Finite Time Encryption Schedule in the Presence of an Eavesdropper with Operation Cost

Lingying Huang*, Alex S. Leong+, Daniel E. Quevedo+, Ling Shi*

***Abstract*— In this paper, we consider a remote state estimation problem in the presence of an eavesdropper. A smart sensor takes measurement of a discrete linear time-invariant (LTI) process and sends its local state estimate through a wireless network to a remote estimator. An eavesdropper can overhear the sensor transmissions with a certain probability. To enhance the system privacy level, we propose a novel encryption strategy to minimize a linear combination of the expected error covariance at the remote estimator and the negative of the expected error covariance at the eavesdropper, taking into account the cost of the encryption process. We prove the existence of an optimal deterministic and Markovian policy for such an encryption strategy over a finite time horizon. Two situations, namely, with or without knowledge of the eavesdropper estimation error covariance are studied and the optimal schedule is shown to satisfy the threshold-like structure in both cases. Numerical examples are given to illustrate the results.**

I. Introduction

Cyber-physical systems (CPSs) integrate sensing, computing and communication capabilities with physical systems [1]. The introduction of a wireless network enables CPSs to be applied to a wide range of applications. However, it also introduces more challenges to protect privacy. Since information in CPSs is transmitted through unprotected wireless networks in most cases, CPSs are often vulnerable to unauthorized users including malicious attackers. A leakage of confidential information will result in severe consequences, e.g., disclosure of customers' privacy and economic losses [2], [3].

The most common method to improve system confidentiality is encrypting transmitted packets, e.g., symmetric-key encryption and public-key encryption. Only the legitimate user has the ability to decrypt messages, blocking the access from other adversaries. Reason [4] proposed that encrypted information should satisfy the avalanche effect property. This property leads to the increase of the average mean squared error at the legitimate receiver as it enlarges the one-bit-error. In addition, cryptography requires more storage and computation services, adding extra burden. Hence, there is a trade-off between the privacy level and the estimation quality as well as a privacy-preserving cost.

The work by L. Huang and L. Shi is supported by a Hong Kong ITC research fund ITS/066/17FP-A.

* Department of Electronic Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong lhuangaq@connect.ust.hk; eesling@ust.hk

+ Department of Electrical Engineering (EIM-E), Paderborn University, Paderborn, Germany alex.leong@upb.de; dquevedo@ieee.org

A fairly large body of literature exists in studying the independent and identically distributed (i.i.d.) packets losses. In this case, the throughput in wireless network serves as an evaluation indicator in legitimate estimation quality. Haleem et al. [5] presented a mathematical model to capture the security-throughput trade-off. Aysal and Barner [6] derived an optimal estimator of a deterministic signal using stochastic bit flipping and analyzed the effect.

On the other hand, it is more general and more difficult to consider that collected packets are measurement vectors of a dynamical system when there is an eavesdropper. Wiese et al. [7] showed that by applying sufficiently large coding length, one could make the estimation error of the eavesdropper unbounded while the legal receiver still has a bounded error covariance for unstable systems (perfect secrecy). Tsiamis et al. [8] concluded that by exploiting packet erasures policy, perfect secrecy is achieved when the arrival rate of the legitimate receiver is larger than that of eavesdroppers. They also showed in [9] that perfect secrecy is achieved with at least one occurrence of the essential event, when the user receives the packet while the eavesdropper fails to intercept it. Furthermore, Leong et al. [10] proposed a policy to erase packets based on the estimation error where the system can achieve perfect secrecy even when the eavesdropper has greater probability to obtain information.

Different from [10], we study a more general encryption strategy. We formulate a novel mathematical model to illustrate the effect of encryption strategy (Fig. 1) considering a remote estimator and an eavesdropper. Based on this model, we derive structural results on the optimal encryption schedule with (Theorem 3), or without (Theorem 5) knowledge of the eavesdropper's estimation error covariance. We also introduce the influence of the encryption cost into this optimization problem. With more decision variables, we prove that the threshold structure still holds in both situations (Theorems 3,5).

This paper is organized as follows. Section II establishes the system model. After analyzing the remote estimator's and the eavesdropper's performance, we introduce the mathematical formulation of the main problem. Section III proves the existence and the structure of an optimal deterministic and Markovian policy in a finite time horizon with or without knowledge of the eavesdropper's estimation error covariance. Numerical simulations are given in Section IV. Section V draws conclusions.

Notation: $\mathbb{N}$ is the set of natural numbers. $\mathbb{R}$ and $\mathbb{R}^n$ represent the set of real numbers and $n-$dimensional real column vectors. For a matrix X, X' and $tr(X)$ denote

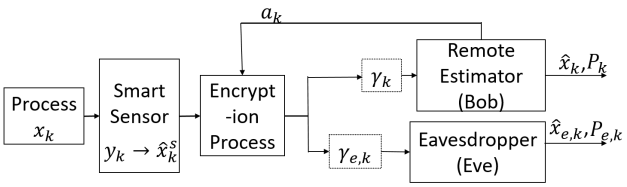


Fig. 1: System structure.

its transpose and trace, respectively. When X is a positive semidefinite matrix, it is written as $X \geq 0$. The notation $\mathbb{P}(\cdot)$ and $\mathbb{E}[\cdot]$ are the probability and expectation of a random matrix, respectively, and $\mathbb{E}[\cdot|\cdot]$ is its conditional expectation. For functions f, f_1 and f_2, $f_1 \circ f_2$ is defined as $f_1 \circ f_2 = f_1(f_2(X))$ and f^k is defined as $f^k(X) = \underbrace{f \circ f \circ \ldots \circ f}_{k \text{ times}}(X)$, with $f^0(X) = X$. A function $F(\cdot)$ is increasing if $X \leq Y \Rightarrow F(X) \leq F(Y)$. A function $F(\cdot)$ is decreasing if $X \leq Y \Rightarrow F(X) \geq F(Y)$.

II. System model and problem formulation

A. System Model

Consider the linear time-invariant (LTI) system in Fig 1, which is given as follows

$$\begin{aligned} x_{k+1} &= Ax_k + w_k, \\ y_k &= Cx_k + v_k, \end{aligned} \tag{1}$$

where $k \in \mathbb{N}$ is the time index, $x_k \in \mathbb{R}^n$ is the system state, $y_k \in \mathbb{R}^m$ is the measurement vector taken by the sensor at time k, $w_k \in \mathbb{R}^n$ and $v_k \in \mathbb{R}^m$ are two i.i.d. zero-mean Gaussian random noises with covariances $Q \geq 0$ and $R > 0$, respectively. The initial state x_0 is a zero-mean Gaussian random vector that is uncorrelated with w_k or v_k, and has covariance $\Pi_0 \geq 0$. We further assume that $(A, \sqrt{Q})$ is controllable and (A, C) is observable.

A smart sensor equipped with computation and memory capacity is capable of running a local Kalman filter. The sensor transmits quantities $\hat{x}_k^s$ to a remote estimator (Bob). According to Anderson and Moore [11], since $(A, \sqrt{Q})$ is controllable and (A, C) is observable, posteriori estimation error covariance P_k^s converges exponentially fast to a steady state P^*. For simplicity, we assume $P_k^s = P^*$.

Let $a_k \in \{0, 1\}$ be a decision variable. When $a_k = 0$, the sensor transmits its local state estimate $\hat{x}_k^s$ to the remote estimator. Otherwise, when $a_k = 1$, the local estimate $\hat{x}_k^s$ is first encrypted before transmitting. The decision variable a_k is determined at the remote estimator, which is assumed to have more computational capabilities than the sensor. It uses the information available at time $k-1$, and then feeds back to the sensor before transmission at time k.

We use γ_k to represent whether the remote estimator receives $\hat{x}_k^s$ successfully at time k, i.e., $\gamma_k = 1$ indicates that the local estimate is received successfully by the remote estimator at time k and $\gamma_k = 0$ otherwise. We make the following assumption about effects of the encryption process on the packet arrival rate.

Assumption 1. *The packet arrival rate is memoryless and is only affected if the transmitted messages are encrypted, i.e., $\{\gamma_k\}$ is i.i.d.. It is assumed that encryption contributes an impact factor $\epsilon_1 (0 \leq \epsilon_1 \leq 1)$ to the arrival rate. The following equality holds for any $k \geq 1$,*

$$\mathbb{P}(\gamma_k = 1) = \begin{cases} \lambda, \text{ if } a_k = 0, \\ \epsilon_1 \lambda, \text{ if } a_k = 1. \end{cases} \tag{2}$$

Remark 1. *The impact factor can be determined by the type of the encryption. A large number of published studies focus on specific impact factor of different encryption methods. For example, in paper [10] , the impact factor of packet erasure method is 0. Meanwhile, paper [4] showed that the perceptual degradation in subjective quality caused by confidentiality closely follows the quantitative degradation in bit-error rate. Therefore, if the packet length is known to the remote estimator in advance, the impact factor is deterministic and we simplify it as a general constant ϵ_1.*

There exists an eavesdropper (Eve) who can overhear the sensor transmission. Let $\gamma_{e,k}$ be a random variable such that $\gamma_{e,k} = 1$ if $\hat{x}_k^s$ is overheard and decrypted successfully by the eavesdropper, and $\gamma_{e,k} = 0$ otherwise. We make the following assumption about the influence of successful eavesdropping rate (which means the message is obtained and decrypted successfully) at the eavesdropper.

Assumption 2. *The successful eavesdropping rate for the eavesdropper is memoryless. If the message is encrypted, the eavesdropper has fixed probability $\epsilon_2 (0 \leq \epsilon_2 \leq 1)$ to decrypt it. Therefore, the following equality holds for $k \geq 1$,*

$$\mathbb{P}(\gamma_{e,k} = 1) = \begin{cases} \lambda_e, \text{ if } a_k = 0, \\ \epsilon_2 \lambda_e, \text{ if } a_k = 1. \end{cases} \tag{3}$$

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

Remark 2. *To make the decryption probability memoryless, if we use key to encrypt the messages, we need to change the key from time to time from being deciphered by the eavesdropper.*

It is assumed that the remote estimator knows the decision variable a_k and whether the transmission was successful or not, i.e., γ_k. According to [12], the remote estimator's state estimate $\hat{x}_k$ and the corresponding error covariance P_k at time k are given by

$$(\hat{x}_k, P_k) = \begin{cases} (A\hat{x}_{k-1}, h(P_{k-1})), \text{ if } \gamma_k = 0, \\ (\hat{x}_k^s, P^*), \text{ if } \gamma_k = 1, \end{cases} \tag{4}$$

where the Lyapunov operator $h(X) \triangleq AXA + Q$.

Similarly, the eavesdropper knows if it has eavesdropped successfully, i.e., $\gamma_{e,k}$. The state estimate $\hat{x}_{e,k}$ and error covariance $P_{e,k}$ at time k are

$$(\hat{x}_{e,k}, P_{e,k}) = \begin{cases} (A\hat{x}_{e,k-1}, h(P_{e,k-1})), \text{ if } \gamma_k = 0, \\ (\hat{x}_k^s, P^*), \text{ if } \gamma_k = 1. \end{cases} \tag{5}$$

Lemma 1. *([13]) For any $k_1 \geq k_2 \geq 0$, $h^{k_1}(P^*) \geq h^{k_2}(P^*)$. Therefore, $tr(h^{k_1}(P^*)) \geq tr(h^{k_2}(P^*))$.*

Define $\mathbf{S} \triangleq \{P^*, h(P^*), h^2(P^*) \ldots\}$ which consists of all possible values of P_k and $P_{e,k}$. From Lemma 1, there is a total ordering $P^* \leq h(P^*) \leq \cdots$, thus $\mathbf{S}$ is a total order set.

B. Problem of interest

Considering the finite time horizon, our goal is to minimize a linear combination of the expected error covariance at the remote estimator and the negative of the expected error covariance at the eavesdropper, while taking into account the operation cost of the encryption process. The integrated cost J_k considering the privacy level, the system performance and the encryption cost is

$$\min_{a_k \in \{0,1\}} J_k \triangleq \sum_{k=1}^{N} \mathbb{E}[\beta tr(P_k) - (1-\beta) tr(P_{e,k}) + a_k \mathcal{C}]. \quad (6)$$

The coefficient $\beta \in (0,1)$ weighs the importance of the error covariance of the system compared with that of the eavesdropper. With larger β, it means that maintaining the system performance is of more importance than minimizing the information leakage, and vice versa. The parameter $\mathcal{C}$ is the normalized total cost of the encryption process.

Remark 3. *Packet erasure presented in paper [10] can be viewed as a special encryption strategy in our model with $\epsilon_1 = \epsilon_2 = 0$ and $\mathcal{C} = 0$. In our subsequent analysis, we will show that optimal policies are still of threshold-type.*

III. Finite Time Horizon MDP Framework

A. Eavesdropper State Known at Remote Estimator

We first consider the easier case where the eavesdropper error covariance is known at the remote estimator. We derive a discrete time Markov decision process (MDP) problem.

1) The state $s_k \triangleq (P_{k-1}, P_{e,k-1})$ at time k belongs to the state space $\mathbb{S} \subset \mathbf{S} \times \mathbf{S}$.
2) The action $a_k \in \{0,1\}$ belongs to the action space $\mathbb{A}$.
3) The state transition probability distribution $\mathbb{P}(s'|s,a)$ is time homogeneous, where $s', s \in \mathbb{S}$, $a \in \mathbb{A}$ by dropping the time index and s' is next state when taking action a at current state s. Denote $s_{00} \triangleq (h(P), h(P_e)), s_{01} \triangleq (h(P), P^*), s_{10} \triangleq (P^*, h(P_e)), s_{11} \triangleq (P^*, P^*)$ and $s = (P, P_e)$, then we obtain

$$\begin{aligned}
&\mathbb{P}_{00}(0) \triangleq \mathbb{P}(s_{00}|s,0) = (1-\lambda)(1-\lambda_e),\\
&\mathbb{P}_{01}(0) \triangleq \mathbb{P}(s_{01}|s,0) = (1-\lambda)\lambda_e,\\
&\mathbb{P}_{10}(0) \triangleq \mathbb{P}(s_{10}|s,0) = \lambda(1-\lambda_e),\\
&\mathbb{P}_{11}(0) \triangleq \mathbb{P}(s_{11}|s,0) = \lambda\lambda_e,\\
&\mathbb{P}_{00}(1) \triangleq \mathbb{P}(s_{00}|s,1) = (1-\epsilon_1\lambda)(1-\epsilon_2\lambda_e),\\
&\mathbb{P}_{01}(1) \triangleq \mathbb{P}(s_{01}|s,1) = (1-\epsilon_1\lambda)\epsilon_2\lambda_e,\\
&\mathbb{P}_{10}(1) \triangleq \mathbb{P}(s_{10}|s,1) = \epsilon_1\lambda(1-\epsilon_2\lambda_e),\\
&\mathbb{P}_{11}(1) \triangleq \mathbb{P}(s_{11}|s,1) = \epsilon_1\lambda\epsilon_2\lambda_e.
\end{aligned} \quad (7)$$

4) The one-stage cost function at time k is

$$\begin{aligned}
&c_k(P_{k-1}, P_{e,k-1}, a_k) \triangleq a_k \mathcal{C}\\
&+ \mathbb{E}[\beta tr(P_k) - (1-\beta) tr(P_{e,k}) | P_{k-1}, P_{e,k-1}, a_k]\\
&= a_k \mathcal{C} + \beta[(a_k\epsilon_1\lambda + (1-a_k)\lambda) tr(P^*)\\
&+ (1 - a_k\epsilon_1\lambda - (1-a_k)\lambda) tr(h(P_{k-1}))]\\
&- (1-\beta)[(a_k\epsilon_2\lambda_e + (1-a_k)\lambda_e) tr(P^*)\\
&+ (1 - a_k\epsilon_2\lambda_e - (1-a_k)\lambda_e) tr(h(P_{e,k-1}))].
\end{aligned} \quad (8)$$

Remark 4. *From Lemma 1, the one-stage cost function c_k increases in P_{k-1} and decreases in $P_{e,k-1}$.*

By above definitions, problem (6) is equal to

$$\min_{a_k \in \{0,1\}} \sum_{k=1}^{N} c_k(P_{k-1}, P_{e,k-1}, a_k). \quad (9)$$

Define the optimality equation (Bellman equation) as

$$\begin{aligned}
&V_k(P, P_e) = \min_{a \in \{0,1\}} \{c_k(P, P_e, a) + \mathbb{P}_{00}(a) V_{k+1}(s_{00}) +\\
&\mathbb{P}_{01}(a) V_{k+1}(s_{01}) + \mathbb{P}_{10}(a) V_{k+1}(s_{10}) + \mathbb{P}_{11}(a) V_{k+1}(s_{11})\},
\end{aligned} \quad (10)$$

where $V_k(\cdot,\cdot)$ for $k = 1, 2, \ldots, N$ is a real valued function and $V_{N+1}(P, P_e) = 0$.

Theorem 1. *There exists an optimal deterministic Markovian policy to problem* (9)*.*

Proof. In a finite time horizon, the state set $\mathbb{S}$ is finite and the corresponding action set $\mathbb{A}$ is finite. As the action set $\mathbb{A}$ is finite, there always exists a deterministic and Markovian optimal policy [14]. □

Let $H_k = (s_0, a_1, \ldots, s_{k-1}, a_k, s_k)$ stand for the history information up to time k. We will make the action a_{k+1} based on H_k to minimize the total integrated cost. The Markovian property determined by Theorem 1 guarantees that the future is independent of the past given the present [14] [15]. Hence, choosing actions a_{k+1} based on s_k would be the same as choosing actions based on H_k and problem (9) can be solved in a recursive way as

$$\begin{aligned}
&V_{N+1}(P, P_e) = 0,\\
&V_k(P, P_e) = \min_{a \in \{0,1\}} \{c_k(P, P_e, a) + \mathbb{P}_{00}(a) V_{k+1}(s_{00}) +\\
&\mathbb{P}_{01}(a) V_{k+1}(s_{01}) + \mathbb{P}_{10}(a) V_{k+1}(s_{10}) + \mathbb{P}_{11}(a) V_{k+1}(s_{11})\}.
\end{aligned}$$

The following theorem will be used to establish that the optimal solution has a threshold property (Theorem 3).

Theorem 2. *The optimal value function $V_k(P, P_e)$ is an increasing function in P and a decreasing function in P_e.*

Proof. See Appendix A. □

Theorem 3. *(1) For a fixed $P_{e,k-1}$, the optimal solution to problem* (9) *is a threshold policy on P_{k-1}*

$$a_k^*(P_{k-1}, P_{e,k-1}) = \begin{cases} 1, \textit{if } P_{k-1} \leq h^{m(k)}(P^*), \\ 0, \textit{otherwise} \ . \end{cases} \quad (11)$$

where the threshold $m(k) \in \mathbb{N}$ depends on k and $P_{e,k-1}$.

(2) For a fixed P_{k-1}, the optimal solution to problem (9) *is a threshold policy on $P_{e,k-1}$*

$$a_k^*(P_{k-1}, P_{e,k-1}) = \begin{cases} 1, \textit{if } P_{e,k-1} \geq h^{m_e(k)}(P^*), \\ 0, \textit{otherwise} . \end{cases} \quad (12)$$

where the threshold $m_e(k) \in \mathbb{N}$ depends on k and P_{k-1}.

Proof. See Appendix B. □

Remark 5. *Theorem 3 can be viewed in an intuitive way, i.e., (1) shows that the optimal policy is to transmit the packet without encryption to Bob when P_{k-1} is large, as we want to reduce P_k but the encryption makes the arrival rate smaller. For (2), it can be understand as that it is more efficient to encrypt the message when $P_{e,k-1}$ is large, since we want $P_{e,k}$ to increase even further.*

B. Eavesdropper State Unknown at Remote Estimator

In real situations, the malicious eavesdropper would hide itself from being detected by the remote estimator as far as possible. Therefore, it is difficult to know the eavesdropper's error covariance. Here we assume that the remote estimator knows the leakage probability λ_e from previous measurements, but is not aware of the actual realization of $\gamma_{e,k}$. This can be viewed as a partially observable MDP (POMDP) problem. This POMDP can be converted to a completely observable MDP using belief vector states.

Define the belief vector $\pi_{e,k}$, which represents the probability distribution of $P_{e,k}$ given the encryption schedule as

$$\pi_{e,k} \triangleq \begin{bmatrix} \pi_{e,k}^0 \\ \pi_{e,k}^1 \\ \vdots \\ \pi_{e,k}^N \end{bmatrix} = \begin{bmatrix} \mathbb{P}(P_{e,k} = P^* | a_1, \ldots, a_k) \\ \mathbb{P}(P_{e,k} = h(P^*) | a_1, \ldots, a_k) \\ \vdots \\ \mathbb{P}(P_{e,k} = h^N(P^*) | a_1, \ldots, a_k) \end{bmatrix}. \quad (13)$$

Denote the set of all possible $\pi_{e,k}$'s as $\Pi_e \subseteq R^{N+1}$. By our assumption, we have $P_{e,0} = P^*$ and $\pi_{e,0} = \begin{bmatrix} 1 & 0 & \ldots & 0 \end{bmatrix}^T$.

We can obtain a recursive relationship for $\pi_{e,k}$ as

$$\pi_{e,k} = \Phi(\pi_{e,k-1}, a_k), \quad (14)$$

where

$$\Phi(\pi_e, a) \triangleq \begin{cases} \begin{bmatrix} \lambda_e & (1-\lambda_e)\pi_e^0 & \ldots & (1-\lambda_e)\pi_e^{N-1} \end{bmatrix}^T, \text{ if } a = 0, \\ \begin{bmatrix} \epsilon_2\lambda_e & (1-\epsilon_2\lambda_e)\pi_e^0 & \ldots & (1-\epsilon_2\lambda_e)\pi_e^{N-1} \end{bmatrix}^T, \text{ if } a = 1. \end{cases}$$

Different from Section III-A, Bob will make the decision a_k based on its own P_{k-1} and the belief vector $\pi_{e,k-1}$ since $P_{e,k}$ is unknown to Bob. Therefore, in this subsection, the discrete time MDP problem is the following

1) The state $s_k \triangleq (P_{k-1}, \pi_{e,k-1})$ at time k belongs to the state space $\mathbb{S} \subset \mathbf{S} \times \Pi_e$.
2) The action $a_k \in \{0, 1\}$ is in the action space $\mathbb{A}$.
3) Denote $s \triangleq (P, \pi_e)$, $s' \triangleq (P^+, \pi_e^+)$. The state transition probability distribution $\mathbb{P}(s'|s, a)$ is

$$\mathbb{P}(P^+, \pi_e^+ | s, a) = \begin{cases} \lambda, \text{if } a = 0, P^+ = P^*, \text{ if } \pi_e^+ = \Phi(\pi_e, 0), \\ 1-\lambda, \text{if } a = 0, P^+ = h(P), \text{ if } \pi_e^+ = \Phi(\pi_e, 0), \\ \epsilon_1\lambda, \text{if } a = 1, P^+ = P^*, \text{ if } \pi_e^+ = \Phi(\pi_e, 1), \\ 1-\epsilon_1\lambda, \text{if } a = 1, P^+ = h(P), \text{ if } \pi_e^+ = \Phi(\pi_e, 1). \end{cases} \quad (15)$$

4) The one-stage cost function at time k is

$$c_k(P_{k-1}, \pi_{e,k-1}, a_k) \triangleq \beta\mathbb{E}[tr(P_k)|P_{k-1}, \pi_{e,k-1}, a_k] - (1-\beta)\sum_{i=0}^{N} tr(h^i(P^*))\pi_{e,k}^i + a_k\mathcal{C}, \quad (16)$$

where $\mathbb{E}[tr(P_k)|P_{k-1}, \pi_{e,k-1}, a_k] = (a_k\epsilon_1\lambda + (1-a_k)\lambda)tr(P^*) + (1 - a_k\epsilon_1\lambda + (1-a_k)\lambda)tr(h(P_{k-1}))$ and $\pi_{e,k} = \Phi(\pi_{e,k-1}, a_k)$.

Remark 6. *From Lemma 1, we obtain that one-stage cost function $c_k(P_{k-1}, \pi_{e,k-1}, a_k)$ increases in P_{k-1}.*

Then, problem (6) is equal to

$$\min_{a_k \in \{0,1\}} \sum_{k=1}^{N} c_k(P_{k-1}, P_{e,k-1}, a_k). \quad (17)$$

Similar to Section III-A, we will make the action a_{k+1} based on s_k instead of H_k by the Markov property proved in the same way as Theorem 1, to minimize the total integrated cost. Define the optimality equation (Bellman equation) as

$$\begin{aligned} &V_{N+1}(P, \pi_e) = 0, \\ &V_k(P, \pi_e) = \min_{a \in \{0,1\}} \{c_k(P, \pi_e, a) \\ &+ \mathbb{P}(h(P), \Phi(\pi_e, a)|s, a)V_{k+1}(h(P), \Phi(\pi_e, a)) \\ &+ \mathbb{P}(P^*, \Phi(\pi_e, a)|s, a)V_{k+1}(P^*, \Phi(\pi_e, a))\}, \end{aligned}$$

where $s = (P, \pi_e)$ and $V_k(\cdot, \cdot)$ for $k = 1, 2, \ldots, N$ is a real valued function.

Theorem 4. *$V_k(P, \pi_e)$ is an increasing function in P.*

Proof. For fixed π_e, we can use the same induction argument as in the proof of Theorem 2 to prove that the optimal solution $V_k(P, \pi_e)$ is an increasing function in P. □

Theorem 5. *For a fixed $\pi_{e,k-1}$, the optimal solution to problem* (17) *is a threshold policy on P_{k-1} of the form*

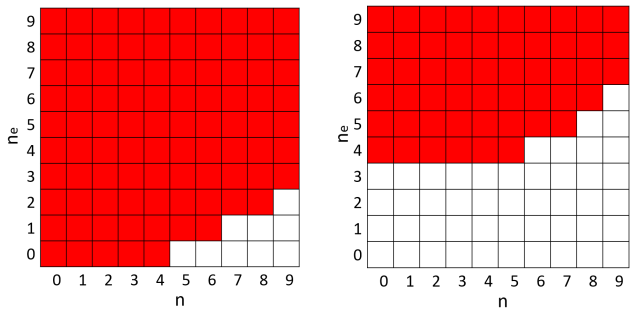
$$a_k^*(P_{k-1}, \pi_{e,k-1}) = \begin{cases} 1, \textit{if } P_{k-1} \leq h^{m(k)}(P^*), \\ 0, \textit{otherwise}. \end{cases} \quad (18)$$

where the threshold $m(k) \in \mathbb{N}$ depends on k and $\pi_{e,k-1}$

Proof. Using the similar method in the proof of Theorem 3 in Appendix B, it is sufficient to prove that

$$(1-\epsilon_1\lambda)V_{k+1}(h^n(P), \pi_e) - (1-\lambda)V_{k+1}(h^n(P), \pi_e') \quad (19)$$

is a increasing function of P for all $k = 0, 1, \ldots, N$, $n \in \mathbb{N}$ and $\pi_e, \pi_e' \in \Pi_e$. Therefore, for fixed k and π_e, $m(k) = \min\{t \in \mathbb{N} : \phi_k(h^t(P^*), \pi_e) \geq 0\}$. □



(a) $k = 5$. (b) $k = 10$.

Fig. 2: Optimal policy at different time steps.

Theorem 5 guarantees the threshold structure without knowledge of the eavesdropper's estimation error covariance.

IV. SIMULATION

In this section, we use numerical examples to illustrate our optimal policies. Consider a system with $A = \begin{bmatrix} 1.5 & 0 \\ 0 & 0.9 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}$, $R = 0.6$, $\lambda = \lambda_e = 0.7$, $\epsilon_1 = 0.9$ and $\epsilon_2 = 0.18$. The normalized encryption cost is $\mathcal{C} = 6$. Set the weighted parameter $\beta = 0.5$.

Consider a finite time horizon with $N = 10$. Fig. 2(a) plots a_k^* for different values of $P_{k-1} = h^n(P^*)$ and $P_{e,k-1} = h^{n_e}(P^*)$ at time step $k = 5$. Fig. 2(b) plots a_k^* at time $k = 10$. Red blocks represent $a_k^* = 1$, while white ones represent $a_k^* = 0$. It is shown in these two figures that the threshold structure of the optimal policy a_k^* in both P_{k-1} and $P_{e,k-1}$. Meanwhile, the optimal policy is dependent on time k as proved in Theorem 3.

Furthermore, TABLE. I makes a comparison between the following four different encryption methods

1) θ^1: always transmit the packet directly to the remote estimator without encryption, i.e., $a_k = 0$, for all k;
2) θ^1: always encrypt the packet before each transmission, i.e., $a_k = 1$, for all k;
3) θ^{*1}: the optimal strategy derived from Section III-A with knowledge of the eavesdropper's estimation error covariance;
4) θ^{*2}: the optimal strategy derived from Section III-B without knowledge of the eavesdropper's estimation error covariance.

Consider the finite time horizon with $N = 6$. We run 1000 Monte Carlo tests. We can see from TABLE. I that the optimal encryption strategy reduces the total integrated cost significantly compared with using no encryption method and is better than encrypting all the messages. Furthermore, if we cannot obtain the exact error covariance of the eavesdropper, the optimal cost is larger than that when the error covariance is known to the remote estimator.

TABLE I: A comparison between encryption strategies

	$\sum_{k=1}^{N} \mathbb{E}[tr(P_k)]$	$\sum_{k=1}^{N} \mathbb{E}[tr(P_{e,k})]$	J_k
θ^1	22.2487	22.2657	-0.0085
θ^2	24.1176	118.8861	-11.3843
θ^{*1}	23.6582	114.0609	-18.0513
θ^{*2}	23.8272	118.2655	-12.3692

V. CONCLUSION

In this paper, we consider an optimal encryption schedule for a remote state estimation system in the presence of an eavesdropper. Our objective is to determine when to encrypt transmitted messages to minimize a linear combination of error covariance at the remote estimator and the eavesdropper, taking into account the cost of the encryption process. This problem is shown to be formulated as a MDP, either with or without knowledge of the estimation error covariance at the eavesdropper. The optimal policy is proved to have a threshold structure in each situation.

The current setup only focuses on the problem of a finite time horizon where the state space is finite. It would be interesting to consider situations with a infinite time horizon.

APPENDIX

A. Proof of Theorem 2

As $V_{N+1}(P, P_e) = 0$, it is trivial to see that $V_{N+1}(P, P_e)$ is an increasing function in P. Therefore, we prove the monotonicity using a backward induction way.

Assume that $V_t(P, P_e)$ is increasing for $t = k+1, \ldots, N+1$, then we only need to prove $V_k(P, P_e)$ is an increasing function in P. We choose $P' \geq P$, one has $h(P') \geq h(P)$. Denote $s' \triangleq (P', P_e), s'_{00} \triangleq (h(P'), h(P_e)), s'_{01} \triangleq (h(P'), P^*)$. As function c_k increases in P and $\mathbb{P}(s'|s, a)$ is only dependent on action a, we have

$$
\begin{aligned}
&V_k(P, P_e) = \min_{a\in\{0,1\}} \{c_k(P, P_e, a) + \mathbb{P}_{00}(a)V_{k+1}(s_{00}) + \\
&\mathbb{P}_{01}(a)V_{k+1}(s_{01}) + \mathbb{P}_{10}(a)V_{k+1}(s_{10}) + \mathbb{P}_{11}(a)V_{k+1}(s_{11})\} \\
&\leq c_k(P, P_e, a^*_{s'}) + \mathbb{P}_{00}(a^*_{s'})V_{k+1}(s_{00}) + \mathbb{P}_{01}(a^*_{s'})V_{k+1}(s_{01}) \\
&+ \mathbb{P}_{10}(a^*_{s'})V_{k+1}(s_{10}) + \mathbb{P}_{11}(a^*_{s'})V_{k+1}(s_{11}) \\
&\leq c_k(P', P_e, a^*_{s'}) + \mathbb{P}_{00}(a^*_{s'})V_{k+1}(s'_{00}) + \mathbb{P}_{01}(a^*_{s'})V_{k+1}(s'_{01}) \\
&+ \mathbb{P}_{10}(a^*_{s'})V_{k+1}(s'_{10}) + \mathbb{P}_{11}(a^*_{s'})V_{k+1}(s_{11}) = V_k(P', P_e).
\end{aligned}
$$

The proof is completed.

We can use the same method to prove that $V_k(P, P_e)$ is a decreasing function in P_e. The proof is omitted.

B. Proof of Theorem 3

Denote the difference of $V_k(P, P_e)$ when $a^* = 1$ and $a^* = 0$ as $\phi_k(P, P_e)$. It can be calculated directly that

$$
\begin{aligned}
&\phi_k(P, P_e) = \beta(1-\epsilon_1)\lambda(tr(h(P)) - tr(h(P'))) - \\
&(1-\beta)(1-\epsilon_2)\lambda_e(tr(h(P_e)) - tr(h(P'))) + \mathcal{C} + \\
&p_1 V_{k+1}(s_{00}) + p_2 V_{k+1}(s_{01}) + p_3 V_{k+1}(s_{10}) + p_4 V_{k+1}(s_{11}),
\end{aligned}
$$

where $p_1 \triangleq \mathbb{P}_{00}(1) - \mathbb{P}_{00}(0)$, $p_2 \triangleq \mathbb{P}_{01}(1) - \mathbb{P}_{01}(0)$, $p_3 \triangleq \mathbb{P}_{10}(1) - \mathbb{P}_{10}(0)$, $p_4 \triangleq \mathbb{P}_{11}(1) - \mathbb{P}_{11}(0)$. If $\phi_k(P, P_e) \geq 0$, the optimal strategy at time k is $a_k^* = 0$, otherwise $a_k^* = 1$.

(1) It is equivalent to prove $\phi_k(P, P_e)$ increases in P for fixed P_e. Considering elements which relate to P in $\phi_k(P, P_e)$, for $P \geq P'$, we have

$$\begin{aligned}
&\phi_k(P, P_e) - \phi_k(P', P_e) = \beta(1-\epsilon_1)\lambda(tr(h(P)) - tr(h(P'))) \\
&+ p_1[V_{k+1}(h(P), h(P_e)) - V_{k+1}(h(P'), h(P_e))] \\
&+ p_2[V_{k+1}(h(P), P^*) - V_{k+1}(h(P'), P^*)].
\end{aligned}$$

From Lemma 1, the first element $\beta(1-\epsilon_1)\lambda(tr(h(P)) - tr(h(P'))) \geq 0$, it suffices to prove that

$$p_1 V_{k+1}(h(P), h(P_e)) + p_2 V_{k+1}(h(P), P^*), \tag{20}$$

is an increasing function of P for all k. We will prove this statement using a backward induction way. We prove the slightly more general statement that $p_1 V_{k+1}(h^n(P), P_e) + p_2 V_{k+1}(h^n(P), P_e')$ is an increasing function of P for all $k = 0, 1, \ldots, N$, $n \in \mathbb{N}$ and $P, P_e, P_e' \in \mathbf{S}$.

As $V_{N+1}(P, P_e) = 0$, it is trivial to see that the statement holds for $k = N$. Assume that $\forall P \geq P'$,

$$\begin{aligned}
&p_1 V_{t+1}(h^n(P), P_e) + p_2 V_{t+1}(h^n(P), P_e') \\
&- p_1 V_{t+1}(h^n(P'), P_e) - p_2 V_{t+1}(h^n(P'), P_e') \geq 0
\end{aligned} \tag{21}$$

holds for $t = k+1, \ldots, N$. Then

$$\begin{aligned}
&p_1 V_k(h^n(P), P_e) + p_2 V_k(h^n(P), P_e') \\
&- p_1 V_k(h^n(P'), P_e) - p_2 V_k(h^n(P'), P_e') \\
&\geq \min_{a \in \{0,1\}} \{p_1[c_k(h^n(P), P_e, a) + \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P), h(P_e)) \\
&+ \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P), P^*) - \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P'), P^*) \\
&- c_k(h^n(P'), P_e, a) - \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P'), h(P_e))] \\
&+ p_2[c_k(h^n(P), P_e', a) + \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P), h(P_e')) \\
&+ \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P), P^*) - \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P'), P^*) \\
&- \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P'), h(P_e')) - c_k(h^n(P'), P_e', a)]\} \\
&\geq \min_{a \in \{0,1\}} \{p_1[\mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P), h(P_e)) \\
&+ \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P), P^*) - \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P'), P^*) \\
&- \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P'), h(P_e))] + p_2[\mathbb{P}_{00}(a) \\
&\cdot V_{k+1}(h^{n+1}(P), h(P_e')) + \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P), P^*) \\
&- \mathbb{P}_{00}(a) V_{k+1}(h^{n+1}(P'), h(P_e')) \\
&- \mathbb{P}_{01}(a) V_{k+1}(h^{n+1}(P'), P^*)]\} \\
&= \min_{a \in \{0,1\}} \{\mathbb{P}_{00}(a)[p_1 V_{k+1}(h^{n+1}(P), h(P_e)) + p_2 \\
&\cdot V_{k+1}(h^{n+1}(P), h(P_e')) - p_1 V_{k+1}(h^{n+1}(P'), h(P_e)) - p_2 \\
&\cdot V_{k+1}(h^{n+1}(P'), h(P_e'))] + \mathbb{P}_{01}(a)[p_1 V_{k+1}(h^{n+1}(P), P^*)) \\
&+ p_2 V_{k+1}(h^{n+1}(P), P^*)) - p_1 V_{k+1}(h^{n+1}(P'), P^*)) \\
&- p_2 V_{k+1}(h^{n+1}(P'), P^*))]\} \geq 0
\end{aligned}$$

where the first inequality holds since a which denotes a_{k+1} is determined by the function ϕ_{k+1}. Meanwhile, the second inequality holds since $c_k(h^n(P), P_e, a)$ increases in P and the last inequality holds by the induction hypothesis (21) and $\mathbb{P}_{00}(a), \mathbb{P}_{01}(a) \geq 0$ for $\forall a \in \mathbb{A}$.

Therefore, for fixed k and P_e, $m(k) = \min\{t \in \mathbb{N} : \phi_k(h^t(P^*), P_e) \geq 0\}$.

(2) As $-tr(h(P_e))$ decreases in P_e, it is equivalent to prove that $p_1 V_{k+1}(h(P), h(P_e)) + p_3 V_{k+1}(P^*, h(P_e))$ is a decreasing function of P_e. Similar to the first part, we prove by induction the slightly more general statement $p_1 V_{k+1}(P, h^n(P_e)) + p_3 V_{k+1}(P', h^n(P_e))$ is a decreasing function of P_e for all $k = 0, 1, \ldots, N$, $n \in \mathbb{N}$ and $P, P', P_e \in \mathbf{S}$. The details are omitted.

REFERENCES

[1] R. Poovendran, K. Sampigethaya, S. K. S. Gupta, I. Lee, K. V. Prasad, D. Corman, and J. L. Paunicka, "Special issue on cyber-physical systems [scanning the issue]," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 6–12, 2012.

[2] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[3] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*. IEEE, 2008, pp. 495–500.

[4] J. M. Reason, *End-to-end confidentiality for continuous-media applications in wireless systems*. University of California, Berkeley, 2001.

[5] M. Haleem, C. Mathur, R. Chandramouli, and K. Subbalakshmi, "Opportunistic encryption: A trade-off between security and throughput in wireless networks," *IEEE Transactions on Dependable and secure computing*, vol. 4, no. 4, pp. 313–324, 2007.

[6] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 273–289, 2008.

[7] M. Wiese, K. H. Johansson, T. J. Oechtering, P. Papadimitratos, H. Sandberg, and M. Skoglund, "Secure estimation for unstable systems," in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 5059–5064.

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

[9] ——, "State estimation codes for perfect secrecy," in *Decision and Control (CDC), 2017 IEEE 56th Annual Conference on*. IEEE, 2017, pp. 176–181.

[10] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper," *IEEE Transactions on Automatic Control*, 2018.

[11] B. D. Anderson and J. B. Moore, "Optimal filtering," *Englewood Cliffs*, vol. 21, pp. 22–95, 1979.

[12] 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.

[13] L. Shi, M. Epstein, and R. M. Murray, "Kalman filtering over a packet-dropping network: A probabilistic perspective," *IEEE Transactions on Automatic Control*, vol. 55, no. 3, pp. 594–604, 2010.

[14] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming*. John Wiley & Sons, 2014.

[15] D. P. Bertsekas, *Dynamic programming and optimal control*. Athena scientific Belmont, MA, 2005, vol. 1, no. 3.