University Library



A gateway to Melbourne's research publications

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Murguia, C;Shames, I;Farokhi, F;Nesic, D

Title:
On Privacy of Quantized Sensor Measurements through Additive Noise

Date:
2018-01-01

Citation:
Murguia, C., Shames, I., Farokhi, F. & Nesic, D. (2018). On Privacy of Quantized Sensor Measurements through Additive Noise. Proceedings of the 57th IEEE Conference on Decision and Control (CDC), 2018-December, pp.2531-2536. IEEE. https://doi.org/10.1109/CDC.2018.8619535.

Persistent Link:
https://hdl.handle.net/11343/297946

On Privacy of Quantized Sensor Measurements through Additive Noise

Carlos Murguia, Iman Shames, Farhad Farokhi, and Dragan Nešić

arXiv:1809.03133v1 [cs.SY] 10 Sep 2018

***Abstract*— We study the problem of maximizing privacy of quantized sensor measurements by adding random variables. In particular, we consider the setting where information about the state of a process is obtained using noisy sensor measurements. This information is quantized and sent to a remote station through an unsecured communication network. It is desired to keep the state of the process private; however, because the network is not secure, adversaries might have access to sensor information, which could be used to estimate the process state. To avoid an accurate state estimation, we add random numbers to the quantized sensor measurements and send the sum to the remote station instead. The distribution of these random variables is designed to minimize the mutual information between the sum and the quantized sensor measurements for a desired level of distortion – how different the sum and the quantized sensor measurements are allowed to be. Simulations are presented to illustrate our results.**

I. Introduction

During the past half-century, scientific and technological advances have greatly improved the performance of engineering systems. However, these new technologies have also led to vulnerabilities within critical infrastructure – e.g., power, water, transportation. Advances in communication and computing power have given rise to adversaries with enhanced and adaptive capabilities. Depending on adversary's resources and system defenses, opponents may infer critical information about the operation of systems or even deteriorate their functionality. Therefore, designing efficient defence mechanisms is of importance for guaranteeing privacy, safety, and proper operation of critical systems. All these new challenges have attracted the attention of researchers from different fields (e.g., computer science, information theory, control theory) in the broad area of privacy and security of Cyber-Physical Systems (CPS) [1]-[16].

In most engineering applications, information about the state of systems is obtained through sensor measurements. Once this information is collected, it is usually quantized, encoded, and sent to a remote station for signal processing and decision-making purposes through communication networks. Examples of such systems are numerous: water and electricity consumption meters, traffic monitoring systems, industrial control systems, and so on. If the communication network is public or unsecured, adversaries might access and estimate the state of the system. To avoid an accurate state estimation, we add random noise to the quantized sensor measurements before transmission and send the sum to the remote station instead. This noise is designed to increase privacy of the transmitted data. Note, however, that it is not desired to overly distort the original sensor data by injecting noise. We might change the data excessively for practical purposes. Hence, when designing the additive noise, we need to take into account the trade-off between *privacy* and *distortion*.

In this manuscript, we follow an information-theoretic approach. We propose to use *mutual information* between quantized-sensor-data and quantized-sensor-data plus privacy noise as *privacy metric*, and the *mean square error* between them as *distortion metric*. The design of the *discrete* additive noise is posed as a convex optimization problem. In particular, the distribution of the noise is designed to minimize the mutual information for a desired level of maximal distortion.

The use of additive noise to increase privacy is common practice. In the context of privacy of databases, a popular approach is differential privacy [12]-[17], where noise is added to the response of queries so that private information stored in the database cannot be inferred. In differential privacy, because it provides certain privacy guarantees, Laplace noise is usually used [18]. However, when maximal privacy with minimal distortion is desired, Laplace noise is generally not the optimal solution. This raises the fundamental question: for a given allowable distortion level, what is the noise distribution achieving maximal privacy? This question has many possible answers depending on the particular privacy and distortion metrics being considered and the system configuration [19]-[22]. There are also results addressing this question from an information theoretic perspective, where information metrics – e.g., mutual information, entropy, Kullback-Leibler divergence, and Fisher information – are used to quantify privacy [1]-[4],[23]-[25].

In general, if the data to be kept private follows continuous distributions, the problem of finding the optimal additive noise to maximize privacy (even without considering distortion) is hard to solve. If a close-form solution for the distribution is desired, the problem amounts to solving a set of nonlinear partial differential equations which, in general, might not have a solution, and even if they do have a solution, it is hard to find [1]. This problem has been addressed by imposing some particular structure on the considered distributions or assuming the data to be kept private is deterministic [1],[20],[21].

The authors in [20],[21] consider deterministic input data sets and treat optimal distributions as distributions that con-

This work was partially supported by the Australian Research Council (ARC) under the Discovery Project DP170104099.

Carlos Murguia, Iman Shames, Farhad Farokhi, and Dragan Nešić are with the Department of Electrical and Electronic Engineering, at the University of Melbourne, Australia.

Emails: carlos.murguia@unimelb.edu.au, iman.shames@unimelb.edu.au farhad.farokhi@unimelb.edu.au & dnesic@unimelb.edu.au.

centrate probability around zero as much as possible while ensuring differential privacy. Under this framework, they obtain a family of piecewise constant density functions that achieve minimal distortion for a given level of privacy. In [1], the authors consider the problem of preserving the privacy of deterministic databases using constrained additive noise. They use the Fisher information and the Cramer-Rao bound to construct a privacy metric between noise-free data and the one with the additive noise and find the probability density function that minimizes it. Moreover, they prove that, in the unconstrained case, the optimal noise distribution minimizing the Fisher information is Gaussian.

Most of the aforementioned papers propose optimal continuous distributions assuming deterministic data. However, in a networked context, unavoidable sensor noise leads to stochastic data and thus existing tools do not fit this setting. Here, we identify two possibilities for addressing our problem: 1) we might inject continuous noise to sensor measurements, then quantize the sum, and send it over the unsecured network; or 2), the one considered here, quantize sensor measurements, add noise with discrete distribution, and send the sum over the network. As motivated above, to address the first option, even assuming deterministic sensor data, we have to impose some particular structure on the distributions of the additive noise; and, if sensor data is stochastic, the problem becomes hard to solve (sometimes even untractable). As we prove in this manuscript, if we select the second alternative, under some mild assumptions on the alphabet of the injected noise, we can cast the problem of finding the optimal noise as a constrained convex optimization. To the best of the authors knowledge, this problem has not been considered before as it is posed it here.

II. Preliminaries

A. Entropy, Joint Entropy, and Conditional Entropy

Consider a discrete random variable X with alphabet $\mathcal{X}$ and probability mass function $p(x) = \Pr[X = x]$, $x \in \mathcal{X}$, where $\Pr[a]$ denotes probability of event a. We denote the probability mass function by $p(x)$ rather than $p_X(x)$ to simplify notation. Thus, $p(x)$ and $p(y)$ refer to two different random variables, and are in fact different probability mass functions, $p_X(x)$ and $p_Y(y)$, respectively.

Definition 1 *The entropy of a discrete random variable X with alphabet $\mathcal{X}$ and probability mass function $p(x)$ is defined as $H[X] := -\sum_{x\in\mathcal{X}} p(x)\log p(x)$.*

The $\log$ is base 2 and thus the entropy is expressed in bits. We use the convention that $0\log 0 = 0$ [26].

Definition 2 *The joint entropy of a pair of discrete random variables (X, Y) with alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively, and joint probability mass function $p(x, y)$ is defined as $H[X, Y] := -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x, y)\log p(x, y)$.*

Definition 3 *Let $(X, Y) \sim p(x, y)$, then the conditional entropy of Y given X, $H[Y|X]$, is defined as*

$$H[Y|X] := -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x, y)\log p(y|x).$$

Lemma 1 [26] *(Chain Rules for Entropy)*

- $H[X, Y] = H[X] + H[Y|X]$.
- $H[X, Y|Z] = H[X|Z] + H[Y|X, Z]$.
- $H[Y_1, \ldots, Y_n] = \sum_{i=1}^{n} H[Y_i|Y_{i-1}, \ldots, Y_1]$.
- *Let $Z = Z_1, \ldots, Z_m$, then:* $H[Y_1, \ldots, Y_n|Z] = \sum_{i=1}^{n} H[Y_i|Y_{i-1}, \ldots, Y_1, Z]$.

B. Mutual Information

Definition 4 *Consider two random variables, X and Y, with joint probability mass function $p(x, y)$ and marginal probability mass functions, $p(x)$ and $p(y)$, respectively. Their mutual information $I[X; Y]$ is defined as the relative entropy between the joint distribution and the product distribution $p(x)p(y)$, i.e.,*

$$I[X; Y] := -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x, y)\log\frac{p(x, y)}{p(x)p(y)}.$$

Lemma 2 [26] *(Mutual Information and Entropy)*

- $I[X; Y] = H[X] - H[X|Y] = H[Y] - H[Y|X]$.
- $I[X; Y|Z] = H[X|Z] - H[X|Y, Z]$.
- *Let $Z = Z_1, \ldots, Z_m$, then:* $I[Y_1, \ldots, Y_n; Z] = H[Y_1, \ldots, Y_n] - H[Y_1, \ldots, Y_n|Z]$.

The mutual information between two jointly distributed random variables, X and Y, is a measure of the dependence between X and Y. The following properties of mutual information can be found in [26] and references therein. Also, sketches of the proofs can be found in [27].

($\mathbf{P_1}$) $I[X; Y] = 0$ if and only if X and Y are independent.

($\mathbf{P_2}$) Let Y and Z be independent discrete random variables and $V = Y + Z$; then, $I[V; Y] = H[V] - H[Z]$, i.e., $H[Y + Z|Y] = H[Z]$.

($\mathbf{P_3}$) The mutual information does not increase for functions of the random variables (*data processing inequality*):

$$I[f(X); Y] \leq I[X; Y].$$

Lemma 3 [26] *(Chain Rule for Mutual Information)*

- *Let $Y = Y_1, \ldots, Y_n$, and $Z = Z_1, \ldots, Z_m$, then:* $I[Y; Z] = \sum_{i=1}^{n} I[Y_i; Y_{i-1}, \ldots, Y_1, Z]$.

Lemma 4 *Let $Y = Y_1, \ldots, Y_m$ and $Z = Z_1, \ldots, Z_m$ be $2m$ independent discrete random variables and $V = Y + Z$, i.e, $V_i = Y_i + Z_i$, $i = 1, \ldots, m$; then:*

$$I[V; Y] = \sum_{i=1}^{m} I[V_i; Y_i] = \sum_{i=1}^{m} H[V_i] - H[Z_i].$$

Proof: By Lemma 2, $I[V; Y] = H[V] - H[V|Y]$, and, by Lemma 1, $H[V] - H[V|Y] = \sum_{i=1}^{n} H[V_i|V_{i-1}, \ldots, V_1] - H[V_i|V_{i-1}, \ldots, V_1, Y]$. By assumption, the elements of

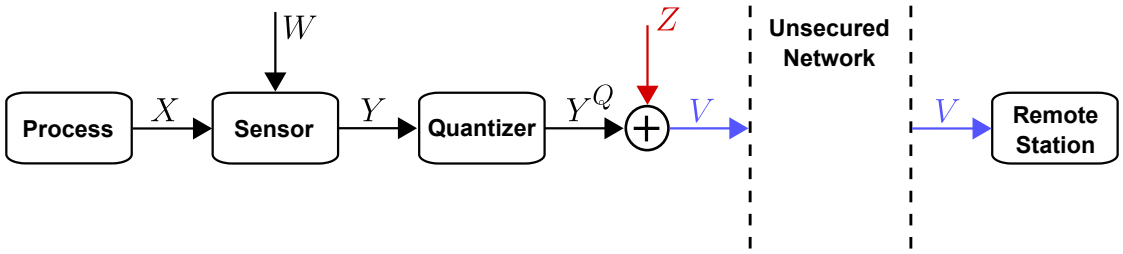


Fig. 1. System Configuration.

$\{Z, Y\}$ are all independent; then, the elements of V are also independent. It follows that

$$\begin{aligned} H[V] - H[V|Y] &= \sum_{i=1}^{n} H[V_i] - H[V_i|Y] \\ &= \sum_{i=1}^{n} H[V_i] - H[Y_i + Z_i|Y] \\ &= \sum_{i=1}^{n} H[V_i] - H[Z_i] \\ &= \sum_{i=1}^{n} I[V_i; Y_i], \end{aligned}$$

where the last equality follows from (P_2) given above. ■

III. Problem Setup

Let $X \in \mathbb{R}^n$ be the state of some deterministic process that must be kept private. Information about the state is obtained through m sensors of the form:

$$Y = CX + W, \tag{1}$$

with sensor measurements $Y \in \mathbb{R}^m$, matrix $C \in \mathbb{R}^{m\times n}$, and sensor noise $W \in \mathbb{R}^m$, $E[W] = \mathbf{0}$, $\Sigma_W := E[WW^T]$, $\Sigma_W > 0$. The entries of the noise are uncorrelated, i.e., $\Sigma_W = \text{diag}[\sigma_1^2, \ldots, \sigma_m^2]$. Then, $E[Y] = CX$, the covariance $\Sigma_Y := E[(Y - CX)(Y - CX)^T] = \Sigma_W$, and the entries of Y are uncorrelated. We assume that the probability distribution of Y is *known*. This is not an strong assumption since it is often possible to obtain a number of realization of Y to estimate its distribution. Let $Y = (Y_1, \ldots, Y_m)^T$. Each sensor measurement Y_i, $i = 1, \ldots, m$ is quantized using a uniform quantizer on a finite range $Q_i(Y_i, y_i^1, \Delta_i, N_i)$:

$$Q_i(Y_i, y_i^1, \Delta_i, N_i) := \begin{cases} y_i^1 \text{ if } Y_i \in (-\infty, y_i^1 + \frac{\Delta_i}{2}], \\ y_i^2 \text{ if } Y_i \in (y_i^1 + \frac{\Delta_i}{2}, y_i^2 + \frac{\Delta_i}{2}], \\ y_i^3 \text{ if } Y_i \in (y_i^2 + \frac{\Delta_i}{2}, y_i^3 + \frac{\Delta_i}{2}], \\ \vdots \\ y_i^{N_i} \text{ if } Y_i \in (y_i^{N_i - 1} + \frac{\Delta_i}{2}, \infty), \end{cases} \tag{2}$$

where $y_i^j = y_i^1 + (j-1)\Delta_i$, $j = 1, \ldots, N_i$. Thus, for each sensor, the N_i quantization levels are given by

$$\mathcal{Y}_i^Q := \{y_i^1, y_i^1 + \Delta_i, \ldots, y_i^1 + (N_i - 1)\Delta_i\}.$$

It follows that the vector of quantized sensor measurements $Y^Q := (Y_1^Q, \ldots, Y_m^Q)^T$, $Y_i^Q := Q_i(Y_i, y_i^1, \Delta_i, N_i)$ is determined by the initial quantization level $y_i^1 \in \mathbb{R}$, the quantization step $\Delta_i \in \mathbb{R}_{>0}$, and the number of intervals $N_i \in \mathbb{N}$, $i = 1, \ldots, m$. Note that, because we know the distribution of Y and the quantizer, we can always obtain the probability mass function $p(y^Q)$ of Y^Q (and thus also $p(y_i^Q)$ of Y_i^Q). Moreover, the alphabet of the *discrete* random variable Y_i^Q is the set of quantization levels $\mathcal{Y}_i^Q$.

After Y is quantized, a random vector Z is added to Y^Q to obtain $V := Z + Y^Q$. The vector V is transmitted over an unsecured communication network to a remote station, see Fig. 1. Notice that, if we do not add Z to Y^Q before transmission, information about the state is directly accessible through the unsecured network. To minimize this information leakage, we send the sum $V = Z + Y^Q$ to the remote station instead of directly sending Y^Q. Note, however, that we do not want to make Y^Q and $Y^Q + Z$ overly different either. By adding Z, we might *distort* Y^Q excessively for any practical purposes. Hence, when designing the distribution of Z, we need to consider the trade-off between *privacy* and *distortion*. In this manuscript, we propose to use the mutual information between $V = Z + Y^Q$ and Y^Q, $I[V; Y^Q]$, as *privacy metric*, and the mean square error, $E[(V - Y^Q)^2]$, as *distortion metric*. Thus, we aim at minimizing $I[V; Y^Q]$ using the probability mass function of Z, $p(z)$, as optimization variable subject to $E[(V - Y^Q)^2] = E[Z^2] \leq \epsilon$, for a desired level of distortion $\epsilon \in \mathbb{R}_{>0}$. In what follows, we formally present the optimization problem we seek to address.

Problem 1 *For given Y^Q with corresponding $p(y^Q)$ and desired distortion level $\epsilon \in \mathbb{R}_{\geq 0}$, find the probability mass function $p(z)$ of Z solution of the optimization problem:*

$$\begin{cases} \min\limits_{p(z)} \; I[Y^Q + Z; Y^Q], \\ \text{s.t. } E[Z^2] \leq \epsilon. \end{cases} \tag{3}$$

Remark 1 *Note that if we had access to Z at the other end of the network, and saturation to $Y^Q + Z$ does not occur, we could recover Y^Q exactly from Z, and thus cast the optimization problem in* (3) *without the distortion constraint.*

Remark 2 *In Problem 1, we could consider individual constraints for the distortion, i.e., $E[Z_i^2] \leq \epsilon_i$, $\epsilon_i \in \mathbb{R}_{\geq 0}$, $i = 1, \ldots, m$, instead of the joint constraint $E[Z^2] \leq \epsilon$. Indeed, if $E[Z_i^2] \leq \epsilon_i$, then $E[Z^2] \leq \sum_{i=1}^m \epsilon_i$.*

IV. Results

To delimit the solution of Problem 1, we restrict the class of probability mass functions of Z. First, we fix the alphabet $\mathcal{Z}_i$ of Z_i – the i-th component of Z – to be equal to the

TABLE I

PROBABILITY MASS FUNCTION $p(v_i)$ OF V_i.

V_i	$v_i^1 := 2y_i^1$	$v_i^2 := 2y_i^1 + \Delta_i$	$\cdots$	$v_i^{N_i} := 2y_i^1 + (N_i-1)\Delta_i$	$v_i^{N_i+1} := 2y_i^1 + N_i\Delta_i$	$\cdots$	$v_i^{2N_i-1} := 2y_i^1 + 2(N_i-1)\Delta_i$
$p(v_i)$	$p_{i,1}^V := p_{i,1}^Y p_{i,1}^Z$	$p_{i,2}^V := p_{i,1}^Y p_{i,2}^Z + p_{i,2}^Y p_{i,1}^Z$	$\cdots$	$p_{i,N_i}^V := p_{i,N_i}^Y p_{i,1}^Z + p_{i,N_i-1}^Y p_{i,2}^Z + p_{i,N_i-2}^Y p_{i,3}^Z + \cdots + p_{i,1}^Y p_{i,N_i}^Z$	$p_{i,N_i+1}^V := p_{i,N_i}^Y p_{i,2}^Z + p_{i,N_i-1}^Y p_{i,3}^Z + \cdots + p_{i,2}^Y p_{i,N_i}^Z$	$\cdots$	$p_{i,2N_i-1}^V := p_{i,N_i}^Y p_{i,N_i}^Z$

alphabet $\mathcal{Y}_i^Q$ of Y_i^Q, i.e., equal to the quantization levels. This imposes a tractable convex structure on the objective and restrictions, and reduces the optimization variables to the probabilities of each element of the alphabet. The case with arbitrary alphabet leads to a combinatorial optimization problem where the objective of (3) changes its structure for different combinations. In this manuscript, we do not address this case; it is left as a future work.

Next, note that, because X is deterministic and the covariance matrix Σ_W is diagonal, the elements of the vector Y^Q are mutually independent. Then, if we let Z to have independent components, the objective function $I[Y^Q + Z; Y^Q]$ in (3) can be written as follows.

Proposition 1 *Let the components of Z be mutually independent; then, $I[Y^Q + Z; Y^Q] = \sum_{i=1}^m I[Y_i^Q + Z_i; Y_i^Q]$ and $I[Y_i^Q + Z_i; Y_i^Q] = H[V_i] - H[Z_i]$, $i = 1, \ldots, m$.*

Proof: Proposition 1 follows from Lemma 4.

To impose a decoupled structure in the optimization problem, as pointed out in Remark 2, we consider individual constraints for the distortion, i.e., $E[Z_i^2] \leq \epsilon_i$, $\epsilon_i \in \mathbb{R}_{\geq 0}$, $i = 1, \ldots, m$. Then, we can replace (3) by the following m decoupled optimization problems:

$$\begin{cases} \min\limits_{p(z_i)} \; H[V_i] - H[Z_i], \\ \textit{s.t. } E[Z_i^2] \leq \epsilon_i, \;\; i = 1, \ldots, m, \end{cases} \tag{4}$$

where $p(z_i)$ denotes the probability mass function of Z_i and ϵ_i is the desired distortion level associated with the mean square error $E[(V_i - Y_i^Q)^2]$.

In what follows, we focus on the solution of (4) assuming independence of Z and restricting the alphabet $\mathcal{Z}_i$ of Z_i to be equal to $\mathcal{Y}_i^Q$.

Assumption 1 *The entries of Z are mutually independent and the alphabet $\mathcal{Z}_i$ of Z_i is equal to the quantization levels $\mathcal{Y}_i^Q$, i.e., it equals the alphabet of Y_i^Q.*

Next, we write $I[Y_i^Q + Z_i; Y_i^Q] = H[V_i] - H[Z_i]$ in (4) in terms of $p(y_i^Q)$ and $p(z_i)$. Denote the probabilities of Y_i^Q and Z_i as follows:

$$p_{i,j}^Y := \Pr[Y_i^Q = y_i^j], \tag{5}$$

$$p_{i,j}^Z := \Pr[Z_i = y_i^j], \tag{6}$$

with $j = 1, \ldots, N_i$. Then, the entropy $H[Z_i]$ is given by $H[Z_i] = -\sum_{j=1}^{N_i} p_{i,j}^Z \log p_{i,j}^Z$ and $E[Z_i^2] = \sum_{j=1}^{N_i} (y_i^j)^2 p_{i,j}^Z$. Moreover, since $y_i^j = y_i^1 + (j-1)\Delta_i$, then, in terms of the quantizer parameters, $E[Z_i^2] = \sum_{j=1}^{N_i} (y_i^1 + (j-1)\Delta_i)^2 p_{i,j}^Z$.

To get an expression for $H[V_i]$, we need the probability mass function $p(v_i)$ of V_i. We compute all the possible elements of the alphabet of $V_i = Y_i^Q + Z_i$ and their corresponding probabilities in terms of the elements of the alphabet $\mathcal{Y}_i^Q$, $y_i^j = y_i^1 + (j-1)\Delta_i$. Thus, the random variable V_i has an alphabet with $2N_i - 1$ elements and the corresponding probabilities are the sums of the probabilities of equal elements. The probability mass function $p(v_i)$ of V_i is given in Table I.

Now, we can write an explicit expression for the objective function in (4):

$$\begin{aligned} I[Y_i^Q + Z_i; Y_i^Q] &= H[V_i] - H[Z_i], \\ &= -\sum_{j=1}^{2N_i-1} p_{i,j}^V \log p_{i,j}^V + \sum_{j=1}^{N_i} p_{i,j}^Z \log p_{i,j}^Z, \end{aligned} \tag{7}$$

where

$$v_i^j := 2y_i^1 + (j-1)\Delta_i, \; j = 1, \ldots, 2N_i - 1, \tag{8}$$

$$\begin{aligned} p_{i,j}^V &:= \Pr[V_i = v_i^j] \\ &= \begin{cases} \sum\limits_{k=1}^{j} p_{i,j+1-k}^Y p_{i,k}^Z, \; j = 1, \ldots, N_i, \\ \sum\limits_{k=j+1-N_i}^{N_i} p_{i,j+1-k}^Y p_{i,k}^Z, \; j = N_i+1, \ldots, 2N_i - 1. \end{cases} \end{aligned} \tag{9}$$

The expressions in (7)-(9) give a complete characterization of the objective $I[Y_i^Q + Z_i; Y_i^Q]$ in terms of the *known* probabilities of the quantized sensors $p_{i,j}^Y$, $j = 1, \ldots, N_i$, and the *optimization variables*, the probabilities of the injected noise $p_{i,j}^Z$, $j = 1, \ldots, N_i$. Moreover, the distortion constraint $E[Z_i^2] = \sum_{j=1}^{N_i} (y_i^1 + (j-1)\Delta_i)^2 p_{i,j}^Z \leq \epsilon_i$ is linear in $p_{i,j}^Z$. Therefore, if the objective is convex, we could, in principle, efficiently solve (4) numerically. However, since $I[Y_i^Q + Z_i; Y_i^Q] = H[V_i] - H[Z_i]$, $H[V_i]$ is concave in $p_{i,j}^V$, and $H[Z_i]$ is concave in $p_{i,j}^Z$ [26], it is not clear whether $H[V_i] - H[Z_i]$ is convex in $p_{i,j}^Z$ or not.

Proposition 2 *For given $p_{i,j}^Y$, the function $I[Y_i^Q + Z_i; Y_i^Q]$ is convex in the probabilities $p_{i,j}^Z$, $j = 1, \ldots, N_i$.*

Proof: Define the sum:

$$f_i^V := -\sum_{j=2}^{2N_i-2} p_{i,j}^V \log p_{i,j}^V.$$

The entropy of V_i can be written in terms of f_i^V as

$$H[V_i] = f_i^V - p_{i,1}^V \log p_{i,1}^V - p_{i,2N_i-1}^V \log p_{i,2N_i-1}^V, \quad (10)$$

$$= f_i^V - p_{i,1}^Y p_{i,1}^Z \log p_{i,1}^Y - p_{i,1}^Y p_{i,1}^Z \log p_{i,1}^Z - p_{i,N_i}^Y p_{i,N_i}^Z \log p_{i,N_i}^Y - p_{i,N_i}^Y p_{i,N_i}^Z \log p_{i,N_i}^Z,$$

where the last equality follows from (9). Write the entropies $H[Z_i]$ and $H[Y_i^Q]$ as

$$H[Z_i] = -\underbrace{\left(p_{i,1}^Y + \ldots + p_{i,N_i}^Y\right)}_{=1} \sum_{j=1}^{N_i} p_{i,j}^Z \log p_{i,j}^Z, \quad (11)$$

$$=: f_i^Z - p_{i,1}^Y p_{i,1}^Z \log p_{i,1}^Z - p_{i,N_i}^Y p_{i,N_i}^Z \log p_{i,N_i}^Z,$$

$$H[Y_i^Q] = -\underbrace{\left(p_{i,1}^Z + \ldots + p_{i,N_i}^Z\right)}_{=1} \sum_{j=1}^{N_i} p_{i,j}^Y \log p_{i,j}^Y, \quad (12)$$

$$=: f_i^Y - p_{i,1}^Y p_{i,1}^Z \log p_{i,1}^Y - p_{i,N_i}^Y p_{i,N_i}^Z \log p_{i,N_i}^Y.$$

Combining (10)-(12), we can write

$$H[Z_i] + H[Y_i^Q] = f_i^Z + f_i^Y + H[V_i] - f_i^V,$$

which implies $H[V_i] = H[Z_i] + H[Y_i^Q] + f_i^V - f_i^Z - f_i^Y$ and thus $I[Y_i^Q + Z_i; Y_i^Q] = H[Y_i^Q] + f_i^V - f_i^Z - f_i^Y$. The entropy $H[Y_i^Q]$ is constant; then, $I[Y_i^Q + Z_i; Y_i^Q]$ is convex if and only if $f_i(p_{i,1}^Z, \ldots, p_{i,N_i}^Z) := f_i^V - f_i^Z - f_i^Y$ is convex. Next, collecting the $p_{i,j}^Z$ terms and using properties of logarithmic functions, we can write $f_i(p_{i,1}^Z, \ldots, p_{i,N_i}^Z)$ as follows

$$f_i = \begin{cases} \sum_{k=1}^{j} p_{i,k}^Y p_{i,j+1-k}^Z \log \left(\dfrac{p_{i,k}^Y p_{i,j+1-k}^Z}{\sum_{l=1}^{j} p_{i,l}^Y p_{i,j+1-l}^Z} \right), \\ \text{for } j = 2, \ldots, N_i, \\ \sum_{k=j-1-N_i}^{N_i} p_{i,k}^Y p_{i,j+1-k}^Z \log \left(\dfrac{p_{i,k}^Y p_{i,j+1-k}^Z}{\sum_{l=1}^{j} p_{i,l}^Y p_{i,j+1-l}^Z} \right), \\ \text{for } j = N_i + 1, \ldots, 2N_i - 2. \end{cases}$$

Note that every element of $f_i(p_{i,1}^Z, \ldots, p_{i,N_i}^Z)$ above is a function of the form $g(a, b, c, \ldots, r) = a \log\left(\frac{a}{a+b+c+\cdots+r}\right)$, $a, b, c \ldots, r \in [0, 1]$. The function $g(a, b, c, \ldots, r)$ can be proved to be convex using Theorem 2.7.1 in [26] – *the log sum inequality*. Hence, $f_i(p_{i,1}^Z, \ldots, p_{i,N_i}^Z)$ is the sum of convex functions and thus convex as well. ■

Note that the ultimate goal is to make it hard for adversaries to infer X from $V = Y^Q + Z$. That is, if someone estimates X using the available data at the public network V, the estimation $\hat{X}(V)$ should carry less information about X than an estimate $\hat{X}(Y^Q)$ obtained using Y^Q directly. In other words, we want to make $I[\hat{X}(V); \hat{X}(Y^Q)]$ small.

Proposition 3 *For some functions $h_V, h_Y : \mathbb{R}^m \to \mathbb{R}^m$, let $\hat{X}(V) := h_V(V)$ and $\hat{X}(Y^Q) := h_Y(Y^Q)$ be estimates of X using $V = Y^Q + Z$ and Y^Q, respectively. Then, it is satisfied that $I[\hat{X}(Y^Q + Z); \hat{X}(Y^Q)] \leq I[Y^Q + Z; Y^Q]$ for any pair of functions $h_Y(\cdot)$ and $h_V(\cdot)$.*

Proof: The assertion follows from property (P_3) in Section II – the *data processing inequality* [26].

Remark 3 *Proposition 3 has a nice interpretation: for any pair of estimators $(\hat{X}(Y^Q + Z), \hat{X}(Y^Q))$ that can be constructed using $Y^Q + Z$ and Y^Q, respectively; the mutual information between them is always upper bounded by $I[Y^Q + Z; Y^Q]$ independently of the estimators. This implies that by minimizing $I[Y^Q + Z; Y^Q]$, we are decreasing the information $I[\hat{X}(Y^Q + Z); \hat{X}(Y^Q)]$. Indeed, the tightness of this bound depends on the particular choice of estimators.*

A. Multiple Observations

In real-time applications, we often have consecutive observations of the variable X in (1), i.e., a system of the form:

$$Y(t) = CX + W(t), \ t \in \mathbb{N}, \quad (13)$$

with different realizations of sensor data $Y(t) \in \mathbb{R}^m$ and sensor noise $W(t) \in \mathbb{R}^m$ at each time step t. If the noise $W(t)$ is an i.i.d. process (which is the case most of the time) with $\Sigma_W := E[W(t)W(t)^T] = \text{diag}[\sigma_1^2, \ldots, \sigma_m^2]$ and $E[W(t)] = \mathbf{0}$ for all t, the time-dependent model (13) can be written as a static one for a finite number of time-steps M. That is, we can collect sensor data for a time window of M steps, stack each set of sensor measurements as $\tilde{Y}_M := (Y(1)^T, \ldots, Y(M)^T)^T \in \mathbb{R}^{Mm}$, and use this stacked vector to produce a stacked system:

$$\tilde{Y}_M = \tilde{C}_M X + \tilde{W}_M, \quad (14)$$

with sensor noise $\tilde{W}_M := (W(1)^T, \ldots, W(M)^T)^T \in \mathbb{R}^{Mm}$ and stacked matrix $\tilde{C}_M := (C^T, \ldots, C^T)^T \in \mathbb{R}^{Mm \times n}$. Because $W(t)$ is an i.i.d. process and Σ_W is diagonal, all entries of $\tilde{W}_M$ and $\tilde{Y}_M$ are mutually independent. Hence, we can use the tools described above to design the distribution of a noise vector $\tilde{Z}_M \in \mathbb{R}^{Mm}$ that minimizes the mutual information $I[\tilde{Y}_M^Q + \tilde{Z}_M; \tilde{Y}_M^Q]$, where $\tilde{Y}_M^Q$ denotes the quantized $\tilde{Y}_M$. Actually, if we let $\tilde{Z}_M := (Z(1)^T, \ldots, Z(M)^T)^T$ and $Z(t)$ be an i.i.d. process with independent entries, it can be proved that $I[\tilde{Y}_M^Q + \tilde{Z}_M; \tilde{Y}_M^Q] = MI[Y^Q + Z; Y]$, where, with abuse of notation, Y^Q and Z denote two random vectors thrown from the distributions of the i.i.d. processes $Y^Q(t)$ and $Z(t)$. That is, the mutual information $I[\tilde{Y}_M^Q + \tilde{Z}_M; \tilde{Y}_M^Q]$ is simply M times $I[Y^Q + Z; Y]$. It follows that, the distribution of $Z(t) = (Z_1(t)^T, \ldots, Z_m(t)^T)^T$ that minimizes $I[\tilde{Y}_M^Q + \tilde{Z}_M; \tilde{Y}_M^Q]$, for arbitrary large M, is the solution, $p(z_i)$, $i = 1, \ldots, m$, of problem (4), i.e., $Z_i(t) \sim p(z_i)$, $t \in \mathbb{N}$ is the optimal solution.

V. Simulations Results

Consider system (1) with $X = (\pi^2, \pi^2/4)^T$, $C = I_2$, and sensor noise $W = (W_1, W_2)^T$, $W_1 \sim \mathcal{N}(0, \sigma_1^2)$, $\sigma_1^2 = \pi$, $W_2 \sim \mathcal{U}(-a, a)$, $a = \pi^2/40$, $\sigma_2^2 = (1/3)a^2$. Each sensor measurement Y_i, $i = 1, 2$, is quantized using the uniform quantizer (2) with $y_1^1 = \pi^2 - 3\sigma_1$, $\Delta_1 = 6\sigma_1/N_1$, $N_1 = 11$, and $y_2^1 = 9.09a$, $\Delta_2 = 2a/N_2$, $N_2 = 11$. In Figure 2, we show the optimal distribution $p(z_1)$ of Z_1 solution of (4), first without the distortion constraint, and then for the distortion levels $\epsilon_1 = 60, 40$. The distortion level for the unconstrained case is $E[Z_1^2] = 105.03$. For comparison, we also show the distributions $p(y_1^Q)$ of Y_1^Q and the one of the sum $V_1 = Y_1^Q + Z_1$, $p(v_1)$. In Figure 3, we show the corresponding results for sensor 2: the optimal distributions

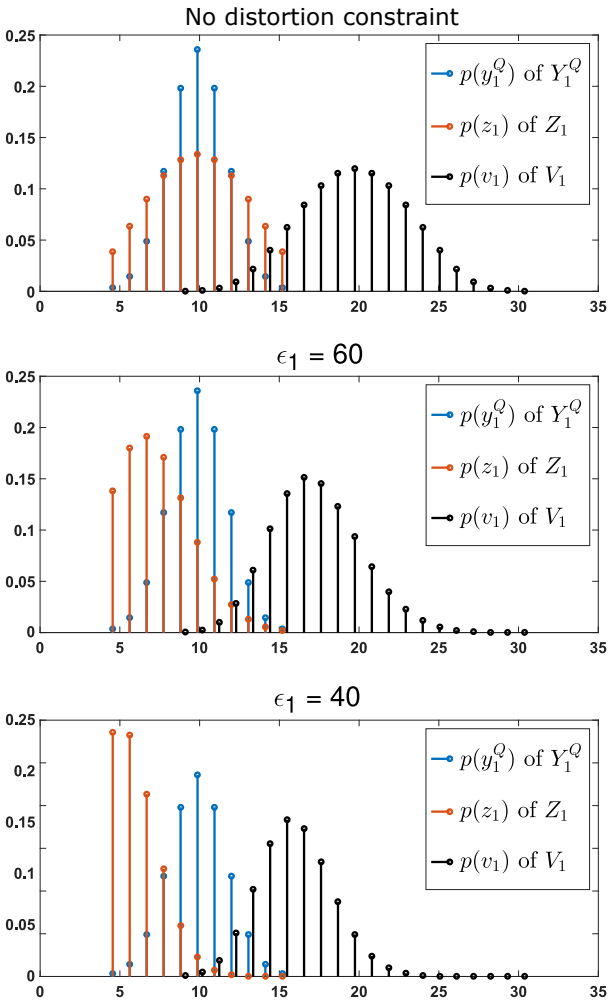


Fig. 2.

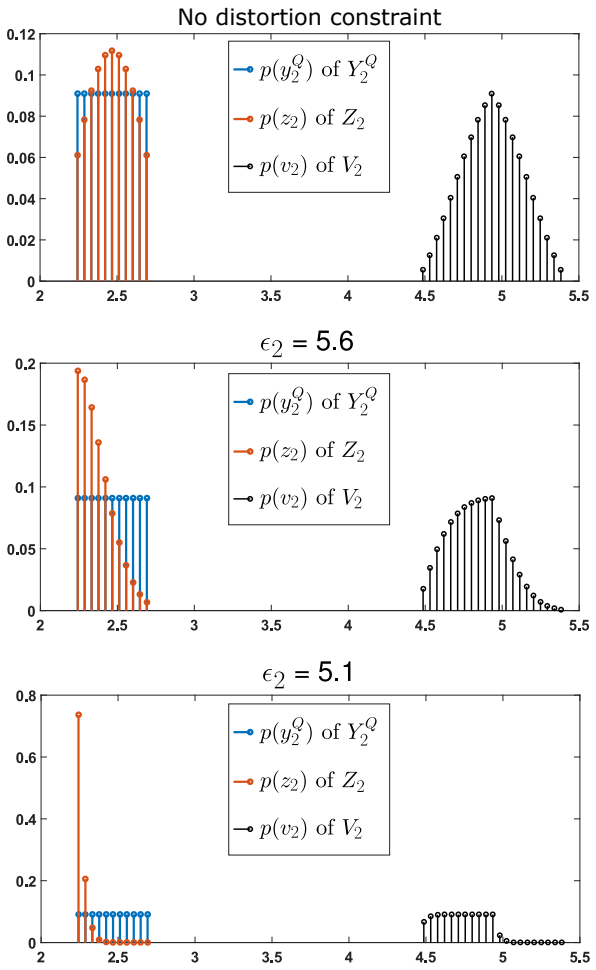


Fig. 3.

for the unconstrained case, which yields $E[Z_2^2] = 6.10$, and then for the distortion levels $\epsilon_2 = 5.6, 5.1$.

VI. Conclusion

We have provided results on privacy of quantized noisy sensor measurements by adding optimal random variables. To minimize the information leakage due to unsecured communication networks, we have proposed to add random variables to the quantized sensor measurements before transmission. The distributions of these discrete random variables have been designed to minimize the mutual information between the sum and the quantized sensor measurements for a desired level of distortion. In particular, we have posed the design problem as a convex optimization where the optimization variables are the probabilities of the injected noise. We have provided simulation results to test the performance of our tools.

References

[1] F. Farokhi and H. Sandberg, "Optimal privacy-preserving policy using constrained additive noise to minimize the fisher information," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017.

[2] F. Farokhi, H. Sandberg, I. Shames, and M. Cantoni, "Quadratic Gaussian privacy games," in *2015 54th IEEE Conference on Decision and Control (CDC)*, 2015, pp. 4505–4510.

[3] C. Murguia and J. Ruths, "On reachable sets of hidden cps sensor attacks," in *proceedings of the American Control Conference (ACC), 2018*, 2018.

[4] F. Farokhi and G. Nair, "Privacy-constrained communication," *IFAC-PapersOnLine*, vol. 49, pp. 43 – 48, 2016.

[5] C. Murguia and J. Ruths, "Cusum and chi-squared attack detection of compromised sensors," in *proceedings of the IEEE Multi-Conference on Systems and Control (MSC)*, 2016.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, pp. 2715–2729, 2013.

[7] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding sensor outputs for injection attacks detection," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*, 2014, pp. 5776–5781.

[8] C. Murguia and J. Ruths, "Characterization of a cusum model-based sensor attack detector," in *proceedings of the 55th IEEE Conference on Decision and Control (CDC)*, 2016.

[9] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[10] L. H. Ozarow and A. D. Wyner, "Wire-tap channel ii," in *Advances in Cryptology*, T. Beth, N. Cot, and I. Ingemarsson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 33–50.

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

[12] J. L. Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, pp. 341–354, 2014.

[13] N. Hashemil, C. Murguia, and J. Ruths, "A comparison of stealthy

sensor attacks on control systems," in *proceedings of the American Control Conference (ACC), 2018*, 2018.

[14] C. Murguia, N. van de Wouw, and J. Ruths, "Reachable sets of hidden cps sensor attacks: Analysis and synthesis tools," in *proceedings of the IFAC World Congress*, 2016.

[15] S. H. Kafash, J. Giraldo, C. Murguia, A. A. Cardenas, and J. Ruths, "Constraining attacker capabilities through actuator saturation," in *proceedings of the American Control Conference (ACC), 2018*, 2018.

[16] C. Murguia, I. Shames, J. Ruths, and D. Nešić, "Security metrics of networked control systems under sensor attacks," in eprint arXiv:1809.01808, 2018.

[17] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 1–19.

[18] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, pp. 211–407, 2014.

[19] S. Han, U. Topcu, and G. J. Pappas, "Differentially private convex optimization with piecewise affine objectives," in *53rd IEEE Conference on Decision and Control*, 2014.

[20] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Information Sciences*, vol. 250, pp. 200 – 214, 2013.

[21] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *2014 IEEE International Symposium on Information Theory*, 2014, pp. 2371–2375.

[22] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Entropy-minimizing mechanism for differential privacy of discrete-time linear feedback systems," in *53rd IEEE Conference on Decision and Control*, 2014, pp. 2130–2135.

[23] F. du Pin Calmon and N. Fawaz, "Privacy against statistical inference," in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012.

[24] S. Salamatian, A. Zhang, F. du Pin Calmon, S. Bhamidipati, N. Fawaz, B. Kveton, P. Oliveira, and N. Taft, "Managing your private and public data: Bringing down inference attacks against your privacy," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, pp. 1240–1255, 2015.

[25] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1331–1341, 2013.

[26] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[27] M. Madiman, "On the entropy of sums," in *2008 IEEE Information Theory Workshop*, 2008, pp. 303–307.