This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

State-Secrecy Codes for Networked Linear Systems

Anastasios Tsiamis, *Student Member, IEEE,* Konstantinos Gatsis, *Member, IEEE,* and George J. Pappas, *Fellow, IEEE*

***Abstract*—In this paper, we study the problem of remote state estimation, in the presence of a passive eavesdropper. An authorized user estimates the state of an unstable linear plant, based on the packets received from a sensor, while the packets may also be intercepted by the eavesdropper. Our goal is to design a coding scheme at the sensor, which encodes the state information, in order to impair the eavesdropper's estimation performance, while enabling the user to successfully decode the sent messages. We introduce a novel class of codes, termed State-Secrecy Codes, which use acknowledgment signals from the user and apply linear time-varying transformations to the current and previously received states. By exploiting the properties of the system's process noise, the channel physical model and the dynamics, these codes manage to be fast, efficient, and suitable for real-time dynamical systems. We prove that under minimal conditions, State-Secrecy Codes achieve perfect secrecy, namely the eavesdropper's minimum mean square error (mmse) grows unbounded almost surely, while the user's estimation performance is optimal. These conditions only require that at least once, the user receives the corresponding packet while the eavesdropper fails to intercept it. Even one occurrence of this event renders the eavesdropper's mmse unbounded with asymptotically optimal rate of increase. State-Secrecy Codes are provided and studied for two cases, i) when direct state measurements are available, and ii) when we only have output measurements. The theoretical results are illustrated in simulations.**

***Index Terms*—Eavesdropping, State-Secrecy Codes, Perfect secrecy, Kalman filtering**

I. Introduction

The recent emergence of the Internet of Things (IoT) as a collection of interconnected sensors and actuators has created a new attack surface for adversarial attacks [1], [2]. Research efforts in the context of control systems have targeted denial-of-service attacks [3] and data integrity of compromised sensors [4], [5], [6], [7]. Another fundamental vulnerability of such interconnected systems is eavesdropping attacks, especially when the underlying medium of communication is of a broadcast nature, i.e. as in wireless systems [8]. This data leakage, not only compromises confidentiality, but could be also used to perform more complex attacks [9].

In this paper, we study passive eavesdropping attacks in the context of real-time dynamical systems, where the source of information is a dynamical system. In many IoT applications, sensors collect state information about the dynamical system and send it to an authorized user, e.g. a controller or a cloud server, through a (wireless) channel, see Figure 1. Our goal is to design codes such that the user receives the confidential state information, while any eavesdroppers are confused about the true state. One of the main challenges in designing such codes for real-time dynamical systems is the tradeoff between code complexity and security. A direction we explore is whether we can exploit model knowledge about the underlying physical processes, i.e. knowledge about the communication channel or the system's dynamics, in order to design simple and secure secrecy codes.

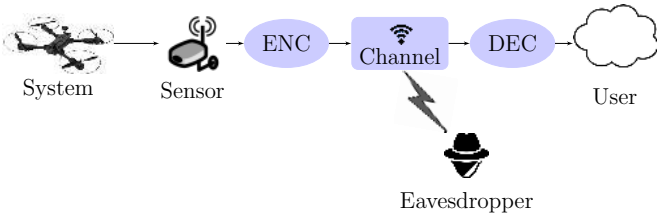


Fig. 1: A sensor sends confidential information about the state of a dynamical system to an authorized user, e.g. a controller or a cloud server. Meanwhile, an eavesdropper might intercept the sent messages. The goal is to design encoder-decoder pairs such that confidentiality is protected.

Most of the current defense mechanisms involve encryption-based tools [10]. These are generic tools, which do not require any model knowledge about the underlying physical processes. However, their confidentiality guarantees are based on the assumption that the eavesdroppers have limited computational power. Some encryption methods, e.g. the AES encryption [10], also require the transmitter and the receiver to share a secret key beforehand. In some cases, encryption may also introduce computation and communication overheads, which might be significant for real-time systems [11]. Chaotic synchronization has also been proposed for secrecy [12]. A chaotic dynamical system acts as an encoder of arbitrary information sources. The eavesdropper cannot easily decode the messages unless it knows the chaotic system's parameters, which are assumed to be secret. Such methods are also independent of the underlying physical process and require prior shared secrets between the receiver and the transmitter.

Another direction is to develop defense mechanisms in the physical layer of wireless communications [13], [14]. These methods exploit model knowledge about the underlying channel used for communication, e.g., the wireless medium, to offer provable guarantees about confidentiality against eaves-

This work was supported in part by ONR N00014-17-1-2012, and by NSF CNS-1505799 grant and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy.

The authors are with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104. Emails: {atsiamis,kgatsis,pappasg}@seas.upenn.edu

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

droppers. Information-theoretic approaches [15]–[17] define a notion of secrecy capacity of channels and give conditions about the existence of codes such that the eavesdropper receives no information. Remote estimation problems have also been studied in this context [18]–[20]. Finding such codes is challenging in practice and requires knowledge of the eavesdropper's channel, which may not be available. Nonetheless, in the case of packet erasure channels, those erasures can be exploited to randomly create secrets, thus leading to more practical defense mechanisms [21].

New approaches, which we term control-theoretic, were recently employed in [22]–[24]. Motivated by physical layer security methods, they exploit the channel model. However, the key innovation with respect to previous approaches is that they also take advantage of the system dynamics to provide security guarantees, which in contrast to, e.g., encryption approaches, do not depend on the eavesdropper's computational capabilities. In that respect, these approaches are specialized for sources which are dynamical systems. Another distinction is that the security and performance objectives are expressed in terms of control/estimation theoretic metrics, e.g. the minimum mean square error (mmse). In [22]–[24], the main goal is to achieve large mmse for the eavesdropper, while the user's mmse remains small. A secrecy mechanism was used, which withholds information, either randomly [22] or deterministically [23], [24]. In the case of unstable systems, under certain conditions, the eavesdropper's expected mmse is shown to grow to infinity while the user's expected mmse remains bounded. However, the secrecy guarantees hold only in expectation; with high probability the actual eavesdropper's mmse is small frequently. The user's estimation performance is also degraded as a side effect.

This paper is the first within the control-theoretic approaches to introduce encoding. We develop a novel class of codes, called State-Secrecy Codes, which explicitly exploit the system dynamics. When direct state measurements are available, the system's state is encoded by subtracting a weighted version of the user's most recently received state from the current state. This operation has a simple implementation and only requires acknowledgment signals from the user back to the sensor. By exploiting the underlying model, i.e. the dynamics, the inherent process noise of the system, and the channel's randomness, State-Secrecy Codes achieve strong guarantees with low computational cost. In particular, confidentiality is guaranteed if at some time the user receives the encoded state while the eavesdropper fails to intercept it. Due to our code, a single occurrence of this event, which we call critical event, makes the eavesdropper lose important information about the system state. Then, as time passes, the dynamics amplify the uncertainty of the eavesdropper created by this information loss, regardless of the eavesdropper's computational capabilities.

In Section II we present the problem formulation. The dynamical system is modeled as linear, while the channel is modeled as a packet-drop one. Similar to [19], [20], [22], [24], we assume that the system is unstable (see Section II for discussion). Both the user and the eavesdropper know the coding scheme and use minimum mean square error estimators as decoders. We introduce a novel control-theoretic notion of perfect secrecy, requiring that the eavesdropper's mmse grows unbounded almost surely, while the user's mmse is optimal. In Section III, where direct state measurements are available, we show that by employing State-Secrecy Codes, perfect secrecy can be guaranteed under remarkably mild conditions (Theorem 1). Even one occurrence of the critical event renders the eavesdropper's error unbounded with asymptotically optimal rate of increase (Corollary 1). In Section IV, we extend the results to the case of output measurements (Theorem 2). The sensor performs local Kalman filtering before applying a State-Secrecy Code to the local estimates. In summary, our main contributions, are the following:

- Our work is the first to introduce coding within the control-theoretic approaches. By exploiting the dynamics, state-secrecy codes manage to be fast and secure. The security guarantees do not depend on the computational capabilities of the eavesdropper. Moreover, we do not require the existence of prior private shared information between the sensor and the user.
- This is the first work that achieves unbounded eavesdropper's mmse almost surely using a control-theoretic approach. Meanwhile, the user's estimation performance remains optimal. This supersedes the results in [22], [23] where unbounded eavesdropper's mmse is achieved only in expectation and the user's performance is degraded.
- The condition for perfect secrecy is remarkably minimal and channel-free. It is only required that the critical event occurs at least once, i.e. at some time the user receives the encoded message while the eavesdropper misses it. This will hold in most channels of practical interest.

In Section V we discuss how the user's estimation scheme can be made robust against random acknowledgment drops, quantization errors, and some other practical issues. We conclude this paper by illustrating the performance of State-Secrecy Codes in simulations in Section VI, and with remarks in Section VII. All proofs are included in the Appendices. A paper with preliminary results appeared in [25]. Sections III-A, IV, V are new and they study the eavesdropper's mmse rate of increase, the output measurement case, and practical considerations respectively. After this paper was written, we extended state-secrecy codes to stable systems–see [26].

II. Problem formulation

A. Dynamical system model

The considered remote estimation architecture is shown in Figure 2 and consists of a sensor observing a dynamical system, a legitimate user, and an eavesdropper. The dynamical system is discrete-time, linear, and has the following form:

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

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

where $x_k \in \mathbb{R}^n$ is the state and $y_k \in \mathbb{R}^m$ is the output. Matrices $A \in \mathbb{R}^{n\times n}$ and $C \in \mathbb{R}^{m\times n}$ are the system and output matrices respectively. Signals $w_k \in \mathbb{R}^n$ and $v_k \in \mathbb{R}^m$ are the process and measurement noises respectively and are modeled as independent Gaussian random variables with zero mean and

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

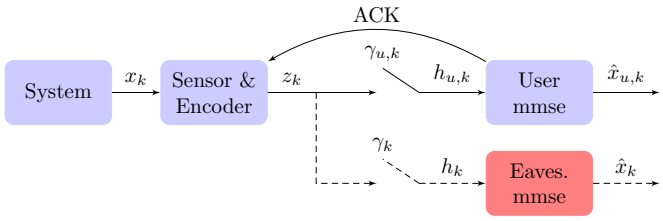


Fig. 2: A sensor collects the output y_k of system (1) and transmits an encoded version z_k of it over the channel. The messages might be dropped by the user, as captured by $\gamma_{u,k}$. Meanwhile, they might be intercepted by the eavesdropper, as captured by γ_k. To decode the messages, both entities compute the minimum mean square error (mmse) estimates $\hat{x}_{u,k}$ and $\hat{x}_k$ respectively.

covariance matrices Q and R. The initial state x_0 is also a Gaussian random variable with zero mean and covariance Σ_0 and is independent of the noise signals. Matrices Q, R, Σ_0 are assumed to be positive definite. In more compact notation $Q, R, \Sigma_0 \succ 0$, where $\succ$ ($\succeq$) denotes comparison in the positive definite (semidefinite) cone. We also assume that the pair (A, C) is detectable. All system and noise parameters A, C, Q, R, Σ_0 are assumed to be **public knowledge**, available to the sensor, the user, and the eavesdropper. Throughout this paper, we assume the system is unstable.

Assumption 1. *We assume that the dynamical system* (1) *is unstable i.e., its spectral radius is* $\rho(A) = \max_i |\lambda_i(A)| > 1$.

Estimation of unstable open-loop systems has been a problem of independent interest in control systems–see for example [27]. It has also been studied in the presence of eavesdroppers, i.e. [19], [20], [22], [24]. The ultimate goal is to close the loop and apply control, but first, estimation of the open-loop systems should be studied. Besides, due to network imperfection, feedback might fail occasionally. In this case, the controlled system goes open-loop and might be unstable. During this open-loop phase, the system's state might start growing unbounded, hence, it is critical to perform state estimation to monitor it.

B. Channel model

The sensor communicates over a channel with two outputs/receivers as shown in Figure 2. The input to the channel is denoted by $z_k \in \mathbb{R}^n$. The first output, denoted by $h_{u,k}$, is the authorized one to the user, while the second, denoted by h_k, is the unauthorized one to the eavesdropper. Communication follows the packet-based paradigm commonly used in networked control systems [27]–[29]. We neglect quantization effects in the main sections (Sections III, IV), but we discuss quantization issues in Section V.

Communication with the user is unreliable, i.e., may undergo packet drops. Respectively, communication is not secure against the eavesdropper, i.e., the latter may intercept transmitted packets. We denote by $\gamma_{u,k} \in \{0, 1\}$ the outcome of the user packet reception at time k, and by $\gamma_k \in \{0, 1\}$ the outcome of the eavesdropper's packet interception. When $\gamma_{u,k} = 1$ (or $\gamma_k = 1$), then the reception (interception) is successful. Otherwise the reception (interception) is not successful and the respective packet is dropped. Thus, the outputs of the channel are modeled as:

$$h_{u,k} = \begin{cases} z_k, & \text{if } \gamma_{u,k} = 1 \\ \varepsilon, & \text{if } \gamma_{u,k} = 0 \end{cases}, \; h_k = \begin{cases} z_k, & \text{if } \gamma_k = 1 \\ \varepsilon, & \text{if } \gamma_k = 0 \end{cases} \tag{3}$$

where symbol ε, is used to represent the "no information" outcome. The channel outcomes $\{\gamma_{u,k}, \gamma_k, k = 0, 1, \dots\}$ are assumed to be independent of the initial state x_0, the process noise w_k, and the measurement noise v_k, for $k = 0, 1, \dots$. No specific joint distribution of the channel outcomes is assumed.

In addition to the main channel, the user can reliably send acknowledgment signals back to the sensor via the reverse channel. We deal with unreliable acknowledgments in Section V. Thus, at any time step the sensor knows what is the latest received message z_k at the user. Meanwhile, we assume that the eavesdropper is able to intercept all acknowledgment signals In that respect, we model a powerful eavesdropper. On the other hand, neither the sensor nor the user have any knowledge about the eavesdropper's intercept successes γ_k.

C. Encoder definition

The sensor collects output measurements y_k and encodes them by sending $z_k \in \mathbb{R}^p$ over the channel at each time step k, where p is an integer to be designed. Under this definition and by (3), the channel outputs $h_{u,k}$, h_k take values in $\mathbb{R}^p \cup \{\varepsilon\}$. The encoder may compute z_k given all the information at the sensor at time k, i.e. current and past outputs y_t for $t \leq k$, past sent messages z_t for $t < k$, as well as past user's channel outcomes $\gamma_{u,t}$ for $t < k$:

$$z_k = f_k \left(y_k, y_t, z_t, \gamma_{u,t}, t < k \right), \tag{4}$$

where f_k is a function from $\mathbb{R}^{m(k+1)+pk} \times \{0, 1\}^k$ to $\mathbb{R}^p$.

D. MMSE Estimation

Both the user and the eavesdropper know the coding scheme and use the minimum mean square error (mmse) estimate to decode the received/intercepted messages. This estimate depends on their information up to time k. We define the batch vector of received channel outputs $\boldsymbol{h}_{u,0:k} = (h_{u,0}, \dots, h_{u,k})$ and channel outcomes $\boldsymbol{\gamma}_{u,0:k} = (\gamma_{u,0}, \dots, \gamma_{u,k})$ for the user. The eavesdropper's batch vectors $\boldsymbol{h}_{0:k}$, $\boldsymbol{\gamma}_{0:k}$ are defined similarly. Then, the user's information at time k is denoted by $\mathcal{I}_k^u = \{\boldsymbol{h}_{u,0:k}\}$, with $\mathcal{I}_{-1}^u = \emptyset$. Respectively, we denote the eavesdropper's information by

$$\mathcal{I}_k = \left\{ \boldsymbol{h}_{0:k}, \boldsymbol{\gamma}_{u,0:k} \right\}, \; \mathcal{I}_{-1} = \emptyset. \tag{5}$$

The two information sets are asymmetric, i.e. the eavesdropper has the additional information of the user's reception success history. The eavesdropper's mmse estimate $\hat{x}_k$ and the respective covariance matrix P_k are given by:

$$\hat{x}_k = \mathbb{E}\left\{ x_k | \mathcal{I}_k \right\}, \quad P_k = \mathrm{Cov}\left\{ x_k | \mathcal{I}_k \right\}, \tag{6}$$

where $\mathrm{Cov}\left\{ x_k | \mathcal{I}_k \right\} = \mathbb{E}\left\{ (x - \hat{x}_k)(x - \hat{x}_k)' | \mathcal{I}_k \right\}$. The user's mmse estimate $\hat{x}_{u,k}$ and the respective mmse covariance matrix $P_{u,k}$ are defined similarly.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

E. Problem

The goal of this work is to design a coding scheme at the sensor, so that *perfect secrecy* is achieved, introduced in the following definition. We require the eavesdropper's mmse to grow unbounded, while the user successfully decodes the information and has optimal estimation performance. The secrecy requirement is motivated by the worst case performance for the eavesdropper, i.e. the open-loop prediction case when all packets are missed. In this situation, the eavesdropper maintains a trivial open-loop estimate $\hat{x}_k^{op} = 0$ and the respective mmse diverges to infinity due to the unstable dynamics–see also Section III-A. The user's estimation scheme is optimal when at the successful reception times, the mmse estimate is the same as if no packet had been dropped (see also [30]).

Definition 1 (Perfect Secrecy)**.** *Given system* (1)*,* (2) *and channel model* (3)*, a coding scheme* (4) *achieves perfect secrecy if and only if both of the following conditions hold:*

(i) *the user's performance is optimal:*

$$\left.\begin{aligned}\hat{x}_{u,k} &= \mathbb{E}\left\{x_k|\boldsymbol{y}_{0:k}\right\}\\ P_{u,k} &= \mathrm{Cov}\left\{x_k|\boldsymbol{y}_{0:k}\right\}\end{aligned}\right\}, \text{ when } \gamma_{u,k}=1, \quad (7)$$

where $\boldsymbol{y}_{0:k} = (y_0, \dots, y_k)$.

(ii) *the eavesdropper's mmse diverges to infinity*[1] *with probability one:*

$$\mathbf{tr}\, P_k \overset{a.s.}{\to} \infty, \quad (8)$$

where $\mathbf{tr}$ *is the trace operator.*

This notion of secrecy is asymptotic, which is an inherent property of the problem. Even without any interceptions, the eavesdropper can maintain the trivial open-loop prediction estimate, i.e. $\hat{x}_k^{op} = 0$, that has unbounded but finite estimation error at any time k. Moreover, we remark that (8) guarantees aggregate state secrecy in that, at least one but not necessarily all eigenvalues of the eavesdropper's error covariance grow unbounded (see also Section VI). With this definition, we formally present the problem that we solve in this paper.

Problem. *Given system* (1)*,* (2) *and channel model* (3)*, design a coding scheme* (4) *such that perfect secrecy is achieved, as described in Definition 1.*

In the following sections, we present and analyze State-Secrecy Codes for two cases. In Section III, we ignore the output model ($C = I$, $R = 0$) and assume that the sensor measures the state perfectly. In Section IV, we include the output model (general C, $R \succ 0$). In both cases, perfect secrecy is achieved by exploiting the acknowledgment signals, the unstable system dynamics, the process noise, as well as the randomness of the channel.

III. Perfect Secrecy with State Measurements

In this section, we introduce State-Secrecy Codes for the case of direct state measurements ($C = I$ and $R = 0$). Informally, the sensor encodes and transmits the current state measurement x_k as a weighted state difference of the form $x_k - A^{k-t_k}x_{t_k}$, where x_{t_k} is a previous state called the *reference state* of the encoded message, for some $t_k < k$ depending on k. The sensor and the user can agree on this reference state via the acknowledgment signals, e.g., it can be the most recent state received at the user's end. At the user's side, no information is lost with this encoding; upon receiving a new message $x_k - A^{k-t_k}x_{t_k}$, she can first recover x_k by adding $A^{k-t_k}x_{t_k}$ and then notify the sensor to use x_k as the reference state for the next transmission.

Algorithm 1 State-Secrecy Code

Input: A and x_k at each $k \geq 0$
Output: Encoded signals z_k, for all $k \geq 0$.
Let t represent the time of user's most recent message.
Initialize $t = -1$, $x_{-1} = 0$
for $k = 0, 1, \dots$ **do**
  Transmit $z_k = x_k - A^{k-t}x_t$
  if Acknowledgment received **then** $t = k$
  end if
end for

On the other hand, on the event that the eavesdropper fails to intercept that reference packet x_{t_k} at time t_k, her error starts increasing. That is because the eavesdropper misses the reference state x_{t_k} and, thus, cannot decode a following packet of the form $x_k - A^{k-t_k}x_{t_k}$ to obtain x_k. But this also obstructs the eavesdropper from decoding future packets, as any following reference state x_k for some $k > t_k$, depends on the current reference state x_{t_k} and so on. This triggers an irreversible chain reaction effect, which combined with the unstable system dynamics, leads to an exponentially growing eavesdropper's estimation error. For this reason, we call this event, when the user receives a packet at time t_k while the eavesdropper misses it, the *critical event*.

Let us now formally present the coding scheme. We define the *reference time* t_k to be the time of the most recent successful reception at the user before k:

$$t_k = t_k(\boldsymbol{\gamma}_{u,0:k-1}) = \max\left\{t:\ 0 \leq t < k,\ \gamma_{u,t} = 1\right\}. \quad (9)$$

Before the first successful transmission, when the set $\{t : 0 \leq t < k :\ \gamma_{u,t} = 1\}$ is empty, we use the convention $t_k = -1$, $x_{-1} = 0$.

Definition 2 (State-Secrecy Code)**.** *Given the unstable system matrix* A *in* (1)*, a State-Secrecy Code* [2] *applies the following time-varying linear operation*

$$z_k = x_k - A^{k-t_k}x_{t_k}, \quad (10)$$

where t_k *is the reference time defined in* (9)*.* ◇

The intuition about selecting the weighting factor A^{t-t_k} can be found in Remark 1. The implementation of the scheme is described in Algorithm 1. The memory required for the encoder is minimal ($\mathcal{O}(n)$) and the only computational burden is a matrix-vector multiplication ($\mathcal{O}(n^2)$). The critical event

[1] The secrecy requirement here is different from the one in [26] for stable systems, where we require the eavesdropper's mmse covariance to converge to a finite value.

[2] For stable systems in [26], we use the code $z_k = x_k - L^{k-t_k}x_{t_k}$, for some matrix $L \neq A$, which leads to a different code.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

formally defined below, is crucial for reinforcing secrecy with our coding scheme.

Definition 3 (Critical event)**.** *A critical event occurs at time k if the user receives the packet while the eavesdropper misses it:*

$$\gamma_{u,k} = 1,\ \gamma_k = 0. \tag{11}$$

An example to clarify the coding scheme and the critical event is presented next.

Example 1. *Suppose that for $k = 0, 1, 2, 3$ we have the channel outcomes as shown in the first three rows of the following table:*

k	0	1	2	3
user $\gamma_{u,k}$	0	1	1	1
eavs. γ_k	1	0	1	1
t_k	-1	-1	1	2
z_k	x_0	x_1	$x_2 - Ax_1$	$x_3 - Ax_2$
user $h_{u,k}$	ε	x_1	$x_2 - Ax_1$	$x_3 - Ax_2$
eavs. h_k	x_0	ε	$x_2 - Ax_1$	$x_3 - Ax_2$

The last four rows of the table are constructed using the definitions of the reference times (9)*, of the coding scheme* (10)*, and the channel outcomes* (3)*. Notice that the critical event occurs at time $k = 1$, when the user receives x_1, while the eavesdropper misses it. Then, the user can recover x_2 at time $k = 2$ by adding Ax_1 to $h_{u,2}$. However, since the eavesdropper does not know x_1, she cannot precisely recover x_2. Since $\gamma_{u,2} = 1$, x_2 is the next reference state at time $k = 3$. Thus, the eavesdropper will also not be able to recover x_3, from $h_3 = x_3 - Ax_2$. A single occurrence of the critical event impairs future estimation at the eavesdropper.* ◇

The following theorem, for the case of state measurements, formally proves the previous observations. If the critical event $\{\gamma_{u,k_0} = 1,\ \gamma_{k_0} = 0\}$ occurs at some time k_0, then the eavesdropper's mmse starts to grow unbounded exponentially fast. On the other hand, the user's performance is optimal.

Theorem 1 (Perfect secrecy)**.** *Consider system* (1)*, with channel model* (3) *and coding scheme* (10)*. If*

$$\mathbb{P}(\gamma_{u,k} = 1,\ \gamma_k = 0,\ \textit{for some } k \geq 0) = 1, \tag{12}$$

then:

(i) *perfect secrecy is achieved according to Definition 1.*

(ii) *conditioned on the event $\{\gamma_{u,k_0} = 1,\ \gamma_{k_0} = 0\}$ for some $k_0 \geq 0$, the eavesdropper's mmse grows unbounded:*

$$\mathbf{tr}\, P_k \geq c\rho\left(A\right)^{2(k-k_0)},\ \textit{for } k \geq k_0 \tag{13}$$

where P_k is the mmse covariance defined in (6) *and $c > 0$ is a constant independent of k_0.* ◇

The above theorem is remarkable as the condition (12) for perfect secrecy is minimal. It only requires the critical event, when the user receives a message without the eavesdropper intercepting it, to occur at least once. Any joint distribution of packet receptions and interceptions that satisfies this condition is covered, and in this sense the result is channel-free.

The proof of Theorem 1 is a consequence of the following lemma, which can be thought as the worst case, in terms of secrecy, of Theorem 1. That is when the critical event $\{\gamma_{u,k_0} = 1,\ \gamma_{k_0} = 0\}$ occurs at time k_0 and the eavesdropper receives all the following packets for $k > k_0$.

Lemma 1 (Worst case analysis)**.** *Consider system* (1) *with channel model* (3) *and coding scheme* (10)*. Define the events*

$$\mathcal{B} = \{\gamma_{u,k_0} = 1,\ \gamma_{k_0} = 0\},\ \textit{for some } k_0 \geq 0 \tag{14}$$

$$\mathcal{C} = \{\gamma_k = 1, \textit{for all } k \geq k_0 + 1\}. \tag{15}$$

If both $\mathcal{B}$, $\mathcal{C}$ occur for some $k_0 \geq 0$, then

$$P_k = A^{k-k_0} P_{k_0} \left(A'\right)^{k-k_0} \tag{16}$$

for $k \geq k_0$ in $\mathcal{B} \cap \mathcal{C}$, where $'$ denotes the transpose matrix. ◇

Notice that the linear recursion $P_k = A^{k-k_0} P_{k_0} \left(A'\right)^{k-k_0}$ is unstable with rate $\rho\left(A^2\right)$. Hence, even in the most pessimistic scenario for confidentiality, the eavesdropper still has unbounded mmse. In the general case when the eavesdropper does not intercept all packets after k_0, the eavesdropper's mmse will be even larger (cf. Lemma 5 in Appendix).

Remark 1. *The choice of A^{k-t_k} is pivotal for achieving secrecy. From* (1)*, the difference $x_k - A^{k-t_k} x_{t_k}$ is a linear combination of the process noises from time $t_k + 1$ up to k:*

$$x_k - A^{k-t_k} x_{t_k} = \sum_{j=t_k+1}^{k} A^{k-j} w_j.$$

If the critical event occurs at some time k_0, then the eavesdropper permanently loses all information about the process noise w_{k_0} at time k_0. This loss of information is amplified by the unstable system dynamics over time leading to unbounded eavesdropper's mmse. ◇

Remark 2. *Suppose that the channel outcomes are independent over time, and assume that there is a positive probability that the critical event occurs at any time k, i.e., $P\left(\gamma_{u,k} = 1,\ \gamma_k = 0\right) > \delta > 0$. For example, in a wireless communication setting this may be due to attenuation of the transmitted signal at the eavesdropper or due to environmental interference. By the Borel-Cantelli lemma [31], the critical event will occur infinitely often. Hence, the condition* (12) *for perfect secrecy of Theorem 1 will be satisfied.* ◇

A. Rate of increase of eavesdropper's error covariance

Under the proposed coding scheme, the rate of increase of the eavesdropper's mmse is asymptotically optimal. Once the critical event occurs, the eavesdropper's mmse starts increasing as the open-loop prediction mmse, i.e. when all measurements are lost. This open-loop mmse is the largest possible error in expectation for the eavesdropper as we explain in (20) later.

Formally, the open-loop prediction estimate and error covariance matrix are defined as:

$$x_k^{op} = \mathbb{E}\left\{x_k\right\} = 0, \quad P_k^{op} = \mathrm{Cov}\left\{x_k\right\}, \tag{17}$$

which implies:

$$P_k^{op} = AP_{k-1}^{op} A' + Q, \tag{18}$$

with $P_0^{op} = \Sigma_0$.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

The following result, which is a corollary of Theorem 1, shows that the eavesdropper's mmse under our coding scheme is lower bounded by the open-loop prediction mmse up to a multiplicative constant, once the critical event occurs. This constant depends on the time k_0 of the first critical event.

Corollary 1 (Rate of increase)**.** *Consider system* (1)*, with channel model* (3) *and coding scheme* (10)*. Let k_0 be the first time the critical event* (11) *occurs. Let also P_k^{op}, P_k be the open-loop prediction covariance matrix* (18) *and the eavesdropper's covariance matrix* (6) *respectively. Then,*

$$c\rho(A)^{-2k_0}\,\mathbf{tr}\,P_k^{op} \leq \mathbf{tr}\,P_k,\ \textit{for } k \geq k_0 \tag{19}$$

where $c > 0$ is some constant independent of k_0 $\diamond$

Remark 3. *The open-loop prediction mmse is the maximum possible in expectation since it holds that:*

$$P_k^{op} = \mathrm{Cov}\left\{x_k\right\} \succeq \mathbb{E}\left\{\mathrm{Cov}\left\{x_k|\mathcal{I}_k\right\}\right\} = \mathbb{E}\left\{P_k\right\} \tag{20}$$

for any information set $\mathcal{I}_k$, where the inequality follows by [31, p. 230]. From (19)*, under our coding scheme and once the critical event occurs, the eavesdropper's mmse error increases at least as fast as the open-loop prediction one. In that sense, our coding scheme is asymptotically optimal with respect to the rate of increase of the eavesdropper's mmse error.*

The determining factor in inequality (19) is the time k_0 of the first critical event. If the critical event occurs more than once, although the eavesdropper's error gets even larger, its rate of growth does not differ from the case when it occurs just once. If the probability of the critical event occurring is one, then also $P\left(\rho(A)^{-2k_0} > 0\right) = 1$. Hence, with even a single occurrence, the error starts increasing as in the open-loop asymptotically.

One caveat is that the first time k_0 the critical event occurs is in general random and not in our control. If the eavesdropper's interception rate is very high, the event may take some time to occur. In this case, secrecy is compromised at the first time steps and the term $\rho(A)^{-2k_0}$ is small.

Remark 4. *A possible remedy to accelerate the critical event is to force it by using another more secure and perhaps more expensive encoding, e.g., encryption [10] or some physical-layer security scheme [21]. In this case, it is sufficient to securely and reliably transmit just the first packet at time $k = 0$ using such an additional scheme. Then, letting our simple coding scheme take over achieves perfect secrecy. In that sense, State-Secrecy Codes can be effectively used alongside other coding schemes.*

IV. Perfect secrecy with output measurements

In this section, we adapt the coding scheme (10) to achieve perfect secrecy in the case of output measurements (general C, $R \succ 0$). Before applying any coding, we propose that the sensor implements a local Kalman filter scheme as shown in Figure 3. The architecture of employing a local Kalman filter on the sensor's side before transmission is inspired by previous work [28], [30]. This architecture requires additional computational cost at the sensor, mainly because of the matrix inversion of the Kalman filter. Nonetheless, if we transmit one message at a time, it is necessary to have a local Kalman filter for the user's estimation performance to be optimal [30].

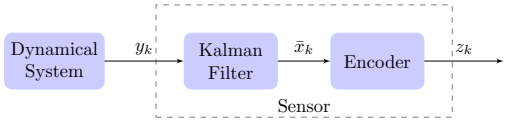


Fig. 3: In the case of output measurements, the sensor first computes the local Kalman Filter estimate $\bar{x}_k$. Then, it computes the encoded signal z_k.

The sensor's local Kalman Filter estimates are denoted by:

$$\bar{x}_k = \mathbb{E}\left\{x_k|\boldsymbol{y}_{0:k}\right\},\ \bar{x}_{-1} = \mathbb{E}\left\{x_0\right\} = 0 \tag{21}$$

with prediction mmse covariance matrix:

$$\bar{P}_{k+1|k} = \mathrm{Cov}\left\{x_{k+1}|\boldsymbol{y}_{0:k}\right\},\ \bar{P}_{0|-1} = \mathrm{Cov}\left\{x_0\right\} = \Sigma_0 \tag{22}$$

where $\boldsymbol{y}_{0:k} = (y_0, \ldots, y_k)$. In this case, the State-Secrecy Code is computed with respect to the local state estimates:

$$z_k = \bar{x}_k - A^{k-t_k}\bar{x}_{t_k}, \tag{23}$$

where t_k is the reference time defined in (9).

Now, recall that in the classic Kalman filter derivation [32], we have the following recursive equation:

$$\bar{x}_k = A\bar{x}_{k-1} + K_k\left(y_k - CA\bar{x}_{k-1}\right) = A\bar{x}_{k-1} + K_k\bar{w}_k, \tag{24}$$

where $\bar{w}_k$ denotes the innovation sequence $y_k - CA\bar{x}_{k-1}$ and

$$K_k = \bar{P}_{k|k-1}C'\left(C\bar{P}_{k|k-1}C' + R\right)^{-1}$$

is the Kalman gain. The innovation sequence $y_k - CA\bar{x}_{k-1}$ is Gaussian white noise [32] with covariance $C\bar{P}_{k|k-1}C' + R$. In this sense, equation (24) is similar to the state equation (1).

Since the pair (A, C) is detectable and $Q \succ 0$ (so that $\left(A, Q^{1/2}\right)$ is controllable), the covariance matrix $\bar{P}_{k|k-1}$ of the Kalman filter converges to a limit $\bar{P}$, which is the positive semidefinite solution of the discrete algebraic Riccati equation:

$$\bar{P} = A\bar{P}A' + Q - A\bar{P}C'\left(C\bar{P}C' + R\right)^{-1}C\bar{P}A' \tag{25}$$

while the Kalman gain converges to

$$K = \bar{P}C'\left(C\bar{P}C' + R\right)^{-1}. \tag{26}$$

We assume that at time $k = 0$ the sensor has an initial local state estimate with covariance equal to the steady state error covariance $\Sigma_0 = \bar{P}$. Since the Kalman filter converges fast, it is reasonable to assume that it has already converged at the beginning of the system operation.

The following theorem states that coding scheme (23) achieves the same secrecy guarantees as in the direct state information case.

Theorem 2. *Consider system* (1) *with output model* (2)*, channel model* (3)*, coding scheme* (23) *and $\Sigma_0 = \bar{P}$. If*

$$\mathbb{P}(\gamma_{u,k} = 1,\ \gamma_k = 0,\ \textit{for some } k \geq 0) = 1, \tag{27}$$

then:

(i) *perfect secrecy is achieved according to Definition 1.*

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

(ii) *conditioned on the event* $\{\gamma_{u,k_0}=1,\,\gamma_{k_0}=0\}$ *for some* $k_0\geq 0$*, the eavesdropper's mmse grows unbounded:*

$$\mathbf{tr}\,P_k\geq c\rho\left(A\right)^{2(k-k_0)}-c',\ \textit{for } k\geq k_0, \tag{28}$$

where P_k *is the mmse covariance defined in* (6) *and* $c,c'>0$ *are some constants independent of* k_0. ◇

To prove Theorem 2, we can use the techniques of the previous section to show an intermediate result first; that the eavesdropper's error with respect to $\bar{x}_k$ grows unbounded when the critical event occurs, as the following lemma states. We denote the mean square estimate of $\bar{x}_k$ and the corresponding conditional error covariance matrix by:

$$\eta_k=\mathbb{E}\left\{\bar{x}_k|\mathcal{I}_k\right\},\quad H_k=\mathrm{Cov}\left\{\bar{x}_k|\mathcal{I}_k\right\}, \tag{29}$$

with $\bar{\Sigma}_0=\mathrm{Cov}\left\{\bar{x}_0\right\}=K\left(C\bar{P}C'+R\right)K'$.

Lemma 2. *Consider system* (1) *with output model* (2)*, channel model* (3)*, coding scheme* (23) *and* $\Sigma_0=\bar{P}$*. Conditioned on the event* $\mathcal{B}=\{\gamma_{u,k_0}=1,\,\gamma_{k_0}=0\}$ *for some* $k_0\geq 0$*, the eavesdropper's mmse with respect to* $\bar{x}_k$ *grows unbounded:*

$$\mathbf{tr}\,H_k\geq c\rho\left(A\right)^{2(k-k_0)},\ \textit{for } k\geq k_0, \tag{30}$$

where H_k *is the mmse covariance defined in* (29) *and* $c>0$ *is a constant independent of* k_0. ◇

We use this intermediate result to show that the eavesdropper's error with respect to x_k also grows unbounded when the critical event occurs. The main idea is to lower-bound the error $\mathbf{tr}\,P_k$ in terms of $\mathbf{tr}\,H_k$.

In the next section we show how to make State-Secrecy codes more robust against unreliable backwards channels and quantization errors. We also discuss some practical issues.

V. Extensions and practical issues

A. Unreliable acknowledgments

The previous theoretical results require the backwards channel to be reliable. In this subsection, we show how State Secrecy Codes could be adapted to deal with random acknowledgment packet drops as shown in Figure 4. The following analysis is for the case of direct state measurements, but it can be repeated for the case of output measurements as well.

Let $\gamma_{a,k}\in\{0,1\}$ be the indicator of the acknowledgment transmission outcome at time k, for $k=0,1,\ldots$. If $\gamma_{a,k}=1$, then the sensor successfully receives the acknowledgment from the user. Otherwise, if $\gamma_{a,k}=0$, the acknowledgment signal is dropped. We assume that the backward channel outcomes are independent of the state x_k.

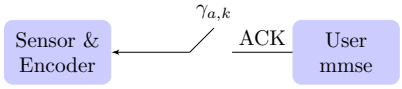


Fig. 4: The backward channel model can also be unreliable. If $\gamma_{a,k}=1$ then the sensor receives the acknowledgment signal from the user. If $\gamma_{a,k}=0$ then the acknowledgment signal is dropped.

Under the original coding scheme (10), unreliable acknowledgments might cause disagreement between the sensor and the user about the reference time t_k. To overcome this problem, we propose that the sensor, instead of (10), transmits:

$$z_k=\left\{x_k-A^{k-\tilde{t}_k}x_{\tilde{t}_k},\,\tilde{t}_k\right\}, \tag{31}$$

where

$$\tilde{t}_k=\max\left\{t:\ 0\leq t<k,\,\gamma_{u,t}=1,\,\gamma_{a,t}=1\right\}, \tag{32}$$

is the most recent time that the user successfully received the respective packet and also the sensor successfully received the acknowledgment. Knowing the correct value of $\tilde{t}_k$, the user can always decode the successfully received packets.

On the other hand, the condition for the eavesdropper's error to grow unbounded is slightly different. A critical event now occurs at time k if: i) the user receives the packet at time k; ii) the eavesdropper fails to intercept the packet at time k; iii) the sensor successfully receives the acknowledgment signal at time k. The following theorem shows that if this event occurs at least once, then perfect secrecy is achieved. The proof is similar to the one of Theorem 1 and, thus, omitted.

Theorem 3 (Perfect secrecy under Unreliable ACKs)**.** *Consider system* (1)*, with forward channel model* (3)*, backward channel model described by* $\gamma_{a,k}$ *and coding scheme* (31)*. If*

$$\mathbb{P}(\gamma_{u,k}=1,\,\gamma_k=0,\,\gamma_{a,k}=1\ \textit{for some}\ k\geq 0)=1, \tag{33}$$

then:

(i) *perfect secrecy is achieved according to Definition 1.*

(ii) *conditioned on the event*

$$\{\gamma_{u,k_0}=1,\,\gamma_{k_0}=0,\,\gamma_{a,k_0}=1\}$$

for some $k_0\geq 0$*, the eavesdropper's mmse grows unbounded as in* (13)*,*

where P_k *is the mmse covariance defined in* (6) *and* $c>0$ *is a constant independent of* k_0. ◇

It is slightly more difficult for the critical event to occur, since we have the additional requirement for the acknowledgments. Still, as in the analysis of Remark 2, in most channels of practical interest the critical event will occur not only once but infinitely often.

B. Quantization error

Without any modifications, the scheme might be vulnerable to quantization errors. Denote by $[x]$ the quantized version of a variable x. In practice, the user can only receive quantized signals $[z_k]$ instead of z_k. Under scheme (4), if we do not compensate for quantization, the user's decoding will be:

$$\hat{x}_{u,k}=[z_k]+A^{k-t_k}\hat{x}_{u,t_k},\ \text{when}\ \gamma_{u,k}=1 \tag{34}$$

where $\hat{x}_{u,k}$ is the user's mmse estimate. However, due to quantization errors we might have $\hat{x}_{u,t_k}\neq x_{t_k}$. Then, under the user's decoding these quantization errors might be accumulated to future decodings and amplified by the unstable A^{k-t_k}, which can lead to unbounded user's error.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

Our scheme can be made robust to quantization errors if the user and the sensor use the same quantizer. Instead of (4), the sensor can transmit the following:

$$z_k = x_k - A^{k-t_k} x_{q,t_k}, \tag{35}$$

where

$$x_{q,k} = [z_k] + A^{k-t_k} x_{q,t_k},\ x_{q,-1} = 0. \tag{36}$$

With $x_{q,k}$, the sensor simulates the user's decoding procedure and compensates for quantization errors.

Under the decoding process (34) and by the definition of $x_{q,k}$, it follows that $x_{q,k} = \hat{x}_{u,k}$ when $\gamma_{u,k} = 1$. Thus, the quantization error does not propagate and it is not amplified anymore since:

$$\hat{x}_{u,k} - x_k = [z_k] - z_k, \text{ when } \gamma_{u,k} = 1, \tag{37}$$

which implies that the error between the true state and the estimated state is just the quantization error of z_k. This is similar to having an error of the form $[x_k] - x_k$, when we use no encoder. More information about quantizers can be found in other references, e.g. [33].

C. Channel errors

The channel model assumed that if a packet is successfully received, then it will also be intact. This is justified because practical communication schemes include the use of cyclic redundancy checks (CRC) for error detection that can drive the probability of undetected errors to very small values [34, Ch. 4].

In the unlikely event that such an error is introduced, the user's estimation will be compromised under our code. In this case, we can use some of the following solutions in practice.

1) The sensor can restart the whole process occasionally, i.e. after some time $T > 0$ reset $t_k = -1$, $x_{-1} = 0$. Since the probability of undetected channel error for the user is small, this T can be selected to be large. Under this variation, the secrecy guarantees will be weaker, i.e. the eavesdropper will have large but bounded mmse.
2) The user can send z_k back to the sensor to check if it is corrupted. The code works almost like the acknowledgment drop case. However, for the critical event to occur at time k, the eavesdropper should also miss the reverse transmission at time k; the reverse channel should also be unreliable for the eavesdropper.
3) The user can use encryption, e.g. AES encryption, **only occasionally** to transmit back to the sensor the encrypted $\hat{x}_{u,k}$; if the sensor discovers any error, it can compensate for it in the next transmission. At the same time encryption guarantees that the eavesdropper cannot decrypt the message as long as she does not have access to the encryption key. As in case i), this transmission can occur every T time steps for some $T > 0$, where T can be large since the error probability is small.

Notice that the last two methods exploit the reverse channel. It is an interesting future direction to explore more efficient error correction methods which exploit the reverse channel.

D. Active attacks

The present coding scheme is based on the assumption that the eavesdropper is passive. If the eavesdropper is active, then our scheme will be vulnerable to integrity attacks, e.g. fake acknowledgments might damage the user's estimation. Dealing with integrity attacks, is a much different problem and requires other approaches–see [35]. In practice, we could combine different codes to defend against active attacks and eavesdropping at the same time. In particular, we could employ Message Authentication Codes (MACs) (see [35]) alongside our coding scheme, i.e. on top of the acknowledgment signals and the encoded messages sent from the sensor to the user. MAC is an authentication tool from cryptography where the receiver can check: i) the authenticity of the message (sender's identity) and ii) whether the received message has been tampered (data integrity). The analysis of such a method is left for future work.

Finally, we would like to point out that our scheme does not make the user estimation more vulnerable to jamming attacks. The communication failures due to jamming can be treated as packet/acknowledgment drops in our coding scheme.

VI. Simulations

In this section, we illustrate the efficiency of our proposed coding schemes in numerical simulations in MATLAB. We consider two scenarios. In the first one, we compare the user's, the eavesdropper's, and the open loop estimation performance in the case of output measurements. In the second one, we contrast the performance achieved by the State-Secrecy Codes with the one achieved by the mechanisms in [22], [23], in the case of direct state measurements. The system under consideration has state matrix $A = \begin{bmatrix} 1.1 & 0.1 \\ 0 & 0.5 \end{bmatrix}$ and process noise covariance matrix $Q = \begin{bmatrix} 0.6 & 0.2 \\ 0.2 & 0.5 \end{bmatrix}$. For the channel model, we assume that the channel outcomes are independent across time and stationary with probabilities $P(\gamma_{u,k} = i, \gamma_k = j) = p_{ij}$, for $i, j \in \{0, 1\}$. For the estimation scheme of the eavesdropper we used equation (41) in Appendix. Since the user can decode all signals, we used the formula:

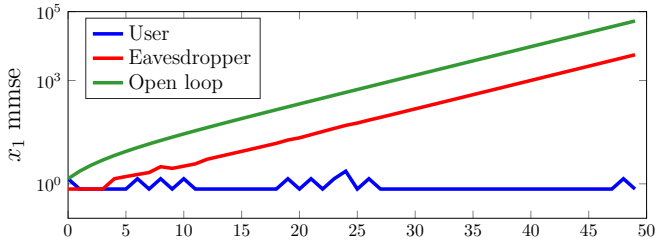
$$P_{u,k} = \begin{cases} \bar{P} - KC\bar{P} & \text{if } \gamma_{u,k} = 1 \\ AP_{u,k-1}A' + Q & \text{if } \gamma_{u,k} = 0 \end{cases}$$

where $\bar{P} - KC\bar{P} = 0$ in the case of direct state measurements.

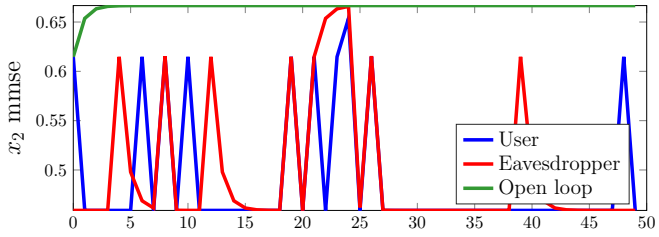
For the first scenario with output state measurements, we assume that $C = \begin{bmatrix} 1 & 1 \end{bmatrix}$, $R = 1$ and the channel outcomes have the probabilities $p_{11} = 0.7$, $p_{00} = 0.1$, $p_{01} = 0.1$ and $p_{10} = 0.1$. We also assume $\Sigma_0 = \bar{P}$ (see (25)). Figure 5 shows the user's, the eavesdropper's and the open-loop prediction mmse over time for the states x_1 and x_2 (the two diagonal elements of the covariance matrices respectively). As shown in Figure 5, the eavesdropper's mmse for the unstable state x_1 starts growing unbounded at time $k = 3$, when the first critical event occurs; the rate of increase is asymptotically the same as in the open-loop case. It is worth noting that the eavesdropper's mmse for the stable state x_2 remains bounded.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control



(a) mmse for state x_1 and one sample of channel outcomes.



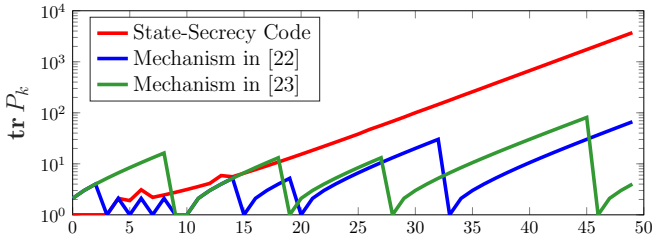
(b) mmse for state x_2 and one sample of channel outcomes.

Fig. 5: We compare the eavesdropper's, user's and open loop mmse for the states x_1 and x_2 in the case of output measurements. The first critical event occurs at time $k = 3$. After that, the eavesdropper's mmse regarding the unstable part grows unbounded with asymptotically the same rate as the open-loop error. The eavesdropper still has bounded mmse for the stable state x_2. However, the open-loop prediction mmse for x_2 shows that the eavesdropper cannot have unbounded mmse with respect to the stable dynamics, regardless the code.

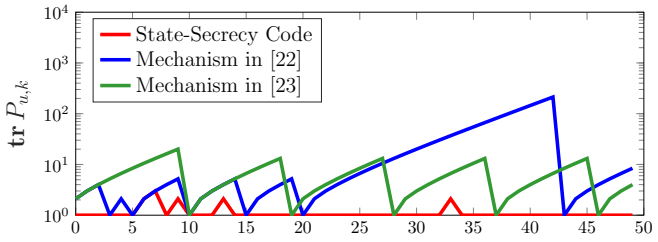
But it is fundamentally impossible to have unbounded mmse for the stable part, regardless the code, as even the open-loop prediction mmse is bounded for state x_2.

In the second scenario, we assume direct state information ($C = I$, $R = 0$). We consider channel outcomes with probabilities $p_{11} = 0.54$, $p_{00} = 0.04$, $p_{01} = 0.06$, $p_{10} = 0.36$, and initial state error covariance matrix $\Sigma_0 = Q$. First, we compare the performance of our code with the one of the mechanisms in [22] and [23], in the case of one random sequence of channel outcomes–see Figure 6. The comparison is with respect to the user's and eavesdropper's mmse ($\mathbf{tr}\, P_{u,k}$ and $\mathbf{tr}\, P_k$ respectively). For the mechanism in [22], which randomly withholds state information with probability p, we selected $p = 0.21$. For the infinite horizon mechanism in [23], which transmits state information only if the user loses more than t consecutive packets, we used $t = 9$. Figure 6 shows that the eavesdropper's mmse is small very often under the mechanisms in [22], [23], since unboundedness is guaranteed in expectation, not almost surely. In contrast, our coding scheme achieves unbounded eavesdropper's mmse for every channel sequence with probability one. Also notice that the user's estimation performance is degraded in [22], [23].

Second, for completeness, we repeat the comparison for the expected mmse, i.e. the averages $\mathbb{E}\{\mathbf{tr}\, P_k\}$ over all channel sequences–see Figure 7. The expected values were computed approximately based on Monte Carlo simulation with 100000 iterations. Initially, the eavesdropper's expected mmse under our scheme is smaller than the one in [22], [23]. This is because the critical event for some samples takes some time

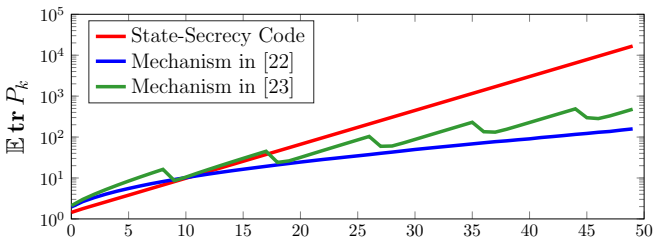


(a) Eavesdropper's mmse for one sample of channel outcomes.

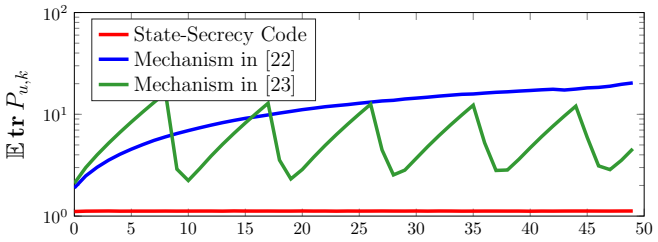


(b) User's mmse for one sample of channel outcomes.

Fig. 6: We compare our coding scheme with the mechanisms in [22], [23] for a typical channel outcome sequence in the case of direct state measurements. For the log-plots, we use function $\log(x + 1)$ instead of $\log(x)$. It outperforms the mechanisms in both confidentiality (eavesdropper's mmse) and efficiency (user's mmse).



(a) Eavesdropper's simulated expected mmse.



(b) User's simulated expected mmse.

Fig. 7: We compare the expected mmse under our coding scheme with the one under the schemes in [22], [23]. For the expectations we implemented Monte Carlo simulation with 100000 iterations.

to occur. However, our scheme will eventually outperform them and will provide an unbounded estimation error at a higher rate at the eavesdropper, both almost surely and in expectation. Meanwhile, the estimation performance of the user is compromised in [22], [23], while in our scheme there is no such undesirable effect.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

VII. Conclusion

The presence of an eavesdropper adds new challenges to the problem of remote estimation. Nonetheless, by using a simple State-Secrecy Code, which explicitly exploits the system dynamics, we can achieve powerful confidentiality guarantees with minimal computational cost and no communication overhead. At the same time, the user's estimation performance remains optimal. Perfect secrecy is achieved under minimal and channel-free conditions; a single occurrence of the critical event, when the user receives more information than the eavesdropper, is sufficient.

Having studied secure estimation of open-loop unstable systems, the next step is to adapt the codes to closed-loop control systems. Another open problem is to find secure coding schemes where the output filtering is performed by the user and not by the sensor. Future work also includes experimental evaluation of the proposed scheme in a real system and comparison with encryption and physical layer security schemes.

Appendix A
Estimation formulas

In this appendix, we derive two formulas for the eavesdropper's estimation error covariance in the case of state measurements. The first one, equation (41) in Lemma 4, expresses the conditional expectation with respect to the non-Gaussian eavesdropper's information $\mathcal{I}_k$ (see (5)) in terms of conditional expectations with respect to Gaussian variables. The second one, equation (43) in Proposition 1, is the main estimation formula, which will be used to prove Lemma 1. An identical analysis can be followed to find the estimation formulas for η_k, H_k in (29) for the case of output measurements. Thus, it is omitted.

We denote by $\boldsymbol{x}_{0:k} = \left[\ x_k', \ldots, x_0'\ \right]'$ the batch state vector up to time k taking values in $\mathbb{R}^{(k+1)n}$. We also denote the batch channel outcomes up to time k by

$$\boldsymbol{g}_{0:k} = \left(\boldsymbol{\gamma}_{u,0:k}, \boldsymbol{\gamma}_{0:k}\right) = \left(\gamma_{u,0}, \ldots, \gamma_{u,k}, \gamma_0, \ldots, \gamma_k\right) \tag{38}$$

taking values in the set $\{0,1\}^{2k+2}$. Now let

$$s_{0:k} = \left(s_{u,0}, \ldots, s_{u,k}, s_0, \ldots, s_k\right)$$

be any fixed element of $\{0,1\}^{2k+2}$. For symbol economy, we write $s = s_{0:k}$ and we omit the subscript $0:k$. Given this element s, we define $s_{0:m} = \left(s_{u,0}, \ldots, s_{u,m}, s_0, \ldots, s_m\right)$ to be the part of s until time m, for $m \leq k$. We also define $s_{u,0:m} = \left(s_{u,0}, \ldots, s_{u,m}\right)$ to be the part of s related to the user until time m, for $m \leq k$.

Next, we alternatively describe the information $\mathcal{I}_k$ that the eavesdropper has on the event that the channel outcomes $\boldsymbol{g}_{0:k}$ take exactly the value s. Formally it is the set

$$\begin{aligned} &\mathcal{J}_k(s) = \left\{z_m(s) : s_m = 1,\, m \leq k\right\}, \text{ where} \\ &z_m(s) = x_m - A^{m - t_m\left(s_{u,0:m-1}\right)} x_{t_m\left(s_{u,0:m-1}\right)} \end{aligned} \tag{39}$$

and $t_m(\cdot)$ is defined in (9). In other words, given fixed channel outcomes, the eavesdropper only keeps the successfully intercepted channel outputs from $\boldsymbol{h}_{0:k}$ (see (3)). Notice that every element of $\mathcal{J}_k(s)$ depends linearly on $\boldsymbol{x}_{0:k}$. The next example clarifies this definition.

Example 2. *Suppose we are given* $s = s_{0:2} = (s_{u,0}, s_{u,1}, s_{u,2}, s_0, s_1, s_2) = (1,0,1,1,0,1)$. *Then,* $t_0(s) = -1$, $t_1(s) = t_2(s) = 0$ *and*

$$\mathcal{J}_2(s) = \left\{x_2 - A^2 x_0, x_0\right\}.$$

Notice that $\mathcal{J}_2(s)$ *depends only on* $\boldsymbol{x}_{0:2}$ *and is Gaussian.* ◇

A. Sigma algebra of $\mathcal{I}_k$.

Before we prove the estimation formulas, we describe the sigma-algebra $\sigma(\mathcal{I}_k)$, induced by the eavesdropper's information $\mathcal{I}_k$ (see (5)). The following lemma describes the sigma algebra $\sigma(\mathcal{I}_k)$, in terms of $\sigma\left(\mathcal{J}_k(s)\right)$.

Lemma 3 (Sigma algebra of $\mathcal{I}_k$)**.** *Fix a* k *and let* $S = \{0,1\}^{2k+2}$. *Let* $\mathcal{I}_k$, $\boldsymbol{g}_{0:k}$, *and* $\mathcal{J}_k(s)$ *be as defined in* (5), (38), *and* (39). *Then every set* D *in the sigma algebra of* $\mathcal{I}_k$ *has the following form:*

$$D = \bigcup_{s \in S} \left\{\boldsymbol{g}_{0:k} = s, \mathcal{J}_k(s) \in F_s\right\}, \tag{40}$$

for some $F_s \in \sigma\left(\mathcal{J}_k(s)\right)$, *for all* $s \in S$.

Proof. Since $\boldsymbol{g}_{0:k}$ is discrete-valued, we can partition every set $D \in \sigma(\mathcal{I}_k)$ according to the values of $\boldsymbol{g}_{0:k}$ as:

$$D = \bigcup_{s \in S} D_s,$$

where

$$D_s = \left\{\boldsymbol{g}_{0:k} = s, \boldsymbol{h}_{0:k} \in E_s\right\},$$

for some set E_s that belongs in $\sigma\left(\boldsymbol{h}_{0:k}\right)$. But we have that:

$$\left\{\gamma_t = 0\right\} \Leftrightarrow \left\{h_t = \varepsilon\right\}, \text{ for all } 0 \leq t \leq k.$$

Moreover, if $\boldsymbol{g}_{0:k} = s$, this fully determines t_m for $m \leq k$. As a result, the set D_s can be equivalently described by

$$D_s = \left\{\boldsymbol{g}_{0:k} = s, \mathcal{J}_k(s) \in F_s\right\},$$

for some $F_s \in \sigma\left(\mathcal{J}_k(s)\right)$. □

B. First estimation formula

Here, we express the conditional expectation with respect to $\mathcal{I}_k$ in terms of conditional expectations with respect to $\mathcal{J}_k(s)$. This is presented in the following lemma, and is a consequence of Lemma 3 and independence of $\boldsymbol{x}_{0:k}$ and $\boldsymbol{g}_{0:k}$.

Lemma 4. *Fix a* k *and let* $\mathcal{I}_k$, $\boldsymbol{g}_{0:k}$, *and* $\mathcal{J}_k(s)$ *be as defined in* (5), (38), *and* (39). *Suppose* $Y = Y\left(\boldsymbol{g}_{0:k}\right)$ *is a random vector, such that:*

$$Y\left(\boldsymbol{g}_{0:k}\right) = \sum_{s \in S} Y(s)\, \mathbb{1}_{\left\{\boldsymbol{g}_{0:k} = s\right\}}$$

where $Y(s)$ *are integrable and depend only on* $\boldsymbol{x}_{0:m}$, *for some* m *(possibly different than* k*). Then:*

$$\mathbb{E}\left\{Y | \mathcal{I}_k\right\} = \mathbb{E}\left\{Y(s) | \mathcal{J}_k(s)\right\} \ \textit{in}\ \left\{\boldsymbol{g}_{0:k} = s\right\}. \tag{41}$$

By $\mathbb{1}$ *we denote the indicator function.* ◇

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

Proof. Define $S = \{0,1\}^{2k+2}$. Since $\boldsymbol{g}_{0:k}$ is $\sigma(\mathcal{I}_k)$-measurable, we have:

$$\begin{aligned}\mathbb{E}\{Y|\mathcal{I}_k\} &= \sum_{s\in S} \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{I}_k\} \\ &= \mathbb{E}\{Y(s)|\mathcal{I}_k\} \text{ in } \{\boldsymbol{g}_{0:k}=s\}.\end{aligned}$$

Thus, it is sufficient to show that

$$\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{I}_k\} = \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{J}_k(s)\}. \quad (42)$$

Since $\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{I}_k\} = \mathbb{E}\{\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} Y(s)|\mathcal{I}_k\}$, the truth of (42) can be verified if we show the basic property of conditional expectation:

$$\mathbb{E}\{\mathbb{1}_D \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} Y(s)\} = \mathbb{E}\{\mathbb{1}_D \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{J}_k(s)\}\},$$

for any $D \in \sigma(\mathcal{I}_k)$. From Lemma 3, we have:

$$D = \bigcup_{s\in S} D_s,$$

where

$$D_s = \{\boldsymbol{g}_{0:k} = s, \mathcal{J}_k(s) \in F_s\},$$

for some $F_s \in \sigma(\mathcal{J}_k(s))$. As a result, $\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{1}_D = \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{1}_{\mathcal{J}_k(s)\in F_s}$.

Observe that $\mathcal{J}_k(s)$ and $Y(s)$ depend only on the values of x_t, $t \le m$, while the indicator $\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}}$ depends on the channel outcomes. Hence:

$$\begin{aligned}&\mathbb{E}\{\mathbb{1}_D \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} Y(s)\} = \mathbb{E}\{\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{1}_{\mathcal{J}_k(s)\in F_s} Y(s)\} \\ &= \mathbb{E}\{\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}}\} \mathbb{E}\{\mathbb{1}_{\mathcal{J}_k(s)\in F_s} Y(s)\} \\ &= \mathbb{E}\{\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}}\} \mathbb{E}\{\mathbb{1}_{\mathcal{J}_k(s)\in F_s} \mathbb{E}\{Y(s)|\mathcal{J}_k(s)\}\} \\ &= \mathbb{E}\{\mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{1}_{\mathcal{J}_k(s)\in F_s} \mathbb{E}\{Y(s)|\mathcal{J}_k(s)\}\} \\ &= \mathbb{E}\{\mathbb{1}_D \mathbb{1}_{\{\boldsymbol{g}_{0:k}=s\}} \mathbb{E}\{Y(s)|\mathcal{J}_k(s)\}\}\end{aligned}$$

where the second and fourth equalities follow from independence, while the third follows from the properties of conditional expectation. □

The benefit of Equation (41) is that it allows us to work with $\mathcal{J}_k(s)$, which includes only Gaussian elements, that depend linearly on $\boldsymbol{x}_{0:k}$. In contrast, it is not easy to work directly with $\mathcal{I}_k$, which is non-Gaussian.

C. Second estimation formula

We finally prove our main estimation formula for P_k by leveraging the technical intermediate formula (41).

Proposition 1 (Estimation formula)**.** *Consider system* (1)*, channel* (3) *under coding scheme* (10)*. Fix any $k \ge 0$. Let the covariance matrix of x_k and z_k given $\mathcal{I}_{k-1}$ be written in a block form:*

$$\mathrm{Cov}\left\{\begin{bmatrix} x_k \\ z_k \end{bmatrix} | \mathcal{I}_{k-1}\right\} = \begin{bmatrix} \Sigma_{xx} & \Sigma_{xz} \\ \Sigma_{zx} & \Sigma_{zz} \end{bmatrix}$$

Then, $\Sigma_{xx} = AP_{k-1}A' + Q$ if $k > 0$ and $\Sigma_{xx} = \Sigma_0$ if $k = 0$, where P_{k-1} is the estimation error covariance of the eavesdropper at time $k-1$ defined in (6)*, and the conditional covariance at time k is given by:*

$$P_k = \Sigma_{xx} - \gamma_k \Sigma_{xz} (\Sigma_{zz})^\dagger \Sigma_{zx}, \quad (43)$$

where $(\cdot)^\dagger$ denotes the Moore-Penrose pseudoinverse [36]. ◇

Proof. First, we prove the formula for Σ_{xx}. When $k = 0$, $\mathcal{I}_{-1}$ is an empty set, thus, $\Sigma_{xx} = \Sigma_0$. When $k > 0$, we argue that $\Sigma_{xx} = AP_{k-1}A' + Q$. By the system dynamics in (1) we have that $x_k = Ax_{k-1} + w_k$. But by assumption the noise w_k is independent of the state vectors $x_0, \ldots, x_{k-1}$ and of $\boldsymbol{g}_{0:k}$ and, hence, also independent of $\mathcal{I}_{k-1}$. Thus, the state prediction is $\mathbb{E}\{x_k|\mathcal{I}_{k-1}\} = A\hat{x}_{k-1}$ and the covariance of $x_k - \mathbb{E}\{x_k|\mathcal{I}_{k-1}\}$ given $\mathcal{I}_{k-1}$ equals $\Sigma_{xx} = AP_{k-1}A' + Q$.

Second, we prove (43). Fix an element $s = s_{0:k} \in \{0,1\}^{2k+2}$, and consider the event $C = \{\boldsymbol{g}_{0:k} = s_{0:k}\}$. By the definition (6) of P_k and equation (41), we have $P_k = \mathrm{Cov}\{x_k|\mathcal{J}_k(s_{0:k})\}$ in C. There exist two cases:

Case I: $s_k = 0$. In this case, by the definition (39), we have $\mathcal{J}_k(s_{0:k}) = \mathcal{J}_k(s_{0:k-1})$. Therefore:

$$\begin{aligned}P_k &= \mathrm{Cov}\{x_k|\mathcal{J}_k(s_{0:k})\} = \mathrm{Cov}\{x_k|\mathcal{J}_k(s_{0:k-1})\} \\ &= \mathrm{Cov}\{x_k|\mathcal{I}_{k-1}\} = \Sigma_{xx} \text{ in } C.\end{aligned}$$

where the third equality follows from (41).

Case II: $s_k = 1$. Here, by (41):

$$\begin{aligned}P_k &= \mathrm{Cov}\{x_k|\mathcal{J}_k(s_{0:k})\} \\ &= \mathrm{Cov}\{x_k|\mathcal{J}_k(s_{0:k-1}), z_k(s_{0:k})\}, \text{ in } C,\end{aligned}$$

where $z_k(s_{0:k})$ is defined in (39). Since all variables are Gaussian, we can compute the posterior estimation error using the Schur complement formula applied to the covariance matrix of x_k and $z_k(s_{0:k})$ given $\mathcal{J}_k(s_{0:k-1})$ (see [32]). By (41), in C we have

$$\mathrm{Cov}\left\{\begin{bmatrix} x_k \\ z_k(s_{0:k}) \end{bmatrix} | \mathcal{J}_k(s_{0:k-1})\right\} = \begin{bmatrix} \Sigma_{xx} & \Sigma_{xz} \\ \Sigma_{zx} & \Sigma_{zz} \end{bmatrix}.$$

Hence, by the Schur's complement formula, we have $P_k = \Sigma_{xx} - \Sigma_{xz}(\Sigma_{zz})^\dagger \Sigma_{zx}$ in C, when $s_k = 1$.

We can describe both cases with one equation:

$$\begin{aligned}P_k &= \Sigma_{xx} - s_k \Sigma_{xz} (\Sigma_{zz})^\dagger \Sigma_{zx} \text{ in } C \\ &= \Sigma_{xx} - \gamma_k \Sigma_{xz} (\Sigma_{zz})^\dagger \Sigma_{zx} \text{ in } C,\end{aligned}$$

since $s_k = \gamma_k$ in C. But this holds for any event $C = \{\boldsymbol{g}_{0:k} = s_{0:k}\}$. Thus, the result holds everywhere, since the events $\{\boldsymbol{g}_{0:k} = s\}$, $s \in \{0,1\}^{2k+1}$ are a partition of the probability space. □

APPENDIX B
PROOFS OF RESULTS

A. Proof of Lemma 1

The proof follows by induction. For $k = k_0$ it is immediate. Suppose it is true for $k-1 \ge k_0$. Since in $\mathcal{C}$ the eavesdropper receives all packets for $k > k_0$, we have $\gamma_k = 1$, for $k > k_0$. Hence, according to the recursive formula (43), to find P_k, we should compute the covariance of x_k and z_k, conditioned on $\mathcal{I}_{k-1}$. By independence of w_k from $\mathcal{I}_{k-1}$, it follows that $x_k - \mathbb{E}\{x_k|\mathcal{I}_{k-1}\} = A(x_{k-1} - \hat{x}_{k-1}) + w_k$. Now, we claim $z_k - \mathbb{E}\{z_k|\mathcal{I}_{k-1}\} = w_k$, for $k > k_0$, which we prove in the

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

next paragraph. Thus, the covariance matrix of x_k and z_k, conditioned on $\mathcal{I}_{k-1}$ is:

$$\mathrm{Cov}\left\{\left[\begin{array}{c} x_k \\ z_k \end{array}\right] |\mathcal{I}_{k-1}\right\} = \left[\begin{array}{cc} AP_{k-1}A'+Q & Q \\ Q & Q \end{array}\right], \text{ in } \mathcal{B}\cap\mathcal{C}$$

Thus, by (43), for $k > k_0$ we have

$$P_k = AP_{k-1}A' + Q - QQ^{-1}Q = AP_{k-1}A' \tag{44}$$

in $\mathcal{B}\cap\mathcal{C}$. Hence, by the induction hypothesis, we get (16).

Finally, we prove the claim

$$z_k - \mathbb{E}\left\{z_k|\mathcal{I}_{k-1}\right\} = w_k, \text{ for } k > k_0, \text{ in } \mathcal{B}\cap\mathcal{C}. \tag{45}$$

Since the critical event happened at time k_0, the reference time at k_0+1 is $t_{k_0+1} = k_0$ in $\mathcal{B}$ (equation (9)). Hence, all reference times t_k , for $k > k_0$ satisfy $t_k \geq k_0$ in $\mathcal{B}$. There are only two possible cases depending on $\gamma_{u,k-1}$:
Case I: $t_k = k-1 \geq k_0$, when $\gamma_{u,k-1} = 1$
Case II: $t_k = t_{k-1} \geq k_0$ when $\gamma_{u,k-1} = 0$
In the former one, the intercepted signal by (10) is $z_k = x_k - Ax_{k-1} = w_k$. But the process noise w_k is independent of $\mathcal{I}_{k-1}$, thus, $\mathbb{E}\left\{w_k|\mathcal{I}_{k-1}\right\} = 0$ and equation (45) holds. In the latter one, we have

$$z_k = x_k - A^{k-t_k}x_{t_k} = x_k - A^{k-t_{k-1}}x_{t_{k-1}}, \tag{46}$$

since $t_k = t_{k-1}$. Adding and subtracting Ax_{k-1} at the right hand side of the above equation, we obtain

$$\begin{aligned} z_k &= x_k - Ax_{k-1} + A\left(x_{k-1} - A^{k-1-t_{k-1}}x_{t_{k-1}}\right) \\ &= w_k + Az_{k-1}, \end{aligned} \tag{47}$$

where the second equality follows from the definition of z_{k-1} in (10). But $k-1 > k_0$ (since $\gamma_{u,k-1} = 0$), thus, the eavesdropper has intercepted z_{k-1}, which in turn implies $z_{k-1} = \mathbb{E}\left\{z_{k-1}|\mathcal{I}_{k-1}\right\}$ in $\mathcal{B}\cap\mathcal{C}$ (follows from (41) and properties of conditional expectation). Hence, from (47), $\mathbb{E}\left\{z_k|\mathcal{I}_{k-1}\right\} = Az_{k-1}$ in $\mathcal{B}\cap\mathcal{C}$, which along with (47) prove equation (45). □

B. Monotonicity results.

In this subsection, we prove that the case described in Lemma 1, where the eavesdropper receives everything after the critical event, is indeed the worst case of Theorem 1, in terms of confidentiality. To formally describe the above statement, we need to define a new channel outcome sequence $\tilde{\gamma}_{u,k}$, $\tilde{\gamma}_k$ that is coupled with the original outcome sequence $\gamma_{u,k}$, γ_k as follows:

$$\begin{aligned} &(\tilde{\gamma}_{u,k}, \tilde{\gamma}_k) = (\gamma_{u,k}, \gamma_k), \text{ for all } 0 \leq k \leq k_0 \\ &(\tilde{\gamma}_{u,k}, \tilde{\gamma}_k) = (\gamma_{u,k}, 1), \text{ for all } k > k_0, \end{aligned} \tag{48}$$

i.e. in this new outcome sequence, the eavesdropper receives everything after time k_0 but the user's outcomes remain the same. Similarly to (38), we denote the batch vector of the new outcomes up to time k by $\tilde{\boldsymbol{g}}_{0:k}$. Next, we define again the channel outputs (3), the eavesdropper's information (5) and the covariance matrix (6), but with the original channel outcomes γ_k replaced by $\tilde{\gamma}_k$:

$$\tilde{h}_k = \left\{\begin{array}{ll} z_k, & \text{if } \tilde{\gamma}_k = 1 \\ \varepsilon, & \text{if } \tilde{\gamma}_k = 0 \end{array}\right., \quad \tilde{\mathcal{I}}_k = \left\{\tilde{\boldsymbol{h}}_{0:k}, \boldsymbol{\gamma}_{u,0:k}\right\}, \tag{49}$$

$$\tilde{P}_k = \mathrm{Cov}\left\{x_k|\tilde{\mathcal{I}}_k\right\}. \tag{50}$$

The next lemma formally states that when the eavesdropper receives all measurements from some time k_0 on, then it has the smallest possible covariance matrix.

Lemma 5 (Comparison lemma)**.** *Let P_k be the nominal error covariance matrix, as defined in* (6) *and $\tilde{P}_k$ be the error covariance matrix of the coupled process as defined in* (48)–(50)*. Then, with probability one:*

$$P_k \succeq \tilde{P}_k, \text{ for all } k \geq 0. \tag{51}$$

◇

Before we prove Lemma 5, we prove an intermediate result. The following lemma compares the estimation error covariance of a Gaussian random vector x, given two different Gaussian information sets $\mathcal{J}_1$ and $\mathcal{J}_2$, when the first information set is smaller than the second or $\mathcal{J}_1 \subseteq \mathcal{J}_2$. Intuitively, the result states that given more information we have less error.

Lemma 6. *Let $x \in \mathbb{R}^m$ be normal and let $\mathcal{J}_1$, $\mathcal{J}_2$ be two sets, the elements of which are vectors that depend linearly on x. Then, if $\mathcal{J}_1 \subseteq \mathcal{J}_2$, we have:*

$$\mathrm{Cov}\left\{x|\mathcal{J}_1\right\} \succeq \mathrm{Cov}\left\{x|\mathcal{J}_2\right\}. \tag{52}$$

Proof. Since x is normal and the vectors in the sets $\mathcal{J}_1$, $\mathcal{J}_2$ depend linearly on x, the joint distributions of $(x, \mathcal{J}_i)$, $i = 1, 2$ are normal. Then, it is a well know property of joint normal distributions that the conditional covariance matrices are constant or $\mathbb{E}\left\{\mathrm{Cov}\left\{x|\mathcal{J}_1\right\}\right\} = \mathrm{Cov}\left\{x|\mathcal{J}_1\right\}$ and $\mathbb{E}\left\{\mathrm{Cov}\left\{x|\mathcal{J}_2\right\}\right\} = \mathrm{Cov}\left\{x|\mathcal{J}_2\right\}$ [32].

Next, recall that:

$$\mathrm{Cov}\left\{x|\mathcal{J}_1\right\} = \mathbb{E}\left\{(x - \mathbb{E}\left\{x|\mathcal{J}_1\right\})(x - \mathbb{E}\left\{x|\mathcal{J}_1\right\})'|\mathcal{J}_1\right\}.$$

Adding and subtracting $\mathbb{E}\left\{x|\mathcal{J}_2\right\}$, we obtain the sum of four terms:

$$\mathrm{Cov}\left\{x|\mathcal{J}_1\right\} = T_1 + T_2 + T_2' + T_3,$$

where:

$$\begin{aligned} T_1 =& \mathbb{E}\left\{\left(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\}\right)\left(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\}\right)'|\mathcal{J}_1\right\} \\ T_2 =& \mathbb{E}\left\{\left(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\}\right)\left(\mathbb{E}\left\{x|\mathcal{J}_2\right\} - \mathbb{E}\left\{x|\mathcal{J}_1\right\}\right)'|\mathcal{J}_1\right\} \\ T_3 =& \mathrm{Cov}\left\{\mathbb{E}\left\{x|\mathcal{J}_2\right\}|\mathcal{J}_1\right\} \end{aligned}$$

Since $\mathcal{J}_1 \subseteq \mathcal{J}_2$, by the tower property:

$$\begin{aligned} T_1 &= \mathbb{E}\left\{\mathbb{E}\left[(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\})(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\})'|\mathcal{J}_2\right]|\mathcal{J}_1\right\} \\ &= \mathbb{E}\left\{\mathrm{Cov}\left\{x|\mathcal{J}_2\right\}|\mathcal{J}_1\right\} = \mathrm{Cov}\left\{x|\mathcal{J}_2\right\}, \end{aligned}$$

since $\mathrm{Cov}\left\{x|\mathcal{J}_2\right\}$ is constant. Using similar arguments, we can show that $T_2 = 0$ since:

$$\begin{aligned} &\mathbb{E}\left\{\mathbb{E}\left[(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\})(\mathbb{E}\left\{x|\mathcal{J}_2\right\} - \mathbb{E}\left\{x|\mathcal{J}_1\right\})'|\mathcal{J}_2\right]|\mathcal{J}_1\right\} \\ &= \mathbb{E}\left\{\mathbb{E}\left[(x - \mathbb{E}\left\{x|\mathcal{J}_2\right\})|\mathcal{J}_2\right](\mathbb{E}\left\{x|\mathcal{J}_2\right\} - \mathbb{E}\left\{x|\mathcal{J}_1\right\})'|\mathcal{J}_1\right\} \\ &= \mathbb{E}\left\{0|\mathcal{J}_1\right\} = 0, \end{aligned}$$

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

where the first equality holds since $\mathbb{E}\{x|\mathcal{J}_2\} - \mathbb{E}\{x|\mathcal{J}_1\}$ is measurable with respect to $\sigma(\mathcal{J}_2)$. Finally, $T_3 \succeq 0$ almost surely, which completes the proof. □

Proof of Lemma 5. Fix some time $k \geq 0$. If $k \leq k_0$ then equation (51) is trivially satisfied with equality. Since the channel outcomes are identical up to time k_0, then also $P_k = \tilde{P}_k$, for $k \leq k_0$.

Suppose that $k > k_0$. Fix the original channel outcomes to be $\boldsymbol{g}_{0:k} = s = (s_{u,0}, \ldots, s_{u,k}, s_0, \ldots, s_k)$, for some $s \in \{0,1\}^{2k+2}$. Then due to the coupling we have:

$$\tilde{\boldsymbol{g}}_{0:k} = \tilde{s} = (s_{u,0}, \ldots, s_{u,k}, s_0, \ldots, s_{k_0}, 1 \ldots, 1).$$

But from the definition (39), it follows that the set $\mathcal{J}_k(s)$ is included in $\mathcal{J}_k(\tilde{s})$. Thus, we have $\mathcal{J}_k(s) \subseteq \mathcal{J}_k(\tilde{s})$, where both sets have elements that depend linearly on the Gaussian $\boldsymbol{x}_{0:k}$. Hence, if we apply Lemma 6, with $x = \boldsymbol{x}_{0:k}$, $\mathcal{J}_1 = \mathcal{J}_k(s)$ and $\mathcal{J}_2 = \mathcal{J}_k(\tilde{s})$, we obtain that $\mathrm{Cov}\{\boldsymbol{x}_{0:k}|\mathcal{J}_k(s)\} \succeq \mathrm{Cov}\{\boldsymbol{x}_{0:k}|\mathcal{J}_k(\tilde{s})\}$, which also implies that the same relation holds for the $n \times n$ submatrices $\mathrm{Cov}\{x_k|\mathcal{J}_k(s)\} \succeq \mathrm{Cov}\{x_k|\mathcal{J}_k(\tilde{s})\}$. Thus, by (41), we have $P_k \succeq \tilde{P}_k$ in $\{\boldsymbol{g}_{0:k} = s\}$, for all $s \in \{0,1\}^{2k+2}$. Since the sets $\{\boldsymbol{g}_{0:k} = s\}$ are a partition of the probability space, we obtain that $P_k \succeq \tilde{P}_k$ with probability one. □

C. Proof of Theorem 1

Let us first prove equation (13). From the worst case Lemma 1, we obtain that $P_k = A^{k-k_0} P_{k_0} (A')^{k-k_0}$ in $\mathcal{B} \cap \mathcal{C}$. Here, we prove that for all $k \geq k_0$:

$$P_k \succeq A^{k-k_0} P_{k_0} (A')^{k-k_0} \text{ in } \mathcal{B}. \tag{53}$$

From Lemma 5, we obtain that with probability one:

$$P_k \succeq \tilde{P}_k,$$

where $\tilde{P}_k$ is the error covariance matrix of the coupled channel outcome sequence as defined in (48)–(50). What remains to show is that in $\mathcal{B}$, we have $\tilde{P}_k = A^{k-k_0} P_{k_0} (A')^{k-k_0}$. Notice that since $\tilde{\gamma}_{u,k_0} = \gamma_{u,k_0}$ and $\tilde{\gamma}_{k_0} = \gamma_{k_0}$, the following events are equal:

$$\tilde{\mathcal{B}} = \{\tilde{\gamma}_{u,k_0} = 1, \tilde{\gamma}_{k_0} = 0\} = \mathcal{B}.$$

Also observe that since $\tilde{\gamma}_k = 1$, $k > k_0$, the event

$$\tilde{\mathcal{C}} = \{\tilde{\gamma}_k = 1, \text{ for all } k \geq k_0 + 1\} = \Omega$$

is the whole probability space. Thus, applying Lemma 1 for $\boldsymbol{g}_{0:k}$ replaced with $\tilde{\boldsymbol{g}}_{0:k}$ and the events $\tilde{\mathcal{B}}$ and $\tilde{\mathcal{C}}$, we obtain $\tilde{P}_k = A^{k-k_0} \tilde{P}_{k_0} (A')^{k-k_0}$, for $k \geq k_0$ in $\mathcal{B}$. But since $\boldsymbol{g}_{0:k_0}$ and $\tilde{\boldsymbol{g}}_{0:k_0}$ are identical, we have $\tilde{P}_{k_0} = P_{k_0}$. Combining the two previous results, we prove (53).

Next, we show that $P_{k_0} \succeq Q$ or $P_{k_0} = \Sigma_0$ in $\mathcal{B}$. From the conditional expectation formula (43) for P_{k_0}, we get that when the packet is lost ($\gamma_{k_0} = 0$), then the estimation error covariance is equal to the prediction error covariance or $P_{k_0} = \Sigma_{xx}$. Hence by Proposition 1, if $k_0 > 0$, we have $P_{k_0} = AP_{k_0-1}A' + Q \succeq Q \succ 0$ in $\mathcal{B}$, while if $k_0 = 0$, we have $P_0 = \Sigma_0 \succ 0$ in $\mathcal{B}$.

Now, suppose that v is a left-eigenvector of A corresponding to the spectral radius $\rho(A)$. Then, pre-multiplying and post-multiplying by v in (53), we obtain:

$$v' P_k v \geq \rho(A)^{2(k-k_0)} v' P_{k_0} v.$$

But either $P_{k_0} \succeq Q$ or $P_{k_0} = \Sigma_0$, which implies

$$v' P_k v \geq c\rho(A)^{2(k-k_0)} v' v,$$

where $c = \min\{\lambda_{min}(Q), \lambda_{min}(\Sigma_0)\} > 0$ and $\lambda_{min}(\cdot)$ denotes the smallest eigenvalue. This, in turn, proves (13) since

$$\mathbf{tr}\, P_k \geq \lambda_{max}(P_k) \geq \frac{v' P_k v}{v' v},$$

where $\lambda_{max}(\cdot)$ denotes the largest eigenvalue.

To prove that the coding scheme achieves perfect secrecy, notice that the user always knows x_{t_k} and, thus, she can reconstruct the states x_k, when $\gamma_{u,k} = 1$. But this exactly implies that the condition (7) of perfect secrecy is satisfied, since $P_{u,k} = 0 = \mathrm{Cov}\{x_k|\boldsymbol{x}_{0:k}\}$, when $\gamma_{u,k} = 1$ (recall that $y_k = x_k$ in the case of state measurements). Finally, (13) along with the hypothesis (12) prove that $\mathbf{tr}\, P_k \to \infty$ with probability one. □

D. Proof of Corollary 1

Let e_j denote the unit vector of $\mathbb{R}^n$ in the j-th direction. Then

$$e_j' A^i Q (A^i)' e_j \leq \rho(Q) \left\| A^i e_j' \right\|_2^2 \leq \rho(Q) \left\| A^i \right\|_2^2,$$

where $\left\| A^i \right\|_2$ is the Euclidean matrix norm. Repeating the procedure for all j, we obtain the inequality:

$$\begin{aligned} \mathbf{tr}\, P_k^{op} &= \sum_{i=0}^{k-1} \mathbf{tr}\left(A^i Q (A')^i\right) + \mathbf{tr}\left(A^k \Sigma_0 (A')^k\right) \\ &\leq n c_1 \sum_{i=0}^{k} \left\| A^i \right\|_2^2, \end{aligned}$$

where $c_1 = \max\{\rho(Q), \rho(\Sigma_0)\}$. But by the Gelfand's formula [36], $\left\| A^k \right\|_2 \sim \rho(A)^k$ asymptotically, which implies that there exists a constant $c_2 > 0$ such that:

$$\mathbf{tr}\, P_k^{op} \leq c_2 \sum_{i=0}^{k} \rho(A)^{2i} = c_2 \frac{\rho(A)^{2(k+1)} - 1}{\rho(A)^2 - 1}.$$

or

$$\rho(A)^{2(k+1)} \geq \frac{\rho(A)^2 - 1}{c_2} \mathbf{tr}\, P_k^{op} + 1 \geq \frac{\rho(A)^2 - 1}{c_2} \mathbf{tr}\, P_k^{op}$$

On the other hand, suppose that the first critical event occurs at k_0. Then, from Theorem 1, we obtain:

$$\mathbf{tr}\, P_k \geq c_3 \rho(A)^{2(k-k_0)}, \text{ for } k \geq k_0,$$

for some constant $c_3 > 0$ independent of k_0. Combining the previous two inequalities, we obtain:

$$c\rho(A)^{-2k_0} \mathbf{tr}\, P_k^{op} \leq \mathbf{tr}\, P_k,\ k \geq k_0 \tag{54}$$

for some constant $c > 0$ independent of k_0. □

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

E. Proof of Lemma 2

Consider equation (24). Since the weighted innovation sequence $K\bar{w}_k$ is white noise with covariance

$$\bar{Q} = K\left(C\bar{P}C' + R\right)K',$$

the steps of the proof of Theorem 1 can be repeated. First, applying Lemma 1 to system (24) with coding scheme (23) (with $\bar{x}_k$, η_k, H_k, $\bar{Q}$ instead of x_k, $\hat{x}_k$, P_k, Q), we obtain:

$$H_k = A^{k-k_0} H_{k_0} \left(A'\right)^{k-k_0}, \text{ for } k \geq k_0, \text{ in } \mathcal{B} \cap \mathcal{C}, \quad (55)$$

where the events $\mathcal{B}$, $\mathcal{C}$ are defined in (14), (15).

Second, similar to (53) in the proof of Theorem 1, the previous equality holds with inequality in $\mathcal{B}$ or:

$$H_k \succeq A^{k-k_0} H_{k_0} \left(A'\right)^{k-k_0} \text{ in } \mathcal{B}. \quad (56)$$

Third, since the critical event $\mathcal{B}$ occurs at k_0 then we have:

1) $H_{k_0} = AH_{k_0-1}A' + \bar{Q} \succeq \bar{Q}$ if $k_0 > 0$
2) $H_{k_0} = \mathrm{Cov}\left\{\bar{x}_0\right\} = \bar{Q}$ if $k_0 = 0$.

The part that is different is proving that the trace grows unbounded. Let v be the (nonzero) left-eigenvector of A corresponding to the spectral radius $\rho(A)$. Pre-multiplying and post-multiplying by v in (56), we obtain:

$$v'H_k v \geq \rho(A)^{2(k-k_0)} v'H_{k_0} v.$$

But either $H_{k_0} \succeq \bar{Q}$ or $H_{k_0} = \bar{Q}$, which implies

$$v'H_k v \geq c\rho^{2(k-k_0)} v'v,$$

where

$$c = \frac{v'\bar{Q}v}{v'v} \geq 0.$$

Since we have

$$\mathbf{tr}\, H_k \geq \lambda_{\max}(H_k) \geq \frac{v'H_k v}{v'v},$$

we obtain (30) if we show that c is strictly positive or $v'\bar{Q}v > 0$. We will argue by contradiction. Suppose that $v'\bar{Q}v = 0$. Substituting this in equation (25) we then have:

$$\begin{aligned} v'\bar{P}v &= \rho(A)^2 v'\bar{P}v + v'Qv - \rho(A)^2 v'\bar{Q}v \\ &= \rho(A)^2 v'\bar{P}v + v'Qv, \end{aligned}$$

which is a contradiction since $Q \succ 0$ and $v'Qv > 0$, while $\left\{1 - \rho(A)^2\right\} v'\bar{P}v \leq 0$, since the system is unstable. Thus, $v'\bar{Q}v > 0$ and $c > 0$. □

F. Proof of Theorem 2

First we prove (28). By optimality of linear estimation we have that the estimate η_k minimizes the conditional error or:

$$\eta_k = \underset{x \in \sigma(\mathcal{I}_k)}{\arg\min}\, \mathbb{E}\left\{\|\bar{x}_k - x\|_2^2 \,|\mathcal{I}_k\right\},$$

where $x \in \sigma(\mathcal{I}_k)$ denotes that x is measurable with respect to $\sigma(\mathcal{I}_k)$. Thus, if we replace η_k with $\hat{x}_k$, we obtain the following bound:

$$\mathbf{tr}\, H_k = \mathbb{E}\left\{\|\bar{x}_k - \eta_k\|_2^2 \,|\mathcal{I}_k\right\} \leq \mathbb{E}\left\{\|\bar{x}_k - \hat{x}_k\|_2^2 \,|\mathcal{I}_k\right\}. \quad (57)$$

Then by the inequality $\|a-b\|_2^2 \leq 2\|a-c\|_2^2 + 2\|b-c\|_2^2$, we obtain:

$$\begin{aligned} \mathbf{tr}\, H_k &\leq 2\mathbb{E}\left\{\|x_k - \hat{x}_k\|_2^2 \,|\mathcal{I}_k\right\} + 2\mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\mathcal{I}_k\right\} \\ &= 2\,\mathbf{tr}\, P_k + 2\,\mathbf{tr}\left(\bar{P} - KC\bar{P}\right). \end{aligned} \quad (58)$$

The first term of the equality above holds by the equality $\mathbf{tr}\, P_k = \mathbb{E}\left\{\|x_k - \hat{x}_k\|_2^2 \,|\mathcal{I}_k\right\}$ from the definition of P_k in (6). To show the equality about the second term in (58), by the tower property:

$$\mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\mathcal{I}_k\right\} = \mathbb{E}\left\{\mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\boldsymbol{y}_{0:k}, \boldsymbol{g}_{0:k}\right\} |\mathcal{I}_k\right\}$$

since $\sigma(\mathcal{I}_k) \subseteq \sigma(\boldsymbol{y}_{0:k}, \boldsymbol{g}_{0:k})$. But by independence $\mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\boldsymbol{y}_{0:k}, \boldsymbol{g}_{0:k}\right\} = \mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\boldsymbol{y}_{0:k}\right\}$. The right-hand expression denotes the estimation error covariance of the Kalman filter which by assumption is assumed to be at steady state and hence equals $\bar{P} - KC\bar{P}$, where $\bar{P}$ is the steady state prediction error covariance. As a result,

$$\begin{aligned} \mathbb{E}\left\{\|x_k - \bar{x}_k\|_2^2 \,|\mathcal{I}_k\right\} &= \mathbb{E}\left\{\mathbf{tr}\left(\bar{P} - KC\bar{P}\right) |\mathcal{I}_k\right\} \\ &= \mathbf{tr}\left(\bar{P} - KC\bar{P}\right). \end{aligned}$$

which verifies (58). Finally substituting the result of Lemma 2 in (58) we have:

$$\mathbf{tr}\, P_k \geq \frac{1}{2} c\rho(A)^{2(k-k_0)} - \mathbf{tr}\left(\bar{P} - KC\bar{P}\right), \text{ in } \mathcal{B},$$

for $k \geq k_0$ and some $c > 0$ independent of k_0, which proves (28).

To prove that perfect secrecy is achieved (statement (i) of the Theorem), notice first that the user's performance is optimal. At every successful reception time k, the user receives $\bar{x}_k - A^{k-t_k}\bar{x}_{t_k}$ and recovers $\bar{x}_k$. As a result, the user knows $\bar{x}_k$ at the successful reception times. But from (21), (22) this is exactly the optimal estimation scheme as defined in (7). The fact that the eavesdropper's error diverges to infinity almost surely follows from (28) and the hypothesis (27). □

REFERENCES

[1] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *HotSec*, 2008.

[2] H. Sandberg, S. Amin, and Johansson, K.H. (Organizers), "Cyberphysical Security in Networked Control Systems [Special Issue]," *IEEE Control Systems*, vol. 35, no. 1, 2015.

[3] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *49th IEEE Conference on Decision and Control (CDC)*. IEEE, 2010, pp. 1096–1101.

[4] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, "Robustness of attack-resilient state estimators," in *ICCPS'14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)*. IEEE Computer Society, 2014, pp. 163–174.

[5] Y. Mo, J. P. Hespanha, and B. Sinopoli, "Resilient detection in the presence of integrity attacks," *IEEE Transactions on Signal Processing*, vol. 62, no. 1, pp. 31–43, 2014.

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

[7] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110–127, 2015.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TAC.2019.2927459, IEEE Transactions on Automatic Control

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

[10] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2014.

[11] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[12] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," *Physical review letters*, vol. 74, no. 25, p. 5028, 1995.

[13] P. A. Regalia, A. Khisti, Y. Liang, and Tomasin, S. (Eds.), "Secure Communications via Physical-Layer and Information-Theoretic Techniques [Special Issue]," *Proceedings of the IEEE*, vol. 103, no. 10, 2015.

[14] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

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

[16] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[17] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[18] H. Li, L. Lai, and W. Zhang, "Communication requirement for reliable and secure state estimation and control in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 3, pp. 476–486, 2011.

[19] M. Wiese, K. H. Johansson, T. J. Oechtering, P. Papadimitratos, H. Sandberg, and M. Skoglund, "Uncertain wiretap channels and secure estimation," in *2016 IEEE International Symposium on Information Theory (ISIT)*, July 2016, pp. 2004–2008.

[20] ——, "Secure estimation for unstable systems," in *IEEE 55th Conference on Decision and Control (CDC)*. IEEE, 2016, pp. 5059–5064.

[21] I. Safaka, L. Czap, K. Argyraki, and C. Fragouli, "Creating secrets out of packet erasures," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1177–1191, 2016.

[22] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation with secrecy against eavesdroppers," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 8385–8392, 2017.

[23] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Remote state estimation over packet dropping links in the presence of an eavesdropper," *arXiv preprint arXiv:1702.02785*, 2017.

[24] A. S. Leong, D. E. Quevedo, and S. Dey, "State estimation over markovian packet dropping links in the presence of an eavesdropper," in *IEEE 56th Conference on Decision and Control (CDC)*, 2017.

[25] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation codes for perfect secrecy," in *IEEE 56th Conference on Decision and Control (CDC)*, 2017.

[26] ——, "State-secrecy codes for stable systems," in *American Control Conference (ACC), 2018*.

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

[28] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, p. 138, 2007.

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

[30] V. Gupta, B. Hassibi, and R. M. Murray, "Optimal LQG control across packet-dropping links," *Systems & Control Letters*, vol. 56, no. 6, pp. 439–446, 2007.

[31] R. Durrett, *Probability: theory and examples*. Cambridge university press, 2010.

[32] B. Anderson and J. Moore, *Optimal Filtering*. Dover Publications, 2005.

[33] L. Xing, C. Wen, Y. Zhu, H. Su, and Z. Liu, "Output feedback control for uncertain nonlinear systems with input quantization," *Automatica*, vol. 65, pp. 191–202, 2016.

[34] T. K. Moon, *Error correction coding: mathematical methods and algorithms*. Wiley, 2005.

[35] V. Lesi, I. Jovanov, and M. Pajic, "Security-aware scheduling of embedded control tasks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 5s, p. 188, 2017.

[36] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.



Anastasios Tsiamis (S'16) received the Diploma degree in electrical and computer engineering from the National Technical University of Athens, Greece, in 2014. Currently, he is a Ph.D. student in the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA, USA. His research interests include machine learning for control, system identification, control systems security, and networked control systems. Mr. Tsiamis was a finalist for the IFAC Young Author Prize at IFAC 2017 World Congress and a finalist for the Best Student Paper Award at American Control Conference 2019.



Konstantinos Gatsis (S'10) received the Ph.D. degree in electrical and systems engineering from the University of Pennsylvania, Philadelphia, PA, USA, in 2017.

Currently, he is a Postdoctoral Researcher in the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia. His research interests include cyber-physical systems, networked control systems, as well as security and resource optimization problems arising in them.

Mr. Gatsis received the 2014 O. Hugo Schuck Best Paper Award, the Student Best Paper Award at the 2013 American Control Conference, and was a Best Paper Award Finalist at the 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS).

.



George J. Pappas (S'90–M'91–SM'04–F'09) received the Ph.D. degree in electrical engineering and computer sciences from the University of California, Berkeley, CA, USA, in 1998. He is currently the Joseph Moore Professor and Chair of the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA, USA. He also holds a secondary appointment with the Department of Computer and Information Sciences and the Department of Mechanical Engineering and Applied Mechanics. He is a Member of the GRASP Lab and the PRECISE Center. He had previously served as the Deputy Dean for Research with the School of Engineering and Applied Science. His research interests include control theory and, in particular, hybrid systems, embedded systems, cyberphysical systems, and hierarchical and distributed control systems, with applications to unmanned aerial vehicles, distributed robotics, green buildings, and biomolecular networks. Dr. Pappas has received various awards, such as the Antonio Ruberti Young Researcher Prize, the George S. Axelby Award, the Hugo Schuck Best Paper Award, the George H. Heilmeier Award, the National Science Foundation PECASE award, and numerous best student papers awards at ACC, CDC, and ICCPS.

0018-9286 (c) 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.