2017 IEEE 56th Annual Conference on Decision and Control (CDC)
December 12-15, 2017, Melbourne, Australia

State Estimation Over Markovian Packet Dropping Links in the Presence of an Eavesdropper

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

Abstract— **Remote state estimation problems in the presence of an eavesdropper have recently been studied. In this setup, a sensor transmits over a random packet dropping link to a remote estimator, which at the same time can be randomly overheard by an eavesdropper. For i.i.d. packet dropping links to the remote estimator and to the eavesdropper, it has been shown that with unstable systems one can keep the expected estimation error covariance bounded, while the expected eavesdropper error covariance becomes unbounded in the infinite horizon. In this paper we show that the same behaviour can be achieved when transmission of local state estimates occur over a Markovian packet dropping link, and eavesdropping occurs according to another Markovian packet dropping link.**

I. Introduction

Nowadays, more and more data is being transmitted wirelessly, e.g. using Wi-Fi or smartphones. Due to the broadcast nature of the wireless medium, other agents in the vicinity can often overhear what is being transmitted, and there is a need to protect systems from eavesdroppers. Traditionally, associated information security issues have been studied in the context of cryptography. However, due to the often limited computational power available at the transmitters to implement strong encryption, as well as the increased computational power available to malicious agents, achieving security using solely cryptographic methods may not necessarily 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 [1].

In information theoretic security, a communication system is regarded as secure 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 [2]. 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. [3], [4].

Motivated in part by the ideas of physical layer security, the consideration of security issues in signal processing and estimation systems has also started to gain the attention of researchers. In estimation problems with eavesdroppers, studies include [5]–[8] for estimation of constants or i.i.d. sources, and [9]–[11] for state estimation of dynamical systems.

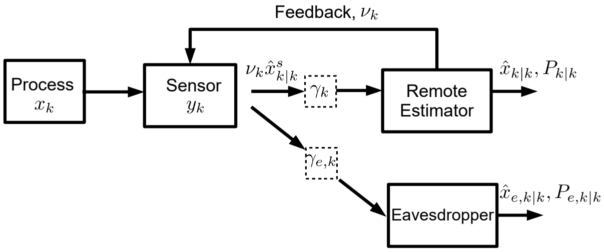

Fig. 1. Remote State Estimation with an Eavesdropper

The current paper is most closely related to [10], [11] in considering state estimation of dynamical systems. A sensor transmits to the remote estimator over a packet dropping link, which might be overheard by an eavesdropper over another packet dropping link. For i.i.d. packet drops and unstable systems, without using feedback acknowledgements mechanisms were derived in [10] for making the expected eavesdropper error covariance unbounded while keeping the expected estimation error covariance bounded, under the condition that the eavesdropping probability is less than the packet reception probability. With the use of feedback, the same behaviour can be achieved for all eavesdropping probabilities strictly less than one [11]. The current paper extends the result in [11] to correlated packet drops, in particular to Markovian packet drop channels. In a slightly different context with coding over uncertain wiretap channels, it was shown in [9] 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.

The remainder of this paper is organized as follows. Section II describes the system model. Section III presents our main results. Numerical studies are given in Section IV. Section V draws conclusions.

II. System Model

A diagram of the system model is shown in Fig. 1. We 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] There is a sensor with measurements

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

A. Leong and D. Quevedo are with the Department of Electrical Engineering (EIM-E), Paderborn University, Paderborn, Germany. E-mail: alex.leong@upb.de, dquevedo@ieee.org. S. Dey is with the Department of Engineering Science, Uppsala University, Uppsala, Sweden. E-mail: Subhra.Dey@signal.uu.se.

[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.

978-1-5090-2873-3/17/$31.00 ©2017 IEEE

where $y_k \in \mathbb{R}^n$ and v_k is Gaussian with zero mean and covariance $R > 0$. We assume the noise processes $\{w_k\}$ and $\{v_k\}$ to be mutually independent.

The sensor transmits local estimates $\hat{x}^s_{k|k}$ to the remote estimator [12]. The local 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 filter. 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. In order to simplify the subsequent presentation, the local Kalman filter will be assumed to be operating in the steady state regime, so that $P^s_{k|k} = \bar{P}, \forall k$. We note that under the assumptions stated, the local Kalman filter will in general 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. We shall focus on a situation where the decision variables ν_k are determined at the remote estimator (based on information available at time $k - 1$), and then fed back to the sensor.

Sensor transmissions occur over a temporally correlated Markovian packet dropping channel to the remote estimator. Let γ_k be random variables such that $\gamma_k = 1$ if a sensor transmission at time k is successfully received by the remote estimator, and $\gamma_k = 0$ otherwise. The process $\{\gamma_k\}$ is a time-homogeneous Markov chain, with transition probabilities (using notation similar to [13]):

$$p \triangleq \mathbb{P}(\gamma_k = 0|\gamma_{k-1} = 1), \; q \triangleq \mathbb{P}(\gamma_k = 1|\gamma_{k-1} = 0). \quad (3)$$

The sensor transmissions can be overheard by an eavesdropper over another Markovian packet dropping channel. Let $\gamma_{e,k}$ be random variables such that $\gamma_{e,k} = 1$ if a sensor transmission at time k will be overheard by the eavesdropper, and $\gamma_{e,k} = 0$ otherwise. The process $\{\gamma_{e,k}\}$ is a time-homogeneous Markov chain with

$$p_e \triangleq \mathbb{P}(\gamma_{e,k} = 0|\gamma_{e,k-1} = 1), \; q_e \triangleq \mathbb{P}(\gamma_{e,k} = 1|\gamma_{e,k-1} = 0).$$

We will assume that $p, q, p_e, q_e \in (0, 1)$, so that the stationary distributions of $\{\gamma_k\}$ and $\{\gamma_{e,k}\}$ exist. The processes $\{\gamma_k\}$ and $\{\gamma_{e,k}\}$ are also assumed to be mutually independent.[2]

At time 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:

$$\begin{aligned} \hat{x}_{k|k-1} &\triangleq \mathbb{E}[x_k|\mathcal{I}_{k-1}], \quad \hat{x}_{k|k} \triangleq \mathbb{E}[x_k|\mathcal{I}_k], \\ P_{k|k-1} &\triangleq \mathbb{E}[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})^T|\mathcal{I}_{k-1}], \\ P_{k|k} &\triangleq \mathbb{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})^T|\mathcal{I}_k]. \end{aligned} \quad (4)$$

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:

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

For simplicity of presentation, we will assume that the initial covariances $P_{0|0} = \bar{P}$ and $P_{e,0|0} = \bar{P}$, and that γ_0 and $\gamma_{e,0}$ have the stationary distributions of $\{\gamma_k\}$ and $\{\gamma_{e,k}\}$ respectively.

As previously mentioned, the transmission decisions ν_k are determined at the remote estimator and fed back to the sensor.[3] In this paper we will allow ν_k to 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, see also [11] where only i.i.d. packet drops were considered.[4] The optimal remote estimator can be shown to have the form

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

where

$$f(X) \triangleq AXA^T + Q, \quad (6)$$

while, at the eavesdropper, the estimator has the form[5]

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

Define the countable set of matrices:

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

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

[2] In wireless communications, channel fading becomes approximately independent for receivers separated by distances greater than half a wavelength of the transmitted signal [14, p.71]. For current wireless communication standards (e.g. 3G/4G, Wi-Fi), such wavelengths are on the order of centimeters.

[3] The case of imperfect feedback acknowledgements can also be handled, see Section II-C of [15].

[4] In fact, the threshold policy of Section III will only require knowledge of $P_{k-1|k-1}$.

[5] This assumes that the eavesdropper knows the system parameters A, C, Q, R. If these are unknown, then the performance at the eavesdropper will in general be worse. Such an assumption is similar to Kerckhoff's principle in cryptography [16], where a cryptosystem should be secure even if the enemy knows everything about the system except the secret key.

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. [17])

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

III. Main Results

In this paper we are interested in the case where A is unstable, i.e. the spectral radius $\rho(A) > 1$. In this section, we will show that for unstable systems, in the infinite horizon situation (or as time $k \to \infty$) there exist transmission policies which can drive the expected eavesdropper error covariance unbounded while keeping the expected estimator error covariance bounded. This can be achieved for all Markovian packet dropping channels with $p_e \in (0,1)$ and $q_e \in (0,1)$.

Similar to the scheme proposed in [11] for the case of i.i.d. packet drops, 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 $t \in \mathbb{N}$ (by (8) such a comparison can always be made). In Theorem 3.3 we show that this policy has the required properties when t is sufficiently large. In order to obtain our result, we will first analyze the performance of this policy at the remote estimator.

Define the function $g(.)$ by

$$g(x) \triangleq (1-q)x + p(1-x), \tag{9}$$

with p and q as in (3). Let $g^n(.)$ be the n-fold composition of $g(.)$, where we use the convention that $g^0(x) \triangleq x$.

Lemma 3.1: Suppose that A is unstable, and that $(1-q)\rho(A)^2 < 1$. 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 $t \in \mathbb{N}$. Under this policy, $\{P_{k|k}\}$ has a stationary distribution and as $k \to \infty$,

$$\begin{aligned}
&\lim_{K\to\infty} \frac{1}{K}\sum_{l=1}^{K} \text{tr}\mathbb{E}[P_{l|l}] = \text{tr}\mathbb{E}[P_{k|k}] \\
&= \pi_{0,1}\text{tr}\left[\bar{P} + \sum_{j=1}^{t} f^j(\bar{P}) + g^t(p)\sum_{j=t+1}^{\infty}(1-q)^{j-t-1}f^j(\bar{P})\right] \\
&< \infty
\end{aligned} \tag{10}$$

for all finite $t \in \mathbb{N}$, where

$$\pi_{0,1} = \frac{q}{q(t+1) + g^t(p)}. \tag{11}$$

Proof: See Appendix ■

Remark 3.2: The equations (10)-(11) provide an analytical expression for the performance of the threshold policy, which can be easily computed numerically.

Theorem 3.3: Suppose that A is unstable, and that $(1-q)\rho(A)^2 < 1$. Consider the threshold policy which transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$, where t is sufficiently large that

$$\rho(A)\left[\left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right)\frac{p_e}{p_e+q_e}\right]^{1/2(t+1)} > 1 \tag{12}$$

is satisfied, with $g(.)$ defined by (9). Then $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{k|k}]$ is bounded and, at the eavesdropper, $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}]$ is unbounded.

Proof: Since $(1-q)\rho(A)^2 < 1$, Lemma 3.1 shows that $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{k|k}] < \infty$ for any finite $t \in \mathbb{N}$. So it remains to show that $\lim_{K\to\infty}\frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}]$ is unbounded.

For a horizon $K > t$, consider the event ω where each transmission is successfully received at the remote estimator, and unsuccessfully received by the eavesdropper. By a similar argument to [18], we will show that the contribution of the event ω will already cause the expected eavesdropper covariance to become unbounded as $K \to \infty$. Now under this event, and using the threshold policy, the number of transmissions which occur over the horizon K is $\lfloor K/(t+1)\rfloor$. The probability that each transmission is successfully received is given by

$$\begin{aligned}
&\left(\frac{\pi_{t,0}}{\pi_{t,0}+\pi_{t,1}}q + \frac{\pi_{t,1}}{\pi_{t,0}+\pi_{t,1}}(1-p)\right)^{\lfloor K/(t+1)\rfloor} \\
&= \left(\frac{\pi_{t,0}}{\pi_{0,1}}q + \frac{\pi_{t,1}}{\pi_{0,1}}(1-p)\right)^{\lfloor K/(t+1)\rfloor} \\
&= \left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right)^{\lfloor K/(t+1)\rfloor}
\end{aligned}$$

where $\pi_{t,0}$ and $\pi_{t,1}$ are defined in (13), and the second and third lines make use of the relations (15) and (16). Since none of the transmissions are successfully eavesdropped, the eavesdropper error covariances are given by $P_{e,k|k} = f^k(\bar{P}), k = 1,\ldots,K$, with a probability

$$\Big(\mathbb{P}(\gamma_{e,k-1}=0)(1-q_e) + \mathbb{P}(\gamma_{e,k-1}=1)p_e\Big)^{\lfloor K/(t+1)\rfloor}$$

of this occurring, where we have the stationary probabilities

$$\mathbb{P}(\gamma_{e,k-1}=0) = \frac{p_e}{p_e+q_e}, \quad \mathbb{P}(\gamma_{e,k-1}=1) = \frac{q_e}{p_e+q_e}.$$

Then by independence of the remote estimator and eavesdropper channels, the probability of the event ω is

$$\begin{aligned}
\mathbb{P}[\omega] &= \left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right)^{\lfloor K/(t+1)\rfloor} \\
&\quad\times\left(\frac{p_e}{p_e+q_e}(1-q_e) + \frac{q_e}{p_e+q_e}p_e\right)^{\lfloor K/(t+1)\rfloor}.
\end{aligned}$$

Let ω^c denote the complement of ω. We have

$$\begin{aligned}
&\frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}] \\
&= \frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}|\omega]\times\mathbb{P}(\omega) + \frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}|\omega^c]\times\mathbb{P}(\omega^c) \\
&> \frac{1}{K}\sum_{k=1}^{K}\text{tr}\mathbb{E}[P_{e,k|k}|\omega]\mathbb{P}(\omega) \\
&= \frac{1}{K}\sum_{k=1}^{K}\text{tr}\Big(A^k\bar{P}(A^k)^T + \sum_{m=0}^{k-1}A^mQ(A^m)^T\Big) \\
&\quad\times\left[\left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right)\frac{p_e}{p_e+q_e}\right]^{\lfloor K/(t+1)\rfloor}
\end{aligned}$$

$$
\begin{aligned}
&> \frac{1}{K}\mathrm{tr}(A^K \bar{P}(A^K)^T) \\
&\quad \times \left[\left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right) \frac{p_e}{p_e+q_e} \right]^{K/(t+1)} \\
&\to \infty \text{ as } K \to \infty,
\end{aligned}
$$

where the last line holds if condition (12) is satisfied. Since $\rho(A) > 1$ and

$$
\begin{aligned}
&\left(g^{t-1}(p)q + (1-g^{t-1}(p))(1-p)\right) \frac{p_e}{p_e+q_e} \\
&> \min(q, 1-p)\frac{p_e}{p_e+q_e} > 0,
\end{aligned}
$$

condition (12) will always be satisfied when t is sufficiently large. As $\frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{k|k}]$ remains bounded for every finite $t \in \mathbb{N}$ by Theorem 3.1, 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 (12) is satisfied, will have the required properties that $\lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{k|k}]$ is bounded and $\lim_{K\to\infty} \frac{1}{K}\sum_{k=1}^{K} \mathrm{tr}\mathbb{E}[P_{e,k|k}]$ is unbounded.

Remark 3.4: The condition (12) provides a sufficient condition for determining how large t needs to be before the expected eavesdropper covariance becomes unbounded. In the case of i.i.d. packet drops with packet reception probability λ and eavesdropping probability λ_e, we have $p = 1-\lambda$, $q = \lambda$, $p_e = 1-\lambda_e$, $q_e = \lambda_e$. Then $g(p) = g(1-\lambda) = 1-\lambda$, which implies that $g^{t-1}(1-\lambda) = 1-\lambda$. Thus condition (12) reduces to

$$
\rho(A)(\lambda(1-\lambda_e))^{1/2(t+1)} > 1,
$$

which is equivalent to the condition derived in [11].

Remark 3.5: For i.i.d. packet drops, when transmitting measurements and without using feedback acknowledgements, mechanisms were derived in [10] for making the expected eavesdropper error covariance unbounded while keeping the expected estimation error covariance bounded, under the condition that $\lambda_e < \lambda$. With the use of feedback and transmitting local state estimates, the same behaviour can be achieved for all $\lambda_e < 1$ [11]. Theorem 3.3 extends the result in [11] to all Markovian packet drop channels with $p_e, q_e \in (0,1)$.

Remark 3.6: The result of Theorem 3.3 can still apply even without exact knowledge of p_e and q_e. For instance, suppose we only have upper bounds on q_e and $1-p_e$ (the probabilities of successfully eavesdropping the next transmission). Since $p_e/(p_e+q_e)$ is decreasing in q_e and increasing in p_e (or decreasing in $1-p_e$), using a t that satisfies (12) for the upper bounds on q_e and $1-p_e$ will ensure that (12) is also satisfied for all values of q_e and $1-p_e$ less than the upper bounds.

IV. Numerical Studies

We consider an example with parameters

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

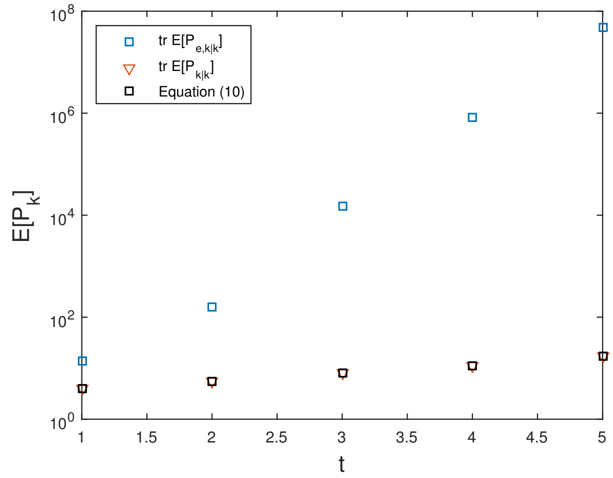

Fig. 2. Expected error covariance at estimator and expected error covariance at eavesdropper. $p = 0.4, q = 0.8, p_e = 0.4, q_e = 0.8$.

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 first consider the case with $p = 0.4, q = 0.8$, $p_e = 0.4, q_e = 0.8$. Using the threshold policy which transmits at time k if and only if $P_{k-1|k-1} \geq f^t(\bar{P})$, Fig. 2 plots $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$ for different values of t, obtained by taking the time average of a Monte Carlo run of length 1000000. For comparison, the analytical expression for $\mathrm{tr}\mathbb{E}[P_{k|k}]$ in equation (10) is also given. In this case, we can verify that $(1-q)\rho(A)^2 < 1$ holds, and that condition (12) for unboundedness of the expected eavesdropper covariance is satisfied when $t \geq 2$

Next we consider an asymmetric case with $p = 0.5, q = 0.7$, $p_e = 0.3, q_e = 0.9$. From the definitions of p, q, p_e, q_e we see that the eavesdropper's channel is better than the estimator's channel in this case. Fig. 3 plots $\mathrm{tr}\mathbb{E}[P_{k|k}]$ and $\mathrm{tr}\mathbb{E}[P_{e,k|k}]$ for different thresholds, together with the analytical expression (10). In this case, $(1-q)\rho(A)^2 < 1$ also holds and condition (12) is satisfied for $t \geq 3$.

We see that by using a sufficiently large t, in both cases we can make the expected error covariance of the eavesdropper very large, while keeping the expected error covariance at the remote estimator bounded.

V. Conclusion

In this paper we have studied remote state estimation over a Markovian packet dropping link, where each transmission can be overheard by an eavesdropper according to another Markovian packet dropping link. In the infinite horizon situation, we have shown that if the underlying process is unstable, one can keep the expected estimation error covariance bounded while the expected eavesdropper error covariance becomes unbounded. The constructed scheme is a simple threshold policy on the estimation error covariance.

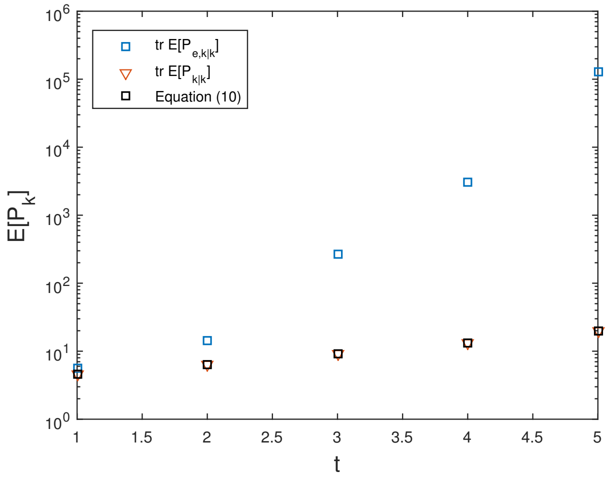

Fig. 3. Expected error covariance at estimator and expected error covariance at eavesdropper. $p = 0.5, q = 0.7, p_e = 0.3, q_e = 0.9$.

Appendix

Proof of Lemma 3.1. We can firstly describe the behaviour of this policy using a Markov chain with transition diagram shown in Fig. 4. where the first component of each state (P, γ) represents the value of $P_{k-1|k-1}$, and the second component the value of γ_{k-1}. For $p \in (0,1)$ and $q \in (0,1)$, this Markov chain can be easily shown to be irreducible, aperiodic, and with all states being positive recurrent. Then the stationary probabilities

$$\pi_{i,j} \triangleq \mathbb{P}(P_{k-1|k-1} = f^i(\bar{P}), \gamma_{k-1} = j) \text{ as } k \to \infty \quad (13)$$

will exist, and $\{P_{k|k}\}$ will have a stationary distribution. Enumerate the states of this Markov chain in the order $(\bar{P}, 1)$, $(f(\bar{P}), 0)$, $(f(\bar{P}), 1)$, $(f^2(\bar{P}), 0)$, $(f^2(\bar{P}), 1), \dots,$ $(f^t(\bar{P}), 0)$, $(f^t(\bar{P}), 1)$, $(f^{t+1}(\bar{P}), 0)$, $(f^{t+2}(\bar{P}), 0), \dots$. The transition probability matrix $\mathbf{P}$ is then given by (14). Call

$$\boldsymbol{\pi} \triangleq \begin{bmatrix} \pi_{0,1} & \pi_{1,0} & \pi_{1,1} & \pi_{2,0} & \pi_{2,1} & \dots & \pi_{t,0} & \pi_{t,1} \\ & & & & & \pi_{t+1,0} & \pi_{t+2,0} & \dots \end{bmatrix}.$$

The stationary probabilities can then be found be solving the equation $\boldsymbol{\pi} = \boldsymbol{\pi}\mathbf{P}$. The first few relations are:

$$\begin{aligned} \pi_{1,0} &= p\pi_{0,1} \\ \pi_{1,1} &= (1-p)\pi_{0,1} \\ \pi_{2,0} &= (1-q)\pi_{1,0} + p\pi_{1,1} \\ \pi_{2,1} &= q\pi_{1,0} + (1-p)\pi_{1,1} \\ &\vdots \\ \pi_{t,0} &= (1-q)\pi_{t-1,0} + p\pi_{t-1,1} \\ \pi_{t,1} &= q\pi_{t-1,0} + (1-p)\pi_{t-1,1}, \end{aligned}$$

from which we obtain

$$\pi_{0,1} = \pi_{1,0} + \pi_{1,1} = \pi_{2,0} + \pi_{2,1} = \dots = \pi_{t,0} + \pi_{t,1}. \quad (15)$$

We will now show that $\pi_{j,0} = g^{j-1}(p)\pi_{0,1}$ and $\pi_{j,1} = (1 - g^{j-1}(p))\pi_{0,1}$ for $j = 1, 2, \dots, t$. The proof is by induction. The statement is clearly true for $\pi_{1,0}$ and $\pi_{1,1}$. Now assume that the statement is true for $\pi_{j-1,0}$ and $\pi_{j-1,1}$. Then

$$\begin{aligned} \pi_{j,0} &= (1-q)\pi_{j-1,0} + p\pi_{j-1,1} \\ &= (1-q)g^{j-2}(p)\pi_{0,1} + p(1-g^{j-2}(p))\pi_{0,1} \\ &= g(g^{j-2}(p))\pi_{0,1} = g^{j-1}(p)\pi_{0,1}, \end{aligned}$$

where the second line used the induction hypothesis and the third line used (9). Furthermore, from (15) we have

$$\pi_{j,1} = \pi_{0,1} - \pi_{j,0} = (1 - g^{j-1}(p))\pi_{0,1},$$

which completes the induction argument.

Continuing on, it is straightforward to show that $\pi_{j,0} = g^t(p)(1-q)^{j-t-1}\pi_{0,1}$ for $j = t+1, t+2, \dots$. In summary, we have derived that:

$$\begin{aligned} \pi_{j,0} &= g^{j-1}(p)\pi_{0,1}, & j &= 1, 2, \dots, t \\ \pi_{j,1} &= (1 - g^{j-1}(p))\pi_{0,1}, & j &= 1, 2, \dots, t \\ \pi_{j,0} &= g^t(p)(1-q)^{j-t-1}\pi_{0,1}, & j &= t+1, t+2, \dots \end{aligned} \quad (16)$$

Since the probabilities must sum to one, we have

$$\begin{aligned} \pi_{0,1} &+ \sum_{j=1}^{t}(\pi_{j,0} + \pi_{j,1}) + \sum_{j=t+1}^{\infty} \pi_{j,0} \\ &= \left(t + 1 + \frac{g^t(p)}{q} \right) \pi_{0,1} = 1 \end{aligned}$$

or $\pi_{0,1} = \frac{q}{q(t+1)+g^t(p)}$, from which all the other stationary probabilities can be calculated using (16). The expected error covariance as $k \to \infty$ can then be expressed as

$$\begin{aligned} &\mathbb{E}[P_{k|k}] = \mathbb{E}[P_{k-1|k-1}] \\ &= \pi_{0,1}\bar{P} + \sum_{j=1}^{t}(\pi_{j,0} + \pi_{j,1})f^j(\bar{P}) + \sum_{j=t+1}^{\infty} \pi_{j,0}f^j(\bar{P}) \\ &= \pi_{0,1}\left[\bar{P} + \sum_{j=1}^{t} f^j(\bar{P}) + g^t(p) \sum_{j=t+1}^{\infty} (1-q)^{j-t-1}f^j(\bar{P}) \right]. \end{aligned} \quad (17)$$

We want to show that the infinite series above converges if and only if $(1-q)\rho(A)^2 < 1$. Note that for the case where one always transmits local estimates over a Markovian packet dropping link, which corresponds to $t = 0$, we have $\pi_{0,1} = \frac{q}{q+p}$, and so

$$\mathbb{E}[P_{k|k}] = \frac{q}{q+p}\left[\bar{P} + p\sum_{j=1}^{\infty}(1-q)^{j-1}f^j(\bar{P}) \right].$$

From [19], we know that $\mathbb{E}[P_{k|k}]$ is bounded if and only if $(1-q)\rho(A)^2 < 1$, so that

$$\sum_{j=1}^{\infty}(1-q)^{j-1}f^j(\bar{P}) < \infty \text{ iff } (1-q)\rho(A)^2 < 1.$$

Then

$$\begin{aligned} \sum_{j=t+1}^{\infty} (1-q)^{j-t-1}f^j(\bar{P}) &= \frac{1}{(1-q)^t} \sum_{j=t+1}^{\infty} (1-q)^{j-1}f^j(\bar{P}) \\ &< \infty \text{ iff } (1-q)\rho(A)^2 < 1, \end{aligned}$$

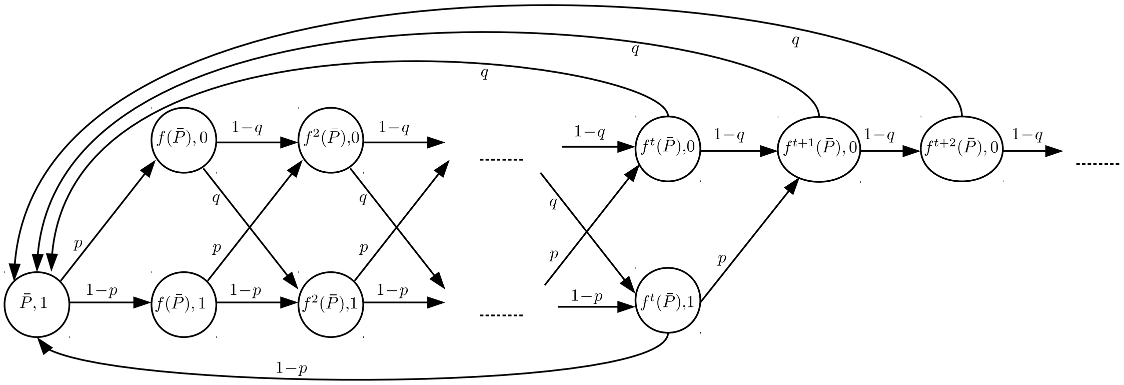

Fig. 4. Markov chain for threshold policy

$$\mathbf{P}=\left[\begin{array}{cccccccccccccc}
0 & p & 1-p & 0 & 0 & 0 & 0 & \cdots & & & & & & \cdots\\
0 & 0 & 0 & 1-q & q & 0 & 0 & \cdots & & & & & & \cdots\\
0 & 0 & 0 & p & 1-p & 0 & 0 & \cdots & & & & & & \cdots\\
0 & 0 & 0 & 0 & 0 & 1-q & q & & & & & & & \cdots\\
0 & 0 & 0 & 0 & 0 & p & 1-p & & & & & & & \cdots\\
\vdots & \vdots & & & & & & \ddots & & & & & & \\
0 & 0 & \cdots & & & & & \cdots & 1-q & q & 0 & 0 & 0 & \cdots\\
0 & 0 & \cdots & & & & & \cdots & p & 1-p & 0 & 0 & 0 & \cdots\\
q & 0 & \cdots & & & & & \cdots & 0 & 0 & 1-q & 0 & 0 & \cdots\\
1-p & 0 & \cdots & & & & & \cdots & 0 & 0 & p & 0 & 0 & \cdots\\
q & 0 & \cdots & & & & & \cdots & 0 & 0 & 0 & 1-q & 0 & \cdots\\
q & 0 & \cdots & & & & & \cdots & 0 & 0 & 0 & 0 & 1-q & \cdots\\
\vdots & \vdots & & & & & & & & & & & & \ddots
\end{array}\right] \qquad (14)$$

and thus, from (17), we have that $\text{tr}\mathbb{E}[P_{k|k}] < \infty$ for any finite $t \in \mathbb{N}$.

REFERENCES

[1] P. A. Regalia, A. Khisti, Y. Liang, and S. Tomasin, Eds., *Special Issue on Secure Communications via Physical-Layer and Information-Theoretic Techniques*. Proc. IEEE, Oct. 2015, vol. 103, no. 10.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] ——, "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.

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

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

[11] 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 Congress*, Toulouse, France, Jul. 2017, pp. 7600–7605.

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

[13] M. Huang and S. Dey, "Stability of Kalman filtering with Markovian packet losses," *Automatica*, vol. 43, pp. 598–607, 2007.

[14] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[15] 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.

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

[17] 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.

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

[19] V. Gupta, B. Hassibi, and R. M. Murray, "Optimal LQG control across packet-dropping links," *Systems and Control Letters*, vol. 56, pp. 439–446, 2007.