2022 IEEE 61st Conference on Decision and Control (CDC)
December 6-9, 2022. Cancún, Mexico

On Differential Privacy and Traffic State Estimation Problem for Connected Vehicles

Suyash C. Vishnoi, Ahmad F. Taha, Sebastian A. Nugroho, and Christian G. Claudel

Abstract— **This letter focuses on the problem of traffic state estimation for highway networks with junctions in the form of on- and off-ramps while maintaining differential privacy of traffic data. Two types of sensors are considered, fixed sensors such as inductive loop detectors and connected vehicles which provide traffic density and speed data. The celebrated nonlinear second-order Aw-Rascle-Zhang (ARZ) model is utilized to model the traffic dynamics. The model is formulated as a nonlinear state-space difference equation. Sensitivity relations are derived for the given data which are then used to formulate a differentially private mechanism which adds a Gaussian noise to the data to make it differentially private. A Moving Horizon Estimation (MHE) approach is implemented for traffic state estimation using a linearized ARZ model. MHE is compared with Kalman Filter variants namely Extended Kalman Filter, Ensemble Kalman Filter and Unscented Kalman Filter. Several research and engineering questions are formulated and analysis is performed to find corresponding answers.**

2022 IEEE 61st Conference on Decision and Control (CDC) | 978-1-6654-6761-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CDC51059.2022.9993094

I. Introduction and Letter Contributions

The rise of connected vehicles (CVs) technology has provided transportation professionals with additional sources of data to monitor the state of traffic in real time. While more data produces better results when used for state estimation and control, it imposes greater privacy threats on the provider of such data. The location data provided by CVs can be used by criminals for tracking the vehicles, or identifying and profiling the travelers [1], [2]. Even with sensors that provide aggregate density and speed data, the privacy of individual vehicles is not ensured as it is possible to reconstruct individual trajectories using this data [3], [4]. Rising concern about data privacy in general has led to development of privacy preservation algorithms which can be categorized into anonymity based, obfuscation based and policy based algorithms [2]. Among these, obfuscation based algorithms such as those which add noise to the data are preferred for tackling location based privacy issues. Such algorithms can be used to ensure differential privacy (DP) [5] of data. DP is a strong notion of privacy that guarantees the safety of individuals' records when publicly sharing aggregate information from databases. In context of roadway traffic, DP preserves the location privacy of individual vehicles, both CV and non-CV, when publicly sharing traffic state estimates [6], [7].

Introducing DP to traffic data however deteriorates the quality of data which could result in a trade off between the level of privacy and estimation accuracy. Since different state estimation algorithms work with different assumptions and approximations, there is reason to believe that some algorithms work better than others when it comes to differentially private state estimation. Therefore it is important to identify such techniques that can produce high quality state estimates while ensuring necessary levels of privacy.

Past works on differentially private traffic state estimation (TSE) use variants of the Kalman Filter (KF) namely Extended KF (EKF) [6] and Ensemble KF (EnKF) [7] to perform state estimation. KFs are known to suffer from certain issues including the absence of state constraints and required assumptions on the distribution of the noise. A technique which traditionally overcomes these drawbacks is Moving Horizon Estimation (MHE) [8] which is unexplored in the context of differentially private TSE. Therefore, in this work we implement MHE for differentilly private TSE and compare its performance with EKF, EnKF and Unscented KF (UKF) [9]. Note that unlike [10] which proposes a privacy preserving MHE to ensure privacy of the estimates produced using non-private data, here we consider that the received data itself is private and use a more traditional MHE formulation. This allows for privacy from the source of data itself. Also, unlike the past studies which use a first-order traffic model, here we use the second-order Aw-Rascle-Zhang [11], [12] model. Second-order models can reproduce certain real-world traffic phenomena like capacity drop which makes them more suitable for estimation and control purposes. Additionally, we also model junctions which adds more complexity to the model.

Besides, the past work assumes that the speed and density data is obtained from fixed locations on the highway while here we use CVs to obtain data from different parts of the highway.

The overall flow of processes in this study is as follows: sensors collect aggregate density and speed data and add privacy preserving noise it. This data is then sent to the network operator who uses it along with a traffic model to perform TSE to obtain density and speed estimates for the road stretch.

Given that the main research gap on this topic is the absence of a comparative study between different state-estimation techniques for TSE using a second-order model in the presence of DP, we highlight the main contributions of this letter:

- We present a nonlinear state-space formulation for the second-order ARZ model with junctions. The state-space description is appended to include the measurement model which is also nonlinear.
- We derive sensitivity relations for the measured density and speed data. These relations are important for developing differentially private mechanisms that add a Gaussian noise of certain variance to the data to ensure DP.
- The performance of various state estimation techniques is investigated in terms of accuracy using the SUMO traffic simulation software in the presence of privacy preserving additive noise. As a departure from estimation based on KFs, we also investigate MHE for TSE.

The letter is organized as follows. Section II presents the state-space formulation for the ARZ model and the measurement

Suyash C. Vishnoi and Christian G. Claudel are with the Department of Civil, Architectural, and Environmental Engineering, The University of Texas at Austin, 301 E. Dean Keeton St. Stop C1700, Austin, TX 78712. Ahmad F. Taha is with the Department of Civil and Environmental Engineering, Vanderbilt University, 2201 West End Ave, Nashville, TN 37235. Sebastian A. Nugroho is with the Department of Electrical Engineering and Computer Science, University of Michigan, 1301 Beal Ave., Ann Arbor, MI 48109. Emails: scvishnoi@utexas.edu, ahmad.taha@vanderbilt.edu, snugroho@umich.edu, christian.claudel@utexas.edu. This work is partially supported by the National Science Foundation (NSF) under Grants 1636154, 1728629, 1739964, 1917056, 2152928, and 2152450, and USDOT CAMMSE.

model. Section III presents the definitions associated with DP, the sensitivity relations for the data and the differentially private mechanism. It also presents the MHE formulation for TSE. Section IV presents a case study carried out using a realistic traffic simulation software. The letter is concluded by summarizing the results and discussion along with the scope of future work.

II. Nonlinear ARZ Traffic Dynamics Model

This section presents a state-space formulation for the nonlinear second-order ARZ model [11], [12] describing the evolution of traffic density on highways with ramps. Second-order traffic models, unlike their first-order counterparts, consider traffic density and speed to be independent variables which offers a natural way to incorporate both density and speed data provided by the fixed sensors and CVs. While other second-order models exist and have been used for TSE in the past [13], these models unlike the ARZ model face certain limitations [14] such as physical inconsistency under heterogeneous traffic conditions which makes them unreliable.

To represent the model as a series of difference, state-space equations, we discretize the ARZ model with respect to both space and time, also referred to as the Godunov scheme [15]. This allows us to divide the highway and the attached ramps into segments of equal length l and time into steps of equal duration T. The segments forming the highway are referred to as mainline segments and those forming the ramps are called ramp segments. Throughout the letter, $\Omega,\hat{\Omega}$, and $\check{\Omega}$ denote the set of mainline, on-ramp and off-ramp segments respectively such that $N:=|\Omega|, N_I:=|\hat{\Omega}|$ and $N_O:=|\check{\Omega}|$.

The model consists of two states for each segment namely the traffic density (vehicles per unit distance) denoted by $\rho_i[k]$, where k is the index of the time step and i is the index of the segment, and the relative flow (vehicles per unit time) denoted by $\psi_i[k]$. The discrete time traffic density and relative flow conservation equations for any Segment $i\in\Omega$ can be written for any time step k as

$$\rho_i[k+1]=\rho_i[k]+\frac{T}{l}(q_{i-1}[k]-q_i[k]), \tag{1a}$$

$$\psi_i[k+1]=\frac{\tau-1}{\tau}\psi_i[k]+\frac{T}{l}(\phi_{i-1}[k]-\phi_i[k])+\frac{v_f}{\tau}\rho_i[k]. \tag{1b}$$

Here, $q_i[k]$ and $\phi_i[k]$ denote the quantities traffic flow and relative flux leaving Segment $i\in\Omega$ at time step k, and v_f denoting the free flow speed of a segment, and τ are parameters of the ARZ model. Similar equations can be written for ramp segments as well. Mathematical expressions for $q_i[k]$ and $\phi_i[k]$ can be written using the expressions for certain other quantities namely the demand ($D[k]$), supply and driver characteristic ($w[k]$) which are not presented in this article for brevity. These quantities are given as nonlinear functions of the states and inputs defined similar to [16]. The state vector for this system can be defined as

$$\boldsymbol{x}[k]:=[\rho_i[k]\ \psi_i[k]\ \ldots\ \hat{\rho}_j[k]\ \hat{\psi}_j[k]\ \ldots\ \check{\rho}_l[k]\ \check{\psi}_l[k]\ \ldots]^\top$$

where $\boldsymbol{x}[k]\in\mathbb{R}^{2(N+N_I+N_O)}$ and $i\in\Omega$, $j\in\hat{\Omega}$ and $k\in\check{\Omega}$. The variables with $\hat{\cdot}$ are associated with the on-ramps and those with $\check{\cdot}$ are associated with off-ramps. The input vector is defined as,

$$\boldsymbol{u}[k]:=[D_{in}[k]\ w_{in}[k]\ \rho_{out}[k]\ \ldots\ \hat{D}_{in,j}[k]\ \hat{w}_{in,j}[k]\ldots\ \check{\rho}_{out,l}[k]\ \ldots]^\top$$

where $\boldsymbol{u}[k]\in\mathbb{R}^{3+2N_I+N_O}$, $j\in\hat{\Omega}$ and $l\in\check{\Omega}$.

The evolution of traffic density and relative flow described in (1) can be written in a compact state-space form as follows

$$\boxed{\boldsymbol{x}[k+1]=\boldsymbol{A}\boldsymbol{x}[k]+\boldsymbol{G}\boldsymbol{f}(\boldsymbol{x},\boldsymbol{u}),} \tag{2}$$

where $\boldsymbol{A}\in\mathbb{R}^{n_x\times n_x}$ for $n_x:=2(N+N_I+N_O)$ represents the linear portion of the dynamics of the system, $\boldsymbol{f}:\mathbb{R}^{n_x}\times\mathbb{R}^{n_u}\to\mathbb{R}^{n_x}$ where $n_u=3+2N_I+N_O$ is a vector valued function representing nonlinearities in the state-space equation, and $\boldsymbol{G}\in\mathbb{R}^{n_x\times n_x}$ is a matrix representing the distribution of nonlinearities. The nonlinearities in $\boldsymbol{f}$ are in the form of minimum of weighted nonlinear functions of the states and inputs. The structure of the above mentioned functions are similar to those presented in [16]. The modeling approach can be applied to roads with any number of lanes given the maximum density is adjusted based on the number of lanes. Next, we discuss the measurement model which is also nonlinear in nature.

We consider two types of sensors, fixed sensors like the inductive loop detectors and CVs. This study assumes that it is possible to retrieve aggregate density and speed data for road segments from both these sensors. Such data can be obtained from fixed sensors directly using techniques such as in [17]. With CVs, the average speed of a segment is assumed to be the average of the speed of all the queried CVs in a segment similar to [18]. To obtain density data from CVs, we assume additional functionality like spacing measurement equipment available in advanced driver assistance systems [19] or availability of vehicular ad-hoc networks (VANETs) which allow vehicles to communicate with each other in a neighbourhood around the queried CV [20]. A sufficient penetration of CVs is necessary on the segments which are queried for data. The spacing data or neighbourhood counts can then be converted to density measurements before adding the privacy preserving noise to them and sending them to a network operator to perform estimation.

Among these measurements, density $\rho_i[k]$ for any mainline segment $i\in\Omega$, and similarly for the ramps, is directly a state and is used as it is, while the speed $v_i[k]$ can be written in terms of the states as follows:

$$v_i[k]=\frac{\psi_i[k]}{\rho_i[k]}-p(\rho_i[k]),$$

where $p(\cdot)$ is called the pressure function and is defined as part of the ARZ model framework. We define a nonlinear measurement function $\boldsymbol{h}(\boldsymbol{x}[k])$ such that
$h_{2i-1}(\boldsymbol{x}[k])=x_{2i-1}[k]$, and $h_{2i}(\boldsymbol{x}[k])=\dfrac{x_{2i}[k]}{x_{2i-1}[k]}-p(x_{2i-1}[k])$.
Now, we can define the measurement vector $\boldsymbol{y}[k]$ as

$$\boxed{\boldsymbol{y}[k]=\boldsymbol{C}[k]\boldsymbol{h}(\boldsymbol{x}[k])+\boldsymbol{\nu}[k],} \tag{3}$$

where $\boldsymbol{C}[k]$ is the observation matrix at time k describing the availability of measurements from sensors. Note, that the observation matrix here is variable in time because of the measurements from CVs which are taken from different segments at different times. At any time k, $n_p[k]$ is the number of measurements. Here, $\boldsymbol{\nu}[k]\in\mathbb{R}^{n_\nu[k]}, n_\nu[k]=n_p[k]$ lumps all the measurement errors including the sensor noise into a single vector.

In the following section we discuss some definitions related to differential privacy with respect to the traffic data, the dynamics (2), and the measurement model (3).

III. Differential Privacy of Traffic Data and MHE

Making the data differentially private is considered as an adequate measure against privacy attacks such as unwanted tracking of vehicles and identifying individuals based on location data. While certain cryptographic methods maintain privacy by preventing attackers from reading the data, under the possibility that the attacker finds a way to read it, differential privacy adds another layer of defense which statistically guarantees that individual's records cannot be extracted from the data set. It also allows sharing of estimates obtained from this data with third-parties keeping the same guarantee. DP is achieved by processing the data through differentially private mechanisms which are functions that take entire data sets as input and produce a differentially private output. In the following sections we discuss some definitions that are needed to formally define DP.

A. Adjacency and DP

DP is defined in terms of adjacent data sets. Mathematically, *adjacency* is defined as a binary symmetric relation denoted by Adj on a space of data sets, say D, such that for $d,d' \in D$ $Adj(d,d')$ holds if and only if d and d' differ by the data of a single individual. In this work, we consider two spaces of data sets, the traffic density data sets and the traffic speed data sets which are composed of the average vehicle density and average vehicle speed values from several road segments and several time steps. Two data sets from either of these spaces are said to be adjacent if they differ by the trajectory of a single vehicle. With this definition of adjacency, a differentially private mechanism can be defined similar to [7] as,

Let D be a space of data sets, and let $(\mathrm{R},\mathcal{M})$ be a measurable space where $\mathcal{M}$ is a σ-algebra on R. Let $\epsilon,\delta \geq 0$. A mechanism $M: D \to R$ is $(\epsilon,\delta)-$differentially private if for all $d,d' \in D$ such that $\mathrm{Adj}(d,d')$, we have

$$\mathbb{P}(M(d) \in S) \leq e^{\epsilon}\mathbb{P}(M(d') \in S) + \delta, \forall S \in \mathcal{M} \tag{4}$$

This means that the distribution of the outputs produced by the mechanism M on any two adjacent data sets is very close which makes it difficult to determine which data set was used as input by looking at the output of the mechanism. Thus, attackers are unable to extract individual specific information from the mechanism's output. Releasing this output instead of the original data protects individual's privacy against attacks. M is therefore said to provide (ϵ,δ)-DP to the data. Smaller values of both ϵ and δ provide higher privacy. In this work, we assume that such a privacy preserving mechanism is applied to the density and speed data collected by the fixed sensors and CVs at the source and the output is sent to the network operator.

An important property [6] which allows the network operator to use this data for state estimation and control while maintaining the DP guarantee is called *resilience-to-post-processing*. According to this property, if another mechanism is applied to the output of a differentially private mechanism, the obtained result will have the same DP guarantees as the initial output. In context of this work, the mechanism applied after receiving the differentially private outputs from the sensors is the estimation process. Thus, the final state estimates are also differentially private.

To write the mechanisms capable of producing differentially private outputs, we need to first define sensitivity relations for the two types of data sets.

B. Sensitivity relations

The sensitivity of a function is defined as the maximum difference in the value of the function produced by two adjacent data sets. In this work we are concerned about the sensitivity of data coming from the traffic sensors. Since both the type of sensors considered in this study provide the same two type of data, that is the segment density and speed, we do not have a separate sensitivity relation for CV data than for fixed sensor data. Specifically, we care about the Euclidean norm between adjacent data sets, that is, $\|\boldsymbol{\rho}-\tilde{\boldsymbol{\rho}}\|_2$ and $\|\mathbf{v}-\tilde{\mathbf{v}}\|_2$ where $\boldsymbol{\rho},\tilde{\boldsymbol{\rho}}$ and $\boldsymbol{v},\tilde{\boldsymbol{v}}$ are any two adjacent pairs of density and speed data respectively. We can write

$$\|\boldsymbol{\rho}-\tilde{\boldsymbol{\rho}}\|_2^2 = \sum_{k=0}^{\infty}\sum_{i=1}^{n_p[k]} |\rho^i[k]-\tilde{\rho}^i[k]|^2$$

where $\rho^i[k]$ represents the density measured at the i^{th} density sensor at time step k. Largest sensitivity value occurs when the differentiating vehicle passes all the sensors at different times in the two data sets. Since the density of a segment can be defined as the number of vehicles per unit length of the segment, the density measurements in the two data sets can be assumed to differ by $\frac{1}{l}$ when the differentiating vehicle is present on a measured segment in one data set and absent in the other as the difference is caused by a single vehicle being present or absent on that segment. The total time during which the density for a segment differs between the two data sets at any such instance can be approximated based on the average time spent by a vehicle on that segment. Let this average time be denoted by T_{avg}, which can be approximated using past CV data for that stretch or by using a simulation-based approach as in [7]. Here T_{avg} for all segments is assumed to be the same but in practice a different T_{avg} can be computed for different segments to get a better approximation of the sensitivity. At all other times the measured densities would be the same in both the data sets. Then,

$$\|\boldsymbol{\rho}-\tilde{\boldsymbol{\rho}}\|_2^2 = \sum_{k=0}^{\infty}\sum_{i=1}^{n_p[k]} |\rho^i[k]-\tilde{\rho}^i[k]|^2 \leq \sum_{i=1}^{N_p} 2T_{avg}\left(\frac{1}{l}\right)^2, \tag{5}$$

$$\implies \|\boldsymbol{\rho}-\tilde{\boldsymbol{\rho}}\|_2 \leq \frac{1}{l}\sqrt{2N_pT_{avg}} =: \Delta_\rho, \tag{6}$$

where N_p is the maximum number of sensors on the highway stretch at any time and Δ_ρ is the sensitivity of the density data sets.

Similarly, for speed measurements we can write

$$\|\boldsymbol{v}-\tilde{\boldsymbol{v}}\|_2^2 = \sum_{k=0}^{\infty}\sum_{i=1}^{n_p[k]} |v^i[k]-\tilde{v}^i[k]|. \tag{7}$$

The effect of the absence or presence of a single vehicle in the segment on the average speed of that segment can be approximately captured indirectly with the help of the equilibrium speed-density relationship of the ARZ model [11], [12] given as

$$V_e(\rho) = v_f\left(1-\left(\frac{\rho}{\rho_m}\right)^{\gamma}\right), \tag{8}$$

which relates the equilibrium speed V_e of a road segment with the density of that segment. Here, ρ_m denoting the maximum density of a segment, and γ are parameters of the ARZ model. We can replace the speeds in the right hand side of (7) with the expression in (8) with $\gamma = 1$ and simplify it to get

$$|v^i[k]-\tilde{v}^i[k]|=\left|\frac{v_f}{\rho_m}\left(\rho^i[k]-\tilde{\rho}^i[k]\right)\right|. \tag{9}$$

Then using the same idea as for the density, we can write

$$\|\boldsymbol{v}-\tilde{\boldsymbol{v}}\|_2 \leq \frac{v_f}{\rho_m l}\sqrt{2N_p T_{avg}} =: \Delta_v, \tag{10}$$

where Δ_v is the sensitivity of the speed data sets. Here, $\gamma=1$ is chosen arbitrarily to simplify the expression (9) to a known constant value. Though γ varies between 1 and 2 [16] (10) serves as a good upper bound in most cases since ρ lies between quarter to one-third of ρ_m under normal flow conditions. The sensitivity Δ_v can be modified under specific scenarios using empirical tests or using a traffic simulation approach as in [7]. In general, ensuring a realistic value of the sensitivity avoids a large privacy-utility trade off.

C. Differentially private mechanisms

Using the sensitivity relations from the previous section, we can implement a Gaussian Mechanism [6] which ensures $(\epsilon,\delta)-$DP.

Let $K = Q^{-1}(\delta)$ for $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-u^2/2}du$, and $\kappa_{\delta,\epsilon} = (K+\sqrt{K^2+2\epsilon})/(2\epsilon)$, then a mechanism publishing the sequence $\bar{\rho}=\rho+w_\rho$ where w_ρ are zero mean iid Gaussian random variables with variance $\kappa^2_{\delta,\epsilon}\Delta_\rho$ is (ϵ,δ)-differentially private. Here ρ is the measured density data and $\bar{\rho}$ is the differentially private output produced by the mechanism which will be sent to the network operator.

Similarly, a mechanism publishing the sequence $\bar{v}=v+w_v$ where w_v are zero mean iid Gaussian random variables with variance $\kappa^2_{\delta,\epsilon}\Delta_v$ is also (ϵ,δ)-differentially private. Here v is the measured speed data and $\bar{v}$ is the differentially private output of the mechanism. For the mechanisms defined here, the output itself is a data set which will henceforth be called differentially private data. In the next section, we discuss the MHE approach applied for TSE using the differentially private data produced by the mechanisms.

D. Moving horizon estimator under DP

The objective of this article is to investigate the TSE performance using ARZ model when considering differentially private data coming from the fixed sensors and CVs. To do so, here we implement a linear MHE approach using linearized versions of the process and measurement models obtained using a first-order Taylor series approximation. Throughout this section, N denotes the size of the horizon for optimization.

1) Decision variables and objective function: The decision variables for the optimization problem solved at time step k are the state vectors from time step $k-N$ to k denoted by $\boldsymbol{x}_k[t]\ \forall\ t\in[k-N,k]$. From the obtained solution we set the final value of the vector $x_k[k]=\boldsymbol{x}_k[k]$. The objective function at time step $k\in[N+1,\infty]$ is denoted by $J[k]:=J$ and is given as

$$J=\mu||\boldsymbol{x}_k[k-N]-\boldsymbol{x}[k-N]||^2+w_1\sum_{i=k-N}^{k}||\boldsymbol{y}[i]-(\tilde{\boldsymbol{C}}_i\boldsymbol{x}_k[i]+\boldsymbol{c}_{2i})||^2$$
$$+w_2\sum_{i=k-N}^{k-1}||\boldsymbol{x}_k[i+1]-(\tilde{\boldsymbol{A}}_i\boldsymbol{x}_k[i]+\boldsymbol{B}_i\boldsymbol{u}[i]+\boldsymbol{c}_{1i})||^2. \tag{11}$$

Here, $\bar{\boldsymbol{x}}[k-N]$ is a prediction of $\boldsymbol{x}[k-N]$ based on a previously obtained state estimate and is expressed as

$$\bar{\boldsymbol{x}}[k-N]=\boldsymbol{A}\hat{\boldsymbol{x}}[k-N-1]+\boldsymbol{G}\boldsymbol{f}(\hat{\boldsymbol{x}}[k-N-1],\boldsymbol{u}[k-N-1]). \tag{12}$$

The notation $\boldsymbol{y}[i]$ defines the data vector at time $i\in[k-N,k]$, $\tilde{\boldsymbol{A}}_i$, $\boldsymbol{B}_i$ and $\boldsymbol{c}_{1i}$ are parameters of the linearized state-space equation $\forall\, i\in[k-N,k-1]$, and $\tilde{\boldsymbol{C}}_i$ and $\boldsymbol{c}_{2i}$ are parameters of the linearized measurement model $\forall\, i\in[k-N,k]$. Here, $\tilde{\boldsymbol{A}}_k$, $\boldsymbol{B}_k$ and $\boldsymbol{c}_{1k}$ are computed at $(\boldsymbol{x}_o,\boldsymbol{u}[k])$ where $\boldsymbol{x}_o=\sum_{i=k-1-N}^{k-1}\boldsymbol{x}_{k-1}[i]/(N+1)$, $\tilde{\boldsymbol{C}}_k$ and $\boldsymbol{c}_{2k}$ are computed at $\boldsymbol{x}_o$.

2) Constraints and optimization problem: The problem only consists of the upper and lower bounds on state values as follows

$$\boldsymbol{x}_{\min}\leq\boldsymbol{x}_k[i]\leq\boldsymbol{x}_{\max},\forall\ i\in[k-N,k] \tag{13}$$

where $\boldsymbol{x}_{\min}=\vec{0}$, and $\boldsymbol{x}_{\max}=[\rho_m\ \ \rho_m v_f\ \ \rho_m\ \ \rho_m v_f\ \ \cdots\ \ \rho_m\ \ \rho_m v_f]^T$. The above objective and constraints are used to write the following optimization problem

$$\underset{\boldsymbol{x}_k[k-N],\ldots,\boldsymbol{x}_k[k]}{\text{minimize}}\quad J[k],\ \text{subject to}\quad (13). \tag{14}$$

The objective function $J[k]$ can also be expressed as a sum of quadratic and linear terms of the state vectors. Defining $\boldsymbol{z}_k$ by concatenating the decision variables from (14) such that $\boldsymbol{z}_k=[\boldsymbol{x}_k[k-N]^T\ \boldsymbol{x}_k[k-N+1]^T\ \cdots\ \boldsymbol{x}_k[k]]^T$, we can write the optimization problem (14) in standard form as follows

$$\boxed{\underset{\boldsymbol{z}_k}{\text{minimize}}\ \boldsymbol{z}_k^T\boldsymbol{H}\boldsymbol{z}_k+\boldsymbol{q}^T\boldsymbol{z}_k,\ \text{subject to}\ \boldsymbol{z}_{\min}\leq\boldsymbol{z}_k\leq\boldsymbol{z}_{\max}} \tag{15}$$

where $\boldsymbol{H}\in\mathbb{R}^{(N+1)n_x\times(N+1)n_x}$ and $\boldsymbol{q}\in\mathbb{R}^{(N+1)n_x}$ consist of the coefficients of the quadratic and linear terms in the objective respectively. $\boldsymbol{z}_{\min}=[(x^T_{min})_{\times(N+1)}]^T$ and $\boldsymbol{z}_{\max}=[(x^T_{max})_{\times(N+1)}]^T$ denote bounds on $\boldsymbol{z}_k$. It can be shown that $\boldsymbol{H}$ is a positive definite matrix which makes (15) a convex quadratic program (QP) that can be solved efficiently using readily available QP solvers like CPLEX or MATLAB's `quadprog` function. Hence, problem (15) is computationally tractable.

IV. Case Study using SUMO

In this section, we apply the implemented MHE along with EKF, UKF and EnKF, on a traffic simulation example generated in SUMO which is an open source the traffic micro-simulation software to compare their performance while keeping the data differentially private. All the simulations are carried out using MATLAB R2019b running on a 64-bit Windows 10 with 3.6GHz Intel$^{\text{R}}$ Core$^{\text{TM}}$ i7-7700 CPU and 65GB of RAM. We use the `quadprog` function of MATLAB to solve the MHE optimization problem.

The main idea of this case study is to test the performance of the state estimation techniques under different conditions of privacy. In particular, we are interested in knowing the answers to the following questions:

- *Q1:* How does the number of CV-segments impact the state estimation performance of each technique while ensuring DP of data?
- *Q2:* What is the impact of the level of privacy on the state estimation performance of each technique?

A. Highway and sensor setup

In this study, we model a highway stretch of length 1.5 km with two on-ramps at 0.3 and 0.9 km from the start and two off-ramps at 0.6 and 1.2 km from the start. Additional 100 m segments are modeled in SUMO before all the entry points and following all the exit points of the highway whose data serves as input

for the system. We use the Weidemann 99 car-following model with default parameters. The ARZ model parameters are calibrated using simulated data from SUMO. The selected values are $v = 102$ km/hr, $\rho_m = 333$ veh/km, $\tau = 60$, and $\gamma = 2$. Under the Godunov scheme, the highway and ramps are divided into segments of length 100 m each with a time-step value of 1 s, which satisfies the CFL condition. The segment mean speeds are provided directly by SUMO while the segment densities can be computed from the vehicle count data provided by SUMO for each segment. There are a total of 38 states in this highway system consisting of 15 mainline segments and 4 ramps. Since the local state-space dynamics for segment-type combinations as in (1) are the same irrespective of the overall structure, the state estimation performance here should be representative of the performance in general.

We force a congestion on the highway to create an interesting scenario for comparison of TSE methods. The mainline demand is kept as 2050 veh/hr throughout except between 200-400 sec when it is increased to 6050 veh/hr owing to say a rush hour. The on-ramp demands are kept as 320 veh/hr and 300 veh/hr respectively. A variable speed sign is implemented in SUMO to emulate a situation where an accident has occurred on Segment 11 of the highway mainline. The maximum allowed speed for this segment is artificially reduced to 10.08 km/hr between 200-400 sec and 50.95 km/hr between 400-500 sec.

Throughout the case study, the fixed sensors are assumed to be placed on the output segments of the network which is necessary to make the system observable. We assumes that there is a sufficient number of CVs on the highway to obtain the density and speed values of decent quality from any road segment. We also assume that we can only query a limited number of CVs at a time due to bandwidth constraints. At every time step we select a subset of segments to obtain data from. In the case study, we select a set of segments at the beginning and update it after every four time steps. At every update, the current segments in the set are replaced by segments right ahead of them. The last mainline segment is replaced by the first mainline segment. Note that a better method to select CVs for querying may be available but is not explored here. No measurement noise is added to the data apart from the privacy preserving noise.

B. Implementation of estimation techniques

a) Parameter tuning: In this work, for all the KF variants, we use diagonal process and measurement noise co-variance matrices of the form $\boldsymbol{Q} = q\boldsymbol{I}$ and $\boldsymbol{R} = r\boldsymbol{I}$ where $q, r \in \mathbb{R}_+$ and $\boldsymbol{I}$ in each case is an identity matrix of appropriate dimensions. The initial guess for the estimate noise co-variance matrix is taken as $\boldsymbol{P} = 10^{-3}\boldsymbol{I}$. We manually tune q and r for different arrangements of sensors and different privacy levels based on the minimization of the root mean squared error (RMSE) of estimated states. The weights in the MHE objective function are also similarly tuned. Regarding other parameters, for UKF [9], we set the following values: $\alpha = 0.1, \kappa = -4$ and $\beta = 2$, for EnKF [21], we set the number of ensemble points to 100, and for MHE, we set N to 10. These values are found to be sufficient for the respective techniques except wherever specified.

b) External bounds in KF: The KFs can produce negative values of the states which are not allowed in the process model (2). It results in numerical issues and forces the estimation to stop. To avoid this estimates are projected to within physical bounds. In case of UKF, the sigma points need to be individually bounded with a lower bound greater than zero to avoid numerical issues within UKF. This method of projecting vectors for EKF and UKF has been shown to fit in the KF theory mathematically and is among the popular methods mentioned in [22].

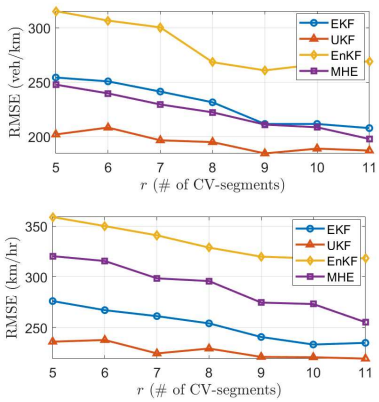

Fig. 1. RMSE for (a) density [top] and (b) speed [bottom] with increasing number of CV-segments while considering (1,0.05)-DP.

c) Choice of comparison metrics: Parameter tuning is done using the RMSE of the estimated states. However, since the relative flow does not hold a direct significance for professionals, we chose to compare the techniques based on the RMSE of density and speed which have more general value.

C. Results and discussion

1) Impact of number of CV-segments: Here, we test the impact of increasing the number CV-segments on the performance of different state estimation techniques. We vary the number of CV-segments from 5 to 11 while keeping them as far apart as possible. Exact arrangement is omitted for brevity. Privacy preserving noise is added to the measurement values based on the mechanism in Section III-C to make the data $(1, 0.05)$-differentially private. Fig. 1 presents the plot of RMSE for the estimated density and speed for each of the techniques. The computation time per time step of simulation for EKF, UKF, EnKF, and MHE are 0.06, 0.026, 0.040, and 0.045 seconds respectively. These include the time taken from receiving the data to producing the estimate for one time step.

It is observed that the estimation performance for all the techniques improves with increasing number of CV-segments which is expected. EnKF sometimes has more variation in consecutive RMSE values as compared to other techniques which can be attributed to the associated randomness. Overall, EnKF performs the worst while UKF performs the best, closely followed by both MHE and EKF in case of density estimation and EKF in case of speed estimation. It is interesting that MHE falls behind EKF in case of speed estimation. This comparison in performance is also observed in the following tests. This is mentioned here to avoid repetition later. Fig. 2 presents a plot of the actual versus estimated density values obtained using UKF, EKF and MHE.

2) Impact of DP parameters: Privacy in this study depends on two parameters ϵ and δ which have their own significance in the DP definition. In this section, we test the impact of varying these parameters on the state estimation performances. We keep the same configuration of fixed sensors as in the previous section while

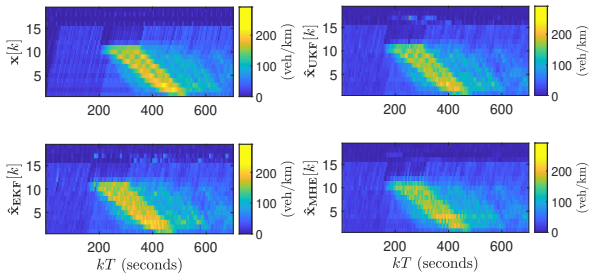

Fig. 2. Traffic densities $\mathbf{x}[k]$ obtained from SUMO along with estimates from EKF denoted by $\hat{\boldsymbol{x}}_{\mathrm{EKF}}[k]$, UKF denoted by $\hat{\boldsymbol{x}}_{\mathrm{UKF}}[k]$, and MHE denoted by $\hat{\boldsymbol{x}}_{\mathrm{MHE}}[k]$ while considering $(1, 0.05)-$DP and 7 CV-segments evenly spaced on the highway stretch.

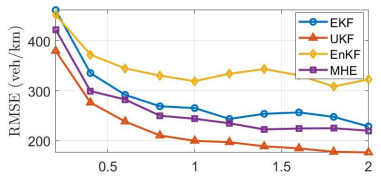

Fig. 3. RMSE for densities with changing ϵ while keeping $\delta = 0.05$.

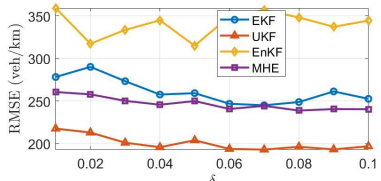

Fig. 4. RMSE for densities with changing δ while keeping $\epsilon = 1$.

the number of CV-segments is fixed to 5. Fig. 3 and Fig. 4 present the variation in RMSE values for density for each technique with changing epsilon keeping a constant $\delta = 0.05$, and changing delta keeping $\epsilon = 1$ respectively. The plots for speed in both cases are very similar to density and are omitted for brevity. The co-variance matrices are tuned as necessary to obtain the best performance.

All the techniques show a similar variation in performance with respect to privacy changes. It is observed that the impact of ϵ is more profound than that of δ when both are varied between respective reasonable bounds. Specifically, the variation in performance is small over the full range of selected δ values. On the other hand, the variation is small for ϵ values above 1, but the performance quickly worsens as we approach 0. While more research might be needed under various scenarios, from the obtained results it can be stated that it is possible to increase the level of privacy to a certain extent without worrying about much additional degradation of estimation quality. Beyond that point, a trade-off would be more apparent and should be considered more seriously.

3) Discussions and preliminary answers: We provide some preliminary suggestions regarding the questions posed earlier in this section:

- *A1:* State estimation error decreases with an increase in the number of CV-segments. UKF outperforms the other methods in both density and speed estimation while EnKF's performance is the worst. EKF and MHE perform comparably.
- *A2:* All the techniques show similar variation in performance with change in privacy levels. In general, ϵ has more influence on the estimation quality than δ.

A drawback of the present study is that it assumes that both the CVs and fixed sensors provide the same measurement values for a segment if present simultaneously. This may not always be true and a reliable approach for data integration may be needed. Studying the data integration problem considering different aggregate measurements from sensors or using trajectory data from CVs for state estimation and its impact on privacy are possible future directions of work. Also, while not studied in this work, the advantage of MHE in implementing arbitrary relations between states which are otherwise un-modeled in the dynamics can also be explored.

References

[1] R. Chen, B. C. Fung, N. Mohammed, B. C. Desai, and K. Wang, "Privacy-preserving trajectory data publishing by local suppression," *Information Sciences*, vol. 231, pp. 83–97, 2013.

[2] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[3] J. Le Ny, *Differential Privacy for Dynamic Data*. Springer, 2020.

[4] F. Xu, Z. Tu, Y. Li, P. Zhang, X. Fu, and D. Jin, "Trajectory recovery from ash: User privacy is not preserved in aggregated mobility data," in *Proceedings of the 26th international conference on world wide web*, 2017, pp. 1241–1250.

[5] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Found. Trends Theor. Comput. Sci.*, vol. 9, no. 3-4, pp. 211–407, 2014.

[6] J. Le Ny, A. Touati, and G. J. Pappas, "Real-time privacy-preserving model-based estimation of traffic flows," in *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2014, pp. 92–102.

[7] H. Andre and J. Le Ny, "A differentially private ensemble kalman filter for road traffic estimation," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2017, pp. 6409–6413.

[8] C. V. Rao, J. B. Rawlings, and J. H. Lee, "Constrained linear state estimation—a moving horizon approach," *Automatica*, vol. 37, no. 10, pp. 1619–1628, 2001.

[9] E. A. Wan and R. Van Der Merwe, "The unscented Kalman filter for nonlinear estimation," in *Proceedings of the IEEE 2000 Adaptive Systems for Signal Processing, Communications, and Control Symposium (Cat. No. 00EX373)*. Ieee, 2000, pp. 153–158.

[10] V. Krishnan and S. Martínez, "A probabilistic framework for moving-horizon estimation: Stability and privacy guarantees," *IEEE Transactions on Automatic Control*, vol. 66, no. 4, pp. 1817–1824, 2021.

[11] A. Aw and M. Rascle, "Resurrection of "second order" models of traffic flow," *SIAM journal on applied mathematics*, vol. 60, no. 3, pp. 916–938, 2000.

[12] H. M. Zhang, "A non-equilibrium traffic model devoid of gas-like behavior," *Transportation Research Part B: Methodological*, vol. 36, no. 3, pp. 275–290, 2002.

[13] Y. Wang, M. Zhao, X. Yu, Y. Hu, P. Zheng, W. Hua, L. Zhang, S. Hu, and J. Guo, "Real-time joint traffic state and model parameter estimation on freeways with fixed sensors and connected vehicles: State-of-the-art overview, methods, and case studies," *Transportation Research Part C: Emerging Technologies*, vol. 134, p. 103444, 2022.

[14] C. F. Daganzo, "Requiem for second-order fluid approximations of traffic flow," *Transportation Research Part B: Methodological*, vol. 29, no. 4, pp. 277–286, 1995.

[15] S. K. Godunov, "A difference method for numerical calculation of discontinuous solutions of the equations of hydrodynamics," *Matematicheskii Sbornik*, vol. 89, no. 3, pp. 271–306, 1959.

[16] O. Kolb, G. Costeseque, P. Goatin, and S. Gottlich, "Pareto-optimal coupling conditions for the Aw–Rascle–Zhang traffic flow model at junctions," *SIAM Journal on Applied Mathematics*, vol. 78, no. 4, pp. 1981–2002, 2018.

[17] C. Lee, J.-B. Lee, and M. Kim, "Density measurement algorithm for freeway segment using two point detectors," *Journal of Advanced Transportation*, vol. 45, no. 3, pp. 207–218, 2011.

[18] N. Bekiaris-Liberis, C. Roncoli, and M. Papageorgiou, "Highway traffic state estimation per lane in the presence of connected vehicles," *Transportation Research Part B: Methodological*, vol. 106, pp. 1–28, 2017.

[19] T. Seo, T. Kusakabe, and Y. Asakura, "Estimation of flow and density using probe vehicles with spacing measurement equipment," *Transportation Research Part C: Emerging Technologies*, vol. 53, pp. 134–150, 2015.

[20] S. Panichpapiboon and W. Pattara-atikom, "Evaluation of a neighbor-based vehicle density estimation scheme," in *2008 8th International Conference on ITS Telecommunications*. IEEE, 2008, pp. 294–298.

[21] G. Evensen, "The ensemble Kalman filter: Theoretical formulation and practical implementation," *Ocean dynamics*, vol. 53, no. 4, pp. 343–367, 2003.

[22] D. Simon, "Kalman filtering with state constraints: a survey of linear and nonlinear algorithms," *IET Control Theory & Applications*, vol. 4, no. 8, pp. 1303–1318, 2010.