A DIFFERENTIALLY PRIVATE ENSEMBLE KALMAN FILTER FOR ROAD TRAFFIC ESTIMATION

Hubert Andre and Jerome Le Ny

Dept. of Electrical Engineering and GERAD, Polytechnique Montreal, QC H3T-1J4, Canada

ABSTRACT

Road traffic estimation systems can rely nowadays on an increasing number and variety of sensors and data sources to provide better coverage and accuracy, from standard static detectors to, more recently, location traces obtained possibly from individual drivers' smartphones. Motivated by privacy concerns raised by such systems, this paper discusses a methodology for estimating the macroscopic traffic state (density, velocity) along a road segment in real-time, while providing formal *differential privacy* guarantees to the individual drivers, a state-of-the-art notion of privacy that protects against adversaries with arbitrary side-information. The impact of the privacy constraint on estimation performance is mitigated by the use of a nonlinear model of the traffic dynamics, fused with the sensor measurements via an Ensemble Kalman Filter, a classical method for data assimilation.

***Index Terms*—** Differential privacy, ensemble Kalman filter, traffic estimation

1. INTRODUCTION

Real-time road traffic estimation has benefited from important advances in sensing technology in the past decade. Traffic cameras together with computer vision algorithms can play a role similar to the traditional induction loops embedded in roadways, counting cars passing at a given location and estimating their velocity. It is now also easy to obtain *floating car data*, i.e., location traces sent by devices inside traveling cars, as measured for example from the cellular network location services, by on-board GPS devices [1] or RFID tags [2].

Integrating an ever-larger number and variety of monitoring sensors improves the coverage of traffic estimates, beyond the major highways where the only sensors used to be located, due to cost considerations. However, an undesirable side effect is the collection of sensitive location information about private individuals, who can be easily tracked by anyone having access to the raw data, even when obvious means of identification such as names are removed from the datasets [3]. In fact, even publishing aggregate estimates of traffic density and velocity on a road network leaks some of the information contained in the measured driver trajectories, which could be used for sophisticated privacy attacks [4], and papers such as [5, 6] illustrate the risks of ruling out such attacks based purely on intuitive reasoning.

The purpose of this paper is to develop a methodology for the design of real-time traffic state estimators providing formal *differential privacy* guarantees [7], as defined in Section 2. Whereas other notions of privacy can be considered for our application, such as k-anonymity [1, 8] and its various extensions [9], differential privacy has been increasingly often adopted in the past decade as a state-of-the-art tool for privacy preserving data analysis [10]. Differentially private mechanisms publish outputs (here, traffic state time-series) that are randomized in such as way that their distribution is not very sensitive to the data of any single individual. As a result, whether an individual provides his data or not does not change significantly the risk that any adversary, no matter how powerful, can make new inferences about him.

The difficulty however is in producing differentially private outputs that are only moderately perturbed, e.g., traffic estimates of sufficiently high accuracy. There has been some previous work on protecting location data via differentially private mechanisms [11, 12], but none of these focuses on model-based estimation, except our previous work [13], on which we improve in Section 3 with an alternate way of sanitizing static sensor data and by considering floating car data as well. The traffic sensor measurements are integrated with a hydrodynamic model of traffic [14] through an Ensemble Kalman Filter (EnKF) producing differentially private outputs, as described in Section 4, and a spatially adaptive sampling scheme helps make more efficient use of the sensitive floating car data. The EnKF [15] builds on ideas from Kalman filtering and Monte-Carlo methods, is quite popular for traffic estimation [16] and leads to a simpler implementation than with the Extended Kalman Filter presented in [13].

2. PROBLEM STATEMENT

2.1. Traffic Dynamics

For simplicity of exposition, we consider the estimation of the traffic state on a single road without intersection. In general, the traffic state at time t and position x is characterized by a density $\rho(x, t)$ (in vehicles per mile say) and a traffic velocity

This research was supported by FRQNT Award 2015-NC-181370.

$v(x,t)$ or traffic flow $q(x,t) := \rho(x,t)v(x,t)$. In first-order models [14], we postulate a static relationship between density and traffic flow, called the *fundamental diagram*, which is often assumed to be triangular

$$q(\rho) = \begin{cases} v_0\rho, & \text{for } \rho \leq \rho_C := \frac{w}{v_0+w}\rho_M \\ -w(\rho - \rho_M), & \text{for } \rho_C \leq \rho \leq \rho_M. \end{cases} \quad (1)$$

Here v_0 is the free traffic speed, ρ_C is the critical density between free traffic (speed $v = v_0$) and congested traffic (speed $v < v_0$), ρ_M is the maximal or "jam" density, associated with a zero speed traffic, and w is the speed at which congestion waves propagate (backwards). We describe the evolution of traffic in discrete time, with time periods of length τ. The road is discretized into N cells of length Δx_j, $1 \leq j \leq N$, with the density $\rho_{j,t}$ in cell j at period $t \geq 0$ assumed approximately constant. Let λ_j denote the number of lanes and $f_{j,t}$ the *numerical flux* during period t (see the definition below) at the interface between cells $j-1$ and j. The dynamics of the density follows a perturbed continuity equation [14]

$$\rho_{j,t+1} = \rho_{j,t} + \left(\frac{\lambda_j}{\lambda_{j+1}} f_{j,t} - f_{j+1,t}\right)\frac{\tau}{\Delta x_j} + \nu_{j,t}, \quad (2)$$

where ν_j is white Gaussian noise whose variance captures for example errors due to the fundamental diagram hypothesis. In the Cell Transmission Model (CTM) [17], the numerical flux compatible with the fundamental diagram (1) is

$$f_{j,t} := \min\{v_0\rho_{j-1,t}, v_0\rho_C, w(\rho_M - \rho_{j,t})\},$$

and (2) is then a stochastic, piecewise linear state-space description of the traffic dynamics, see [14] for more details.

2.2. Sensor Measurements

Standard static sensors are induction loops [14] placed at some fixed locations along the road, assumed to be on some boundary between two cells. A sensor on the boundary between cells $p-1$ and p reports with a certain frequency the counts $c^l_{p,t}$ of vehicles in lane l that crossed the boundary during the last sampling period, and the occupancy $o^l_{p,t} \in [0,1]$, which is the percentage of time during which a car was on top of the sensor in lane l during the last sampling period. In addition, some vehicles are equipped with devices able to transmit their velocity and position when requested. For privacy reasons, we use a location-based sampling scheme introduced in [18] and called Virtual Trip Lines (VTL), where vehicles report their speed only when they cross specific locations along the road, again assumed to be at the interface between two cells. In [13], an estimation scheme was introduced that relied mostly on the count measurements for density estimation, and did not consider the speed measurements. Instead, in this paper we only use the occupancy and speed measurements.

We consider the following measurement models at an interface $(p-1) \to p$ with static detectors and/or a VTL

$$\frac{1}{g_p\lambda_p}\sum_{l=1}^{\lambda_p} o^l_{p,t} = \rho_{p,t} + \mu^o_{p,t}, \quad (3)$$

$$\ln V_{p,t} = \ln\left(\frac{\rho_M}{\rho} - 1\right) + \ln w + \mu^v_{p,t} \text{ if } V_{p,t} < v_0, \quad (4)$$

where g_p is the so-called g-factor [19] (average effective vehicle length at the sensor location), μ^o_p, μ^v_p are white Gaussian noises and in (4) the model was obtained from inverting the second relation in (1). The traffic speed measurements $V_{p,t}$ are defined as geometric means over the last n cars reporting speed that crossed the VTL before time t, i.e., $V_{p,t} = \left(\prod_{i=1}^n v^{(i)}_{p,t}\right)^{\frac{1}{n}}$. The choice of a logarithmic model in (4) and of a geometric mean in for $V_{p,t}$ turns out to be convenient for our privacy preserving scheme.

We would like to produce an estimate of the density ρ in each cell in real-time, from the dynamics model (2) and the measurements (3), (4). However, these measurements capture privacy sensitive information about the drivers' trajectories, and so an additional goal here is to enforce formal privacy guarantees for the drivers in the published estimate.

2.3. Differentially Private Estimation

Our goal is to produce a differentially private (DP) traffic estimate in real-time. We start with a symmetric binary relation, defined in Section 3, on our space of measurement sequences $\{\mathbf{y}_t\}_{t\geq 0}$, with $\mathbf{y}_t = \{o^l_{p,t}, v^{(i)}_{p,t}\}_{p,l,i}$, called *adjacency relation*, and which intuitively relates sequences that differ by the data of a single individual. Sanitization through a differentially private mechanism should make it difficult for an adversary to decide which of any two adjacent sequences $\{\mathbf{y}_t\}_{t\geq 0}$ or $\{\tilde{\mathbf{y}}_t\}_{t\geq 0}$ was used in producing a given output.

Definition 1 ((ϵ, δ)-differential privacy [7]) *Let $\mathcal{Y}$ be a space equipped with a symmetric binary relation denoted Adj, and let $(\mathsf{R}, \mathcal{M})$ be a measureable space. Let $\epsilon, \delta > 0$. A randomized map M from $\mathcal{Y}$ to R is (ϵ, δ)-differentially private for Adj if for all $\mathbf{y}, \tilde{\mathbf{y}} \in \mathcal{Y}$ such that Adj$(\mathbf{y}, \tilde{\mathbf{y}})$, we have*

$$P(M(\mathbf{y}) \in S) \leq e^\epsilon P(M(\tilde{\mathbf{y}}) \in S) + \delta, \forall S \in \mathcal{M}.$$

To put Definition 1 in the context of our application, M is our privacy-preserving estimator, which must necessarily randomize its output to satisfy the differential privacy definition (in practice, by adding a privacy preserving noise signal), in such a way that the distribution over output signals is not very sensitive to differences between adjacent input signals. In addition, a crucial property of differential privacy says that it is *resilient to post-processing*, i.e., manipulating a differentially private output cannot weaken the privacy guarantee, as long as the input signal is not re-accessed, see [20, Theorem 1].

3. TRAFFIC DATA SANITIZATION

Two datasets $\mathbf{y}$ and $\tilde{\mathbf{y}}$ are adjacent if they have been generated by the same traffic except for the trajectory of a single car. Note that a car only moves forward on the road and travels in a specific lane at each cell boundary, hence it can influence $o^l_{p,t}$ for a given location p at only a single value of t and l, and it can cross a VTL only once. The occupancy $o^l_{p,t}$ measured by a static sensor is the sum of the individual occupancies for the cars passing on top of this sensor during period t. We protect only cars that have a bounded influence on occupancy measurements, which we capture through the adjacency relation. Between adjacent datasets, all occupancy measurements must be identical, except for the fact that by changing one trajectory the corresponding car can cross a sensor line at a different time and in a different lane. When there is a difference between some $o^l_{p,t}$ and $\tilde{o}^l_{p,t}$ due to the influence one such car, we assume this difference to be bounded, i.e., $|o^l_{t,p} - \tilde{o}^l_{p,t}| \leq \alpha$, for some α set as discussed below. Considering now the sequence with components $O_{p,t} := \frac{1}{\lambda_p} \sum_{l=1}^{\lambda_p} o^l_{p,t}$ appearing in (3), a straightforward analysis shows that

$$\|O - \tilde{O}\|_2^2 \leq 2\alpha^2 \sum_{p=1}^{P_s} \frac{1}{\lambda_p^2} =: \Delta_o,$$

for adjacent sequences, where P_s is the number of interfaces at which we have static detectors.

Similarly, we only protect against bounded relative variations for cars reporting their speed data when they cross VTLs. Specifically, when a car trajectory changes, it could remain in the same batch of size n used to compute $V_{p,t}$ in (4) or it could be exchanged with another car, but in any case we assume that the single modified value $v^{(i)}_{p,t}$ in some $V_{p,t}$ satisfies $\frac{|v^{(i)}_{p,t} - \tilde{v}^{(i)}_{p,t}|}{\min\{v^{(i)}_{p,t}, \tilde{v}^{(\tilde{i})}_{p,t}\}} \leq \gamma$, for some γ. We then have for the vector L with components $L_{p,t} := \ln V_{p,t}$ that

$$\|L - \tilde{L}\|_2^2 = \sum_{p=1}^{P_v} \sum_{t=1}^{\infty} \left| \frac{1}{n} \sum_{i=1}^{n} \left(\ln v^{(i)}_{p,t} - \ln \tilde{v}^{(i)}_{p,t} \right) \right|^2$$

$$\|L - \tilde{L}\|_2^2 \leq \sum_{p=1}^{P_v} \frac{1}{n^2} |\ln v^{(i_p)}_{p,t_p} - \ln \tilde{v}^{(\tilde{i}_p)}_{p,\tilde{t}_p}|^2$$

$$\|L - \tilde{L}\|_2^2 \leq \frac{\gamma^2}{n^2} P_v =: \Delta_v,$$

where P_v is the number of VTLs.

The following theorem is then an immediate consequence of standard results for the design of differentially privacy mechanisms [10, 20]. Define $K = \mathcal{Q}^{-1}(\delta)$ for $\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{u^2}{2}} du$ and let $\kappa_{\delta,\epsilon} = \left(K + \sqrt{K^2 + 2\epsilon}\right)/(2\epsilon)$.

Theorem 1 *A mechanism publishing the sequence $\bar{O}_{p,t} = O_{p,t} + w^o_{p,t}$, where $w^o_{p,t}$ are iid Gaussian random variables with variance $\kappa^2_{\delta,\epsilon}\Delta_o$, is (ϵ, δ)-differentially private. A mechanism publishing the sequence $\bar{L}_{p,t} = L_{p,t} + w^v_{p,t}$, where $w^v_{p,t}$ are iid Gaussian random variables with variance $\kappa^2_{\delta,\epsilon}\Delta_v$, is (ϵ, δ)-differentially private.*

The values for the constants α and γ should be set based on the acceptable trade-off between privacy and estimation performance. Higher values of α and γ provide better privacy but require more noise to sanitize the data. In order to set α in particular, we reason on a theoretical microscopic traffic model of evenly spaced identical cars, and look at the impact of one car on occupancies, see Fig. 1. A change of trajectory for one car leads to an increasingly large variation of $o^l_{p,t}$ as $o^l_{p,t}/g$ (a measure of density) increases. For example, the model tells us that by setting $\alpha = 0.015$, cars are protected as long as they appear only in density measurements $o^l_{p,t}/g$ that are below 0.081. In the Mobile Century dataset used in Section 5, this represents 98% of occupancy measurements.

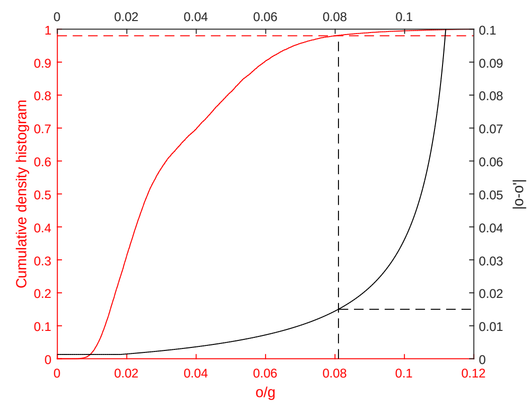

Fig. 1. Determination of the bound α. Left axis: Proportion of values of o/g below a given threshold in the Mobile Century dataset [21].

4. ENSEMBLE KALMAN FILTER

Sanitizing the measurements as described in the previous section leads to new values $\bar{O}_{p,t}$, $\bar{L}_{p,t}$. These follow the same measurement model as in (3), (4), except for the additional Gaussian noises $w^o_{p,t}$, $w^v_{p,t}$ which are simply added to the Gaussian noises $\mu^o_{p,t}$ and $\mu^v_{p,t}$, in effect increasing their variance by the terms of Theorem 1. These perturbed measurements are then combined with the dynamic model (2) via an EnKF [15] to provide the final traffic estimate. This amounts to a post-processing step, so the differential privacy guarantee obtained after sanitizing the measurements is maintained.

The EnKF is similar to the Kalman filter, but uses a set of particles, i.e., sampled state values, to compute the error covariance used to form the Kalman gain. The EnKF algorithm is described in Algorithm 1 for a generic state space system with dynamics $x_{t+1} = f(x_t, \omega_t)$ (with ω_t some noise) and linear measurements $y_t = Hx_t + v_t$, where v_t has a known covariance R_t. In our case, the velocity measurement model (4) is nonlinear, i.e., $y_t = h(x_t) + v_t$, hence we use an extension of the EnKF discussed in more details in [15] for example, which works with augmented state vector $\hat{x} = \begin{bmatrix} x^T & h(x)^T \end{bmatrix}^T$ and the linear measurements $\hat{H} \begin{bmatrix} x \\ y \end{bmatrix} = y$.

Algorithm 1 EnKF algorithm

for $k = 1 \cdots n$ **do**
    $x_0^k \sim \pi_0$ ▷ Draw n samples from Gaussian prior π_0
end for
for $t \geq 0$ **do**
    for $k = 1 \cdots n$ **do**
        $x_t^k \leftarrow f(x_{t-1}^k, \omega_{t-1}^k)$ ▷ Prediction from the model
    end for
    $\bar{x}_t \leftarrow \frac{1}{n} \sum_{k=1}^{n} x_t^k$ ▷ Ensemble mean
    $E = \left[x_t^1 - \bar{x}_t, \cdots, x_t^n - \bar{x}_t \right]$ ▷ Deviation from mean
    $P \leftarrow \frac{1}{K-1} E(E)^T$ ▷ Covariance matrix
    $K_t \leftarrow P(H_t)^T \left[HP_t(H)^T + R_t \right]^{-1}$ ▷ Kalman gain
    for $k = 1 \cdots n$ **do**
        $\xi^k \sim N(0, R_t)$
        $x_t^k \leftarrow x_t^k + K_t \left[y_t - Hx_t^k + \xi^k \right]$ ▷ Update
    end for
    Publish $\bar{x}_t$ ▷ Estimate
end for

Adjustment of the VTL locations. As shown in Section 3, sanitizing speed data requires adding a noise with variance proportional to the number of VTLs. It is therefore important to work with a limited number of VTLs and set their locations to optimize the usefulness of the measurements. We use a scheme where the location of the VTLs is changed online based on the size of the innovations $\|y_t - H\bar{x}_t\|$ in the measurement update step of the EnKF, while making sure that a car does not report twice its speed for the same VTL. We adjust $r_1, \ldots, r_{P_v}$, the positions of the VTL, using an approach based on the minimization of a potential function at each step. Given the current positions $\hat{r}_1, \ldots, \hat{r}_{P_v}$, we obtain the new positions by minimizing (locally) a function of the type

$$\sum_{s=1}^{P_v} \left[\left(\sum_{q=1}^{P_v} f_A(\hat{r}_q, r_s; h_q) \right) + \left(\sum_{\sigma \neq s} f_R(r_s, r_\sigma) \right) + f_B(r_s) \right].$$

Here $f_A(\hat{r}_q, r_s; h_q)$ is a field attracting r_s towards $\hat{r}_q$ with a strength that is increasing with h_q, the norm of the innovation for the measurement at location $\hat{r}_q$. The second term is a repulsive term maintaining sufficient spacing between the sensors, and f_B is a term that prevents the sensor locations to escape outside of the road segment of interest.

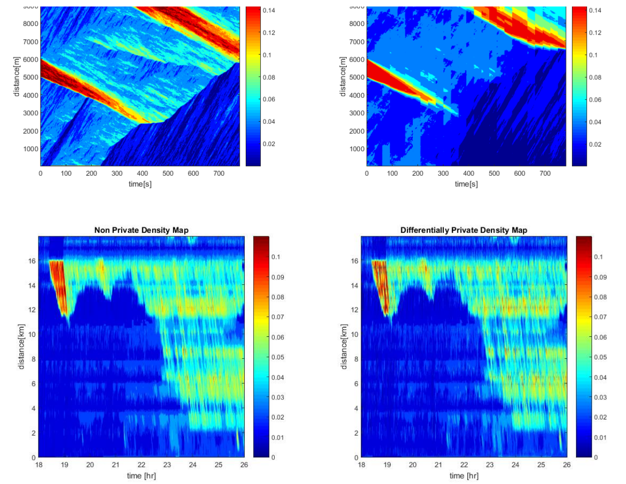

Fig. 2. Synthetic data (top): simulated traffic density map $\rho(x,t)$ (left) vs. (ϵ,δ)-DP estimate. Data from the Mobile Century experiment (bottom): Non-private (left) vs. (ϵ,δ)-DP (right) density map. The density is in vehicles/m.

5. SIMULATION RESULTS

Our differentially private filter is first validated on synthetic (simulated) data for a road with a single lane, which allows us to compare the estimator performance to the simulated ground truth, see Fig. 2. The simulation parameters are: $P_s = 10$ static sensors, $\tau = 0.5$s, $\Delta x_p = 25$ m. We also use the values $v_0 = 90$ km/h, $w = 30$km/h, $\rho_M = 1/7$ vehicles/m, $g = 6$ m for the fundamental diagram. Occupation measurements are obtained periodically every 30 s. The differential privacy parameters are: $\epsilon = \ln(2 + P_s)$, $\delta = 0.05$, and $\alpha = 0.015$, $\gamma = 0.4$ for the adjacency relation. It is found that an adequate number of particles is around 60, with more particles leading to negligible performance improvements. Fig. 2 also shows the results of applying the DP EnKF to the Mobile Century dataset [21], with the same values as above for the various parameters. This dataset contains both static occupancy measurements and GPS traces from floating cars for a day of traffic on Interstate 880 in California, which has either 4 or 5 lanes depending on the location.

6. CONCLUSIONS

We presented a methodology for the publication of differentially private traffic estimates relying on static detector measurements and floating car data. Our scheme sanitizes the measurements directly before integrating them in the estimation scheme, and future work includes the development of more advanced schemes where noise is added after a first processing step for the measurements, as in [20].

7. REFERENCES

[1] B. Hoh, T. Iwuchukwu, Q. Jacobson, M. Gruteser, A. Bayen, J-.C. Herrera, R. Herring, D. Work, M. Annavaram, and J. Ban, "Enhancing privacy and accuracy in probe vehicle based traffic monitoring via virtual trip lines," *IEEE Transactions on Mobile Computing*, vol. 11, no. 5, May 2012.

[2] W. Xin, J. Chang, S. Muthuswamy, and M. Talas, ""Midtown in Motion": A new active traffic management methodology and its implementation in New York City," in *Transportation Research Board Annual Meeting*, 2013.

[3] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific Reports*, vol. 3, 2013.

[4] E. S. Canepa and C. G. Claudel, "A framework for privacy and security analysis of probe-based traffic information systems," in *Proceedings of the 2nd ACM international conference on High confidence networked systems (HiCoNS)*, 2013, pp. 25–32.

[5] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *Journal of Law, Medicine and Ethics*, vol. 25, pp. 98–110, 1997.

[6] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets (how to break anonymity of the Netflix Prize dataset)," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2008.

[7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proceedings of the Third Theory of Cryptography Conference*, 2006, pp. 265–284.

[8] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[9] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: privacy beyond k-anonymity and l-diversity," in *Proceedings of the 23rd IEEE International Conference on Data Engineering*, 2007.

[10] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[11] L. Fan, L. Xiong, and V. Sunderam, "Differentially private multi-dimensional time series release for traffic monitoring," in *27th Conference on Data and Applications Security and Privacy*. 2013, vol. 7964 of *Lecture Notes in Computer Science*, pp. pp 33–48, Springer.

[12] M. E. Andrés, N. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: differential privacy for location-based systems," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'13)*, 2013.

[13] J. Le Ny, A. Touati, and G. J. Pappas, "Real-time privacy-preserving model-based estimation of traffic flows," in *Proceedings of the Fifth International Conference on Cyber-Physical Systems (ICCPS)*, April 2014.

[14] M. Treiber and A. Kesting, "Traffic flow dynamics," *Traffic Flow Dynamics: Data, Models and Simulation, Springer-Verlag Berlin Heidelberg*, 2013.

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

[16] 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 *Proceedings of the 47th IEEE Conference on Decision and Control*, December 2008, pp. 5062–5068.

[17] C. F. Daganzo, "The cell transmission model: A dynamic representation of highway traffic consistent with the hydrodynamic theory," *Transportation Research Part B: Methodological*, vol. 28, no. 4, pp. 269–287, 1994.

[18] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*. ACM, 2008, pp. 15–28.

[19] Z. Jia, C. Chen, B. Coifman, and P. Varaiya, "The PeMS algorithms for accurate, real-time estimates of g-factors and speeds from single-loop detectors," in *Proceedings of the 4th IEEE Conference on Intelligent Transportation Systems*, 2001.

[20] J. Le Ny and G. J. Pappas, "Differentially private filtering," *Automatic Control, IEEE Transactions on*, vol. 59, no. 2, pp. 341–354, 2014.

[21] J. C. Herrera, D. B. Work, R. Herring, X. Ban, Q. Jacobson, and A. M. Bayen, "Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment," *Transportation Research Part C: Emerging Technologies*, vol. 18, no. 4, pp. 568 – 583, 2010.