Information Bounds for State Estimation in the Presence of an Eavesdropper

Alex S. Leong, Daniel E. Quevedo, Daniel Dolz, and Subhrakanti Dey

***Abstract*—Remote state estimation problems in the presence of eavesdroppers have recently been investigated in the literature. For unstable systems, it has been shown that it is possible to keep the expected estimation error covariance bounded, while the expected eavesdropper error covariance becomes unbounded in the infinite horizon. In this note, we consider an alternative notion of security based on the amount of information revealed to the eavesdropper. Upper and lower bounds on the information revealed are derived. In particular, in the infinite horizon, it is shown that with unstable systems, any transmission policy (within the class of stationary deterministic policies where the sensor at each time step can either transmit its local state estimate or not) which keeps the expected estimation error covariance bounded must always reveal a non-zero expected amount of information to the eavesdropper.**

***Index Terms*—Directed information, eavesdropping, security, state estimation.**

I. Introduction

OVER the last decade, the amount of data transmitted wirelessly has increased dramatically, owing to the popularity of 3G/4G smartphones, and other devices communicating via Wi-Fi and Bluetooth such as laptops and tablets. Due to the broadcast nature of the wireless medium, other agents in the vicinity can often overhear what is being transmitted. It is therefore important to protect transmissions from eavesdroppers, which has traditionally been achieved using cryptography. However, due to 1) the often limited computational power available at the transmitters to implement strong encryption, 2) the increased computational power available to malicious agents, and 3) poorly implemented security in some Internet of Things devices, achieving security using solely cryptographic means may not necessarily be guaranteed. Alternative and complementary ways to implement security using physical layer and information theoretic techniques have thus received significant recent interest [1].

The term "physical layer security" refers to approaches to implement security using physical layer characteristics of the wireless channel such as fading, interference, and noise [2]. Using such ideas, estimation problems with eavesdroppers have recently been studied, such as [3]–[6] for estimation of constants or i.i.d. sources, and [7]–[11] for state estimation of dynamical systems. The purpose is usually to keep the mean squared error or estimation error covariance at the eavesdropper above a certain level. For dynamical systems, one of the main results shown in the above works is that for the case of unstable systems, it is possible to drive the expected eavesdropper error covariance unbounded while keeping the expected estimation error covariance at the legitimate remote estimator (or receiver) bounded.

Mutual information is a measure of the additional information gained by receiving a measurement. In the current work, instead of considering the eavesdropper error covariance as the measure of security as in [7]–[11], we instead study the information revealed to the eavesdropper. In particular we consider the sum of conditional mutual informations (also known as the *directed information* [12]) revealed to the eavesdropper. In addition to the wide use of mutual information in information theoretic security measures, directed information has also been justified as a measure of privacy/secrecy for control applications in [13]: it is the unique measure satisfying a number of reasonable postulates, in particular that it should satisfy a data processing inequality and that the total information leakage has a stage-additive form. Other works in control system design using the directed information measure include [14], [15].

In the current work, a sensor makes noisy measurements of a linear dynamical process. The sensor transmits local state estimates to the remote estimator over a packet dropping link. At the same time, an eavesdropper can successfully eavesdrop on the sensor transmission with a certain probability, see Fig. 1. A key feature of the current setup is that one can decide at each instant whether the sensor should transmit or not. Our results in this note show that the expected information revealed to the eavesdropper is both upper and lower bounded. In particular, the lower bound says that information leakage is unavoidable for *all* such transmission policies which keep the expected error covariance at the legitimate receiver bounded. As numerical illustration of these results, we also compare

Manuscript received January 14, 2019; revised March 11, 2019; accepted April 9, 2019. Date of publication April 19, 2019; date of current version May 2, 2019. Recommended by Senior Editor M. Guay. *(Corresponding author: Alex S. Leong.)*

A. S. Leong and D. E. Quevedo are with the Department of Electrical Engineering, Paderborn University, 33098 Paderborn, Germany (e-mail: alex.leong@upb.de; dquevedo@ieee.org).

D. Dolz is with Procter & Gamble, 53881 Euskirchen, Germany (e-mail: ddolz@uji.es).

S. Dey is with the Department of Electronic Engineering, Maynooth University, Maynooth, W23 F2H6 Ireland (e-mail: subhra.dey@mu.ie).

Digital Object Identifier 10.1109/LCSYS.2019.2912262

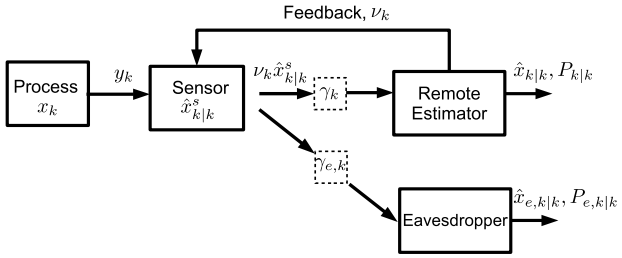

Fig. 1. Remote State Estimation with an Eavesdropper.

our bounds with a transmission scheduling problem minimizing a linear combination of the expected error covariance and expected information revealed.

Notation: Given a square matrix X, we let $\lambda_{\min}(X)$ and $\lambda_{\max}(X)$ denote the minimum and maximum eigenvalues of X respectively if they are real valued, and we use $|\lambda_{\max}(X)|$ to denote the spectral radius of X. We denote the largest singular value of X by $\sigma_{\max}(X)$.

II. System Model

A diagram of the system model is shown in Fig. 1. Consider a discrete time process

$$x_{k+1} = Ax_k + w_k \tag{1}$$

where $x_k \in \mathbb{R}^{n_x}$ and w_k is i.i.d. Gaussian with zero mean and covariance $Q > 0$.[1] The sensor has measurements

$$y_k = Cx_k + v_k, \tag{2}$$

where $y_k \in \mathbb{R}^{n_y}$ and v_k is i.i.d. Gaussian with zero mean and covariance $R > 0$. The noise processes $\{w_k\}$ and $\{v_k\}$ are assumed to be mutually independent, and independent of the initial state x_0.

The sensor forms and transmits local state estimates $\hat{x}^s_{k|k}$ [16] to the remote estimator. The local state estimates and estimation error covariances

$$\begin{aligned}\hat{x}^s_{k|k} &\triangleq \mathbb{E}[x_k|y_0, \ldots, y_k]\\ P^s_{k|k} &\triangleq \mathbb{E}[(x_k - \hat{x}^s_{k|k})(x_k - \hat{x}^s_{k|k})^\top|y_0, \ldots, y_k]\end{aligned}$$

can be computed at the sensor using the standard Kalman filtering equations, see, e.g., [17]. We will assume that the pair (A, C) is observable and the pair $(A, Q^{1/2})$ is controllable. Let $\bar{P} > 0$ be the steady state value of $P^s_{k|k}$ as $k \to \infty$, which exists due to the observability assumption. For simplicity of presentation, we will assume that this local Kalman filter is operating in the steady state regime, so that $P^s_{k|k} = \bar{P}, \forall k$. We note that in general convergence to steady state occurs at an exponential rate [17].

Let $\nu_k \in \{0, 1\}$ be decision variables such that $\nu_k = 1$ if and only if $\hat{x}^s_{k|k}$ is to be transmitted at time k. The decision variables ν_k are determined (following a stationary deterministic policy) at the remote estimator, which is assumed to have more computational capabilities than the sensor, using information available at time $k-1$, and then fed back to the sensor before transmission at time k.[2]

When $\nu_k = 1$, the sensor transmits over a packet dropping channel to the remote estimator. Let $\gamma_k \in \{0, 1\}$ be random variables such that $\gamma_k = 1$ if and only if the sensor transmission at time k is successfully received by the remote estimator. We will assume that $\{\gamma_k\}$ is an i.i.d. Bernoulli process [19] with

$$\mathbb{P}(\gamma_k = 1) = p \in [0, 1].$$

Sensor transmissions can be overheard by an eavesdropper over another packet dropping channel. Let $\gamma_{e,k} \in \{0, 1\}$ be random variables such that $\gamma_{e,k} = 1$ if and only if the sensor transmission at time k is overheard by the eavesdropper. The process $\{\gamma_{e,k}\}$ is i.i.d. Bernoulli with

$$\mathbb{P}(\gamma_{e,k} = 1) = p_e \in [0, 1].$$

We assume the processes $\{\gamma_k\}$ and $\{\gamma_{e,k}\}$ to be mutually independent.

At times where $\nu_k = 1$, it is assumed that the remote estimator knows whether the transmission was successful or not, with dropped packets discarded. Define the information set available to the remote estimator at time k as:

$$\mathcal{I}_k \triangleq \{\nu_0, \ldots, \nu_k, \nu_0\gamma_0, \ldots, \nu_k\gamma_k, \nu_0\gamma_0\hat{x}^s_{0|0}, \ldots, \nu_k\gamma_k\hat{x}^s_{k|k}\}.$$

For further reference, denote the state estimates and estimation error covariances at the remote estimator by:

$$\begin{aligned}\hat{x}_{k|k} &\triangleq \mathbb{E}[x_k|\mathcal{I}_k],\\ P_{k|k} &\triangleq \mathbb{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})^\top|\mathcal{I}_k].\end{aligned} \tag{3}$$

Similarly, the eavesdropper knows if it has eavesdropped sucessfully. Define the information set available to the eavesdropper at time k as:

$$\begin{aligned}\mathcal{I}_{e,k} \triangleq \{&\nu_0, \ldots, \nu_k, \nu_0\gamma_{e,0}, \ldots, \nu_k\gamma_{e,k},\\ &\nu_0\gamma_{e,0}\hat{x}^s_{0|0}, \ldots, \nu_k\gamma_{e,k}\hat{x}^s_{k|k}\},\end{aligned}$$

and the state estimates and estimation error covariances at the eavesdropper by:

$$\begin{aligned}\hat{x}_{e,k|k} &\triangleq \mathbb{E}[x_k|\mathcal{I}_{e,k}],\\ P_{e,k|k} &\triangleq \mathbb{E}[(x_k - \hat{x}_{e,k|k})(x_k - \hat{x}_{e,k|k})^\top|\mathcal{I}_{e,k}].\end{aligned} \tag{4}$$

As previously mentioned, the decision variables ν_k are determined at the (legitimate) remote estimator and fed back to the sensor. We will consider the case where ν_k depends on both $P_{k-1|k-1}$ and $P_{e,k-1|k-1}$, as well as the case where ν_k depends only on $P_{k-1|k-1}$ and the remote estimator's belief of $P_{e,k-1|k-1}$ constructed from knowledge of previous ν_k's. We denote by $\mathcal{V}$ the class of stationary deterministic scheduling policies where the sensor at each time step can either transmit its local estimate or not. The optimal remote estimator can be shown to have the form

$$\begin{aligned}\hat{x}_{k|k} &= \begin{cases} A\hat{x}_{k-1|k-1}, & \nu_k\gamma_k = 0\\ \hat{x}^s_{k|k}, & \nu_k\gamma_k = 1\end{cases}\\ P_{k|k} &= \begin{cases} f(P_{k-1|k-1}), & \nu_k\gamma_k = 0\\ \bar{P}, & \nu_k\gamma_k = 1,\end{cases}\end{aligned} \tag{5}$$

[1]For a symmetric matrix X, we say that $X > 0$ if it is positive definite, and $X \geq 0$ if it is positive semi-definite.

[2]The case of imperfect feedback links can also be handled by adapting techniques used in [18, Sec. II-C].

where

$$f(X) \triangleq AXA^\top + Q. \tag{6}$$

Simlarly, at the eavesdropper the optimal estimator satisfies:

$$\hat{x}_{e,k|k} = \begin{cases} A\hat{x}_{e,k-1|k-1}, & \nu_k\gamma_{e,k} = 0 \\ \hat{x}^s_{k|k}, & \nu_k\gamma_{e,k} = 1 \end{cases}$$

$$P_{e,k|k} = \begin{cases} f(P_{e,k-1|k-1}), & \nu_k\gamma_{e,k} = 0 \\ \bar{P}, & \nu_k\gamma_{e,k} = 1. \end{cases}$$

Define the countable set of matrices:

$$\mathcal{S} \triangleq \{\bar{P}, f(\bar{P}), f^2(\bar{P}), \dots\}, \tag{7}$$

where $f^n(.)$ is the n-fold composition of $f(.)$, with $f^0(X) \triangleq X$. The set $\mathcal{S}$ consists of all possible values of $P_{k|k}$ at the remote estimator, as well as all possible values of $P_{e,k|k}$ at the eavesdropper. There is a total ordering (in the Loewner order) on $\mathcal{S}$ given by (see, e.g., [20])

$$\bar{P} \leq f(\bar{P}) \leq f^2(\bar{P}) \leq \dots \tag{8}$$

III. Bounds on Information Revealed to Eavesdropper

In this section we will show that the expected amount of information revealed to an eavesdropper is both upper and lower bounded. Optimal transmission scheduling problems, which minimize a linear combination of the expected error covariance at the remote estimator and the expected information revealed to the eavesdropper, will be considered in Section IV.

Let $z_{e,k} \triangleq (\nu_k, \nu_k\gamma_{e,k}, \nu_k\gamma_{e,k}\hat{x}^s_{k|k})$ be received by the eavesdropper at time k. The conditional mutual information

$$I_{e,k} \triangleq I(x_k; z_{e,k}|z_{e,0}, \dots, z_{e,k-1})$$

between x_k and $z_{e,k}$ has the expression (see [15], [21]):

$$\begin{aligned} I_{e,k} &= \frac{1}{2}\log\det P_{e,k|k-1} - \frac{1}{2}\log\det P_{e,k|k} \\ &= \frac{1}{2}\log\det f(P_{e,k-1|k-1}) - \frac{1}{2}\log\det P_{e,k|k} \end{aligned} \tag{9}$$

We have the following preliminary result:

Lemma 1: The function

$$g(N) \triangleq \frac{1}{N}\left(\frac{1}{2}\log\det f^N(\bar{P}) - \frac{1}{2}\log\det\bar{P}\right) \tag{10}$$

is decreasing in $N \in \mathbb{N}$.

Proof: See Appendix A. ∎

A. Upper Bound

We will first show (in Theorem 1) that the expected information revealed to the eavesdropper is always upper bounded, for any transmission policy in $\mathcal{V}$ and all p_e. To achieve this, we will use the following result:

Lemma 2: We have

$$g(N) \leq \frac{1}{2}\log\det f(\bar{P}) - \frac{1}{2}\log\det\bar{P} \triangleq \Delta_U < \infty$$

for all $N \in \mathbb{N}$, where $g(N)$ is defined in (10).

Proof: This follows directly from Lemma 1. ∎

Theorem 1: For any transmission policy in $\mathcal{V}$ and all p_e,

$$\limsup_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}] < \Delta_U < \infty,$$

where Δ_U is as given in Lemma 2.

Proof: For a given K, let the random variable $\tau(K)$ count the number of times where $\gamma_{e,k} = 1$ for $k \leq K$. Denote the (in general random) durations between successful eavesdroppings by $N_1, N_2, \dots, N_{\tau(K)}$, with $N_1 + N_2 + \dots + N_{\tau(K)} \leq K$. Then we have

$$\begin{aligned} \frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}] &= \frac{1}{K}\mathbb{E}\left[\sum_{i=1}^{\tau(K)} N_i \times \frac{1}{N_i}\left(\frac{1}{2}\log\det f^{N_i}(\bar{P}) - \frac{1}{2}\log\det\bar{P}\right)\right] \\ &< \frac{1}{K}\mathbb{E}\left[\sum_{i=1}^{\tau(K)} N_i\Delta_U\right] \leq \Delta_U, \end{aligned} \tag{11}$$

where the first inequality comes from Lemma 2. As (11) holds for all K, we thus have $\limsup_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}] < \Delta_U < \infty$. ∎

B. Lower Bound

We will now focus on unstable systems, i.e., where the A matrix in (1) satisfies $|\lambda_{\max}(A)| > 1$. For such systems, it turns out that if one uses a transmission scheduling policy in $\mathcal{V}$ which keeps the expected error covariance of the remote estimator bounded, then unavoidably one will always reveal a non-zero expected amount of information to the eavesdropper. Before proving this result in Theorem 2, we will need the following:

Lemma 3: Let A be an unstable matrix. Then we have

$$g(N) > \log|\lambda_{\max}(A)| \triangleq \Delta_L > 0$$

for all $N \in \mathbb{N}$, where $g(N)$ is defined in (10).

Proof: See Appendix B. ∎

Theorem 2: Let A be an unstable matrix, and assume that $p_e > 0$. Then, for any transmission policy in $\mathcal{V}$ satisfying

$$\limsup_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathrm{tr}\mathbb{E}[P_{k|k}] < \infty, \tag{12}$$

one must have

$$\liminf_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}] > p_e\log|\lambda_{\max}(A)| \triangleq \tilde{\Delta}_L > 0.$$

Proof: We first argue that for any transmission policy in $\mathcal{V}$ satisfying (12), the time between any two successive transmission attempts must be upper bounded by some constant $\kappa_{\max}$, where $\kappa_{\max}$ depends on the particular policy used. Consider the Markov chain induced by a particular stationary deterministic policy satisfying (12). Suppose by contradiction that there exists a state in this Markov chain such that once this state is visited, there will then be an unbounded number of non-transmissions, thereby leading to an unbounded error covariance. As there is a non-zero probability of visiting this state, the expected error covariance will also become unbounded, contradicting (12).

Now fix such a policy satisfying (12). Call a sequence of transmission decisions $\boldsymbol{\nu} \triangleq \{\nu_0, \nu_1, \dots\}$ *admissible* for the policy if there exists a sequence $\{\gamma_0, \gamma_1, \dots, \gamma_{e,0}, \gamma_{e,1}, \dots\}$ which generates it. Let $\boldsymbol{\nu}_{1:k}$ denote the subsequence $\{\nu_0, \nu_1, \dots, \nu_k\}$. We will show that $\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}]$ is lower bounded away from zero for any admissible sequence $\boldsymbol{\nu}$ and all sufficiently large K, thus proving the theorem.

Fix a $K > \kappa_{\max}$ and an admissible sequence $\boldsymbol{\nu}$. Let K' denote the last time over the horizon K when a transmission attempt occurred. Then $K - K' < \kappa_{\max}$, and $K'/K > 1 - \kappa_{\max}/K$ is bounded away from zero for all $K > \kappa_{\max}$. We have

$$\begin{aligned}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}] &= \frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]\times\mathbb{P}(\gamma_{e,K'}=1)\\ &\quad+\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=0]\times\mathbb{P}(\gamma_{e,K'}=0)\\ &\geq \frac{p_e}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]\\ &= \frac{p_eK'}{K}\frac{1}{K'}\sum_{k=1}^{K'}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]\\ &> p_e\Big(1-\frac{\kappa_{\max}}{K}\Big)\frac{1}{K'}\sum_{k=1}^{K'}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]\end{aligned}$$

Now consider the term $\frac{1}{K'}\sum_{k=1}^{K'}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]$. Within this time period K', there could be a number of time instances k where $\gamma_{e,k}=1$. Denote the random durations between successful eavesdroppings by $N_1, N_2, \dots, N_{\tau(K')}$, where the random variable $\tau(K')$ counts the total number of successful eavesdroppings within the time period K' (since $\gamma_{e,K'}=1$, we have $\tau(K')\geq 1$), with $N_1+N_2+\cdots+N_{\tau(K')}=K'$. Then we have

$$\begin{aligned}&\frac{1}{K'}\sum_{k=1}^{K'}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}, \gamma_{e,K'}=1]\\ &\quad=\frac{1}{K'}\mathbb{E}\left[\sum_{i=1}^{\tau(K')}N_i\times\frac{1}{N_i}\left(\frac{1}{2}\log\det f^{N_i}(\bar{P})-\frac{1}{2}\log\det\bar{P}\right)\right]\\ &\quad\geq\frac{1}{K'}\mathbb{E}\left[\sum_{i=1}^{\tau(K')}N_i\Delta_L\right]=\Delta_L\end{aligned}$$

where the inequality and Δ_L come from Lemma 3. Hence $\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}] > p_e(1-\frac{\kappa_{\max}}{K})\Delta_L$ for all $K > \kappa_{\max}$. In particular,

$$\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[I_{e,k}|\boldsymbol{\nu}_{1:k}] > p_e\Delta_L \triangleq \tilde{\Delta}_L$$

for all sufficiently large K. ∎

In [9] (see also [8], [10], [11]) it was shown that for unstable systems, one could always find transmission policies which can keep the expected estimation error covariance bounded, while the expected eavesdropper covariance became unbounded. By contrast, Theorem 2 shows that there are *no* transmission policies in $\mathcal{V}$ which can drive the expected information revealed to the eavesdropper to zero (including the policies studied in [9]). The two measures of security, namely $\mathbb{E}[P_{k|k}]$ investigated in [9], and $\mathbb{E}[I_{e,k}]$ considered in the current work, therefore appear to be fundamentally different.

IV. Optimal Transmission Scheduling

In order to illustrate numerically the results of Section III, we will compare our bounds with the best achievable trade-off between the expected error covariance at the remote estimator and the expected information revealed to the eavesdropper. We thus consider in this section the optimal scheduling of transmissions, in order to minimize a linear combination of the expected error covariance and the expected information revealed. We will consider both cases where the eavesdropper error covariance is either known or unknown to the remote estimator.

A. Eavesdropper Error Covariance Known at Remote Estimator

In this case the decisions ν_k can depend on both $P_{k-1|k-1}$ and $P_{e,k-1|k-1}$. The problem we wish to solve is the infinite horizon problem:

$$\begin{aligned}&\min_{\{\nu_k\}}\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}[\beta\mathrm{tr}P_{k|k}+(1-\beta)I_{e,k}]\\ &=\min_{\{\nu_k\}}\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}\Big[\beta(\nu_kp\mathrm{tr}\bar{P}+(1-\nu_kp)\mathrm{tr}f(P_{k-1|k-1}))\\ &\quad+(1-\beta)\nu_kp_e\Big(\frac{1}{2}\log\det f(P_{e,k-1|k-1})-\frac{1}{2}\log\det\bar{P}\Big)\Big],\end{aligned}\tag{13}$$

where $\beta\in(0,1)$ is a design parameter. Larger values of β will place more importance on keeping $\mathbb{E}[P_{k|k}]$ small, while smaller values of β will place more importance on keeping $\mathbb{E}[I_{e,k}]$ small. When A is unstable, $\mathbb{E}[P_{k|k}]$ can be kept bounded if and only if (see [9])

$$p > 1-\frac{1}{|\lambda_{\max}(A)|^2}.\tag{14}$$

Furthermore, by Theorem 1, the expected information revealed is upper bounded for all p_e. Thus there exist policies for problem (13) with bounded cost under condition (14).

Numerical solutions to problem (13) can be found using, e.g., the relative value iteration algorithm [22, p. 431]. Note that the number of possible values of $(P_{k|k}, P_{e,k|k})$ is infinite. Thus in practice the state space will need to be truncated for numerical solution. Define the finite set $\mathcal{S}^N\subseteq\mathcal{S}$ by

$$\mathcal{S}^N \triangleq \{\bar{P}, f(\bar{P}), \dots, f^N(\bar{P})\},\tag{15}$$

which includes the values of all error covariances with up to N successive packet drops or non-transmissions. Then one can run the relative value iteration algorithm over the finite state space $\mathcal{S}^N\times\mathcal{S}^N$ (of cardinality $(N+1)^2$)), and compare the solutions obtained as N increases to determine an appropriate value for N [23].

B. Eavesdropper Error Covariance Unknown at Remote Estimator

In order to construct $P_{e,k|k}$ at the remote estimator as in Section IV-A, the process $\{\gamma_{e,k}\}$ for the eavesdropper's channel needs to be known, which in practice may be difficult to achieve. Here we consider the situation where the remote estimator knows only the probability of successful eavesdropping p_e and not the actual realizations $\gamma_{e,k}$. Thus the transmit decisions ν_k can only depend on $P_{k-1|k-1}$ and our beliefs of $P_{e,k-1|k-1}$ constructed from knowledge of previous ν_k's.

Consider the belief vector [22, p. 258]

$$\pi_{e,k} = \begin{bmatrix} \pi_{e,k}^{(0)} \\ \pi_{e,k}^{(1)} \\ \pi_{e,k}^{(2)} \\ \vdots \end{bmatrix} \triangleq \begin{bmatrix} \mathbb{P}\big(P_{e,k|k} = \bar{P} | \nu_0, \ldots, \nu_k\big) \\ \mathbb{P}\big(P_{e,k|k} = f(\bar{P}) | \nu_0, \ldots, \nu_k\big) \\ \mathbb{P}\big(P_{e,k|k} = f^2(\bar{P}) | \nu_0, \ldots, \nu_k\big) \\ \vdots \end{bmatrix}. \quad (16)$$

From [9], by defining

$$\Phi(\pi_e, \nu) \triangleq \begin{cases} \begin{bmatrix} 0 & \pi_e^{(0)} & \pi_e^{(1)} & \ldots \end{bmatrix}^\top, & \nu = 0 \\ \begin{bmatrix} p_e & (1-p_e)\pi_e^{(0)} & (1-p_e)\pi_e^{(1)} & \ldots \end{bmatrix}^\top, & \nu = 1 \end{cases}$$

we can obtain the recursive relationship

$$\pi_{e,k+1} = \Phi(\pi_{e,k}, \nu_{k+1}).$$

This leads to the transmission scheduling problem:

$$\min_{\{\nu_k\}} \lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \mathbb{E}\Big[\beta(\nu_k p \mathrm{tr}\bar{P} + (1-\nu_k p)\mathrm{tr} f(P_{k-1|k-1})) + (1-\beta)\nu_k p_e \Big(\sum_{i=0}^{\infty} \frac{1}{2} (\log\det f^{i+1}(\bar{P})) \pi_{e,k-1}^{(i)} - \frac{1}{2}\log\det\bar{P} \Big)\Big], \quad (17)$$

where $\beta \in (0,1)$. Problem (13) can be solved by using the relative value iteration algorithm on the reformulation of this partially observed problem into a fully observed one (a technique described in [22, p. 252]), together with truncation of the belief vector (16).

V. Numerical Studies

We consider an example with parameters

$$A = \begin{bmatrix} 1.2 & 0.2 \\ 0.3 & 0.8 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 1 \end{bmatrix}, \; Q = I, \; R = 1.$$

The steady state error covariance $\bar{P}$ is easily computed as

$$\bar{P} = \begin{bmatrix} 1.3411 & -0.8244 \\ -0.8244 & 1.0919 \end{bmatrix}.$$

We consider the performance obtained by solving the infinite horizon problems (13) and (17) as β is varied, both when the eavesdropper error covariance is known and unknown. We use $p = 0.6$ and $p_e = 0.8$. In numerical solutions we use the truncated set $\mathcal{S}^N$ from (15) with $N = 10$. Fig. 2 plots the trace of the expected error covariance $\mathrm{tr}\mathbb{E}[P_{k|k}]$ vs. the expected information $\mathbb{E}[I_{e,k}]$ revealed to the eavesdropper, with

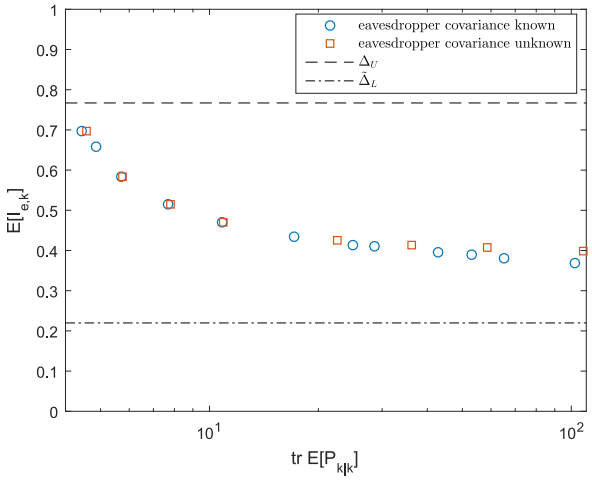

Fig. 2. Expected error covariance at estimator vs expected information revealed to eavesdropper.

$\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathbb{E}[I_{e,k}]$ obtained by taking the time average of a single Monte Carlo run of length 1000000. The upper and lower bounds Δ_U and $\tilde{\Delta}_L$ from Theorems 1 and 2 are also shown. We observe a tradeoff between $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathbb{E}[I_{e,k}]$. Furthermore, as predicted by our result in Theorem 2, the expected information revealed to the eavesdropper is always lower bounded away from zero.

VI. Conclusion

Remote estimation in the presence of eavesdroppers has been recently studied from the viewpoint of keeping the estimation error covariance at the eavesdropper large. In this note, we have considered an alternative notion of security based on the amount of information revealed to the eavesdropper, and bounds on the information revealed have been derived. Our main result shows that for the class of policies considered, if one wishes to keep the expected error covariance bounded, then one must unavoidably reveal a non-zero expected amount of information to the eavesdropper.

Appendix A
Proof of Lemma 1

We will show that $g(N) - g(N+1) \geq 0, \forall N \in \mathbb{N}$. We have

$$g(N) - g(N+1) = \frac{(N+1)\log\det f^N(\bar{P}) - N\log\det f^{N+1}(\bar{P}) - \log\det\bar{P}}{2N(N+1)}$$

and so it suffices to show that

$$\log \frac{(\det f^N(\bar{P}))^{N+1}}{(\det f^{N+1}(\bar{P}))^N \det\bar{P}} \geq 0$$

We now note the following identity [24, Th. 18.1.1], which is also known as the matrix determinant lemma:

$$\det(R + STU) = \det(T^{-1} + UR^{-1}S)\det(R)\det(T),$$

which holds provided the square matrices R and T are invertible. By making repeated use of this identity, we have

$$\begin{aligned}
&\log \frac{(\det f^N(\bar{P}))^{N+1}}{(\det f^{N+1}(\bar{P}))^N \det \bar{P}} \\
&= \log \frac{(\det f^N(\bar{P}))^{N+1}}{(\det(Af^N(\bar{P})A^T + Q))^N \det \bar{P}} \\
&= \log \frac{\det f^N(\bar{P})}{(\det((f^N(\bar{P}))^{-1} + A^T Q^{-1} A) \det Q)^N \det \bar{P}} \\
&= \log \frac{\left(\prod_{n=1}^N \det((f^{N-n}(\bar{P}))^{-1} + A^T Q^{-1} A)\right) \det \bar{P} (\det Q)^N}{(\det((f^N(\bar{P}))^{-1} + A^T Q^{-1} A) \det Q)^N \det \bar{P}} \\
&= \log \frac{\prod_{n=1}^N \det((f^{N-n}(\bar{P}))^{-1} + A^T Q^{-1} A)}{(\det((f^N(\bar{P}))^{-1} + A^T Q^{-1} A))^N}
\end{aligned}$$

From the ordering (8), we have that

$$(f^{N-n}(\bar{P}))^{-1} + A^T Q^{-1} A \geq (f^N(\bar{P}))^{-1} + A^T Q^{-1} A$$

for $n = 1, \ldots, N$, and the result then follows.

Appendix B
Proof of Lemma 3

We have

$$\begin{aligned}
g(N) &= \frac{1}{2N}\Bigg[\log\det\left(A^N \bar{P} A^{N\top} + \sum_{m=0}^{N-1} A^m Q A^{m\top}\right) \\
&\qquad - \log\det \bar{P}\Bigg] \\
&\geq \frac{1}{2N}\Big[\log\det\Big(\lambda_{\min}(\bar{P}) A^N A^{N\top} + Q\Big) - \log\det \bar{P}\Big].
\end{aligned}$$

We also have

$$\lambda_{\max}(A^N A^{N\top}) = \sigma^2_{\max}(A^{N\top}) \geq |\lambda_{\max}(A^{N\top})|^2 = |\lambda_{\max}(A)|^{2N}$$

where the inequality follows from, e.g., [25, p. 347]. By Weyl's Theorem, the largest eigenvalue of $\lambda_{\min}(\bar{P}) A^N A^{N\top} + Q$ will be strictly greater than $\lambda_{\min}(\bar{P})|\lambda_{\max}(A)|^{2N}$, and the remaining eigenvalues of $\lambda_{\min}(\bar{P}) A^N A^{N\top} + Q$ will be larger than $\lambda_{\min}(Q)$. Recalling that n_x is the dimension of x_k, we thus have

$$\begin{aligned}
g(N) &\geq \frac{1}{2N}\Big[\log \prod_i \lambda_i\Big(\lambda_{\min}(\bar{P}) A^N A^{N\top} + Q\Big) - \log\det \bar{P}\Big] \\
&> \frac{1}{2N}\Big[\log\Big(\lambda_{\min}(\bar{P})|\lambda_{\max}(A)|^{2N} \lambda_{\min}^{n_x - 1}(Q)\Big) - \log\det \bar{P}\Big] \\
&= \log(|\lambda_{\max}(A)|) \\
&\quad + \frac{1}{2N}\Big[\log\Big(\lambda_{\min}(\bar{P}) \lambda_{\min}^{n_x - 1}(Q)\Big) - \log\det \bar{P}\Big].
\end{aligned}$$

Let N' be sufficiently large that

$$g(N') > \log(|\lambda_{\max}(A)|) \triangleq \Delta_L,$$

Then we have

$$g(N) > \Delta_L \tag{18}$$

for all $N \geq N'$. By making use of Lemma 1, (18) will also hold for all $N \leq N'$, and hence (18) holds for all $n \in \mathbb{N}$.

References

[1] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin, "Special issue on secure communications via physical-layer and information-theoretic techniques," *Proc. IEEE*, vol. 103, no. 10, pp. 1698–1701, Oct. 2015.

[2] X. Zhou, L. Song, and Y. Zhang, Eds., *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2014.

[3] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 273–289, Jun. 2008.

[4] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO Gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[5] X. Guo, A. S. Leong, and S. Dey, "Estimation in wireless sensor networks with security constraints," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 53, no. 2, pp. 544–561, Apr. 2017.

[6] C. Göken and S. Gezici, "ECRB based optimal parameter encoding under secrecy constraints," *IEEE Trans. Signal Process.*, vol. 66, no. 13, pp. 3556–3570, Jul. 2018.

[7] M. Wiese *et al.*, "Secure estimation for unstable systems," in *Proc. IEEE Conf. Decis. Control*, Las Vegas, NV, USA, Dec. 2016, pp. 5059–5064.

[8] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation with secrecy against eavesdroppers," in *Proc. IFAC World Congr.*, Toulouse, France, Jul. 2017, pp. 8715–8722.

[9] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper," *IEEE Trans. Autom. Control*, to be published. [Online]. Available: https://doi.org/10.1109/TAC.2018.2883246

[10] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation codes for perfect secrecy," in *Proc. IEEE Conf. Decis. Control*, Melbourne, VIC, Australia, Dec. 2017, pp. 176–181.

[11] A. S. Leong, A. Redder, D. E. Quevedo, and S. Dey, "On the use of artificial noise for secure state estimation in the presence of eavesdroppers," in *Proc. Eur. Control Conf.*, Limassol, Cyprus, Jun. 2018, pp. 325–330.

[12] J. L. Massey, "Causality, feedback and directed information," in *Proc. ISITA*, Nov. 1990, pp. 303–305.

[13] T. Tanaka, M. Skoglund, H. Sandberg, and K. H. Johansson, "Directed information and privacy loss in cloud-based control," in *Proc. ACC*, Seattle, WA, USA, May 2017, pp. 1666–1672.

[14] E. I. Silva, M. S. Derpich, and J. Østergaard, "A framework for control system design subject to average data-rate constraints," *IEEE Trans. Autom. Control*, vol. 56, no. 8, pp. 1886–1899, Aug. 2011.

[15] T. Tanaka and H. Sandberg, "SDP-based joint sensor and controller design for information-regularized optimal LQG control," in *Proc. IEEE Conf. Decis. Control*, Osaka, Japan, Dec. 2015, pp. 4486–4491.

[16] Y. Xu and J. P. Hespanha, "Estimation under uncontrolled and controlled communications in networked control systems," in *Proc. IEEE Conf. Decis. Control*, Seville, Spain, Dec. 2005, pp. 842–847.

[17] B. D. O. Anderson and J. B. Moore, *Optimal Filtering*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1979.

[18] A. S. Leong, S. Dey, and D. E. Quevedo, "Sensor scheduling in variance based event triggered estimation with packet drops," *IEEE Trans. Autom. Control*, vol. 62, no. 4, pp. 1880–1895, Apr. 2017.

[19] B. Sinopoli *et al.*, "Kalman filtering with intermittent observations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.

[20] L. Shi and H. Zhang, "Scheduling two Gauss–Markov systems: An optimal solution for remote state estimation under bandwidth constraint," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 2038–2042, Apr. 2012.

[21] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley-Intersci., 2006.

[22] D. P. Bertsekas, *Dynamic Programming and Optimal Control*, vol. 1, 3rd ed. Belmont, MA, USA: Athena Sci., 2005.

[23] L. I. Sennott, *Stochastic Dynamic Programming and the Control of Queueing Systems*. New York, NY, USA: Wiley-Intersci., 1999.

[24] D. A. Harville, *Matrix Algebra From a Statistician's Perspective*. New York, NY, USA: Springer, 1997.

[25] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2013.