23rd International Symposium on Mathematical Theory of Networks and Systems
Hong Kong University of Science and Technology, Hong Kong, July 16-20, 2018

Privacy-aware Minimum Error Probability Estimation: An Entropy Constrained Approach

Ehsan Nekouei, Mikael Skoglund and Karl H. Johansson

***Abstract*— This paper studies the design of an optimal privacy-aware estimator for a single sensor estimation problem. The sensor's measurement is a (possibly non-linear) function of a private random variable, a public random variable and the measurement noise. Both public and private random variables are assumed to be discrete valued, and the measurement noise is arbitrarily distributed. The sensor provides an estimate of the public random variable for an untrusted entity, named the cloud. The objective is to design the estimator of the public random variable such that a level of privacy for the private random variable is guaranteed. The privacy metric is defined as the discrete conditional entropy of the private random variable given the output of the estimator. A binary loss function is considered for the estimation of the public random variable. The optimal estimator design problem is posed as the minimization of the average loss function subject to a constraint on the privacy level of the private random variable. It is shown that the objective function is linear and the privacy constraint is convex in the optimization variables. Thus, the optimal privacy-aware estimator can be designed by solving an infinite dimensional convex optimization problem.**

I. Introduction

A. Motivation

Networked control systems (NCSs) play major roles in our societies by providing critical services such as intelligent transportation and the smart grid. Implementation of a NCS requires substantial computational and storage capabilities due to the complex optimization, signal processing and control algorithms, commonly used in NCSs. Cloud computing technology has been proposed as a promising solution for the storage and computational requirements of NCSs. However, the cloud-based operation of a NCS requires sharing information, *e.g.,* sensors' measurements, with the cloud which might result in the loss of privacy due to the information sharing.

In NCSs, the sensors' measurements not only contain information about the desired variable but also contain information which might be considered as private information, *e.g.,* information regarding stochastic evens or unpredictable disturbances occurring in the sensor's environment. Hence, the estimate of the desired variable will be dependent on the private information which might result in the privacy loss. Thus, to ensure the privacy of a NCS, it is important to confine the leakage of private information due to the estimation process.

B. Contributions

In this paper, we consider an estimation problem in which the sensor's measurement is expressed as a general function of a private random, a public random variable and measurement noise. It is assumed that the private and public random variables take finite values and the measurement noise is arbitrarily distributed. The sensor estimates the public random variable using its measurement. The estimate of the public variable is stored in an untrusted entity, named cloud, which is assumed to be accessible via a network and have storage/computational capabilities.

To quantify the privacy loss of the private random variable, due to the estimation, conditional discrete entropy of the private random variable given the output of estimator is considered as the privacy metric. The privacy metric captures the uncertainty of the cloud regarding the private random variable after observing the estimate of the public random variable. The problem of the minimizing the expected value of (a binary) loss function subject to a privacy level of the private random variable is studied. It is shown that the objective function is linear function of the optimization variables and the privacy constraint is convex.

C. Related Work

The privacy level of hypothesis testing problems with a private and a public hypothesis has been studied in the literature, and various privacy-preserving solutions for improving the privacy level of hypothesis test problems have been proposed, *e.g.,* see [1], [2], [3], [4]. In [5], the authors considered a hypothesis test problem with multiple sensors in which an eavesdropper intercepts the local decisions of a subset of sensors. They studied the optimal decision rule minimizing the Bayes risk at a fusion center subject to a privacy constraint at the eavesdropper. In [6], the authors considered a similar set-up to that of [5] and studied the optimal privacy-aware Neyman-Pearson test with a private hypothesis. We note that improving the privacy of electricity consumers against an eavesdropper using demand management techniques and storage devices was studied in [7].

The authors in [8] studied the state estimation problem in a distribution power network subject to differential privacy constraints for the consumers. In [9], the authors considered the problem of adding stochastic distortion to a variable, which contains private information, such that (i) the mean square error (MSE) of recovering the original variable from its distorted version is minimized, (ii) the minimum MSE of recovering the private information from the distorted variable stays above a certain level. Their results were extend in [10] under the Hamming distance as the distortion criterion and the efficiency of these methods was analysed in [11].

Information-theoretic methods for improving data privacy have also been studied in the literature, *e.g.,* see [12], [13],

[14], [15] and references therein. In this line of research, the objective is to process the observations, which contain private information, such that the distortion between the original observations and the processed observations is minimized while a certain level of privacy is guaranteed. However, in an estimation problem, one is interested in the true value of a variable based on a noisy observation rather than a low distortion representation of the observation.

II. Problem Formulation

Consider an estimation problem with one sensor in which the observation of the sensor can be expressed as $Z = f(X, Y, N)$ where Z is the sensor's measurement, X and Y are, possibly correlated, discrete random variables, N is the measurement noise and independent of X and Y, and $f(\cdot,\cdot,\cdot)$ is a (possibly non-linear) map. The support sets of X, Y and Z are denoted by $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, receptively. Through this paper, we assume that $\mathcal{Z} = \mathbb{R}$ and the random variable Z is absolutely continuous with respect to Lebesgue measure on $\mathbb{R}$ with the probability density function $p_Z(z)$.

The random variable Y contains public information, and the sensor provides the estimate of Y to the cloud. The random variable X carries information which should remain private. Let $\hat{Y}(Z)$ denote the estimate of Y by the sensor. Since $\hat{Y}(Z)$ is correlated with X, the cloud can infer information about X by observing $\hat{Y}(Z)$. Thus, publicly revealing $\hat{Y}(Z)$ will result in privacy loss, *i.e.,* the cloud can infer about X by observing $\hat{Y}(Z)$. A pictorial representation of our system model is illustrated in Fig. 1.

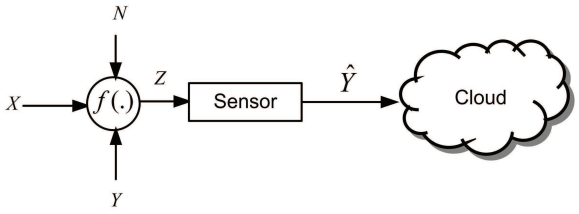

Fig. 1. A single sensor estimation set up with a cloud-based storage.

The objective is to design an estimator for the public random variable Y which minimizes a desired loss function while the information leakage about the private variable X is kept below a certain level. Let $\mathcal{Y} = \{y_1, \cdots, y_m\}$ denote the support set of Y. An estimator of Y is a (possibly randomized) map from $\mathcal{Z}$ to $\mathcal{Y}$. Let $P(z) = [P_i(z)]_{i=1}^m$ denote a set of positive functions where $m = |\mathcal{Y}|$ and $P_i(z)$ is defined on the support set of $\mathcal{Z}$ with $\sum_{i=1}^m P_i(z) = 1$ for all $z \in \mathcal{Z}$. Then, a randomized estimator of Y can be expressed as

$$\hat{Y}_P(z) = \begin{cases} y_1 & \text{w.p.} \quad P_1(z) \\ \vdots & \vdots \\ y_m & \text{w.p.} \quad P_m(z) \end{cases} \tag{3}$$

where w.p. stands for with probability. According to (3), if the sensor's measurement is equal to z, the estimator declares y_i as the estimate of Y with probability $P_i(z)$.

Let $\hat{Y}_P(Z)$ represent the estimator of Y at the sensor using the observation Z. The loss of the estimator, *i.e.,* $L\left(Y, \hat{Y}_P(Z)\right)$, is quantified by the binary loss function

$$L\left(Y, \hat{Y}_P(Z)\right) = \begin{cases} 1 & Y \neq \hat{Y}_P(Z) \\ 0 & Y = \hat{Y}_P(Z) \end{cases}$$

Thus, the estimator's loss is equal to 1 if the output of estimator is different from the true value of Y and there is no loss if these two values agree.

A. Privacy Metric

In this paper, we consider the conditional discrete entropy, or equivocation, as the privacy metric. The conditional discrete entropy of X given $\hat{Y}_P(Z)$, denoted by $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right]$, is defined in (1). Our choice of privacy metric is motivated by the fact that $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right]$ captures the uncertainty in the cloud about X after observing $\hat{Y}_P(Z)$. Since conditioning reduces entropy [16], we have

$$0 \leq \mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right] \leq \mathsf{H}[X]$$

which implies that the maximum privacy is achieved if $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right] = \mathsf{H}[X]$. Recall that if X and $\hat{Y}_P(Z)$ are independent, $\hat{Y}_P(Z)$ contains no information about X and the cloud has maximum ambiguity about X after observing $\hat{Y}_P(Z)$, *i.e.,* $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right] = \mathsf{H}[X]$.

The other motivation for the choice of privacy metric is the fact that the error probability of estimating X after observing $\hat{Y}_P(Z)$ can be lower bounded in terms of $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right]$ using Fano inequality [16]:

$$\mathsf{Pr}\left(X \neq \hat{X}\left(\hat{Y}\right)\right) \geq \frac{\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right] - 1}{\log|\mathcal{X}|} \tag{4}$$

where $\hat{X}\left(\hat{Y}\right)$ is an arbitrary estimator of X (after observing $\hat{Y}_P(Z)$) and $|\mathcal{X}|$ is the cardinality of the support set of X. Thus, by adjusting the value of $\mathsf{H}\left[X \middle| \hat{Y}_P(Z)\right]$, a desired privacy level of the private random variable, X, in the cloud can be guaranteed as long as $|\mathcal{X}| > 2$. We note that the application of Fano's equality in the context of privacy-aware cloud-based control was discussed in [17].

III. Privacy-aware Optimal Estimation

In this section, the design of the optimal privacy-aware estimator of X is studied. In particular, the estimator design is posed as an optimization problem and it is shown that the optimal estimator can be designed by solving a convex optimization problem. The optimal design of the estimator subject to the privacy constraint is given by the solution of

$$\mathsf{H}\left[X\left|\hat{Y}_P\left(Z\right)\right.\right]=-\sum_{y\in\mathcal{Y}}\mathsf{Pr}\left(\hat{Y}_P\left(Z\right)=y\right)\sum_{x\in\mathcal{X}}\mathsf{Pr}\left(X=x|\,\hat{Y}_P\left(Z\right)=y\right)\log\mathsf{Pr}\left(X=x|\,\hat{Y}_P\left(Z\right)=y\right) \tag{1}$$

$$\mathsf{H}\left[X\left|\hat{Y}_P\left(Z\right)\right.\right]=\mathsf{H}\left[X\right]-\sum_j\mathsf{Pr}\left(X=x_j\right)\mathsf{D}\left[p_{\hat{Y}_P}\left(y\,|X=x_j\,\right)\middle\|p_{\hat{Y}_P}\left(y\right)\right] \tag{2}$$

the following optimization problem:

$$\begin{aligned}\underset{\{P_i(z)\}_{i=1}^m}{\text{minimize}}\quad & \mathsf{E}\left[L\left(Y,\hat{Y}_P\left(Z\right)\right)\right]\\ & P_i\left(z\right)\geq 0,\forall i\\ & \sum_i P_i\left(z\right)=1,\quad\forall z\\ & \mathsf{H}\left[X\left|\hat{Y}_P\left(Z\right)\right.\right]\geq\mathsf{H}_0\end{aligned} \tag{5}$$

Based on this optimization problem, the functions $\{P_i\left(z\right)\}_i$ are chosen such that the average loss is minimized and, a certain level of privacy is ensured by keeping the conditional discrete entropy of X given $\hat{Y}_P\left(Z\right)$ above the desired level H_0.

The optimization problem above is a functional optimization problem defined on the space of bounded measurable functions from $\mathbb{R}$ to $\mathbb{R}$, *i.e.,* $\mathsf{B}\left(\mathbb{R},\mathbb{R}\right)$. Note that $\mathsf{B}\left(\mathbb{R},\mathbb{R}\right)$ forms a Banach space under the supremum norm and $P_i\left(z\right)$ belongs to the cone of positive functions in $\mathsf{B}\left(\mathbb{R},\mathbb{R}\right)$. Next lemma derives an expression for the objective function in the optimization problem (5).

Lemma 1: The objective function in (5) can be written as

$$1-\sum_i\int P_i\left(z\right)\mathsf{Pr}\left(Y=y_i|\,Z=z\right)p_Z\left(z\right)dz$$

where $p_Z\left(z\right)$ is the probability density function of Z.

Proof: Please see the full manuscript in [18]. ■

According to Lemma 1 the objective function is linear in $P\left(z\right)=\left[P_i\left(z\right)\right]_i$. Next lemma studies the convexity of the privacy constraint.

Lemma 2: The the privacy constraint can be written as (2) where $\mathsf{H}\left[X\right]$ is the discrete entropy of X, $p_{\hat{Y}_P}\left(y\right)$ and $p_{\hat{Y}_P}\left(y\,|X=x_j\,\right)$ denote the probability mass function of $\hat{Y}_P\left(Z\right)$ and the conditional probability mass function of $\hat{Y}_P\left(Z\right)$ given $X=x_j$, respectively, and $\mathsf{D}\left[\cdot\,\|\cdot\right]$ denotes the Kullback-Libeler (KL) divergence. Furthermore, the privacy constraint is convex in $P\left(z\right)$.

Proof: Please see the full manuscript in [18]. ■

The objective function in the optimization problem (5) is linear and the constraint set is convex. Thus, (5) is a convex optimization problem. This result is formally stated in the next theorem.

Theorem 1: The optimal privacy-aware estimator of the public random variable can be designed by solving the convex optimization problem (5).

IV. Conclusions

In this paper, we studied privacy-aware estimation of a public random variable when the sensor's measurement contains noisy information about a public random variable as well as a private random variable. The optimal estimation of the public random variable, under a binary loss function, with a constraint on the privacy level of the private random variable was studied. The conditional discrete entropy of the private random variable subject to the output of estimator was considered as the privacy metric and it was shown that the optimal estimator can be obtained by solving an infinite dimensional convex optimization problem.

References

[1] X. He, W. P. Tay, and M. Sun, "Privacy-aware decentralized detection using linear precoding," in *2016 IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, July 2016, pp. 1–5.

[2] M. Sun and W. P. Tay, "Privacy-preserving nonparametric decentralized detection," in *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2016, pp. 6270–6274.

[3] X. He and W. P. Tay, "Multilayer sensor network for information privacy," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 6005–6009.

[4] J. Liao, L. Sankar, V. Y. F. Tan, and F. P. Calmon, "Hypothesis testing in the high privacy limit," in *2016 54th Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2016, pp. 649–656.

[5] Z. Li and T. J. Oechtering, "Privacy-aware distributed bayesian detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1345–1357, Oct. 2015.

[6] ——, "Privacy-constrained parallel distributed neyman-pearson test," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 3, no. 1, pp. 77–90, Mar. 2017.

[7] Z. Li, "Privacy-by-design for cyber-physical systems," Ph.D. dissertation, 2017. [Online]. Available: http://kth.diva-portal.org/smash/get/diva2:1131655/FULLTEXT01.pdf

[8] H. Sandberg, G. Dán, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec. 2015, pp. 4492–4498.

[9] S. Asoodeh, F. Alajaji, and T. Linder, "Privacy-aware MMSE estimation," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 1989–1993.

[10] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Privacy-aware guessing efficiency," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 754–758.

[11] ——, "Estimation efficiency under privacy constraints," Tech. Rep., 2017. [Online]. Available: https://arxiv.org/abs/1707.02409

[12] K. Kalantari, L. Sankar, and O. Kosut, "On information-theoretic privacy with general distortion cost functions," in *2017 IEEE International Symposium on Information Theory (ISIT)*, June 2017, pp. 2865–2869.

[13] Y. O. Basciftci, Y. Wang, and P. Ishwar, "On privacy-utility tradeoffs for constrained data release mechanisms," in *2016 Information Theory and Applications Workshop (ITA)*, Jan. 2016, pp. 1–6.

[14] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing*, Oct. 2012, pp. 1401–1408.

[15] B. Moraffah and L. Sankar, "Information-theoretic private interactive mechanism," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing*, Sept. 2015, pp. 911–918.

[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.

[17] T. Tanaka, M. Skoglund, H. Sandberg, and K. Johansson, "Directed information as privacy measure in cloud-based control," KTH Royal Institute of Technology, Sweden, Tech. Rep., 2017. [Online]. Available: https://arxiv.org/abs/1705.02802

[18] E. Nekouei, M. Skoglund, and K. H. Johansson, "Privacy-aware minimum error probability estimation: An entropy constrained approach," KTH Royal Institute of Technology, Tech. Rep., 2018. [Online]. Available: https://www.dropbox.com/s/u7b12ge70uyrxvq/MTNS.pdf?dl=0