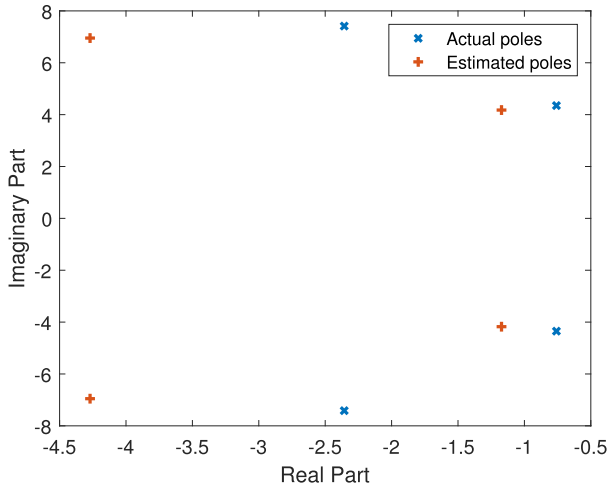

Fig. 9. Comparisons of the actual poles with the estimated poles of S_2 for vehicle 2.

We also perform simulations to show that our information obfuscation framework can protect the privacy of vehicle dynamics without compromising the accuracy of computation results. To this end, we first compare the actual road input signals with the estimated signals with and without implementing our privacy-preserving design. The comparison results for vehicles 1, 2, 3 are presented in Fig. 5, Fig. 6, and Fig. 7, respectively. From the simulation results, we can see that our information obfuscation framework has no influence on the collaborative estimation accuracy since the estimated road inputs using our privacy-preserving design are the same as the ones without privacy design.

We then evaluate the privacy performance of our information obfuscation mechanism. As analyzed in Section IV, instead of sending the sensitive dynamics T_j and S_j, vehicle j sends obfuscated dynamics $\tilde{T}_j$ and $\tilde{S}_j$ which have different orders, zeros, and poles from T_j and S_j. We assume that an attacker knows the orders of dynamics T_j and S_j, and intends to infer the actual zeros and poles of T_j and S_j based on received dynamics $\tilde{T}_j$ and $\tilde{S}_j$. As the attacker knows the actual

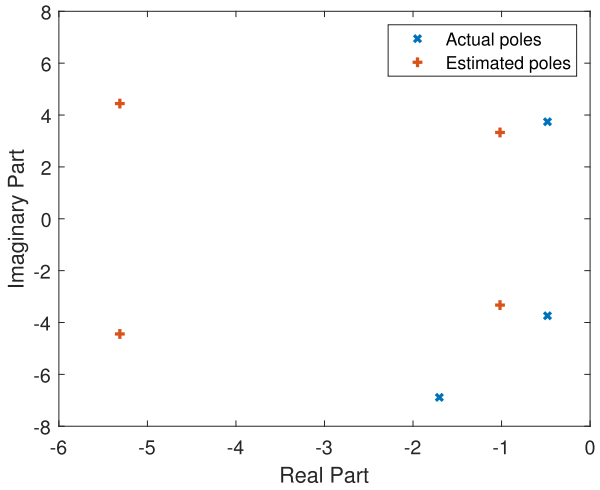

Fig. 10. Comparisons of the actual poles with the estimated poles of S_3 for vehicle 3.

orders, it reduces the orders of $\tilde{T}_j$ and $\tilde{S}_j$ to the orders of T_j and S_j and then infers the zeros and poles of vehicle j. In our simulation, the Model Reducer App in Matlab was used to reduce the order of a dynamical system. The comparison results between the actual poles and estimated poles of S_1, S_2, and S_3 are shown in Fig. 8, Fig. 9, and Fig. 10, respectively. From the simulation results we can see that the attacker cannot have a good estimate of the poles of dynamics S_j.

VI. Conclusion

In this paper we proposed a unified framework for privacy-preserving collaborative estimation to fuse local road estimation from a fleet of networked vehicles. By generalizing the iterative learning control (ILC) technique, we established a novel collaborative estimation framework to enable heterogeneous vehicles to iteratively refine the estimation performance in a completely decentralized manner. Numerical simulations showed that the collaborative estimation approach can significantly enhance estimation performance compared with existing single-vehicle based estimation approaches. Given the importance of privacy protection in networked vehicles, we also developed a new privacy enabling mechanism which was seamlessly integrated in the collaborative estimation approach. By leveraging the inherent dynamical properties of collaborative estimation to obfuscate exchanged messages, our privacy-preserving design can be implemented in a completely decentralized manner without affecting the estimation accuracy or incurring heavy communication/computation overhead. Numerical simulations were provided to confirm the effectiveness of our proposed framework.

References

[1] Z. Li, I. V. Kolmanovsky, E. M. Atkins, J. Lu, D. P. Filev, and Y. Bai, "Road disturbance estimation and cloud-aided comfort-based route planning," *IEEE Trans. Cybern.*, vol. 47, no. 11, pp. 3879–3891, Nov. 2017.

[2] Z. Li, I. Kolmanovsky, E. Atkins, J. Lu, D. Filev, and J. Michelini, "Cloud aided semi-active suspension control," in *Proc. IEEE Symp. Comput. Intell. Vehicles Transp. Syst. (CIVTS)*, Dec. 2014, pp. 76–83.

[3] M. M. S. Kaldas and A. M. A. Soliman, "Influence of active suspension preview control on vehicle ride and braking performance," *SAE Int. J. Passenger Cars-Mech. Syst.*, vol. 7, no. 2, pp. 793–803, Apr. 2014.

[4] E. Ozatay *et al.*, "Cloud-based velocity profile optimization for everyday driving: A dynamic-programming-based solution," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 6, pp. 2491–2505, Dec. 2014.

[5] O. Santin *et al.*, "Adaptive nonlinear model predictive cruise controller: Trailer tow use case," SAE, Warrendale, PA, USA, Tech. Rep.2017-01-0090, 2017.

[6] A. S. Krupadanam, M. M. McDonald, and W. C. Albertson, "Road grade coordinated engine control systems," U.S. Patent 8 606 483, Dec. 10, 2013.

[7] N. Kidambi, R. L. Harne, Y. Fujii, G. M. Pietron, and K. W. Wang, "Methods in vehicle mass and road grade estimation," *SAE Int. J. Passenger Cars-Mech. Syst.*, vol. 7, no. 3, pp. 981–991, Apr. 2014.

[8] K. B. Singh and S. Taheri, "Estimation of tire–road friction coefficient and its application in chassis control systems," *Syst. Sci. Control Eng.*, vol. 3, no. 1, pp. 39–61, Mar. 2015.

[9] Z. Li, I. V. Kolmanovsky, U. V. Kalabić, E. M. Atkins, J. Lu, and D. P. Filev, "Optimal state estimation for systems driven by jump–diffusion process with application to road anomaly detection," *IEEE Trans. Control Syst. Technol.*, vol. 25, no. 5, pp. 1634–1643, Sep. 2017.

[10] X. Zhang and D. Göhlich, "A hierarchical estimator development for estimation of tire-road friction coefficient," *PLoS ONE*, vol. 12, no. 2, 2017, Art. no. e0171085.

[11] M. Doumiati, A. Victorino, A. Charara, and D. Lechner, "Estimation of road profile for vehicle dynamics motion: Experimental validation," in *Proc. Amer. Control Conf.*, Jun. 2011, pp. 5237–5242.

[12] Z. Lendek, R. Babuska, and B. De Schutter, "Fuzzy models and observers for freeway traffic state tracking," in *Proc. Amer. Control Conf.*, Jun. 2010, pp. 2278–2283.

[13] D. B. Work, O.-P. Tossavainen, S. Blandin, A. M. Bayen, T. Iwuchukwu, and K. Tracton, "An ensemble Kalman filtering approach to highway traffic estimation using GPS enabled mobile devices," in *Proc. 47th IEEE Conf. Decis. Control*, Oct. 2008, pp. 5062–5068.

[14] A. Allouch, A. Koubâa, T. Abbes, and A. Ammar, "RoadSense: Smartphone application to estimate road conditions using accelerometer and gyroscope," *IEEE Sensors J.*, vol. 17, no. 13, pp. 4231–4238, Oct. 2017.

[15] Li, Huo, Goldberg, Chu, Yin, and Hammond, "Embracing crowdsensing: An enhanced mobile sensing solution for road anomaly detection," *ISPRS Int. J. Geo-Inf.*, vol. 8, no. 9, p. 412, Sep. 2019.

[16] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "CARAVAN: Providing location privacy for VANET," in *Proc. Embedded Security Cars (ESCAR) Workshop*, vol. 2, 2005, pp. 13–15.

[17] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[18] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proc. Int. Workshop Privacy Enhancing Technol.* Berlin, Germany: Springer, 2005, pp. 197–209.

[19] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 9, pp. 2658–2667, Sep. 2016.

[20] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy*, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[21] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci.*, Nov. 1982, pp. 160–164.

[22] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[23] M. M. Prabhakaran and A. Sahai, *Secure Multi-Party Computing*, vol. 10. Amsterdam, The Netherlands: IOS Press, 2013.

[24] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[25] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.* Berlin, Germany: Springer, 2006, pp. 265–284.

[26] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[27] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Trans. Comput.*, vol. 63, no. 2, pp. 510–524, Feb. 2014.

[28] J. Ni, X. Lin, K. Zhang, and X. Shen, "Privacy-preserving real-time navigation system using vehicular crowdsourcing," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2016, pp. 1–5.

[29] D. A. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 181–196, Oct. 2021.

[30] The San Francisco Chronicle. *Experts Raise Privacy, Hacking Concerns as California Tests Digital License Plates*. Accessed: May 31, 2018. [Online]. Available: https://www.govtech.com/dc/Experts-Raise-Privacy-Hacking-Concerns-as-California-Tests-Digital-License-Plates.html

[31] J.-X. Xu, S. K. Panda, and T. H. Lee, *Real-Time Iterative Learning Control: Design Application*. London, U.K.: Springer, 2008.

[32] B. Wang, W. Chen, B. Zhang, and Y. Zhao, "Regulation cooperative control for heterogeneous uncertain chaotic systems with time delay: A synchronization errors estimation framework," *Automatica*, vol. 108, Oct. 2019, Art. no. 108486.

[33] K. E. Bender, "Optimum linear preview control with application to vehicle suspension," *J. Basic Eng.*, vol. 90, p. 213, Jan. 1968.

[34] N. Louam, D. Wilson, and R. Sharp, "Optimal control of a vehicle suspension incorporating the time delay between front and rear wheel inputs," *Vehicle Syst. Dyn.*, vol. 17, no. 6, pp. 317–336, 1988.

[35] A. Hac and I. Youn, "Optimal semi-active suspension with preview based on a quarter car model," in*Proc. Amer. Control Conf.*, Jun. 1991, pp. 433–438.

[36] *Highway Location Marker*. Accessed: Mar. 20, 2020. [Online]. Available: https://en.wikipedia.org/wiki/Highway_location_marker

[37] U. Kalabiá, I. Kolmanovsky, and J. Buckland, "Multi-input observer for estimation of compressor flow," *Adv. Combustion Engines, Building Energy Syst., Mech. Syst.*, vol. 56123, Oct. 2013, Art. no. V001T04A002.

[38] I. V. Kolmanovsky and T. L. Maizenberg, "Stochastic stability, estimation and control in systems driven by jump-diffusion disturbances and their automotive applications," in *Proc. 45th Conf. Decis. Control*, 2006, pp. 4194–4199.

[39] J. L. Ny and G. J. Pappas, "Differentially private filtering," *IEEE Trans. Autom. Control*, vol. 59, no. 2, pp. 341–354, Feb. 2014.

[40] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 111–125.

[41] J. A. Calandrino, A. Kilzer, A. Narayanan, E. W. Felten, and V. Shmatikov, "'You might also like': Privacy risks of collaborative filtering," in *Proc. IEEE Symp. Secur. Privacy*, May 2011, pp. 231–246.

[42] Q. Wu, J. Domingo-Ferrer, and Ú. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.

[43] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

[44] C. Zhang, M. Ahmad, and Y. Wang, "ADMM based privacy-preserving decentralized optimization," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 565–580, Mar. 2019.

Huan Gao (Member, IEEE) was born in Shandong, China. He received the B.S. degree in automation and the M.Sc. degree in control theory and control engineering from Northwestern Polytechnical University, Xi'an, Shaanxi, China, in 2011 and 2015, respectively, and the Ph.D. degree in electrical engineering from Clemson University, Clemson, SC, USA, in 2020. He is currently an Associate Professor with the School of Automation, Northwestern Polytechnical University. His research interests include collaborative estimation, decentralized optimization, cooperative control, and privacy preservation in distributed systems.

Zhaojian Li (Senior Member, IEEE) received the B.Eng. degree from the Nanjing University of Aeronautics and Astronautics in 2010, and the M.S. and Ph.D. degrees in aerospace engineering (flight dynamics and control) from the University of Michigan, Ann Arbor, in 2013 and 2015, respectively. He is currently an Assistant Professor with the Department of Mechanical Engineering, Michigan State University. His research interests include learning-based control, nonlinear and complex systems, and robotics and automated vehicles. He was a recipient of the NSF CAREER Award.

Yongqiang Wang (Senior Member, IEEE) was born in Shandong, China. He received the B.S. degree in electrical engineering and automation, the B.S. degree in computer science and technology from Xi'an Jiaotong University, Xi'an, Shaanxi, China, in 2004, and the M.Sc. and Ph.D. degrees in control science and engineering from Tsinghua University, Beijing, China, in 2009. From 2007 to 2008, he was with the University of Duisburg-Essen, Germany, as a Visiting Student. He was a Project Scientist with the University of California at Santa Barbara, Santa Barbara. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Clemson University. His current research interests include distributed control, optimization, and learning, with emphasis on privacy protection. He also serves as an Associate Editor for IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS and IEEE TRANSACTIONS ON AUTOMATIC CONTROL.