Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 7339–7344

On Remote State Estimation in the Presence of an Eavesdropper

Alex S. Leong * **Daniel E. Quevedo** * **Daniel Dolz** ** **Subhrakanti Dey** ***

* *Department of Electrical Engineering (EIM-E), Paderborn University, Paderborn, Germany (e-mail: alex.leong@upb.de, dquevedo@ieee.org).*

** *Procter & Gamble, Germany. (e-mail: ddolz@uji.es).*

*** *Department of Engineering Science, Uppsala University, Uppsala, Sweden (e-mail: Subhra.Dey@signal.uu.se)*

Abstract: This paper studies a remote state estimation problem in the presence of an eavesdropper. A sensor transmits local state estimates over a packet dropping link to a remote estimator, which at the same time can be overheard by an eavesdropper 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 behaviour 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.

1. INTRODUCTION

With the ever increasing amounts of data being transmitted wirelessly, the need to protect systems from malicious intruders has become increasingly important. In communications, the notion of information theoretic security dates back to the work of Claude Shannon in the 1940s. 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 (Wyner (1975)). 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. Liang et al. (2008); Zhou et al. (2014).

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. In estimation problems with eavesdroppers, studies include Aysal and Barner (2008); Reboredo et al. (2013); Guo et al. (2017b,a). 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 (Aysal and Barner (2008)), transmit filter design (Reboredo et al. (2013)), and power control (Guo et al. (2017b), Guo et al. (2017a)). The above works deal with estimation of either constants or i.i.d. sources. In contrast, the current paper considers state estimation of *dynamical systems* when there is an eavesdropper. 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 a sufficiently large coding block length (Wiese et al. (2016)). In this paper we are interested primarily in estimation performance, and as such 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. (2016) 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, in this paper we show that the same behaviour can be achieved for all eavesdropping probabilities strictly less than one. The current work deals with passive attacks from eavesdroppers. Estimation and control problems in the presence of active attacks has also been studied, see e.g. Fawzi et al. (2014); Teixeira et al. (2015); Mo and Sinopoli (2015); Li et al. (2017), just to mention a few.

In this paper, we consider a scenario where 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. Within this setup, we consider the problem of deciding at each instant whether the sensor should transmit, in order 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. The scheduling is done at

2405-8963 © 2017, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2017.08.1482

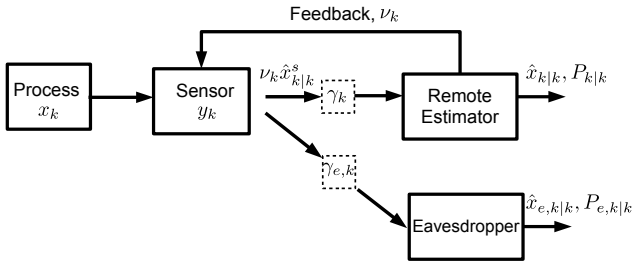

Fig. 1. Remote State Estimation with an Eavesdropper

the remote estimator. We derive structural results on the optimal transmission policy, which are shown to exhibit thresholding behaviour in the estimation error covariances. In addition, in the infinite horizon situation, we show that with unstable systems one can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance becomes unbounded.

2. 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 $x_k \in \mathbb{R}^n$ 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 $y_k \in \mathbb{R}^n$ and v_k is Gaussian with zero mean and covariance $R > 0$. The noise processes $\{w_k\}$ and $\{v_k\}$ are assumed to be mutually independent.

The sensor transmits local state estimates $\hat{x}^s_{k|k}$ to the remote estimator (Xu and Hespanha (2005)). The local state estimates and error covariances

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

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 the 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, and then fed back to the sensor.

[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. Given two symmetric matrices X and Y, we say that $X \leq Y$ if $Y - X$ is positive semi-definite, and $X < Y$ if $Y - X$ is positive definite.

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 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.

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

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

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

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

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

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

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

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

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 3 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 4 we consider the case where ν_k depends only on $P_{k-1|k-1}$ and our beliefs 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. Thus the optimal remote estimator can be shown to have the form

$$\begin{aligned}
\hat{x}_{k|k} &= \begin{cases} A\hat{x}_{k-1|k-1} & ,\ \nu_k\gamma_k = 0\\ \hat{x}^s_{k|k} & ,\ \nu_k\gamma_k = 1 \end{cases}\\
P_{k|k} &= \begin{cases} f(P_{k-1|k-1}) & ,\ \nu_k\gamma_k = 0\\ \bar{P} & ,\ \nu_k\gamma_k = 1 \end{cases}
\end{aligned} \tag{4}$$

where

$$f(X) \triangleq AXA^T + Q, \tag{5}$$

while at the eavesdropper the 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:

$$\mathcal{S} \triangleq \{\bar{P}, f(\bar{P}), f^2(\bar{P}), \dots\}, \tag{6}$$

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. There is a total ordering on the elements of $\mathcal{S}$ given by (see e.g. Shi and Zhang (2012))

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

3. 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.

3.1 Optimal Transmission Scheduling

Our approach to security 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.[2] To accomplish this, we consider the following finite horizon (of horizon K) problem which minimizes a linear combination of the expected estimator error covariance and the negative of the expected eavesdropper error covariance:

$$\begin{aligned}
&\min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k}] \\
&= \min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k} \\
&\qquad\qquad |P_{0,0}, P_{e,0|0}, \mathcal{I}_{k-1}, \mathcal{I}_{e,k-1}, \nu_k]\Big] \\
&= \min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\mathbb{E}[\beta \mathrm{tr} P_{k|k} - (1-\beta)\mathrm{tr} P_{e,k|k} \\
&\qquad\qquad |P_{k-1,k-1}, P_{e,k-1,k-1}, \nu_k]\Big] \\
&= \min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\beta(\nu_k\lambda \mathrm{tr}\bar{P} + (1-\nu_k\lambda)\mathrm{tr} f(P_{k-1|k-1})) \\
&\quad - (1-\beta)(\nu_k\lambda_e \mathrm{tr}\bar{P} + (1-\nu_k\lambda_e)\mathrm{tr} f(P_{e,k-1|k-1}))\Big],
\end{aligned} \tag{7}$$

for some $\beta \in (0,1)$. The second equality in (7) 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 third equality in (7) comes from computing the conditional expectations $\mathbb{E}[P_{k|k}|P_{k-1|k-1}, \nu_k]$ and $\mathbb{E}[P_{e,k|k}|P_{e.k-1|k-1}, \nu_k]$. The design parameter β in problem (7) controls the tradeoff between estimation performance at the remote estimator and the eavesdropper. Problem (7) can be solved numerically using dynamic programming. Define the functions $J_k(\cdot,\cdot) : \mathcal{S} \times \mathcal{S} \to \mathbb{R}$ recursively as:

$$\begin{aligned}
&J_{K+1}(P, P_e) = 0 \\
&J_k(P, P_e) = \min_{\nu\in\{0,1\}} \Big\{\beta(\nu\lambda \mathrm{tr}\bar{P} + (1-\nu\lambda)\mathrm{tr} f(P)) \\
&\quad - (1-\beta)(\nu\lambda_e \mathrm{tr}\bar{P} + (1-\nu\lambda_e)\mathrm{tr} f(P_e)) \\
&\quad + \nu\lambda\lambda_e J_{k+1}(\bar{P}, \bar{P}) + \nu\lambda(1-\lambda_e) J_{k+1}(\bar{P}, f(P_e)) \\
&\quad + \nu(1-\lambda)\lambda_e J_{k+1}(f(P), \bar{P}) \\
&\quad + \big(\nu(1-\lambda)(1-\lambda_e) + 1 - \nu\big) J_{k+1}(f(P), f(P_e))\Big\}
\end{aligned} \tag{8}$$

for $k = K, \dots, 1$. Then problem (7) is solved by computing $J_k(P_{k-1|k-1}, P_{e,k-1|k-1})$ for $k = K, K-1, \dots, 1$.

Remark 1. Note that problem (7) can be solved exactly since, for any horizon K, the possible values of $(P_{k|k}, P_{e,k|k})$ will lie in the finite set $\{\bar{P}, f(\bar{P}), \dots, f^K(\bar{P})\} \times \{\bar{P}, f(\bar{P}), \dots, f^K(\bar{P})\}$, which has cardinality $(K+1)^2$.

3.2 Structural Properties of Optimal Transmission Schedule

In this subsection we will prove some structural properties on the optimal solution to problem (7). In particular, we will show that 1) for a fixed $P_{e,k-1|k-1}$, the optimal policy is to only transmit 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 provides insight into the form of the optimal solution, and can also provide computational savings when solving problem (7) numerically, see Krishnamurthy (2016).

Theorem 1. (i) For fixed $P_{e,k-1|k-1}$, the optimal solution to problem (7) 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 $P_{e,k-1|k-1}$. (ii) For fixed $P_{k-1|k-1}$, the optimal solution to problem (7) 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 Due to paper length restrictions, the proof is omitted, but may be found in Leong et al. (2017b). ■

Remark 2. The actual values of the thresholds P_k^* and $P_{e,k}^*$ in general needs to be found numerically.

3.3 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

[2] Similar notions have been used in Aysal and Barner (2008); Reboredo et al. (2013); Guo et al. (2017b,a), which studied the estimation of constant parameters or i.i.d sources in the presence of an eavesdropper.

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 (Schenato (2008); Xu and Hespanha (2005)). From the results of Xu and Hespanha (2005) and Schenato (2008) we have that $\mathbb{E}[P_{k|k}]$ is bounded if and only if

$$\lambda > 1 - \frac{1}{|\sigma_{\max}(A)|^2}, \tag{9}$$

where $|\sigma_{\max}(A)|$ is the largest magnitude of the eigenvalues of A (i.e. the spectral radius of A). Thus condition (9) will ensure the existence of policies which keep $\mathbb{E}[P_{k|k}]$ bounded.

We will now show that for unstable systems, in the infinite horizon situation, there exists transmission policies which can make 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.

Theorem 2. 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 $\limsup_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{k|k}]$ is bounded and $\liminf_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}]$ is unbounded.

Proof The proof is by construction of a policy with the required properties. Consider the threshold policy which transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$ for some $t \in \mathbb{N}$. Since $\lambda > 1 - \frac{1}{|\sigma_{\max}(A)|^2}$, one can show using results from Section IV-C of Leong et al. (2017a) that $\lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{k|k}] < \infty$ for any $t \in \mathbb{N}$.

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 Shi et al. (2005), we will show that the contribution of this event ω will already cause the expected eavesdropper covariance to become unbounded. Under this event, 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 $P_{e,k|k} = f^k(\bar{P}), k = 1, \ldots, K$. 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 we have

$$\begin{aligned}
&\frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}] \\
&= \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}|\omega]\times\mathbb{P}(\omega) + \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}|\omega^c]\times\mathbb{P}(\omega^c) \\
&> \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}|\omega]\mathbb{P}(\omega) \\
&= \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\Big(A^k\bar{P}(A^k)^T + \sum_{m=0}^{k-1} A^m Q (A^m)^T\Big) \\
&\qquad \times (\lambda(1-\lambda_e))^{\lfloor K/(t+1) \rfloor} \\
&> \frac{1}{K}\mathrm{tr}(A^K\bar{P}(A^K)^T)(\lambda(1-\lambda_e))^{K/(t+1)} \\
&\to \infty \text{ as } K \to \infty,
\end{aligned}$$

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

$$\lambda_e < 1 - \frac{1}{\lambda|\sigma_{\max}(A)|^{2(t+1)}}. \tag{10}$$

Since $|\sigma_{\max}(A)| > 1$, the condition (10) will be satisfied for any $\lambda_e < 1$ when t is sufficiently large. As $\frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{k|k}]$ remains bounded for every $t \in \mathbb{N}$, the result follows. ■

In summary, the threshold policy which transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$, with t large enough that condition (10) is satisfied, will have the required properties.

Remark 3. In a similar setup but transmitting measurements and without using feedback acknowledgements, mechanisms were derived in Tsiamis et al. (2016) 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 different context with coding over uncertain wiretap channels, it was shown in Wiese et al. (2016) 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.

4. EAVESDROPPER ERROR COVARIANCE UNKNOWN AT REMOTE ESTIMATOR

In order to construct $P_{e,k|k}$ at the remote estimator, 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 and not the actual realizations $\gamma_{e,k}$. Thus the transmit decisions ν_k can only depend on $P_{k-1|k-1}$, and on 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"), and then consider the optimal transmission scheduling problem.

4.1 Conditional Distribution of Error Covariances at Eavesdropper

Define

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

We note that $\pi_{e,k}^{(K)} \triangleq \mathbb{P}\big(P_{e,k|k} = f^K(\bar{P})|\nu_0, \ldots, \nu_k\big) = 0$ 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 $\nu_0, \ldots, \nu_k$. We want to derive a recursive relationship between $\pi_{e,k+1}$ and $\pi_{e,k}$ given the next transmission decision ν_{k+1}. When $\nu_{k+1} = 0$, then $P_{e,k+1|k+1} = f(P_{e,k|k})$, and thus $\pi_{e,k+1} =$

$\begin{bmatrix} 0 & \pi_{e,k}^{(0)} & \dots & \pi_{e,k}^{(K-1)} \end{bmatrix}^T$. 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

$$\pi_{e,k+1} = \begin{bmatrix} \lambda_e & (1-\lambda_e)\pi_{e,k}^{(0)} & \dots & (1-\lambda_e)\pi_{e,k}^{(K-1)} \end{bmatrix}^T.$$

Hence, defining

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

we obtain the recursive relationship

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

4.2 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 problem with ν_k dependent on $(P_{k-1|k-1}, \pi_{e,k-1})$. We then have the following problem (c.f. (7)):

$$\min_{\{\nu_k\}} \sum_{k=1}^{K} \mathbb{E}\Big[\beta(\nu_k \lambda \mathrm{tr}\bar{P} + (1-\nu_k\lambda)\mathrm{tr}f(P_{k-1|k-1})) - (1-\beta)\Big(\nu_k\lambda_e \mathrm{tr}\bar{P} + (1-\nu_k\lambda_e)\sum_{i=0}^{K} \mathrm{tr}f^{i+1}(\bar{P})\pi_{e,k-1}^{(i)}\Big)\Big]. \tag{11}$$

4.3 Structural Properties

The following result can be proved using similar techniques as in the proof of Theorem 1.

Theorem 3. For fixed $\pi_{e,k-1}$, the optimal ν_k^* to problem (11) is a threshold policy on $P_{k-1|k-1}$ of the form

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

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

4.4 Infinite Horizon

In the infinite horizon situation, we note that Theorem 2 will still hold, as the threshold policy constructed in the proof does not require knowledge of the eavesdropper error covariances.

5. 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

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

The packet reception probability is chosen to be $\lambda = 0.6$, and the eavesdropping probability $\lambda_e = 0.6$.

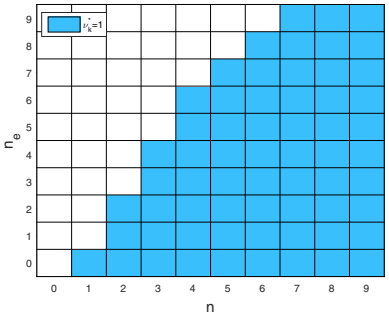

Fig. 2. ν_k^* for different values of $P_{k-1|k-1} = f^n(\bar{P})$ and $P_{e,k-1|k-1} = f^{n_e}(\bar{P})$, at time $k = 4$.

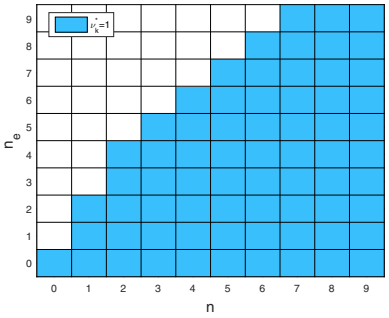

Fig. 3. ν_k^* for different values of $P_{k-1|k-1} = f^n(\bar{P})$ and $P_{e,k-1|k-1} = f^{n_e}(\bar{P})$, at time $k = 6$.

5.1 Finite Horizon

We will here solve the finite horizon problems (7) and (11) with $K = 10$. For problem (7), 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 $k = 4$. Fig. 3 plots ν_k^* at the time step $k = 6$. We observe a threshold behaviour in both $P_{k-1|k-1}$ and $P_{e,k-1|k-1}$, with the thresholds also dependent on the time k, in agreement with Theorem 1.

Next, we consider the performance as β is varied, both when the eavesdropper error covariance is known and unknown. Fig. 4 plots the trace of the expected error covariance at the estimator $\mathrm{tr}\mathbb{E}[P_{k|k}]$ vs. the trace of the expected error covariance at the eavesdropper $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$ for various different values of β, with $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$ each obtained by averaging over 100000 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 performance being better when the eavesdropper error covariance is known.

5.2 Infinite Horizon

We next present results for the infinite horizon situation. Table 1 tabulates 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 1000000, using the threshold policy in the proof of Theorem 2 which transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$. In the case $\lambda = 0.6$, $\lambda_e = 0.6$, condition (10) for unboundedness of the expected eavesdropper covariance is satisfied when $t \geq 2$, and in the case $\lambda = 0.6$, $\lambda_e = 0.8$ (where the eavesdropping probability is higher

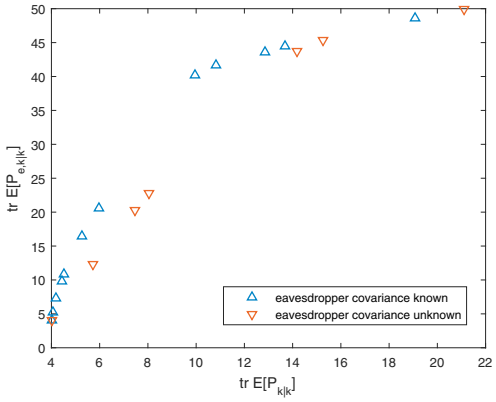

Fig. 4. Expected error covariance at estimator vs expected error covariance at eavesdropper. Finite horizon.

Table 1. Expected error covariance at estimator vs expected error covariance at eavesdropper. Infinite horizon.

	$\lambda = 0.6$, $\lambda_e = 0.6$		$\lambda = 0.6$, $\lambda_e = 0.8$	
t	$\mathrm{tr}\mathbb{E}[P_{k\|k}]$	$\mathrm{tr}\mathbb{E}[P_{e,k\|k}]$	$\mathrm{tr}\mathbb{E}[P_{k\|k}]$	$\mathrm{tr}\mathbb{E}[P_{e,k\|k}]$
1	5.59	19.49	5.32	4.66
2	7.53	523.06	7.60	14.05
3	10.76	2.82×10^5	10.67	136.06
4	15.36	1.21×10^8	15.59	2.14×10^3
5	23.57	1.19×10^{10}	23.34	1.72×10^5
6	35.07	3.68×10^{13}	35.04	6.83×10^6

than the packet reception probability), condition (10) is satisfied for $t \geq 3$. 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.

6. 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 behaviour in the optimal policies. In the infinite horizon situation, we have also shown that with unstable systems one can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance becomes unbounded.

REFERENCES

Aysal, T.C. and Barner, K.E. (2008). Sensor data cryptography in wireless sensor networks. *IEEE Trans. Inf. Forensics Security*, 3(2), 273–289.

Fawzi, H., Tabuada, P., and Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control*, 59(6), 1454–1467.

Guo, X., Leong, A.S., and Dey, S. (2017a). Distortion outage minimization in distributed estimation with estimation secrecy outage constraints. *IEEE Trans. Signal Inf. Process. Netw.*, 3(1), 12–28.

Guo, X., Leong, A.S., and Dey, S. (2017b). Estimation in wireless sensor networks with security constraints. *IEEE Trans. Aerosp. Electron. Syst.* To appear.

Krishnamurthy, V. (2016). *Partially Observed Markov Decision Processes: From Filtering to Controlled Sensing*. Cambridge University Press, Cambridge, UK.

Leong, A.S., Dey, S., and Quevedo, D.E. (2017a). Sensor scheduling in variance based event triggered estimation with packet drops. *IEEE Trans. Autom. Control*, 62(4), 1880–1895.

Leong, A.S., Quevedo, D.E., Dolz, D., and Dey, S. (2017b). Remote state estimation over packet dropping links in the presence of an eavesdropper. Available at https://arxiv.org/abs/1702.02785.

Li, Y., Quevedo, D.E., Dey, S., and Shi, L. (2017). SINR-based DoS attack on remote state estimation: A game-theoretic approach. *IEEE Trans. Control Netw. Syst.* To appear.

Liang, Y., Poor, H.V., and Shamai, S. (2008). Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6), 2470–2492.

Mo, Y. and Sinopoli, B. (2015). Secure estimation in the presence of integrity attacks. *IEEE Trans. Autom. Control*, 60(4), 1145–1151.

Reboredo, H., Xavier, J., and Rodrigues, M.R.D. (2013). Filter design with secrecy constraints: The MIMO Gaussian wiretap channel. *IEEE Trans. Signal Process.*, 61(15), 3799–3814.

Schenato, L. (2008). Optimal estimation in networked control systems subject to random delay and packet drop. *IEEE Trans. Autom. Control*, 53(5), 1311–1317.

Shi, L., Epstein, M., Tiwari, A., and Murray, R.M. (2005). Estimation with information loss: Asymptotic analysis and error bounds. In *Proc. IEEE Conf. Decision and Control*, 1215–1221. Seville, Spain.

Shi, L. and Zhang, H. (2012). Scheduling two Gauss-Markov systems: An optimal solution for remote state estimation under bandwidth constraint. *IEEE Trans. Signal Process.*, 60(4), 2038–2042.

Teixeira, A., Sou, K.C., Sandberg, H., and Johansson, K.H. (2015). Secure control systems: A quantitive risk management approach. *IEEE Control Syst. Mag.*, 35(1), 24–45.

Tsiamis, A., Gatsis, K., and Pappas, G.J. (2016). State estimation with secrecy against eavesdroppers. Available at http://arxiv.org/abs/1612.04942.

Wiese, M., Johansson, K.H., Oechtering, T.J., Papadimitratos, P., Sandberg, H., and Skoglund, M. (2016). Secure estimation for unstable systems. In *Proc. IEEE Conf. Decision and Control*, 5059–5064. Las Vegas, NV.

Wyner, A.D. (1975). The wire-tap channel. *Bell System Technical Journal*, 54(8), 1355–1387.

Xu, Y. and Hespanha, J.P. (2005). Estimation under uncontrolled and controlled communications in networked control systems. In *Proc. IEEE Conf. Decision and Control*, 842–847. Seville, Spain.

Zhou, X., Song, L., and Zhang, Y. (eds.) (2014). *Physical Layer Security in Wireless Communications*. CRC Press, Boca Raton, FL.