Technical Notes and Correspondence

Transmission Scheduling for Remote State Estimation Over Packet Dropping Links in the Presence of an Eavesdropper

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

***Abstract*—This paper studies transmission scheduling for remote state estimation in the presence of an eavesdropper. A sensor transmits local state estimates over a packet dropping link to a remote estimator, while an eavesdropper can successfully overhear each sensor transmission with a certain probability. The objective is to determine when the sensor should transmit, in order to minimize the estimation error covariance at the remote estimator, while trying to keep the eavesdropper error covariance above a certain level. This is done by solving an optimization problem that minimizes a linear combination of the expected estimation error covariance and the negative of the expected eavesdropper error covariance. Structural results on the optimal transmission policy are derived, and shown to exhibit thresholding behavior in the estimation error covariances. In the infinite horizon situation, it is shown that with unstable systems one can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance becomes unbounded, for all eavesdropping probabilities strictly less than one.**

***Index Terms*—Eavesdropping, packet drops, state estimation.**

I. Introduction

With the ever increasing amounts of data being transmitted wirelessly, the need to protect systems from malicious agents has become increasingly important. Traditionally, information security has been studied in the context of cryptography. However, due to the often limited computational power available at the transmitters (e.g., sensors in wireless sensor networks) to implement strong encryption, as well as the increased computational power available to malicious agents, achieving security using solely cryptographic methods may not be sufficient. Thus, alternative ways to implement security using information theoretic and physical layer techniques, complementary to the traditional cryptographic approaches, have attracted significant recent interest [2].

In communications theory, the notion of information theoretic security has been around for many years, in fact dating back to the work of Shannon in the 1940s [3]. Roughly speaking, a communication system is regarded as secure in the information theoretic sense if the mutual information between the original message and what is received at the eavesdropper is either zero or becomes vanishingly small as the block length of the codewords increases [4]. The term "physical layer security" has been used to describe ways to implement information theoretic security using physical layer characteristics of the wireless channel such as fading, interference, and noise, see, e.g., [5] and [6].

Motivated in part by the ideas of physical layer security, the consideration of security issues in signal processing systems has also started to gain the attention of researchers. For a survey on works in detection and estimation in the presence of eavesdroppers, focusing particularly on detection, see [7]. In estimation problems with eavesdroppers, studies which use physical layer security ideas include [8]–[11]. The objective is to minimize the average mean squared error at the legitimate receiver, while trying to keep the mean squared error at the eavesdropper above a certain level, by using techniques such as stochastic bit flipping [8], transmit filter design [9], and power control and addition of artificial noise [10], [11].

The above works deal with estimation of either constants or i.i.d. sources. In contrast, the focus of the current paper is to consider the more general problem of state estimation of *dynamical systems* when there is an eavesdropper, where we try to achieve security by adaptively scheduling the transmissions. For unstable systems, it has recently been shown that when using uncertain wiretap channels, one can keep the estimation error of the legitimate receiver bounded while the estimation error of the eavesdropper becomes unbounded for sufficiently large coding block length [12]. In the current work, we do not assume coding, which can introduce large delays. In a similar setup to the current work, but transmitting measurements and without using feedback acknowledgements, Tsiamis *et al.* [13] derived mechanisms for keeping the expected error covariance bounded while driving the expected eavesdropper covariance unbounded, provided the reception probability is greater than the eavesdropping probability. By allowing for feedback and clever scheduling of the transmissions, in this work, we show that the same behavior can be achieved for *all* eavesdropping probabilities strictly less than one.

In information security, the two main types of attacks are generally regarded as: 1) passive attacks from eavesdroppers, and 2) active attacks such as Byzantine attacks or Denial of Service attacks. This paper is concerned with passive attacks from eavesdroppers. However, estimation and control problems in the presence of active attacks have also been studied. Works in this area include [14]–[19], just to mention a few. Another related area deals with privacy issues in estimation and control, see [20] and [21] and the references therein.

In this paper, 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. Within this setup, we consider the problem of dynamic transmission scheduling, i.e., deciding at each instant whether the sensor should transmit. We seek to minimize a linear combination of the expected error covariance at the remote estimator and the negative of the expected error covariance at the eavesdropper. This scheduling is done at the remote estimator and fed back to the sensor.

Manuscript received June 5, 2018; revised August 30, 2018; accepted November 17, 2018. Date of publication November 23, 2018; date of current version August 28, 2019. A preliminary version of parts of this work was presented at the IFAC World Congress, Toulouse, France, Jul. 2017 [1]. Recommended by Associate Editor Z. Gao. *(Corresponding author: Alex S. Leong.)*

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

D. Dolz is with the Procter & Gamble, 53879 Euskirchen, Germany (e-mail: ddolz@uji.es).

S. Dey is with the Department of Engineering Science, Uppsala University, 752 36 Uppsala, Sweden (e-mail: Subhra.Dey@signal.uu.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2018.2883246

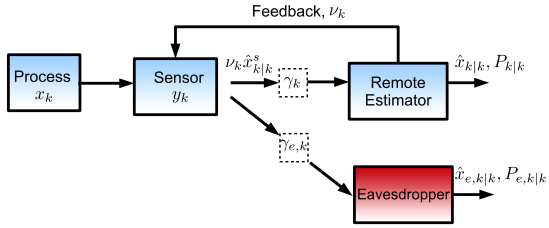

Fig. 1. Remote state estimation with an eavesdropper.

Structural results on the optimal transmission policy will be derived. In the case where knowledge of the eavesdropper's error covariances are available at the remote estimator, our results show that 1) for a fixed value of the eavesdropper's error covariance, the optimal policy has a threshold structure: the sensor should transmit if and only if the remote estimator's error covariance exceeds a certain threshold, and 2) for a fixed value of the remote estimator's error covariance, the sensor should transmit if and only if the eavesdropper's error covariance is below a certain threshold. A similar result can be derived in the case where information regarding the eavesdropper's error covariances are unavailable at the remote estimator. Such threshold policies are similar to schemes considered in event triggered estimation, e.g., [22]–[25]. Furthermore, for unstable systems, it is shown that in the infinite horizon situation there exist transmission policies that can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance is unbounded. This behavior can be achieved for all eavesdropping probabilities strictly less than one.

This paper is organized as follows. Section II describes the system model. Section III considers the case where knowledge of the eavesdropper's error covariances is available at the remote estimator, while Section IV studies the case where this information is unavailable. Numerical studies are given in Section V. Section VI draws conclusions.

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 transmits local state estimates $\hat{x}^s_{k|k}$ [26] to the remote estimator. This requires the sensor to have some computational capabilities (i.e., the sensor is "smart") to run a local Kalman filter. The local state estimates and error covariances

$$\hat{x}^s_{k|k-1} \triangleq \mathbb{E}[x_k | y_0, \ldots, y_{k-1}], \quad \hat{x}^s_{k|k} \triangleq \mathbb{E}[x_k | y_0, \ldots, y_k]$$
$$P^s_{k|k-1} \triangleq \mathbb{E}[(x_k - \hat{x}^s_{k|k-1})(x_k - \hat{x}^s_{k|k-1})^T | y_0, \ldots, y_{k-1}]$$
$$P^s_{k|k} \triangleq \mathbb{E}[(x_k - \hat{x}^s_{k|k})(x_k - \hat{x}^s_{k|k})^T | y_0, \ldots, y_k]$$

can be computed at the sensor using the standard Kalman filtering equations. We will assume that the pair (A, C) is detectable and the pair $(A, Q^{1/2})$ is stabilizable. Let $\bar{P}$ be the steady-state value of $P^s_{k|k}$ as $k \to \infty$, which exists due to the detectability assumption. To simplify the presentation, we will assume that this local Kalman filter is operating in the steady-state regime, so that $P^s_{k|k} = \bar{P}, \forall k$. In general, the local Kalman filter will converge to steady state at an exponential rate.

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 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 without error to the sensor before transmission at time k.[2]

At time instances when $\nu_k = 1$, the sensor transmits its local state estimate $\hat{x}^s_{k|k}$ over a packet dropping channel to the remote estimator. Let γ_k be random variables such that $\gamma_k = 1$ if the sensor transmission at time k is successfully received by the remote estimator, and $\gamma_k = 0$ otherwise. We will assume that $\{\gamma_k\}$ is i.i.d. Bernoulli [28] with

$$\mathbb{P}(\gamma_k = 1) = \lambda \in (0, 1).$$

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

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

The processes $\{\gamma_k\}$ and $\{\gamma_{e,k}\}$ are assumed to be mutually independent.[3]

At instances where $\nu_k = 1$, it is assumed that the remote estimator knows whether the transmission was successful or not, i.e., the remote estimator knows the value γ_k, with dropped packets discarded. Define

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

as the information set available to the remote estimator at time k. Denote the state estimates and error covariances at the remote estimator by

$$\hat{x}_{k|k-1} \triangleq \mathbb{E}[x_k | \mathcal{I}_{k-1}], \ \hat{x}_{k|k} \triangleq \mathbb{E}[x_k | \mathcal{I}_k]$$
$$P_{k|k-1} \triangleq \mathbb{E}[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})^T | \mathcal{I}_{k-1}]$$
$$P_{k|k} \triangleq \mathbb{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})^T | \mathcal{I}_k]. \tag{3}$$

Similarly, the eavesdropper knows if it has eavesdropped successfully. Define

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

as the information set available to the eavesdropper at time k, and the state estimates and error covariances at the eavesdropper by[4]

$$\hat{x}_{e,k|k-1} \triangleq \mathbb{E}[x_k | \mathcal{I}_{e,k-1}], \ \hat{x}_{e,k|k} \triangleq \mathbb{E}[x_k | \mathcal{I}_{e,k}]$$
$$P_{e,k|k-1} \triangleq \mathbb{E}[(x_k - \hat{x}_{e,k|k-1})(x_k - \hat{x}_{k|e,k-1})^T | \mathcal{I}_{e,k-1}]$$
$$P_{e,k|k} \triangleq \mathbb{E}[(x_k - \hat{x}_{e,k|k})(x_k - \hat{x}_{e,k|k})^T | \mathcal{I}_{e,k}]. \tag{4}$$

For simplicity of presentation, we will assume that the initial covariances $P_{0|0} = \bar{P}$ and $P_{e,0|0} = \bar{P}$.

As stated before, the decision variables ν_k are determined at the remote estimator and fed back to the sensor. In Section III, we consider the case where ν_k depends on both $P_{k-1|k-1}$ and $P_{e,k-1|k-1}$, while in Section IV, we consider 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. In either case, the decisions do not depend on the state x_k (or the noisy measurement y_k). Thus, the optimal

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

[2] The case of imperfect feedback links can also be handled, see [27, Sec. II-C] for details.

[3] In wireless communication experiments, it has been shown that channel fading becomes approximately independent for receivers separated by distances greater than half a wavelength of the transmitted signal [29, p. 71]. For the transmission frequencies currently in use in 3G/4G mobiles and Wi-Fi, such wavelengths are on the order of centimeters.

[4] We will assume that the eavesdropper knows the system parameters A, C, Q, R, which gives a bound on the best performance that the eavesdropper can achieve. Such an assumption is similar in spirit to Kerckhoff's principle in cryptography [30], where a cryptosystem should be secure even if the enemy knows everything about the system except the secret key.

remote estimator can be shown to have the form

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

$$P_{k|k} = \begin{cases} f(P_{k-1|k-1}), & \nu_k\gamma_k = 0 \\ \bar{P}, & \nu_k\gamma_k = 1 \end{cases} \tag{5}$$

where

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

while at the eavesdropper, the optimal estimator has the form

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

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

Define the countable set of matrices

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

where $f^n(.)$ is the n-fold composition of $f(.)$, with the convention that $f^0(X) = X$. 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. Given two symmetric matrices X and Y, we say that $X \leq Y$ if $Y - X$ is positive semidefinite, and $X < Y$ if $Y - X$ is positive definite. As shown in [31], see also [27], there is a total ordering on the elements of $\mathcal{S}$ given by

$$\bar{P} \leq f(\bar{P}) \leq f^2(\bar{P}) \leq \ldots$$

III. Eavesdropper Error Covariance Known at Remote Estimator

In this section, we consider the case where the transmission decisions ν_k can depend on the error covariances of both the remote estimator $P_{k-1|k-1}$ and the eavesdropper $P_{e,k-1|k-1}$. While knowledge of $P_{e,k-1|k-1}$ at the remote estimator may be difficult to achieve in practice, this case nevertheless serves as a useful benchmark on the achievable performance. The situation where $P_{e,k-1|k-1}$ is not known at the remote estimator will be considered in Section IV.

A. Optimal Transmission Scheduling

The approach to security taken in this paper is to minimize the expected error covariance at the remote estimator, while trying to keep the expected error covariance at the eavesdropper above a certain level.[5] To accomplish this, we will formulate a problem that minimizes a linear combination of the expected estimation error covariance and the negative of the expected eavesdropper error covariance. The problem we wish to solve is the finite horizon (of horizon K) problem

$$\min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k}] \tag{8}$$

for some $\beta \in (0,1)$.[6] The design parameter β in problem (8) controls the Pareto tradeoff between estimation performance at the remote estimator and at the eavesdropper, with a larger β placing more importance on keeping $\mathbb{E}[P_{k|k}]$ small, and a smaller β placing more importance on keeping $\mathbb{E}[P_{e,k|k}]$ large (or $-\mathbb{E}[P_{e,k|k}]$ small). We can write (8) as

$$\min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k} | P_{0,0}, P_{e,0|0}, \mathcal{I}_{k-1}, \mathcal{I}_{e,k-1}, \nu_k]\Big]$$

$$= \min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k} | P_{k-1|k-1}, P_{e,k-1|k-1}, \nu_k]\Big]$$

$$= \min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\beta(\nu_k\lambda \mathrm{tr}\bar{P} + (1-\nu_k\lambda)\mathrm{tr} f(P_{k-1|k-1}))$$

$$- (1-\beta)(\nu_k\lambda_e \mathrm{tr}\bar{P} + (1-\nu_k\lambda_e)\mathrm{tr} f(P_{e,k-1|k-1}))\Big]. \tag{9}$$

The first equality in (9) holds since $P_{k-1|k-1}$ (similarly for $P_{e,k-1|k-1}$) is a deterministic function of $P_{0|0}$ and $\mathcal{I}_{k-1}$, and $P_{k|k}$ is a function of $P_{k-1|k-1}$, ν_k, and γ_k. The second equality in (9) follows from computing the conditional expectations $\mathbb{E}[P_{k|k}|P_{k-1|k-1}, \nu_k]$ and $\mathbb{E}[P_{e,k|k}|P_{e.k-1|k-1}, \nu_k]$.

Problem (8) can be solved numerically using dynamic programing. For that purpose, define the functions $J_k(\cdot,\cdot) : \mathcal{S} \times \mathcal{S} \to \mathbb{R}$ recursively as

$$J_{K+1}(P, P_e) = 0$$

$$J_k(P, P_e) = \min_{\nu\in\{0,1\}} \Big\{\beta(\nu\lambda \mathrm{tr}\bar{P} + (1-\nu\lambda)\mathrm{tr} f(P))$$

$$- (1-\beta)(\nu\lambda_e \mathrm{tr}\bar{P} + (1-\nu\lambda_e)\mathrm{tr} f(P_e)) + \nu\lambda\lambda_e J_{k+1}(\bar{P}, \bar{P})$$

$$+ \nu\lambda(1-\lambda_e) J_{k+1}(\bar{P}, f(P_e)) + \nu(1-\lambda)\lambda_e J_{k+1}(f(P), \bar{P})$$

$$+ \big(\nu(1-\lambda)(1-\lambda_e) + 1 - \nu\big) J_{k+1}(f(P), f(P_e))\Big\} \tag{10}$$

for $k = K, \ldots, 1$. Then, problem (8) is solved by computing $J_k(P_{k-1|k-1}, P_{e,k-1|k-1})$ for $k = K, K-1, \ldots, 1$ [32, p. 23].

Remark III.1: Note that problem (8) can be solved exactly numerically since, for any horizon K, the possible values of $(P_{k|k}, P_{e,k|k})$ will lie in the finite set $\{\bar{P}, f(\bar{P}), \ldots, f^K(\bar{P})\} \times \{\bar{P}, f(\bar{P}), \ldots, f^K(\bar{P})\}$, which has finite cardinality $(K+1)^2$.

B. Structural Properties of Optimal Transmission Schedules

In this section, we will derive some structural properties on the optimal solution to problem (8). In particular, we will show that 1) for a fixed $P_{e,k-1|k-1}$, the optimal policy is to transmit if and only if $P_{k-1|k-1}$ exceeds a threshold (which in general depends on k on $P_{e,k-1|k-1}$), and 2) for a fixed $P_{k-1|k-1}$, the optimal policy is to transmit if and only if $P_{e,k-1|k-1}$ is below a threshold (which depends on k and $P_{k-1|k-1}$). Knowing that the optimal policies are of threshold-type gives insight into the form of the optimal solution, with characteristics of event triggered estimation, and can also provide computational savings when solving problem (8) via finding the thresholds numerically, see [33, Remark 4.4].

Definition III.1: A function $F(.) : \mathcal{S} \to \mathbb{R}$ is *increasing* if

$$X \leq Y \Rightarrow F(X) \leq F(Y).$$

Lemma III.2: For any $n \in \mathbb{N}$, $\mathrm{tr} f^n(P)$ is an increasing function of P.

Proof: We have

$$\mathrm{tr} f^n(P) = \mathrm{tr}\left(A^n P (A^n)^T + \sum_{m=0}^{n-1} A^m Q (A^m)^T\right)$$

which is increasing with P. ■

The following result proves some structural properties of the optimal solution. Part 1) shows that for fixed $P_{e,k-1|k-1}$, the optimal policy is to transmit if and only if $P_{k-1|k-1}$ exceeds a threshold. Part 2) shows that for fixed $P_{k-1|k-1}$, the optimal policy is to transmit if and only if $P_{e,k-1|k-1}$ is below a threshold.

[5] Similar notions have been used in [8]–[11], which studied the estimation of constant parameters or i.i.d. sources in the presence of an eavesdropper.

[6] One can also consider the equivalent problem $\min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}[\mathrm{tr} P_{k|k} - \alpha \mathrm{tr} P_{e,k|k}]$ for some $\alpha > 0$, with α being a Lagrange multiplier.

Theorem III.3: 1) For fixed $P_{e,k-1|k-1}$, the optimal solution to problem (8) is a threshold policy on $P_{k-1|k-1}$ of the form

$$\nu_k^*(P_{k-1|k-1}, P_{e,k-1|k-1}) = \begin{cases} 0, & \text{if } P_{k-1|k-1} \leq P_k^* \\ 1, & \text{otherwise} \end{cases}$$

where the threshold $P_k^* \in \mathcal{S}$ depends on k and $P_{e,k-1|k-1}$.

2) For fixed $P_{k-1|k-1}$, the optimal solution to problem (8) is a threshold policy on $P_{e,k-1|k-1}$ of the form

$$\nu_k^*(P_{k-1|k-1}, P_{e,k-1|k-1}) = \begin{cases} 0, & \text{if } P_{e,k-1|k-1} \geq P_{e,k}^* \\ 1, & \text{otherwise} \end{cases}$$

where the threshold $P_{e,k}^* \in \mathcal{S}$ depends on k and $P_{k-1|k-1}$.

Proof: See Appendix A. ∎

Remark III.4: Part 1) of Theorem III.3 is quite intuitive, and similar to threshold-based scheduling policies in event triggered estimation [23], [27]. Part 2) is perhaps less intuitive, and one should think of it as saying that it is better to not transmit when the eavesdropper covariance is high, in order to increase the eavesdropper covariance even further at the next time step. By combining parts 1) and 2) of Theorem III.3, we see that at each time k, the values of $(P_{k-1|k-1}, P_{e,k-1|k-1})$ can be divided into a "transmit" and "don't transmit" region separated by a staircase-like threshold, see Fig. 2.

C. Infinite Horizon

We now consider the infinite horizon situation. Let us first give a condition on when $\mathbb{E}[P_{k|k}]$ will be bounded. If A is stable, this is always the case. In the case where A is unstable, consider the policy with $\nu_k = 1, \forall k$, which transmits at every time instant, and is similar to the situation where local state estimates are transmitted over packet dropping links [26], [34]. From the results of [26] and [34], we have that $\mathbb{E}[P_{k|k}]$ is bounded if and only if

$$\lambda > 1 - \frac{1}{|\sigma_{\max}(A)|^2} \tag{11}$$

where $|\sigma_{\max}(A)|$ is the largest magnitude of the eigenvalues of A (i.e., the spectral radius of A). Thus, condition (11) will ensure the existence of policies, which keep $\mathbb{E}[P_{k|k}]$ bounded.

We will show in Theorem III.6 that for unstable systems, in the infinite horizon situation, there exists transmission policies that can drive the expected eavesdropper error covariance unbounded while keeping the expected estimator error covariance bounded. This can be achieved for all probabilities of successful eavesdropping λ_e strictly less than one. First, we have a preliminary result.

Lemma III.5: Suppose that A is unstable, and that $\lambda > 1 - \frac{1}{|\sigma_{\max}(A)|^2}$. Consider the threshold policy that transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$ for some $t \in \mathbb{N}$, where $f(.)$ is defined in (6). Then, $\lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{k|k}] < \infty$ for all finite $t \in \mathbb{N}$, and can be computed as

$$\lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{k|k}]$$

$$= \sum_{j=0}^{t} \frac{\lambda}{\lambda t + 1} \text{tr}(f^j(\bar{P})) + \sum_{j=t+1}^{\infty} \frac{(1-\lambda)^{j-t}\lambda}{\lambda t + 1} \text{tr}(f^j(\bar{P})).$$

Proof: This can be shown using results from [27, Section IV-C].

Theorem III.6: Suppose that A is unstable, and that $\lambda > 1 - \frac{1}{|\sigma_{\max}(A)|^2}$. Then, for any $\lambda_e < 1$, there exist transmission policies in the infinite horizon situation such that $\limsup_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{k|k}]$ is bounded and $\liminf_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{e,k|k}]$ is unbounded.

Proof: The proof is by construction of a policy with the required properties. Consider the threshold policy that transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$ for some $t \in \mathbb{N}$. By Lemma III.5, we have that for this policy $\lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{k|k}] < \infty$ for all finite $t \in \mathbb{N}$.

Now choose a horizon $K > t$. Consider the event ω where each transmission is successfully received at the remote estimator, and unsuccessfully received by the eavesdropper. Using an argument similar to [35], we will show that the contribution of this event ω will already cause the expected eavesdropper covariance to become unbounded. Now under this event ω, and using the threshold policy above, the number of transmissions that occur over the horizon K is $\lfloor K/(t+1) \rfloor$, and the eavesdropper error covariances are given by $P_{e,k|k} = f^k(\bar{P}), k = 1, \ldots, K$. By independence of the estimator and eavesdropper channels, the probability of this event occurring is $(\lambda(1-\lambda_e))^{\lfloor K/(t+1) \rfloor}$. Let ω^c denote the complement of ω. Then

$$\frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{e,k|k}]$$

$$= \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{e,k|k}|\omega] \times \mathbb{P}(\omega) + \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{e,k|k}|\omega^c] \times \mathbb{P}(\omega^c)$$

$$> \frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{e,k|k}|\omega]\mathbb{P}(\omega)$$

$$= \frac{1}{K} \sum_{k=1}^{K} \text{tr}\Big(A^k \bar{P}(A^k)^T + \sum_{m=0}^{k-1} A^m Q(A^m)^T\Big)(\lambda(1-\lambda_e))^{\lfloor K/(t+1) \rfloor}$$

$$> \frac{1}{K} \text{tr}(A^K \bar{P}(A^K)^T)(\lambda(1-\lambda_e))^{K/(t+1)}$$

$$\to \infty \text{ as } K \to \infty$$

where the last line holds if $|\sigma_{\max}(A)|(\lambda(1-\lambda_e))^{1/2(t+1)} > 1$, or equivalently if

$$\lambda_e < 1 - \frac{1}{\lambda |\sigma_{\max}(A)|^{2(t+1)}}. \tag{12}$$

Since $|\sigma_{\max}(A)| > 1$, the condition (12) will be satisfied for any $\lambda_e < 1$ when t is sufficiently large. As $\frac{1}{K} \sum_{k=1}^{K} \text{tr}\mathbb{E}[P_{k|k}]$ remains bounded for every finite $t \in \mathbb{N}$ by Lemma III.5, the result follows. ∎

In summary, the threshold policy that transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$, with t large enough that condition (12) is satisfied, will have the required properties.

Remark III.7: In a similar setup, but transmitting measurements and without using feedback acknowledgements, mechanisms were derived in [13] for making the expected eavesdropper error covariance unbounded while keeping the expected estimation error covariance bounded, under the more restrictive condition that $\lambda_e < \lambda$. In a slightly different context with coding over uncertain wiretap channels, it was shown in [12] that for unstable systems one can keep the estimation error at the legitimate receiver bounded while the eavesdropper estimation error becomes unbounded for a sufficiently large coding block length.

Remark III.8: It is perhaps instructive to give an intuitive explanation for why Theorem III.6 holds, even for instance in cases where $\lambda_e > \lambda$. The main point is that the times of transmission are not i.i.d. or some arbitrary random distribution, but cleverly scheduled based on current system information. First, the threshold policy constructed in the proof of Theorem III.6 will transmit whenever the error covariance at the remote estimator is above a threshold, thus intuitively such a policy should keep the expected estimation error covariance bounded no matter how large the threshold is set (provided condition (11) is satisfied). On the other hand, from the eavesdropper's viewpoint, by independence of the estimator and eavesdropper channels, and since the threshold policy does not depend on the eavesdropper covariances, the times at which these transmissions occur look "random" to the eavesdropper. By increasing the threshold, these "random" times of transmission will occur less and less often, until eventually the expected eavesdropper covariance becomes unbounded, and this will happen no matter how large λ_e is (as long as $\lambda_e < 1$).

Remark III.9: Condition (12) for determining a sufficiently large threshold requires knowledge of λ_e. However, the result in Theorem III.6 can still apply even without exact knowledge of λ_e. For instance, suppose we only know an upper bound on λ_e, so that $\lambda_e \leq \lambda_{e,\max}$.[7] Let t^* be the smallest t satisfying condition (12) for the true value λ_e, and t^+ be the smallest t satisfying condition (12) for $\lambda_{e,\max}$. It is easy to see that $t^+ \geq t^*$. Then, using $f^{t^+}(\bar{P})$ as the threshold, one will still have $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathrm{tr}\mathbb{E}[P_{k|k}]$ being bounded by Lemma III.5, and $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\mathrm{tr}\mathbb{E}[P_{e,k|k}]$ being unbounded, since

$$|\sigma_{\max}(A)|(\lambda(1-\lambda_e))^{1/2(t^++1)} \geq |\sigma_{\max}(A)|(\lambda(1-\lambda_e))^{1/2(t^*+1)} > 1.$$

IV. Eavesdropper Error Covariance Unknown at Remote Estimator

In order to construct $P_{e,k|k}$ at the remote estimator as per Section III, the process $\{\gamma_{e,k}\}$ for the eavesdropper's channel needs to be known, which in practice may be difficult to achieve. In this section, we consider the situation where the remote estimator knows only the probability of successful eavesdropping λ_e (see also Remark III.9) 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. We will first derive the recursion for the conditional distribution of error covariances at the remote estimator (i.e., the "belief states" [32, p. 258]), and then consider the optimal transmission scheduling problem.

A. Conditional Distribution of Error Covariances at Eavesdropper

Define the belief vector

$$\pi_{e,k} = \begin{bmatrix} \pi_{e,k}^{(0)} \\ \pi_{e,k}^{(1)} \\ \vdots \\ \pi_{e,k}^{(K)} \end{bmatrix} \triangleq \begin{bmatrix} \mathbb{P}\left(P_{e,k|k} = \bar{P}|\nu_0,\ldots,\nu_k\right) \\ \mathbb{P}\left(P_{e,k|k} = f(\bar{P})|\nu_0,\ldots,\nu_k\right) \\ \vdots \\ \mathbb{P}\left(P_{e,k|k} = f^K(\bar{P})|\nu_0,\ldots,\nu_k\right) \end{bmatrix}. \quad (13)$$

We note that by our assumption of $P_{e,0|0} = \bar{P}$, we have $\pi_{e,k}^{(K)} \triangleq \mathbb{P}(P_{e,k|k} = f^K(\bar{P})|\nu_0,\ldots,\nu_k) = 0$ for $k < K$. Denote the set of all possible $\pi_{e,k}$'s by $\Pi_e \subseteq \mathbb{R}^{K+1}$.

The vector $\pi_{e,k}$ represents our beliefs on $P_{e,k|k}$ given the transmission decisions $\nu_0,\ldots,\nu_k$. In order to formulate the transmission scheduling problem as a partially observed problem in the next section, we first want to derive a recursive relationship between $\pi_{e,k+1}$ and $\pi_{e,k}$ given the next transmission decision ν_{k+1}. When $\nu_{k+1} = 0$, we have $P_{e,k+1|k+1} = f(P_{e,k|k})$ with probability one, and thus $\pi_{e,k+1} = [\,0\ \pi_{e,k}^{(0)}\ \ldots\ \pi_{e,k}^{(K-1)}\,]^T$. When $\nu_{k+1} = 1$, then $P_{e,k+1|k+1} = \bar{P}$ with probability λ_e and $P_{e,k+1|k+1} = f(P_{e,k|k})$ with probability $1-\lambda_e$, and thus $\pi_{e,k+1} = [\,\lambda_e\ (1-\lambda_e)\pi_{e,k}^{(0)}\ \ldots\ (1-\lambda_e)\pi_{e,k}^{(K-1)}\,]^T$.

Hence, defining

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

we obtain the recursive relationship $\pi_{e,k+1} = \Phi(\pi_{e,k},\nu_{k+1})$.

[7] If we regard λ_e as a decreasing function of the distance from the sensor to the eavesdropper, upper bounding λ_e corresponds to there being no eavesdropper within a certain radius of the sensor.

B. Optimal Transmission Scheduling

We again wish to minimize a linear combination of the expected error covariance at the remote estimator and the negative of the expected error covariance at the eavesdropper. Since $P_{e,k-1|k-1}$ is not available, the optimization problem will now be formulated as a partially observed one with ν_k dependent on $(P_{k-1|k-1},\pi_{e,k-1})$. We then have the following problem [cf., (8)]:

$$\min_{\{\nu_k\}}\sum_{k=1}^{K}\mathbb{E}\Bigg[\beta(\nu_k\lambda\mathrm{tr}\bar{P} + (1-\nu_k\lambda)\mathrm{tr}f(P_{k-1|k-1})) - (1-\beta)\left(\nu_k\lambda_e\mathrm{tr}\bar{P} + (1-\nu_k\lambda_e)\sum_{i=0}^{K}\mathrm{tr}f^{i+1}(\bar{P})\pi_{e,k-1}^{(i)}\right)\Bigg]. \quad (14)$$

Problem (14) can be solved by using the dynamic programing algorithm for partially observed problems [32, p. 256]. Let the functions $\mathcal{J}_k(\cdot,\cdot) : \mathcal{S}\times\Pi_e \to \mathbb{R}$ be defined recursively as

$$\begin{aligned} &\mathcal{J}_{K+1}(P,\pi_e) = 0 \\ &\mathcal{J}_k(P,\pi_e) = \min_{\nu\in\{0,1\}}\Big\{\beta(\nu\lambda\mathrm{tr}\bar{P} + (1-\nu\lambda)\mathrm{tr}f(P)) \\ &\quad - (1-\beta)\Big(\nu\lambda_e\mathrm{tr}\bar{P} + (1-\nu\lambda_e)\sum_{i=0}^{K}\mathrm{tr}f^{i+1}(\bar{P})\pi_e^{(i)}\Big) \\ &\quad + \nu\lambda\mathcal{J}_{k+1}\big(\bar{P},\Phi(\pi_e,1)\big) + \nu(1-\lambda)\mathcal{J}_{k+1}\big(f(P),\Phi(\pi_e,1)\big) \\ &\quad + (1-\nu)\mathcal{J}_{k+1}\big(f(P),\Phi(\pi_e,0)\big)\Big\} \end{aligned} \quad (15)$$

for $k = K,\ldots,1$. Then, problem (14) is solved numerically by computing $\mathcal{J}_k(P_{k-1|k-1},\pi_{e,k-1})$ for $k = K, K-1,\ldots,1$.

Remark IV.1: In the finite horizon situation, the number of possible values of $(P_{k|k},\pi_{e,k})$ is again finite, but now of cardinality $(K+1)\times(1+2+\cdots+2^K) = (K+1)(2^{K+1}-1)$. This is exponential in K, which may be very large when K is large. To reduce the complexity, one could consider instead probability distributions

$$\begin{bmatrix} \pi_{e,k}^{(0)} \\ \pi_{e,k}^{(1)} \\ \vdots \\ \pi_{e,k}^{(N-1)} \\ \pi_{e,k}^{(N)} \end{bmatrix} \triangleq \begin{bmatrix} \mathbb{P}\left(P_{e,k|k} = \bar{P}|\nu_0,\ldots,\nu_k\right) \\ \mathbb{P}\left(P_{e,k|k} = f(\bar{P})|\nu_0,\ldots,\nu_k\right) \\ \vdots \\ \mathbb{P}\left(P_{e,k|k} = f^{N-1}(\bar{P})|\nu_0,\ldots,\nu_k\right) \\ \mathbb{P}\left(P_{e,k|k} \geq f^{N}(\bar{P})|\nu_0,\ldots,\nu_k\right) \end{bmatrix}$$

for some $N < K$, and update the beliefs via

$$\Phi^N(\pi_e,\nu) \triangleq \begin{cases} \begin{bmatrix} 0 & \pi_e^{(0)} & \ldots & \pi_e^{(N-2)} & \pi_e^{(N-1)}+\pi_e^{(N)} \end{bmatrix}^T, & \nu = 0 \\ \begin{bmatrix} \lambda_e & (1-\lambda_e)\pi_e^{(0)} & \ldots & (1-\lambda_e)\pi_e^{(N-2)} \\ (1-\lambda_e)(\pi_e^{(N-1)}+\pi_e^{(N)}) \end{bmatrix}^T, & \nu = 1. \end{cases}$$

Discretizing the space of $\pi_{e,k}$ to include the cases with up to $N-1$ successive packet drops or nontransmissions, with the remaining cases grouped into the single component $\pi_{e,k}^{(N)}$, will then give a state space of cardinality $(K+1)(2^{N+1}-1)$.

C. Structural Properties

We have the following:

Theorem IV.2: For fixed $\pi_{e,k-1}$, the optimal solution to problem (14) is a threshold policy on $P_{k-1|k-1}$ of the form

$$\nu_k^*(P_{k-1|k-1},\pi_{e,k-1}) = \begin{cases} 0, & \text{if } P_{k-1|k-1} \le P^* \\ 1, & \text{otherwise} \end{cases}$$

where the threshold P^* depends on k and $\pi_{e,k-1}$.

Proof: Denote the difference in the values of $\mathcal{J}_k(P,\pi_e)$ when the minimizing ν^* are 0 and 1 by

$$\psi_k(P,\pi_e) \triangleq \beta\lambda \mathrm{tr} f(P) - \beta\lambda \mathrm{tr}\bar{P}$$

$$-(1-\beta)\lambda_e\left(\sum_{i=0}^{K}\mathrm{tr}f^{i+1}(\bar{P})\pi_e^{(i)} - \mathrm{tr}\bar{P}\right) + \mathcal{J}_{k+1}\big(f(P),\Phi(\pi_e,0)\big)$$

$$-\lambda\mathcal{J}_{k+1}\big(\bar{P},\Phi(\pi_e,1)\big) - (1-\lambda)\mathcal{J}_{k+1}\big(f(P),\Phi(\pi_e,1)\big). \quad (16)$$

Theorem IV.2 will be proved by showing that for fixed π_e, the functions $\psi_k(P,\pi_e)$ defined by (16) are increasing functions of P for $k=1,\dots,K$. This will be the case if we can show that

$$\mathcal{J}_k\big(f(P),\Phi(\pi_e,0)\big) - (1-\lambda)\mathcal{J}_k\big(f(P),\Phi(\pi_e,1)\big)$$

is an increasing function of P for all k. Using a similar induction argument as in the proof of Theorem III.3(i), we can establish the slightly more general statement that

$$\mathcal{J}_k\big(f^n(P),\pi_e\big) - (1-\lambda)\mathcal{J}_k\big(f^n(P),\pi_e'\big)$$

is increasing in P for all k, all $n\in\mathbb{N}$ and all $\pi_e,\pi_e'\in\Pi_e$.

D. Infinite Horizon

In the infinite horizon situation, we note that Theorem III.6 will still hold, as the threshold policy constructed in the proof does not require knowledge of the eavesdropper error covariances. In addition, by Remark III.9, exact knowledge of the eavesdropping probability is also not required.

V. Numerical Studies

We consider an example involving the Pendubot, which is a two-link planar robot, see [36] and [37] for details. A linearized continuous time model for balancing the Pendubot in the "top" position can be found on [37, p. 22]. Using a sampling time of 15 ms, we can then obtain the following discrete time model:

$$A = \begin{bmatrix} 1.0058 & 0.0150 & -0.0016 & 0.0000 \\ 0.7808 & 1.0058 & -0.2105 & -0.0016 \\ -0.0060 & 0.0000 & 1.0077 & 0.0150 \\ -0.7962 & -0.0060 & 1.0294 & 1.0077 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},\ R = 0.001\times I,$$

$$Q = qq^T,\ q = \begin{bmatrix} 0.003 & 1.0000 & -0.005 & -2.150 \end{bmatrix}^T$$

where the values for the Q and R matrices are taken from [28]. The eigenvalues of A are $(1.1516, 1.0882, 0.9189, 0.8683)$. The steady-state error covariance $\bar{P}$ is easily computed as

$$\bar{P} = \begin{bmatrix} 0.0003 & 0.0077 & -0.0002 & -0.0148 \\ 0.0077 & 1.3150 & -0.0130 & -2.8174 \\ -0.0002 & -0.0130 & 0.0007 & 0.0289 \\ -0.0148 & -2.8174 & 0.0289 & 6.0613 \end{bmatrix}.$$

A. Finite Horizon

We will here solve the finite horizon problem with $K=10$. The packet reception probability is chosen to be $\lambda=0.6$, and the eavesdropping probability $\lambda_e=0.6$. Note that the condition (11) on the packet reception probability for stability at the remote estimator is $\lambda > 0.2460$. Assuming that the eavesdropper error covariance is available, and using the design parameter $\beta=0.7$, Fig. 2 plots ν_k^* for different values of $P_{k-1|k-1}=f^n(\bar{P})$ and $P_{e,k-1|k-1}=f^{n_e}(\bar{P})$, at the time step $k=4$. We observe a threshold behavior in both $P_{k-1|k-1}$ and $P_{e,k-1|k-1}$, in agreement with Theorem III.3. In general, the thresholds will be different for different times k.

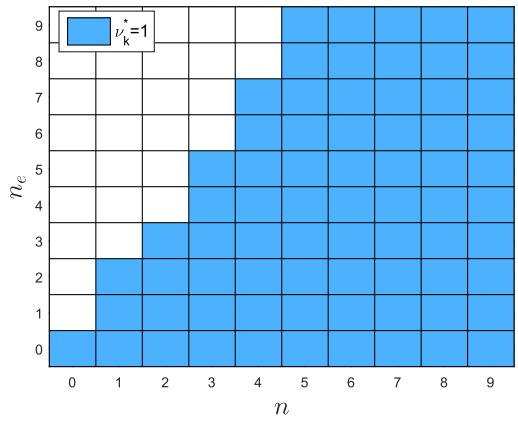

Fig. 2. ν_k^* for different values of $P_{k-1|k-1}=f^n(\bar{P})$ and $P_{e,k-1|k-1}=f^{n_e}(\bar{P})$, at time $k=4$.

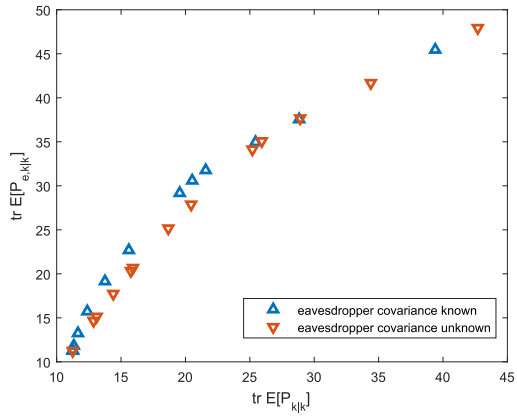

Fig. 3. Expected error covariance at estimator versus expected error covariance at eavesdropper. Finite horizon.

Next, we consider the performance as β is varied, both when the eavesdropper error covariance is known and unknown. Fig. 3 plots the trace of the expected error covariance at the estimator $\mathrm{tr}\mathbb{E}[P_{k|k}]$ versus the trace of the expected error covariance at the eavesdropper $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$. Each point is obtained by averaging over 10^5 Monte Carlo runs. We see that by varying β, we obtain a tradeoff between $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$, with the tradeoff being better when the eavesdropper error covariance is known.

B. Infinite Horizon

We next present results for the infinite horizon situation. Fig. 4 plots some values of $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$, obtained by taking the time average of a Monte Carlo run of length 10^6, using the threshold policy in the proof of Theorem III.6, which transmits at time k if and only if $P_{k-1|k-1}\ge f^t(\bar{P})$. In the case $\lambda=0.6$, $\lambda_e=0.6$, condition (12) for unboundedness of the expected eavesdropper covariance is satisfied when $t\ge 5$, and in the case $\lambda=0.6$, $\lambda_e=0.8$ (where the eavesdropping probability is higher than the packet reception probability), condition (12) is satisfied for $t\ge 7$. We see that in both cases, by using a sufficiently large t, one can make the expected error covariance of the eavesdropper very large, while keeping the expected error covariance at the estimator bounded.

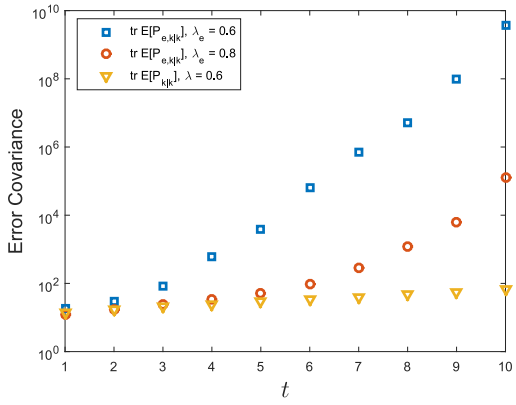

Fig. 4. Expected error covariance at estimator versus expected error covariance at eavesdropper. Infinite horizon.

VI. Conclusion

In this paper, we have studied the scheduling of sensor transmissions for remote state estimation, where each transmission can be overheard by an eavesdropper with a certain probability. The scheduling is done by solving an optimization problem that minimizes a combination of the expected error covariance at the remote estimator and the negative of the expected error covariance at the eavesdropper. We have derived structural results on the optimal transmission scheduling, which show a thresholding behavior in the optimal policies. In the infinite horizon situation, we have shown that with unstable systems, one can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance becomes unbounded. Extensions to the basic framework can also be considered, such as alternative measures of security [38] and Markovian packet drops [39].

Appendix

A. Proof of Theorem III.3

1) From the definition of $J_k(.,.)$ in (10), we know that if the minimizer $\nu^*=0$, then

$$J_k(P,P_e)=\beta\mathrm{tr}f(P)-(1-\beta)\mathrm{tr}f(P_e)+J_{k+1}(f(P),f(P_e)) \tag{17}$$

and if the minimizer $\nu^*=1$ then

$$\begin{aligned}&J_k(P,P_e)\\&=\beta(\lambda\mathrm{tr}\bar{P}+(1-\lambda)\mathrm{tr}f(P))-(1-\beta)(\lambda_e\mathrm{tr}\bar{P}+(1-\lambda_e)\mathrm{tr}f(P_e))\\&+\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})+\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e))\\&+(1-\lambda)\lambda_e J_{k+1}(f(P),\bar{P})+(1-\lambda)(1-\lambda_e)J_{k+1}(f(P),f(P_e)).\end{aligned} \tag{18}$$

Denote the difference of (17) and (18) as

$$\begin{aligned}&\phi_k(P,P_e)\\&\triangleq\beta\lambda\mathrm{tr}f(P)-\beta\lambda\mathrm{tr}\bar{P}-(1-\beta)\lambda_e\mathrm{tr}f(P_e)+(1-\beta)\lambda_e\mathrm{tr}\bar{P}\\&\quad+[1-(1-\lambda)(1-\lambda_e)]J_{k+1}(f(P),f(P_e))-\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})\\&\quad-\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e))-(1-\lambda)\lambda_e J_{k+1}(f(P),\bar{P}).\end{aligned} \tag{19}$$

Note that when $\nu_k^*=1$, i.e., the optimal decision at time k is to transmit, we have $\phi_k(P,P_e)>0$.

Since ν_k only takes on the two values 0 and 1, Theorem III.3(i) will be proved if we can show that the functions $\phi_k(P,P_e)$ defined in (19) are increasing functions of P for $k=1,\ldots,K$. As $\mathrm{tr}f(P)$ is an increasing function of P by Lemma III.2, it is sufficient to show that

$$[1-(1-\lambda)(1-\lambda_e)]J_k(f(P),f(P_e))-(1-\lambda)\lambda_e J_k(f(P),\bar{P})$$

is an increasing function of P for all k. We will prove this using induction. In order to make the induction argument work, we will prove the slightly more general statement that

$$[1-(1-\lambda)(1-\lambda_e)]J_k(f^n(P),P_e)-(1-\lambda)\lambda_e J_k(f^n(P),P_e')$$

is an increasing function of P for all k, all $n\in\mathbb{N}$ and all $P_e,P_e'\in\mathcal{S}$.

The case of $k=K+1$ is clear. Now assume that, for $P\geq P'$

$$\begin{aligned}&[1-(1-\lambda)(1-\lambda_e)]J_l(f^n(P),P_e)-(1-\lambda)\lambda_e J_l(f^n(P),P_e')\\&-[1-(1-\lambda)(1-\lambda_e)]J_l(f^n(P'),P_e)+(1-\lambda)\lambda_e J_l(f^n(P'),P_e')\\&\geq 0\end{aligned} \tag{20}$$

holds for $l=K+1,K,\ldots,k+1$. Then,

$$\begin{aligned}&[1-(1-\lambda)(1-\lambda_e)]J_k(f^n(P),P_e)-(1-\lambda)\lambda_e J_k(f^n(P),P_e')\\&-[1-(1-\lambda)(1-\lambda_e)]J_k(f^n(P'),P_e)+(1-\lambda)\lambda_e J_k(f^n(P'),P_e')\\&\geq\min_{\nu\in\{0,1\}}\Big\{[1-(1-\lambda)(1-\lambda_e)]\Big\{\beta[\nu\lambda\mathrm{tr}\bar{P}+(1-\nu\lambda)\mathrm{tr}f^{n+1}(P)]\\&\quad-(1-\beta)[\nu\lambda_e\mathrm{tr}\bar{P}+(1-\nu\lambda_e)\mathrm{tr}f(P_e)]\\&\quad+\nu\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})+\nu\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e))\\&\quad+\nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P),\bar{P})\\&\quad+[\nu(1-\lambda)(1-\lambda_e)+(1-\nu)]J_{k+1}(f^{n+1}(P),f(P_e))\Big\}\\&-(1-\lambda)\lambda_e\Big\{\beta[\nu\lambda\mathrm{tr}\bar{P}+(1-\nu\lambda)\mathrm{tr}f^{n+1}(P)]\\&\quad-(1-\beta)[\nu\lambda_e\mathrm{tr}\bar{P}+(1-\nu\lambda_e)\mathrm{tr}f(P_e')]\\&\quad+\nu\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})+\nu\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e'))\\&\quad+\nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P),\bar{P})\\&\quad+[\nu(1-\lambda)(1-\lambda_e)+(1-\nu)]J_{k+1}(f^{n+1}(P),f(P_e'))\Big\}\\&-[1-(1-\lambda)(1-\lambda_e)]\Big\{\beta[\nu\lambda\mathrm{tr}\bar{P}+(1-\nu\lambda)\mathrm{tr}f^{n+1}(P')]\\&\quad-(1-\beta)[\nu\lambda_e\mathrm{tr}\bar{P}+(1-\nu\lambda_e)\mathrm{tr}f(P_e)]\\&\quad+\nu\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})+\nu\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e))\\&\quad+\nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P'),\bar{P})\\&\quad+[\nu(1-\lambda)(1-\lambda_e)+(1-\nu)]J_{k+1}(f^{n+1}(P'),f(P_e))\Big\}\\&+(1-\lambda)\lambda_e\Big\{\beta[\nu\lambda\mathrm{tr}\bar{P}+(1-\nu\lambda)\mathrm{tr}f^{n+1}(P')]\\&\quad-(1-\beta)[\nu\lambda_e\mathrm{tr}\bar{P}+(1-\nu\lambda_e)\mathrm{tr}f(P_e')]\\&\quad+\nu\lambda\lambda_e J_{k+1}(\bar{P},\bar{P})+\nu\lambda(1-\lambda_e)J_{k+1}(\bar{P},f(P_e'))\\&\quad+\nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P'),\bar{P})\\&\quad+[\nu(1-\lambda)(1-\lambda_e)+(1-\nu)]J_{k+1}(f^{n+1}(P'),f(P_e'))\Big\}\Big\}\\&=\min_{\nu\in\{0,1\}}\Big\{[1-(1-\lambda)(1-\lambda_e)]\Big\{\beta(1-\nu\lambda)\mathrm{tr}f^{n+1}(P)\\&\quad+\nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P),\bar{P})\\&\quad+[\nu(1-\lambda)(1-\lambda_e)+(1-\nu)]J_{k+1}(f^{n+1}(P),f(P_e))\Big\}\\&-(1-\lambda)\lambda_e\Big\{\beta(1-\nu\lambda)\mathrm{tr}f^{n+1}(P)\end{aligned}$$

$$
\begin{aligned}
&+ \nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P), \bar{P}) \\
&+ [\nu(1-\lambda)(1-\lambda_e) + (1-\nu)] J_{k+1}(f^{n+1}(P), f(P'_e))\Big\} \\
&- [1-(1-\lambda)(1-\lambda_e)]\Big\{\beta(1-\nu\lambda)\mathrm{tr} f^{n+1}(P') \\
&+ \nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P'), \bar{P}) \\
&+ [\nu(1-\lambda)(1-\lambda_e) + (1-\nu)] J_{k+1}(f^{n+1}(P'), f(P_e))\Big\} \\
&+ (1-\lambda)\lambda_e\Big\{\beta(1-\nu\lambda)\mathrm{tr} f^{n+1}(P') \\
&+ \nu(1-\lambda)\lambda_e J_{k+1}(f^{n+1}(P'), \bar{P}) \\
&+ [\nu(1-\lambda)(1-\lambda_e) + (1-\nu)] J_{k+1}(f^{n+1}(P'), f(P'_e))\Big\} \\
&\geq 0
\end{aligned}
$$

where the last inequality holds (for both cases $\nu^* = 0$ and $\nu^* = 1$) by Lemma III.2 and the induction hypothesis (20).

2) As $-\mathrm{tr} f(P_e)$ is a decreasing function of P_e, it is now sufficient to show that

$$[1-(1-\lambda)(1-\lambda_e)] J_k(f(P), f(P_e)) - \lambda(1-\lambda_e) J_k(\bar{P}, f(P_e))$$

is a decreasing function of P_e for all k. Using similar techniques as in the proof of part 1), we can prove by induction the slightly more general statement that

$$[1-(1-\lambda)(1-\lambda_e)] J_k(P, f^n(P_e)) - \lambda(1-\lambda_e) J_k(P', f^n(P_e))$$

is a decreasing function of P_e for all k, all $n \in \mathbb{N}$ and all $P, P' \in \mathcal{S}$. The details are omitted for brevity.

REFERENCES

[1] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "On remote state estimation in the presence of an eavesdropper," in *Proc. IFAC World Congr.*, Toulouse, France, Jul. 2017, pp. 7600–7605.

[2] 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.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

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

[7] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 40–46, Jun. 2015.

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

[9] 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.

[10] 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.

[11] X. Guo, A. S. Leong, and S. Dey, "Distortion outage minimization in distributed estimation with estimation secrecy outage constraints," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 3, no. 1, pp. 12–28, Mar. 2017.

[12] M. Wiese, K. H. Johansson, T. J. Oechtering, P. Papadimitratos, H. Sandberg, and M. Skoglund, "Secure estimation for unstable systems," in *Proc. IEEE Conf. Decis. Control*, Las Vegas, NV, USA, Dec. 2016, pp. 5059–5064.

[13] 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.

[14] Y. Liu, P. Ling, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, May 2011.

[15] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[16] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[17] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1145–1151, Apr. 2015.

[18] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *Proc. Am. Control Conf.*, Chicago, IL, USA, Jul. 2015, pp. 195–200.

[19] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

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

[21] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny , S. Mitra, and G. J. Pappas, "Differential privacy in control and network systems," in *Proc. IEEE Conf. Decis. Control*, Las Vegas, NV, USA, Dec. 2016, pp. 4252–4272.

[22] L. Li, M. Lemmon, and X. Wang, "Event-triggered state estimation in vector linear processes," in *Proc. Am. Control Conf.*, Baltimore, MD, USA, Jun. 2010, pp. 2138–2143.

[23] S. Trimpe and R. D'Andrea, "Event-based state estimation with variance-based triggering," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3266–3281, Dec. 2014.

[24] J. Wu, Q.-S. Jia, K. H. Johansson, and L. Shi, "Event-based sensor data scheduling: Trade-off between communication rate and estimation quality," *IEEE Trans. Autom. Control*, vol. 58, no. 4, pp. 1041–1046, Apr. 2013.

[25] M. Xia, V. Gupta, and P. J. Antsaklis, "Networked state estimation over a shared communication medium," *IEEE Trans. Autom. Control*, vol. 62, no. 4, pp. 1729–1741, Apr. 2017.

[26] 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.

[27] 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.

[28] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry, "Foundations of control and estimation over lossy networks," *Proc. IEEE*, vol. 95, no. 1, pp. 163–187, Jan. 2007.

[29] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[30] C. Paar and J. Pelzl, *Understanding Cryptography*. Heidelberg, Germany: Springer, 2010.

[31] 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.

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

[33] A. S. Leong, S. Dey, and D. E. Quevedo, "Transmission scheduling for remote state estimation and control with an energy harvesting sensor," *Automatica*, vol. 91, pp. 54–60, 2018.

[34] L. Schenato, "Optimal estimation in networked control systems subject to random delay and packet drop," *IEEE Trans. Autom. Control*, vol. 53, no. 5, pp. 1311–1317, Jun. 2008.

[35] L. Shi, M. Epstein, A. Tiwari, and R. M. Murray, "Estimation with information loss: Asymptotic analysis and error bounds," in *Proc. IEEE Conf. Decis. Control*, Seville, Spain, Dec. 2005, pp. 1215–1221.

[36] M. W. Spong and D. J. Block, "The Pendubot: A mechatronic system for control research and education," in *Proc. IEEE Conf. Decis. Control*, New Orleans, LA, USA, Dec. 1995, pp. 555–556.

[37] D. J. Block, "Mechanical design and control of the Pendubot," M.S. thesis, , Univ. Illinois, Peoria, IL, USA, 1996.

[38] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Remote state estimation over packet dropping links in the presence of an eavesdropper," 2017. [Online]. Available: https://arxiv.org/abs/1702.02785

[39] A. S. Leong, D. E. Quevedo, and S. Dey, "State estimation over Markovian packet dropping links in the presence of an eavesdropper," in *Proc. 56th Annu. IEEE Conf. Decis. Control*, Melbourne, Australia, Dec. 2017, pp. 6616–6621.