2018 European Control Conference (ECC)
June 12-15, 2018. Limassol, Cyprus

On the Use of Artificial Noise for Secure State Estimation in the Presence of Eavesdroppers

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

Abstract— **The problem of remote state estimation in the presence of eavesdroppers has recently been investigated in the literature. For unstable systems it has been shown that one can keep the expected estimation error covariance bounded, while the expected eavesdropper error covariance becomes unbounded in the infinite horizon, using schemes based on transmission scheduling. In this paper we consider an alternative approach to achieve security, namely injecting noise into sensor transmissions, similar to the artificial noise technique used in physical layer security for wireless communications. Numerical results demonstrate significant performance improvements using this approach, with respect to the trade-off between the expected estimation error covariance and expected eavesdropper covariance.**

I. Introduction

The amount of data transmitted wirelessly has increased tremendously over the last decade. 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 transmissions from eavesdroppers. Information security issues have traditionally been studied in the context of cryptography. However, due to 1) the often limited computational power available at the transmitters to implement strong encryption, 2) the increased computational power available to malicious agents, and 3) poorly implemented security in e.g. some Internet of Things devices, achieving security using solely cryptographic means may not necessarily be guaranteed. Alternative ways to implement security using information theoretic and physical layer techniques, complementary to the traditional cryptographic approaches, have thus received 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" refers to approaches to implement information theoretic security using physical layer characteristics of the wireless channel such as fading, interference, and noise, [3].

Using physical layer security ideas, estimation problems with eavesdroppers have recently been studied, such as [4]–[7] for estimation of constants or i.i.d. sources, and [8]–[10] for state estimation of dynamical systems. One of the main results shown in the works [9], [10] is that for the case of unstable systems, it is possible to drive the expected eavesdropper error covariance unbounded while keeping the expected estimation error covariance at the legitimate remote estimator (or receiver) bounded. The techniques used to achieve this behaviour involves transmission scheduling by withholding certain transmissions, both with [10] and without [9] feedback. However, withholding transmission means that the performance at the remote estimator will also be affected when no transmissions occur. This motivates us to search for other secure estimation schemes where the performance at the legitimate remote estimator will not deteriorate, or at least not significantly.

The concept of artificial noise [11], where noise is artificially injected into the null space of the legitimate receiver's channel, so that the noise will affect the eavesdropper but not the receiver, is widely regarded as one of the most effective techniques to implement physical layer security in wireless communications [3]. In the current paper we will adapt this technique to remote state estimation of dynamical systems in the presence of eavesdroppers. This technique requires the use of multiple transmit antennas, which have not been considered much in the control literature, but nevertheless are commonly implemented in current wireless communication standards such as Wi-Fi and 4G.

We consider packet dropping links where the probability of a successful reception depends on the received signal-to-noise ratio (SNR), where the received SNR can depend on the fading channel gains, transmission energies and noise powers. In the context of packet drop models with fading, a single antenna model was studied in [12]. This paper considers an extension of the packet drop model with fading to multiple transmit antennas. We show that for sufficiently large transmission energies and artificial noise variances, the expected eavesdropper covariance can be made unbounded while the expected error covariance at the legitimate receiver remains bounded, irrespective of how good/bad the channels are.

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

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

A. Leong, A. Redder, and D. Quevedo are with the Department of Electrical Engineering (EIM-E), Paderborn University, Paderborn, Germany. E-mail: alex.leong@upb.de, adrian.redder@t-online.de, dquevedo@ieee.org. S. Dey is with the Institute for Telecommunications Research, University of South Australia, Adelaide, Australia. E-mail: Subhra.Dey@unisa.edu.au.

[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.

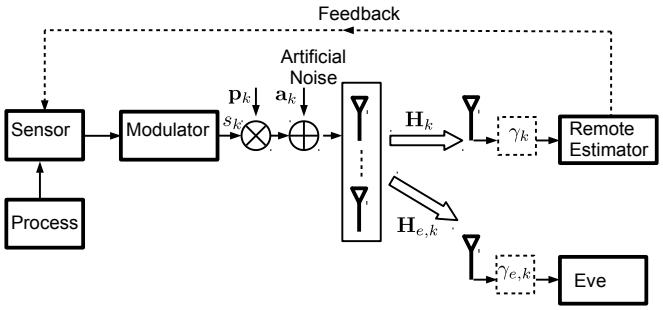

Fig. 1. System Model

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.

Let $x \in \mathcal{X}$,[2] and let $S_k(.) : \mathcal{X} \to \mathbb{C}$ be a mapping such that $S_k(x)$ is the digital symbol of x, represented as a point on a complex signal constellation [13], [14], which in general depends on the modulation scheme used for transmission at time k. We assume there is sufficient bit rate such that quantization effects are negligible. The sensor wishes to send quantities $s_k \in \mathbb{C}$ to the remote estimator. Common choices for s_k are the sensor measurements, i.e. $s_k = S_k(y_k)$, or the local state estimates $s_k = S_k(\hat{x}^s_{k|k})$ [15]. In the case where the local state estimates are transmitted, the local state estimates and estimation error covariances

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

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. In the case where local state estimates are transmitted, 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 in general convergence to steady state occurs at an exponential rate.

A. MIMO Communications and Artificial Noise

In multiple-input multiple-output (MIMO) communications with N_T transmit antennas and N_R receive antennas, it is common to represent the MIMO channel by a $N_R \times N_T$ matrix $\mathbf{H}_k$, where the (i, j)-th element of $\mathbf{H}_k$ represents the complex valued channel gain at time k from transmit antenna j to receive antenna i [16]. In this paper we will investigate the case of multiple transmit antennas and a single receive antenna, and thus $\mathbf{H}_k$ will be a $1 \times N_T$ matrix or row vector (the artificial noise technique can also be extended to multiple receive antennas, provided the number of transmit antennas is greater than the number of receive antennas of the eavesdropper [11]). In order to implement security to the transmission, the technique of adding artificial noise will be used [11]. The transmitted signal $\bar{\mathbf{s}}_k \in \mathbb{C}^{N_T}$ is of the form

$$\bar{\mathbf{s}}_k = \mathbf{p}_k s_k + \mathbf{a}_k. \tag{3}$$

In (3), $\mathbf{p}_k \in \mathbb{C}^{N_T}$ with $||\mathbf{p}_k|| = 1$ is a beamforming vector used to choose the direction of transmission, and $\mathbf{a}_k \in \mathbb{C}^{N_T}$ is the complex Gaussian[3] artificial noise vector. The artificial noise is chosen such that $\mathbf{a}_k$ lies in the null space of $\mathbf{H}_k$, so that $\mathbf{H}_k\mathbf{a}_k = 0$. Specifically, write

$$\mathbf{a}_k = \mathbf{Z}_k\tilde{\mathbf{a}}_k, \tag{4}$$

where the columns of the $N_T \times (N_T - 1)$ matrix $\mathbf{Z}_k$ form an orthonormal basis for the null space of $\mathbf{H}_k$, with $\mathbf{Z}_k$ satisfying $\mathbf{Z}^\dagger_k\mathbf{Z}_k = I$ where $\dagger$ denotes the Hermitian transpose (this can be done by performing a singular value decomposition on $\mathbf{H}_k$), and the components of $\tilde{\mathbf{a}}_k \in \mathbb{C}^{N_T-1}$ are i.i.d. complex Gaussian with zero mean and variance $\sigma^2_{a,k}$. Note that this requires the following assumption:

Assumption 2.1: $\mathbf{H}_k$ is known to the sensor at time k.

Knowledge of $\mathbf{H}_k$ at the sensor can be obtained in practice by using channel estimation algorithms (either estimated at the sensor, or estimated at the remote estimator and fed back to the sensor [11]). We will also assume that the artificial noise variances $\sigma^2_{a,k}$ can be chosen by us to satisfy performance objectives, see Section III.

B. Eavesdropper

The sensor transmissions can be overheard by an eavesdropper (called 'Eve' in Fig. 1) over another channel $\mathbf{H}_{e,k}$. We assume the eavesdropper to have a single receive antenna, so that $\mathbf{H}_{e,k}$ is also a $1 \times N_T$ matrix or row vector. The random processes $\{\mathbf{H}_k\}$ and $\{\mathbf{H}_{e,k}\}$ will be assumed to be mutually independent.[4] The i.i.d. block fading model will be assumed [17], such that $\mathbf{H}_k$ remains constant over a fading block, but are i.i.d. in different blocks (similarly for $\mathbf{H}_{e,k}$). Denote $z_k \in \mathbb{C}$ and $z_{e,k} \in \mathbb{C}$ as the signals received by the remote estimator and eavesdropper respectively. We have

$$z_k = \mathbf{H}_k\bar{\mathbf{s}}_k + n_k = \mathbf{H}_k\mathbf{p}_k s_k + n_k$$
$$z_{e,k} = \mathbf{H}_{e,k}\bar{\mathbf{s}}_k + n_{e,k} = \mathbf{H}_{e,k}\mathbf{p}_k s_k + \mathbf{H}_{e,k}\mathbf{a}_k + n_{e,k}$$

where $n_k \in \mathbb{C}$ and $n_{e,k} \in \mathbb{C}$ are complex Gaussian channel noises with zero means and variances σ^2_n and σ^2_e respectively. The received signals z_k and $z_{e,k}$ are then used by the remote estimator and eavesdropper respectively to demodulate/decode the information signal s_k. In order to

[2] In the case where local state estimates are transmitted, we would have $\mathcal{X} = \mathbb{R}^{n_x}$, and in the case where measurements are transmitted $\mathcal{X} = \mathbb{R}^{n_y}$.

[3] A complex valued random variable $Z = X + jY$ is *complex Gaussian* if X and Y are jointly Gaussian random variables, with mean and variance defined by $\mathbb{E}[Z] = \mathbb{E}[X] + j\mathbb{E}[Y]$ and $\text{Var}[Z] = \text{Var}[X] + \text{Var}[Y]$. A complex random vector $\mathbf{Z} = \mathbf{X} + j\mathbf{Y}$ is complex Gaussian if $\mathbf{X}$ and $\mathbf{Y}$ are jointly Gaussian random vectors [13], [16].

[4] In wireless communication, it is known that channel fading becomes approximately independent for receivers separated by distances greater than half a wavelength of the transmitted signal [16, p.71]. For the transmission frequencies currently in use in 3G/4G mobiles and Wi-Fi, such wavelengths are on the order of centimeters.

perform coherent reception when demodulating the received signals [14], [16], we will make the following assumption.

Assumption 2.2: $\mathbf{H}_k$ is known to the remote estimator at time k, while both $\mathbf{H}_{e,k}$ and $\mathbf{H}_k$ are known to the eavesdropper at time k.

Remark 2.1: The assumption of knowledge of $\mathbf{H}_k$ at the eavesdropper gives an upper bound on the best performance that can be achieved at the eavesdropper,[5] and is in the spirit of Kerckhoff's principle in cryptography [18], namely that a cryptosystem should be secure even if the enemy knows everything about the system except the secret key, to avoid the problem of "security through obscurity".

C. Packet Reception Model

Define random variables γ_k such that $\gamma_k = 1$ if s_k is successfully decoded at the remote estimator, which we will also regard as a successful packet reception, and $\gamma_k = 0$ if there are errors (which we will regard as a packet drop). Similarly, define $\gamma_{e,k}$ such that $\gamma_{e,k} = 1$ if s_k is successfully decoded at the eavesdropper, and $\gamma_{e,k} = 0$ otherwise.

For many digital modulation and demodulation schemes, the probability of correct decoding is an increasing function of the *received* signal-to-noise ratio (SNR), which in turn depends on variables such as the channel fading, transmission energies and noise powers, see e.g. [13], [14]. The conditional probability of successful decoding will be represented by $f(\mathsf{SNR}_k)$, where $f(.) : [0, \infty) \to [0, 1]$ is a monotonically increasing continuous function whose form depends on the particular digital modulation and demodulation (plus possible channel coding) schemes used (see e.g. (19) for the case of quadrature amplitude modulation), and SNR_k denotes the received SNR at time k. We have

$$\begin{aligned}\mathbb{P}(\gamma_k = 1|\mathsf{SNR}_k) &= f(\mathsf{SNR}_k) = f\left(\frac{|\mathbf{H}_k\mathbf{p}_k|^2 E_{s,k}}{\sigma_n^2}\right)\\ \mathbb{P}(\gamma_{e,k} = 1|\mathsf{SNR}_{e,k}) &= f(\mathsf{SNR}_{e,k}) = f\left(\frac{|\mathbf{H}_{e,k}\mathbf{p}_k|^2 E_{s,k}}{\mathbb{E}|\mathbf{H}_{e,k}\mathbf{a}_k|^2 + \sigma_e^2}\right)\\ &= f\left(\frac{|\mathbf{H}_{e,k}\mathbf{p}_k|^2 E_{s,k}}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger\sigma_{a,k}^2 + \sigma_e^2}\right),\end{aligned} \tag{5}$$

where $E_{s,k}$ is the transmission energy of the symbol s_k, and the last equality follows from (4) and Assumption 2.2. In the case of single antenna transmissions, similar models for packet drop in the presence of fading have been used in e.g. [12], [19].

The instantaneous channel of the eavesdropper $\mathbf{H}_{e,k}$ is assumed to be unknown to both the sensor and remote estimator, and we will thus choose the beamforming vector as in [11]:

$$\mathbf{p}_k = \frac{\mathbf{H}_k^\dagger}{||\mathbf{H}_k||}.$$

Then we can further express (5) as

$$\mathbb{P}(\gamma_k = 1|\mathsf{SNR}_k) = f\left(\frac{||\mathbf{H}_k||^2 E_{s,k}}{\sigma_n^2}\right)$$

$$\mathbb{P}(\gamma_{e,k} = 1|\mathsf{SNR}_{e,k}) = f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_{s,k}/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger\sigma_{a,k}^2+\sigma_e^2}\right).$$

D. Remote Estimator

Define

$$\mathcal{I}_k \triangleq \{\gamma_0, \ldots, \gamma_k, \gamma_0 s_0, \ldots, \gamma_k s_k\}$$

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

$$\begin{aligned}&\hat{x}_{k|k-1} \triangleq \mathbb{E}[x_k|\mathcal{I}_{k-1}],\ \hat{x}_{k|k} \triangleq \mathbb{E}[x_k|\mathcal{I}_k],\\ &P_{k|k-1} \triangleq \mathbb{E}[(x_k - \hat{x}_{k|k-1})(x_k - \hat{x}_{k|k-1})^T|\mathcal{I}_{k-1}],\\ &P_{k|k} \triangleq \mathbb{E}[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})^T|\mathcal{I}_k].\end{aligned} \tag{6}$$

Similarly, define

$$\mathcal{I}_{e,k} \triangleq \{\gamma_{e,0}, \ldots, \gamma_{e,k}, \gamma_{e,0} s_0, \ldots, \gamma_{e,k} s_k\}$$

as the information set available to the eavesdropper at time k, and

$$\begin{aligned}&\hat{x}_{e,k|k-1} \triangleq \mathbb{E}[x_k|\mathcal{I}_{e,k-1}],\ \hat{x}_{e,k|k} \triangleq \mathbb{E}[x_k|\mathcal{I}_{e,k}],\\ &P_{e,k|k-1} \triangleq \mathbb{E}[(x_k - \hat{x}_{e,k|k-1})(x_k - \hat{x}_{k|e,k-1})^T|\mathcal{I}_{e,k-1}],\\ &P_{e,k|k} \triangleq \mathbb{E}[(x_k - \hat{x}_{e,k|k})(x_k - \hat{x}_{e,k|k})^T|\mathcal{I}_{e,k}].\end{aligned} \tag{7}$$

Let

$$h(X) \triangleq AXA^T + Q. \tag{8}$$

When local state estimates are transmitted, the optimal remote estimator can be shown to have the form [15]:

$$\begin{aligned}\hat{x}_{k|k} &= \begin{cases} A\hat{x}_{k-1|k-1} & , \quad \gamma_k = 0 \\ \hat{x}_{k|k}^s & , \quad \gamma_k = 1 \end{cases}\\ P_{k|k} &= \begin{cases} h(P_{k-1|k-1}) & , \quad \gamma_k = 0 \\ \bar{P} & , \quad \gamma_k = 1 \end{cases}\end{aligned} \tag{9}$$

while at the eavesdropper:

$$\begin{aligned}\hat{x}_{e,k|k} &= \begin{cases} A\hat{x}_{e,k-1|k-1} & , \quad \gamma_{e,k} = 0 \\ \hat{x}_{k|k}^s & , \quad \gamma_{e,k} = 1 \end{cases}\\ P_{e,k|k} &= \begin{cases} h(P_{e,k-1|k-1}) & , \quad \gamma_{e,k} = 0 \\ \bar{P} & , \quad \gamma_{e,k} = 1. \end{cases}\end{aligned} \tag{10}$$

In the case where measurements are transmitted, the optimal remote estimator has the form [20]:

$$\begin{aligned}\hat{x}_{k+1|k} &= A\hat{x}_{k|k}\\ \hat{x}_{k|k} &= \begin{cases} \hat{x}_{k|k-1}, & \gamma_k = 0 \\ \hat{x}_{k|k-1} + K_k(y_k - C\hat{x}_{k|k-1}), & \gamma_k = 1 \end{cases}\\ P_{k+1|k} &= h(P_{k|k})\\ P_{k|k} &= \begin{cases} P_{k|k-1}, & \gamma_k = 0 \\ P_{k|k-1} - K_k C P_{k|k-1}, & \gamma_k = 1, \end{cases}\\ K_k &= P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1},\end{aligned} \tag{11}$$

and similarly at the eavesdropper.

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

[5] Knowledge of $\mathbf{H}_k$ might also be obtained at the eavesdropper if the remote estimator broadcasts $\mathbf{H}_k$ back to the sensor [11].

III. Secure Estimation Using Artificial Noise

We consider the case where A is unstable, i.e. the spectral radius $\rho(A) > 1$. We will also use the shorthand $P_k \triangleq P_{k|k}$. From Section II we see that there are two power/energy-type parameters[6] which can be varied, namely the symbol energy $E_{s,k}$ and the variance of the artificial noise $\sigma^2_{a,k}$. To allow for possible power control, we will consider the case that $E_{s,k}(\mathbf{H}_k, P_{k-1})$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1})$ can be functions of the channel $\mathbf{H}_k$ and estimation error covariance P_{k-1} (which in turn is a function of $\gamma_0, \ldots, \gamma_{k-1}$). The quantities $E_{s,k}(\mathbf{H}_k, P_{k-1})$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1})$ can be computed at the remote estimator and fed back to the sensor. We note that equations (9)-(11) will still hold, as knowledge of $(\mathbf{H}_k, P_{k-1})$ does not provide additional information about the state x_k.

The following result (Theorem 3.1) provides sufficient conditions on $E_{s,k}(\mathbf{H}_k, P_{k-1})$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1})$, for the expected estimation error covariance to be bounded and the expected eavesdropper covariance to become unbounded. First note that we can write

$$\mathbb{P}(\gamma_k = 1|P_{k-1}) = \int_\Omega f\left(\frac{||\mathbf{H}_k||^2 E_{s,k}(\mathbf{H}_k, P_{k-1})}{\sigma_n^2}\right) d\mathbb{P}(\mathbf{H}_k)$$

$$\begin{aligned}
&\mathbb{P}(\gamma_{e,k} = 1|P_{e,k-1}) \\
&= \int \mathbb{P}(\gamma_{e,k} = 1|P_{e,k-1}, P_{k-1}, \mathbf{H}_k, \mathbf{H}_{e,k}) \\
&\qquad .d\mathbb{P}(P_{k-1}, \mathbf{H}_k, \mathbf{H}_{e,k}|P_{e,k-1}) \\
&= \int_{\mathbf{P}_{k-1}} \int_{\Omega_e} f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_{s,k}(\mathbf{H}_k, P_{k-1})/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger \sigma^2_{a,k}(\mathbf{H}_k, P_{k-1}) + \sigma_e^2}\right) \\
&\qquad .d\mathbb{P}(\mathbf{H}_k, \mathbf{H}_{e,k}) d\mathbb{P}(P_{k-1}|P_{e,k-1})
\end{aligned} \tag{12}$$

where $\mathbf{P}_{k-1}$ represents the support of P_{k-1}, Ω the support of $\mathbf{H}_k$, and Ω_e the support of $(\mathbf{H}_k, \mathbf{H}_{e,k})$.

Theorem 3.1: Let A be unstable. Suppose $E_{s,k}(\mathbf{H}_k, P_{k-1})$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1})$ are such that

$$\mathbb{P}(\gamma_k = 1|P_{k-1}) > 1 - \frac{1}{||A||^2}, \quad \forall P_{k-1} \tag{13}$$

$$\mathbb{P}(\gamma_{e,k} = 1|P_{e,k-1}) < 1 - \frac{1}{\rho(A)^2}, \quad \forall P_{e,k-1}, \tag{14}$$

where $\rho(A)$ is the spectral radius of A, $||A||$ the spectral norm of A, and $\mathbb{P}(\gamma_k = 1|P_{k-1})$ and $\mathbb{P}(\gamma_{e,k} = 1|P_{e,k-1})$ are given by (12). Then

$$\mathbb{E}[\text{tr}P_k] < \infty, \quad \forall k \tag{15}$$

$$\text{and } \mathbb{E}[\text{tr}P_{e,k}] \to \infty \text{ as } k \to \infty. \tag{16}$$

Proof: The proof of the implication (13) $\Rightarrow$ (15) can be shown using similar techniques as in [21], and is omitted for brevity. For the implication (14) $\Rightarrow$ (16), we use the following argument. Consider a horizon $K > 0$. Let ω denote the event that every transmission is unsuccessfully overheard by the eavesdropper. By the definition of ω and the assumption that $P_{e,0} = \bar{P}$, the eavesdropper error covariances are given by $P_{e,k} = h^k(\bar{P}), k = 1, \ldots, K$, where $h^k(.)$ is the k-fold composition of $h(.)$ defined in (8), and $h^0(X) \triangleq X$. We have

$$\begin{aligned}
\mathbb{P}(\omega) &= \mathbb{P}(\gamma_{e,K} = 0, \ldots, \gamma_{e,1} = 0) \\
&= \prod_{k=1}^{K} \mathbb{P}(\gamma_{e,k} = 0|\gamma_{e,k-1} = 0, \ldots, \gamma_{e,1} = 0) \\
&= \prod_{k=1}^{K} \mathbb{P}(\gamma_{e,k} = 0|P_{e,k-1} = h^{k-1}(\bar{P}))
\end{aligned}$$

Let ω^c denote the complement of ω. Then

$$\begin{aligned}
&\text{tr}\mathbb{E}[P_{e,K}] = \text{tr}\mathbb{E}[P_{e,K}|\omega]\mathbb{P}(\omega) + \text{tr}\mathbb{E}[P_{e,K}|\omega^c]\mathbb{P}(\omega^c) \\
&> \text{tr}\mathbb{E}[P_{e,K}|\omega]\mathbb{P}(\omega) \\
&> \text{tr}(A^K \bar{P} (A^K)^T)\mathbb{P}(\omega) \\
&= \text{tr}(A^K \bar{P} (A^K)^T) \prod_{k=1}^{K} \mathbb{P}(\gamma_{e,k} = 0|P_{e,k-1} = h^{k-1}(\bar{P})) \\
&\to \infty \text{ as } K \to \infty,
\end{aligned}$$

where the last line follows from (14). ∎

A. Constant Energies

Verifying the conditions (13) and (14) in Theorem 3.1 for arbitrary $E_{s,k}(\mathbf{H}_k, P_{k-1})$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1})$, in general may not be straightforward. Here we consider the case of constant or time-invariant symbol transmission and artificial noise energies, where $E_{s,k}(\mathbf{H}_k, P_{k-1}) = E_s, \forall k$ and $\sigma^2_{a,k}(\mathbf{H}_k, P_{k-1}) = \sigma_a^2, \forall k$. For this simpler situation, conditions (13) and (14) become

$$\mathbb{P}(\gamma_k = 1) = \int_\Omega f\left(\frac{||\mathbf{H}_k||^2 E_s}{\sigma_n^2}\right) d\mathbb{P}(\mathbf{H}_k) > 1 - \frac{1}{||A||^2} \tag{17}$$

$$\begin{aligned}
&\mathbb{P}(\gamma_{e,k} = 1) \\
&= \int_{\Omega_e} f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_s/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger \sigma_a^2 + \sigma_e^2}\right) d\mathbb{P}(\mathbf{H}_k, \mathbf{H}_{e,k}) \\
&< 1 - \frac{1}{\rho(A)^2}.
\end{aligned} \tag{18}$$

We next show that (17) and (18) can always be satisfied by choosing E_s and σ_a^2 to be sufficiently large.

Lemma 3.2: i) Suppose $f(.)$ satisfies $f(\mathsf{SNR}) \to 1$ as $\mathsf{SNR} \to \infty$. Then (17) holds for all sufficiently large E_s.

ii) Suppose $f(0) < 1 - \frac{1}{\rho(A)^2}$. Then (18) holds for all sufficiently large σ_a^2.

Proof: i) Fix an $\epsilon > 0$. Partition Ω as $\Omega = \Omega_1 \cup \Omega_2$, where

$$\Omega_1 \triangleq \left\{\mathbf{H}_k : f\left(\frac{||\mathbf{H}_k||^2 E_s}{\sigma_n^2}\right) > 1 - \frac{1}{||A||^2} + \epsilon\right\}$$

and $\Omega_1 \cap \Omega_2 = \emptyset$. Since $f(\mathsf{SNR}) \to 1$ as $\mathsf{SNR} \to \infty$, we have $\mathbb{P}(\Omega_1) \to 1$ and $\mathbb{P}(\Omega_2) \to 0$ as $E_s \to \infty$. Then

$$\mathbb{P}(\gamma_k = 1) = \int_{\Omega_1} f\left(\frac{||\mathbf{H}_k||^2 E_s}{\sigma_n^2}\right) d\mathbb{P}(\mathbf{H}_k)$$

[6] In this paper we consider energy on a per channel use basis and will refer to the terms energy and power interchangeably.

$$+\int_{\Omega_2} f\left(\frac{||\mathbf{H}_k||^2 E_s}{\sigma_n^2}\right) d\mathbb{P}(\mathbf{H}_k)$$
$$> \left(1-\frac{1}{||A||^2}+\epsilon\right)\mathbb{P}(\Omega_1)$$
$$\geq \left(1-\frac{1}{||A||^2}+\epsilon\right) \text{ for all sufficiently large } E_s,$$

and so $\mathbb{P}(\gamma_k=1) > 1-\frac{1}{||A||^2}$ for all sufficiently large E_s.

ii) Since $f(0) < 1-\frac{1}{\rho(A)^2}$, there exists some $\epsilon>0$ such that

$$f(0) < 1-\frac{1}{\rho(A)^2}-\epsilon.$$

Now partition Ω_e as $\Omega_e = \Omega_{e,1}\cup\Omega_{e,2}$, where

$$\Omega_{e,1} \triangleq \Bigg\{(\mathbf{H}_k,\mathbf{H}_{e,k}): f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_s/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger\sigma_a^2+\sigma_e^2}\right) < 1-\frac{1}{\rho(A)^2}-\epsilon\Bigg\}$$

and $\Omega_{e,1}\cap\Omega_{e,2}=\emptyset$. From $f(0) < 1-\frac{1}{\rho(A)^2}$ and the continuity of $f(.)$, it is clear that $\mathbb{P}(\Omega_{e,1})\to 1$ and $\mathbb{P}(\Omega_{e,2})\to 0$ as $\sigma_a^2\to\infty$. Then

$$\mathbb{P}(\gamma_{e,k}=1)$$
$$=\int_{\Omega_{e,1}} f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_s/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger\sigma_a^2+\sigma_e^2}\right) d\mathbb{P}(\mathbf{H}_k,\mathbf{H}_{e,k})$$
$$+\int_{\Omega_{e,2}} f\left(\frac{|\mathbf{H}_{e,k}\mathbf{H}_k^\dagger|^2 E_s/||\mathbf{H}_k||^2}{\mathbf{H}_{e,k}\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_{e,k}^\dagger\sigma_a^2+\sigma_e^2}\right) d\mathbb{P}(\mathbf{H}_k,\mathbf{H}_{e,k})$$
$$< \left(1-\frac{1}{\rho(A)^2}-\epsilon\right)\mathbb{P}(\Omega_{e,1})+\mathbb{P}(\Omega_{e,2})$$
$$\leq \left(1-\frac{1}{\rho(A)^2}-\epsilon\right) \text{ for all sufficiently large } \sigma_a^2,$$

and so $\mathbb{P}(\gamma_{e,k}=1) < 1-\frac{1}{\rho(A)^2}$ for all sufficiently large σ_a^2. ■

B. Comparison with Previous Schemes

Similar behaviour as predicted by (15)-(16) has been obtained in [9], [10] using mechanisms which withhold certain transmissions. In the current paper, one does not withhold any transmissions, so that the remote estimator doesn't suffer from the performance degradation due to non-transmissions.

In the case of constant energies, by choosing E_s and σ_a^2 to be sufficiently large, the conditions (13) and (14) can always be satisfied, no matter how good the eavesdropper channel is. For i.i.d. packet dropping channels, it was shown in [10] that (15)-(16) could be achieved for all eavesdropping probabilities strictly less than one, but the constructed scheme required transmission decisions (or alternatively knowledge of whether previous transmissions were successfully decoded) to be determined at the remote estimator and fed back to the sensor. In contrast, in the current scheme, when using constant energies feedback is not required (though in practice obtaining knowledge of $\mathbf{H}_k$ at the sensor will still require either the transmission of pilot training signals or feedback of $\mathbf{H}_k$ from the estimator to the sensor). What *is* required for the current scheme is the availability of multiple transmit antennas at the sensor and additional energy to generate the artificial noise, but as mentioned in the Introduction multiple antenna technology is commonplace in modern wireless communications.

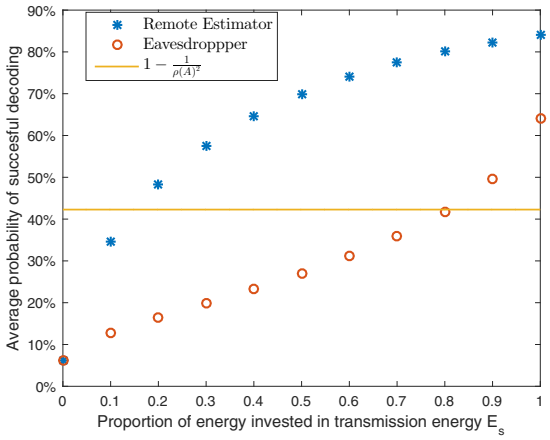

Fig. 2. Average probabilities of successful decoding for different proportions of energy invested in symbol transmission

IV. Numerical Studies

We consider a system 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 communication structure is chosen with $N_T=2$ transmit antennas and 16 Quadrature Amplitude Modulation (16-QAM) for the symbol constellation. For both channels we consider Rayleigh fading, such that $\mathbf{H}_k$ and $\mathbf{H}_{e,k}$ are distributed as complex i.i.d zero mean Gaussian with variance $\sigma_H^2=\sigma_{H_e}^2=1$, which is induced by the assumed block fading. The complex Gaussian channel noise variances are $\sigma_n^2=\sigma_e^2=0.1$ mWh. We will use constant energies as in Section III-A. The complete amount of energy E_C for transmitting and securing the state estimation is defined as:

$$E_C \triangleq E_s+(N_T-1)\sigma_a^2.$$

We consider the case where $E_C=1$ mWh is kept fixed. Fig. 2 plots the average probability for successful remote estimator and eavesdropper decoding vs. different proportions of E_C invested in symbol transmission, obtained by computing the integrals in (17) and (18), where $f(.)$ for M-ary QAM has the form [14, p.226]:

$$f(\mathsf{SNR}) = 1-4\frac{\sqrt{M}-1}{\sqrt{M}}\mathcal{Q}\left(\sqrt{\frac{3\mathsf{SNR}}{M-1}}\right) + 4\left(\frac{\sqrt{M}-1}{\sqrt{M}}\right)^2\mathcal{Q}^2\left(\sqrt{\frac{3\mathsf{SNR}}{M-1}}\right), \quad (19)$$

with $\mathcal{Q}(x)=1/\sqrt{2\pi}\int_x^\infty \exp(-u^2/2)du$ being the Q-function. The integrals are evaluated by Monte Carlo averaging over 10^5 random samples of $(\mathbf{H}_k,\mathbf{H}_{e,k})$. Additionally,

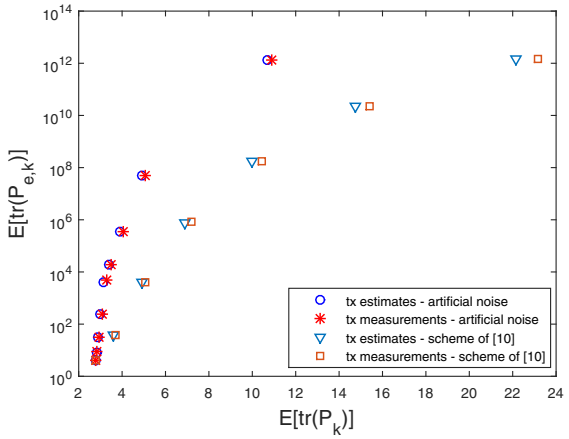

Fig. 3. Artificial noise technique compared to method of [10].

the probability $1-1/\rho(A)^2$ (for eavesdropping) below which $\mathbb{E}[\mathrm{tr}P_{e,k}]$ becomes unbounded is displayed. One can observe that a relatively small proportion (about 20%) of the total energy invested in artificial noise will result in an unbounded expected eavesdropper covariance, while the probability of successful remote estimator decoding does not decrease significantly.

We next compute the expected error covariance at the remote estimator and the eavesdropper for different amounts of artificial noise, while still keeping $E_C = 1$ mWh constant. We consider both cases where local state estimates and measurements are transmitted. Fig. 3 plots $\mathbb{E}[\mathrm{tr}P_k]$ vs. $\mathbb{E}[\mathrm{tr}P_{e,k}]$, where each of the points is obtained by taking the time average of a Monte Carlo run of length 10^6. To reduce variability, each of the simulations was initialized with the same random seed. We see that the results for transmitting local estimates and measurements are similar, with a slightly better trade-off when transmitting local estimates.

For comparison, we also consider the method proposed in [10],[7] where sensor transmissions occur if and only if $\mathrm{tr}(P_{k-1}) \geq \mathrm{tr}(h^t(\bar{P}))$ for some $t \in \mathbb{N}$, where $h^t(.)$ is the t-fold composition of $h(.)$ defined in (8). In this scheme all the energy is used for symbol transmission, i.e. $E_s = E_C = 1$ mWh. Fig. 3 also plots the values of $\mathbb{E}[\mathrm{tr}P_k]$ and $\mathbb{E}[\mathrm{tr}P_{e,k}]$ obtained for different values of t. We observe that the new scheme using artificial noise performs better compared to the method proposed in [10], in that much larger values of $\mathbb{E}[\mathrm{tr}P_{e,k}]$ are obtained for a given $\mathbb{E}[\mathrm{tr}P_k]$. For instance, when $\mathbb{E}[\mathrm{tr}P_k]$ is close to 5, using the scheme of [10] one obtains a simulated $\mathbb{E}[\mathrm{tr}P_{e,k}]$ of around $10^3 - 10^4$, while using the artificial noise technique one obtains an $\mathbb{E}[\mathrm{tr}P_{e,k}]$ of around $10^7 - 10^8$.

V. Conclusion

The use of artificial noise for remote state estimation of linear dynamical systems in the presence of an eavesdropper has been studied in this paper. Numerical results have shown significant performance improvements in this approach when compared to previous schemes which achieve security by withholding certain transmissions.

Other approaches to security using coding have been recently proposed [8], [22]. The artificial noise technique could also be combined with these alternative approaches to further improve performance.

[7]Only the case of local estimate transmission was considered in [10].

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

[4] 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.

[5] 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.

[6] 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.

[7] ——, "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.

[8] 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.

[9] 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.

[10] 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.

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artifical noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[12] D. E. Quevedo, A. Ahlén, A. S. Leong, and S. Dey, "On Kalman filtering over fading wireless channels with controlled transmission powers," *Automatica*, vol. 48, no. 7, pp. 1306 – 1316, Jul. 2012.

[13] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York: McGraw-Hill, 2008.

[14] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. New Jersey: Wiley-Interscience, 2005.

[15] 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.

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

[17] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.

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

[19] K. Gatsis, A. Ribeiro, and G. J. Pappas, "Optimal power management in wireless control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1495–1510, Jun. 2014.

[20] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1453–1464, September 2004.

[21] D. E. Quevedo, J. Østergaard, and A. Ahlén, "Power control and coding formulation for state estimation with wireless sensors," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 2, pp. 413–427, Mar. 2014.

[22] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation codes for perfect secrecy," in *Proc. IEEE Conf. Decision and Control*, Melbourne, Australia, Dec. 2017.