Stealthy Hacking and Secrecy of Controlled State Estimation Systems With Random Dropouts

Jingyi Lu, *Member, IEEE*, Daniel E. Quevedo, *Fellow, IEEE*, Vijay Gupta, *Senior Member, IEEE*, and Subhrakanti Dey, *Senior Member, IEEE*

***Abstract*—We study the maximum information gain that an adversary may obtain through hacking without being detected. Consider a dynamical process observed by a sensor that transmits a local estimate of the system state to a remote estimator according to some reference transmission policy across a packet-dropping wireless channel equipped with acknowledgments (ACK). An adversary overhears the transmissions and proactively hijacks the sensor to reprogram its transmission policy. We define perfect secrecy as keeping the averaged expected error covariance bounded at the legitimate estimator and unbounded at the adversary. By analyzing the stationary distribution of the expected error covariance, we show that perfect secrecy can be attained for unstable systems only if the ACK channel has no packet dropouts. In other situations, we prove that independent of the reference policy and the detection methods, perfect secrecy is not attainable. For this scenario, we devise a Stackelberg game to derive the optimal defensive reference policy for the legitimate estimator and present a branch-and-bound algorithm with global optimality to solve the proposed game.**

***Index Terms*—Bilevel programming, constrained Markov decision process, remote state estimation, stealthy attack, system security and privacy.**

Manuscript received 7 November 2020; revised 24 June 2021; accepted 19 November 2021. Date of publication 30 November 2021; date of current version 28 December 2022. The work of Jingyi Lu was supported by the German Research Foundation (DFG) under Grant 392194080. Recommended by Associate Editor Prashant G. Mehta. *(Corresponding author: Jingyi Lu.)*

Jingyi Lu is with the Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China (e-mail: jylu_cise@ecust.edu.cn).

Daniel E. Quevedo is with the School of Electrical Engineering and Robotics, Queensland University of Technology (QUT), Brisbane, QLD 4000, Australia (e-mail: dquevedo@ieee.org).

Vijay Gupta is with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556 USA (e-mail: vgupta2@nd.edu).

Subhrakanti Dey is with the Hamilton Institute, Maynooth University, Maynooth, Co. Kildare W23F2K8, Ireland (e-mail: Subhra.Dey@signal.uu.se).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2021.3131434.

Digital Object Identifier 10.1109/TAC.2021.3131434

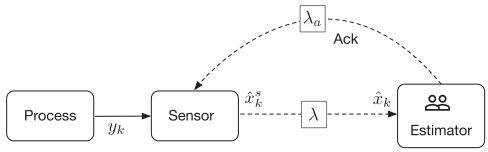


Fig. 1. Remote state estimation across packet-dropping channels.

I. Introduction

CYBER-PHYSICAL systems (CPSs) have been widely applied to many critical infrastructures, including smart grids, transportations, and industrial control systems. CPSs can provide efficiency and versatility by merging computing and communication with the physical world. However, the vulnerability of CPSs to various cyber-attacks, which compromise measurements and actuator data availability, integrity, and confidentiality, brings huge potential security and privacy issues [1]. Numerous malware targeting industrial control systems have been discovered, such as the notorious Stuxnet, Triton, and Havex [2], [3]. By launching a phishing attack to gain remote access to critical components in an autonomous system, the malware is capable of remote monitoring and potentially taking full control of the target for espionage and sabotage [4]. This will often circumvent a digital safety system, thus, potentially serving as a detrimental cyber weapon of mass destruction.

Considering system security and privacy of dynamical systems, a surge of research has been carried out to investigate attack patterns. For example, optimal jamming attacks targeting data availability were discussed in [5] and [6] within the framework of linear quadratic Gaussian control and remote state estimation. False data injection attacks in electric energy systems were studied in [7] and [8] to destroy integrity. Eavesdropping attacks were explored in [9] and [10] for confidentiality violation. From the perspective of a defender, strategies based on encryption [11], [12] and hypothesis testing [13], [14] were proposed for prevention and detection of the attacks. Resilient approaches that take into account the interactive decision-making process between an agent and its adversary were developed through game theory to counter the malicious attacks [15]–[18].

In this article, we focus on confidentiality issues in remote state estimation of dynamical systems. In our setup, a sensor takes measurements of the process and forwards its local estimate of the system state to a remote estimator across a packet-dropping channel; an eavesdropper overhears the transmission to intercept system information (see Fig. 1). This setup was

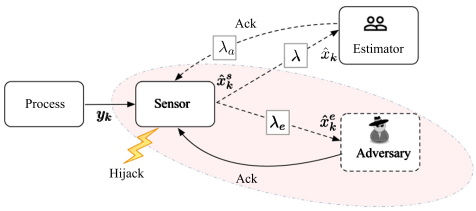


Fig. 2. Problem setup: A sensor transmits the local estimate to a legitimate remote estimator. An adversary overhears the transmissions for espionage. It is capable of (1) hacking the sensor; (2) sending an acknowledgment to the sensor; (3) reprograming the transmission policy according to the acknowledgments from the estimator and the adversary while trying to stay undetected by the estimator.

investigated in [19]–[22]. To preserve privacy for the legitimate estimator, Tsiamis *et al.* [10] introduced a control-theoretic definition of "perfect secrecy" which requires that the user's expected error remains bounded while the eavesdropper's expected error grows unbounded. The authors proved that by applying a secrecy mechanism that randomly withholds sensor information, perfect secrecy can be ensured on the premise that the user's packet reception rate is larger than the adversary's. Our previous work in [9] shows that the perfect secrecy can be achieved without the prerequisite on the packet reception rate, provided acknowledgments (ACK) on successful reception at the legitimate estimator are available to the sensor. Beyond that, schemes that use artificial noise, encoding–decoding mechanism, and a combination of the two were investigated in [10], [19], [22] for protection of the state information. These works consider passive eavesdroppers and focus on the prevention of information leakage from the position of a legitimate estimator. From the adversary's point of view, our recent work [21] proposed an active eavesdropping scheme assuming that the eavesdropper can overhear both the transmission and ACK channel, and is capable of switching between a jamming mode and an eavesdropping mode. By carefully scheduling the two modes, a refined estimation performance can be achieved at the eavesdropper. However, it has not yet been explored how the legitimate party should defend against such active adversaries.

With the development of the attacking techniques, the adversaries become more powerful. Considering the malware, including Stunex and Havex, the adversaries may be capable of simultaneously eavesdropping and hacking into the sensor to falsify the transmission program as discussed in [23]. In the current work, we focus on such adversaries that intend to form their state estimate (see Fig. 2). We aim to answer two fundamental questions: 1) what is the maximum information gain that an adversary may obtain through hacking without being detected by the legitimate remote estimator; and 2) how should the legitimate party maximally reduce the information leakage. Motivated by this, we explore the design of the attacking and defense mechanisms.

As an attacking mechanism, we derive the optimal malicious policy by modeling the transmission process as a constrained Markov decision process (MDP), where the adversary's average of the expected error covariance (AEEC) is minimized and a stealthy constraint is incorporated. We show by analyzing the convergence properties of the MDP's stationary distribution that the reliability of the ACK channel largely determines confidentiality. For situations where the ACK channel has no packet dropouts, we prove the existence of a reference policy that ensures the attainability of perfect secrecy for unstable systems even after the intrusion. In contrast, if the ACK channel has packet dropouts, we show that there always exists a malicious policy that ensures bounded AEEC at the adversary against any stealthy tolerance and any reference policy that gives a bounded AEEC at the legitimate estimator. This indicates that perfect secrecy is unattainable if the ACK channel is not reliable. This property also guarantees the feasibility of the constrained MDP considered and allows us to solve the infinite-state MDP with a finite linear program.

As a defense mechanism, we explore a resilient design of the optimal reference policy from the perspective of the legitimate estimator. The estimator seeks to optimize its estimation performance and reduce information leakage. Assuming that the adversary always commits to the optimal malicious policy for a given reference policy, we formulate this hierarchical decision-making problem as a static Stackelberg game, where the legitimate estimator acts as a leader and the adversary acts as a follower. This results in a bilevel program, whose lower level takes the parameters of the malicious policy as the decision variables and minimizes the adversary's AEEC subject to the stealthy constraint. Moreover, its upper level takes the parameters of the reference policy as the decision variable and minimizes a linear combination of the estimator's AEEC and the negative of the adversary's AEEC. Meanwhile, the lower level problem is embedded as a constraint into the upper level problem.

The contributions of this article are elaborated as follows.

- We study the design of a new attack policy for system confidentiality in remote state estimation, which is more advantageous compared to the passive eavesdroppers in [19]–[22] and the active eavesdropper in [21]. In particular, compared with the active eavesdropper in [21], the adversary considered in the current formulation, whilst having a similar goal, is more capable since the jamming strategies of [21] can also be realized as a special case by withholding certain transmissions. In this sense, the attack scenario considered in the present work is more challenging to the legitimate party.
- We analyze the decisive role of the reliability of the ACK channel in system confidentiality. We show that if the ACK channel has no packet dropouts, then perfect secrecy can be achieved under any stealthy attack. To make this conclusion independent of the detection algorithms being employed, we adopt a notion of stealthiness. This is an information-theoretic quantity relating the marginal distribution of the observations at the legitimate estimator before and after the intrusion according to the MDP discussed above. Here we depart from [21] and [23], where stealthy constraints are designed for some specific detection algorithms. This notion allows us to obtain a fundamental bound on the stealthiness of the adversary by considering the underlying hypothesis detection problem of identifying if an adversary is present, rather than limiting ourselves to specific detection algorithms used to solve that detection problem [24]–[27].
- From the legitimate estimator's perspective, we derive an optimal resilient reference policy by formulating a suitable bilevel program. The global optimum is then obtained with

our proposed depth-first branch-and-bound (BnB) algorithm. Bilevel programs are widely known to be hard due to their intrinsic nonconvexity and nondifferentiability [28]. Even the simplest bilevel linear programs are proved to be $\mathcal{NP}$-hard [29]. Most of the existing algorithms can only provide a suboptimal solution [30], [31]. In this article, we show that our problem can be simplified such that the global optimum can be obtained aided by the duality theorem [30], the linear structure of the objective function, and the special shape of the feasible region. We reformulate the bilevel problem based on the duality theorem and show that the optimal solution is one of the extreme points of the feasible region. Based on this property, the optimal solution can be found by enumerating the extreme points. A depth-first BnB algorithm is further devised to accelerate the enumeration. Numerical examples are provided for validation.

The remaining parts of the article are arranged as follows. Section II provides the system model and problem setup; Section III analyzes the performance at the adversary before an intrusion is launched; Section IV details the design of the stealthy constraint and derivation of the optimal intrusion policy; Section V formulates a bilevel program for the synthesis of the optimal reference policy; Section VI presents the results of the numerical examples; and, finally, Section VII concludes.

Notations: $\mathbb{R}^n$ is the set of n-dimensional vectors. $\mathbb{N}$ is the set of natural numbers. $X \in \mathbb{R}^{n_1 \times n_2}$ indicates that X is an n_1 by n_2 matrix. If X is a square matrix, i.e., $X \in \mathbb{R}^{n \times n}$, $\mathrm{Tr}(X)$ refers to the trace of X. $\sigma_{\max}(X)$ and $|\lambda_{\max}(X)|$ denote the singular value and spectral radius of X. $X \geq 0$ denotes that the matrix X is positive semidefinite. For any positive semidefinite matrix X, its eigenvalues are real and non-negative. Let $\lambda_{\min}(X)$ denote the value of the smallest eigenvalue. $\mathbb{P}(Y \mid z)$ denotes the probability of Y conditional on z. $\mathbb{E}(Y)$ is the mathematical expectation.

II. Problem Formulation

A. System Model

Consider a discrete-time linear system as

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

where $x_k \in \mathbb{R}^{n_s}$ is the system state. The state x_k is measured by a sensor as

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

with $y_k \in \mathbb{R}^{n_y}$ denoting the measurement. $w_k \in \mathbb{R}^{n_s}$ and $v_k \in \mathbb{R}^{n_y}$ are process and measurement noises. Assume w_k and v_k are mutually independent Gaussian process with zero mean. The covariances of w_k and v_k are denoted as $Q \in \mathbb{R}^{n_s \times n_s}$ and $R \in \mathbb{R}^{n_y \times n_y}$. Moreover, it is assumed that the pair (C, A) is observable and $(A, \sqrt{Q})$ is controllable.

As depicted in Fig. 1, we consider a sensor makes measurements of the system output and optimally estimates system states with a Kalman filter. Denote the posterior local state estimate as

$$\hat{x}_k^s \triangleq \mathbb{E}[x_k \mid y_0, \ldots, y_k].$$

The corresponding error covariance $P_k^s \triangleq \mathbb{E}[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)^\top \mid y_0, \ldots, y_k]$ exponentially converges to a steady state [32]. Denote the steady-state value as $\bar{P}$. After obtaining $\hat{x}_k^s$, the sensor broadcasts the estimate to a remote estimator. Denote an indicator variable ν_k as the transmission command such that the sensor transmits if $\nu_k = 1$ and keeps silent if $\nu_k = 0$. Let γ_k be an indicator variable for successful reception, i.e., $\gamma_k = 1$ denoting a successful reception and $\gamma_k = 0$ implying the occurrence of a packet dropout. Assume γ_k is i.i.d Bernoulli distributed, namely,

$$\mathbb{P}[\gamma_k = 1 \mid \nu_k = 1] = \lambda. \tag{3}$$

Define $\mathcal{I}_k$ as a collection of the historical information, i.e., $\mathcal{I}_k \triangleq \{\nu_0\gamma_0, \ldots, \nu_k\gamma_k, \nu_0\gamma_0\hat{x}_0^s, \ldots, \nu_k\gamma_k\hat{x}_k^s\}$. Given that ν_k is independent of $\hat{x}_k^s$, the optimal estimate at the legitimate estimator, denoted as $\hat{x}_k$, is in the form of [33]

$$\hat{x}_k \triangleq \mathbb{E}[x_k \mid \mathcal{I}_k] = \begin{cases} \hat{x}_k^s, & \gamma_k\nu_k = 1 \\ A\hat{x}_{k-1}, & \gamma_k\nu_k = 0. \end{cases} \tag{4}$$

Correspondingly, the error covariance at the estimator, denoted as P_k, is in the form of

$$\begin{aligned} P_k &\triangleq \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^\top \mid \mathcal{I}_k] \\ &= \begin{cases} \bar{P} & \gamma_k\nu_k = 1 \\ f(P_{k-1}), & \gamma_k\nu_k = 0. \end{cases} \end{aligned} \tag{5}$$

Here

$$f(X) \triangleq AXA^T + Q. \tag{6}$$

Denote η_k as the holding time at the receiver, which is defined as the number of time steps since the last successful receipt, i.e.,

$$\eta_k \triangleq \min\{\eta \geq 0 : \gamma_{k-\eta} = 1\}. \tag{7}$$

Then, η_k satisfies the recursion

$$\eta_k = \begin{cases} 0 & \nu_k\gamma_k = 1 \\ \eta_{k-1} + 1 & \nu_k\gamma_k = 0 \end{cases}. \tag{8}$$

Using (5) and (7), P_k can be written as a function of η_k as

$$P_k = f^{\eta_k}(\bar{P}).$$

Here $f^n(\cdot)$ denotes the nth fold composition of $f(\cdot)$ with $f^0(X) = X$. As proved in [34], all possible values of P_k form a totally ordered set $\mathbb{S}$, i.e.,

$$\mathbb{S} \triangleq \{\bar{P}, f(\bar{P}), f^2(\bar{P}), f^3(\bar{P}), \ldots\}$$

and

$$\bar{P} \leq f(\bar{P}) \leq f^2(\bar{P}) \leq \cdots. \tag{9}$$

After receiving the packet, the estimator sends an ACK back to the sensor. This enables the sensor to use information about P_k to make scheduling decisions. The ACK channel is often assumed to be reliable [9], [21]. We go beyond this idealization by taking into account packet dropouts across this channel. In the following sections, we show that the reliability of the ACK channel plays a very crucial role in system privacy. Denote λ_a as the successful reception probability of the ACK signal. Let γ_k^a be an indicator variable such that

$$\gamma_k^a = \begin{cases} 1 \text{ ACK is received by the sensor} \\ 0 \text{ a packet dropout occurs} \end{cases}.$$

Then, the conditional distribution of γ_k^a is given as

$$\begin{aligned} &\mathbb{P}(\gamma_k^a = 1 \mid \gamma_k = 1) = \lambda_a \\ &\mathbb{P}(\gamma_k^a = 0 \mid \gamma_k = 1) = 1 - \lambda_a \\ &\mathbb{P}(\gamma_k^a = 0 \mid \gamma_k = 0) = 1. \end{aligned} \tag{10}$$

B. Problem Setup

We consider a scenario that an adversary can overhear the transmissions and hack the sensor to reschedule the transmissions. Let γ_k^e be an indicator of a successful reception at the adversary, such that $\gamma_k^e = 1$ if the transmission is overheard by the adversary and $\gamma_k^e = 0$ otherwise. Assume the successful reception probability is λ_e. We have

$$\mathbb{P}(\gamma_k^e = 1 \mid \nu_k = 1) = \lambda_e. \tag{11}$$

Similar to (4) and (5), assuming that the processes γ_k^e and γ_k are mutually independent, the adversary's optimal estimate is in the form of

$$\hat{x}_k^e = \begin{cases} \hat{x}_k^s, & \gamma_k^e \nu_k = 1 \\ A\hat{x}_{k-1}^e, & \gamma_k^e \nu_k = 0 \end{cases} \tag{12}$$

$$P_k^e = \begin{cases} \overline{P}, & \gamma_k^e \nu_k = 1 \\ f(P_{k-1}^e), & \gamma_k^e \nu_k = 0 \end{cases} \tag{13}$$

with $\hat{x}_k^e \triangleq \mathbb{E}(x_k \mid \mathcal{I}_k^e)$, $P_k^e = \mathbb{E}[(x_k - \hat{x}_k)(x_k - \hat{x}_k)^\top \mid \mathcal{I}_k^e]$, and $\mathcal{I}_k^e \triangleq \{\nu_0\gamma_0^e, \ldots, \nu_k\gamma_k^e, \nu_0\gamma_0^e\hat{x}_0^s, \ldots, \nu_k\gamma_k^e\hat{x}_k^s\}$.

As depicted in Fig. 2, after launching the attack to the sensor, the adversary sends an ACK signal back to the sensor such that the holding time at the adversary, denoted as η_k^e, can be inferred from the ACKs according to (14)

$$\eta_k^e = \begin{cases} 0, & \nu_k\gamma_k^e = 1 \\ \eta_{k-1}^e + 1, & \nu_k\gamma_k^e = 0 \end{cases}. \tag{14}$$

Transmissions can be rescheduled with η_k^e taken into account. Note that since we aim to keep the intrusion undetected by the legitimate remote estimator, rather than the sensor, sending the ACKs from the adversary to the sensor will not increase the probability of being detected (see Fig. 2).

Remark 1: Equation (14) is established based on the assumption that the ACK channel between the adversary and the sensor has no packet dropouts. We make this assumption since this is the most advantageous scenario to the adversary. Studying this will help us analyze the maximal information leakage to the adversary. If this assumption does not hold, the design and analysis in the following sections are still applicable by forming a belief of η_k^e with the sequence of $\nu_k\gamma_k^e$ and the successful reception rate.

We evaluate the estimation performance with an AEEC defined as

$$J_l = \lim_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{tr}(\mathbb{E}(P_k)), \quad J_e = \lim_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{tr}(\mathbb{E}(P_k^e))$$

where J_l corresponds to the legitimate estimator and J_e corresponds to the adversary. In line with [10], we study "perfect secrecy" at the legitimate estimator, here defined as keeping J_l bounded at the legitimate estimator and J_e unbounded at the adversary.

To study perfect secrecy, we next elucidate the optimal design of the malicious transmission policy for the adversary in the following section.

III. Remote State Estimation Without an Intrusion

Before exploring the malicious transmission policy, we first look at the estimation performance of the adversary without intruding on the sensor. This provides a baseline for the design of the malicious policy.

In remote state estimation, event-based transmission strategies are considered to be more efficient in saving energy [35] and preserving privacy [9]. In particular, the transmission command ν_k often depends on the sensor's belief about the remote estimator's expected error covariance P_{k-1} (which is equivalent to the belief about the holding time η_{k-1}). Denote this belief as η_{k-1}^s. If the ACK channel is reliable, i.e., $\lambda_a = 1$, η_k can be accurately inferred from $\{\gamma_0^a, \ldots, \gamma_k^a\}$ according to (10), i.e., $\eta_k^s = \eta_k$. The sensor can then schedule the transmissions according to

$$\mathbb{P}(\nu_{k+1} = 1 \mid \eta_k^s = i) = \tau_i \tag{15}$$

with $0 \le \tau_i \le 1$. The policy in (15) is referred as a reference policy for the sensor. Different from [9] and [35], where the transmission probability τ_i is either 0 or 1, we consider a randomized covariance-based transmission policy as given in [36] for larger design space.

If $\lambda_a < 1$, as discussed in [37], a belief of η_k can be estimated with Bayesian methods. Since the number of belief states exponentially increases with the time since the last $\gamma_k^a = 1$, this approach will dramatically complicate the design. An easy though suboptimal approach for the sensor is to directly update η_k^s according to the most recent ACK as

$$\eta_k^s = \begin{cases} 0, & \gamma_k^a = 1 \\ \eta_{k-1}^s + 1, & \gamma_k^a = 0 \end{cases}. \tag{16}$$

Note that our conclusions in the latter sections are validated if other estimation approaches are applied to η_k^s. For ease in presentation, we assume that η_k^s evolves according to Eq. (16) in the following.

In view of (3) and (8), it can be verified that the sensor's holding time η_k^s satisfies a Markovian property since the transition probability from η_k^s to η_{k+1}^s solely depends on η_k^s. This enables us to formulate the evolution of η_k^s as a Markov chain. According to this, we analyze the stationary distribution of the expected error covariance at the legitimate estimator and the adversary.

As described in Fig. 3, we define the sensor's holding time η_k^s as the state of the Markov chain. The value of the state is taken from the set $\mathbb{S} = \{0, 1, \ldots, \}$. The transition probabilities can be derived from (3) and (10) as

$$\begin{aligned} \mathbb{P}(\eta_{k+1}^s = i+1 \mid \eta_k^s = i) &= 1 - \tau_i\lambda\lambda_a \\ \mathbb{P}(\eta_{k+1}^s = 0 \mid \eta_k^s = i) &= \tau_i\lambda\lambda_a. \end{aligned} \tag{17}$$

Since the transition probabilities are independent of time, the Markov chain is time-homogeneous. Denote π_i^s as the stationary probability of the state $\eta_k^s = i$. The unique stationary distribution of η_k^s follows [36]

$$\begin{aligned} \pi_0^s &= \frac{1}{1 + \sum_{l=0}^{\infty} \prod_{m=0}^{l} (1 - \tau_m\lambda\lambda_a)} \\ \pi_i^s &= \frac{\prod_{m=0}^{i-1} (1 - \tau_m\lambda\lambda_a)}{1 + \sum_{l=0}^{\infty} \prod_{m=0}^{l} (1 - \tau_m\lambda\lambda_a)}, \ i \ge 1. \end{aligned} \tag{18}$$

Define

$$J_u = \sum_{j=0}^{\infty} \pi_j^s \mathrm{tr}(f^j(\bar{P})). \tag{19}$$

In Proposition 1, we show that J_u is an upper bound on the AEEC at the legitimate estimator.

Proposition 1: For any given transmission policy parameterized by the transmission probability $\{\tau_i\}$, $i \in \mathbb{N}$, the estimator's averaged expected error covariance J_l is upper bounded as

$$J_l \le J_u. \tag{20}$$

The equality is achieved when $\lambda_a = 1$.

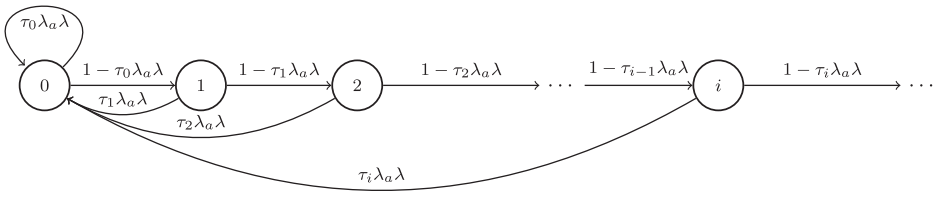


Fig. 3. Markov chain: $\mathbb{P}(\gamma_k|\nu_k=1)=\lambda$. $\mathbb{P}(\gamma_k^a|\gamma_k=1)=\lambda_a$. The state $s_k=i$ denotes the event $\eta_k^s=i$.

Proof: In view of (8), (10), and (16), we have $\eta_k \le \eta_k^s$. Since $P_k = f^{\eta_k}(\bar{P})$ and the function $f^n(\bar{P})$ is nondecreasing with n, it can be derived that

$$J_l = \lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\mathrm{tr}(\mathbb{E}(P_k)) = \lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\mathrm{tr}(\mathbb{E}(f^{\eta_k}(\bar{P})))$$

$$\le \lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\mathrm{tr}(\mathbb{E}(f^{\eta_k^s}(\bar{P}))) = \sum_{j=0}^{\infty}\pi_j^s\mathrm{tr}(f^j(\bar{P})) = J_u.$$

If $\lambda_a = 1$, we have $\eta_k = \eta_k^s$ and the equality is achieved. ■

Since the sensor can hardly infer the exact value of η_k when $\lambda_a < 1$, it can take J_u, which depends on η_k^s, as an index of the legitimate estimator's performance. Sufficient and necessary conditions for a bounded J_u are given in Proposition 3 based on Lemma 2.

Lemma 2: For any positive integer i, there exist scalars $0 < c_l < c_u$ such that $\mathrm{tr}f^i(\bar{P})$ satisfies that

$$c_l + c_l i|\lambda_{\max}(A)|^{2i} \le \mathrm{tr}(f^i(\bar{P})) \le c_u + c_u i^{2n_c+1}|\lambda_{\max}(A)|^{2i}. \tag{21}$$

Here n_c denotes the largest geometric multiplicity of A.

Proof: See Appendix A. ■

Proposition 3: The legitimate estimator's performance index J_u is bounded if there exists an integer $N_h > 0$ such that when $i \ge N_h$, the transmission probability τ_i satisfies that

$$\tau_i > \frac{1}{\lambda\lambda_a}\left(1 - \frac{1}{|\lambda_{\max}(A)|^2}\right). \tag{22}$$

Meanwhile, if J_u is bounded and $|\lambda_{\max}(A)| \ge 1$, then τ_i must satisfy that

$$\lim_{l\to\infty}\prod_{i=0}^{l-1}(1-\tau_i\lambda) = 0. \tag{23}$$

The proof of Proposition 3 is given in Appendix B. Next, we investigate, without specifying the transmission policy, the estimation performance at the adversary on the premise that J_u is bounded.

In view of Lemma 2, the adversary's AEEC J_e is always bounded if the system is strictly stable, i.e., $|\lambda_{\max}(A)| < 1$. Hence, in Proposition 4, we exclude this trivial case and focus on marginally stable and unstable systems.

Proposition 4: If a transmission policy parameterized by $\{\tau_i\}$, $i \in \mathbb{N}$, can make J_u bounded, then the adversary's AEEC J_e has the following properties.

i) If the system is marginally stable, i.e., $|\lambda_{\max}(A)| = 1$, J_e is bounded, but can be made arbitrarily large by properly designing $\{\tau_i\}$. Namely, given any scalar $\underline{b} > 0$, there exists a transmission policy $\{\tau_i\}, i \in \mathbb{N}$, such that $J_e > \underline{b}$.

ii) If $0 < \lambda_e < 1$ and the system is unstable, i.e., $|\lambda_{\max}(A)| > 1$, then there exists a transmission policy ensuring perfect secrecy, i.e., $J_e = \infty$.

Proof: See Appendix C. ■

Proposition 4 suggests that by properly designing the transmission policy, the sensor is capable of driving the AEEC at the adversary to infinity if the dynamics in (1) is unstable, and arbitrarily large if the system is marginally stable. This motivates the adversary to secretly reschedule the transmissions to obtain a more accurate estimate.

IV. Stealthy Malicious Transmission Policy

In this section, we adopt the adversary's perspective and study how to optimize the malicious transmission policy such that it is more advantageous to the adversary while staying undetected. We model the transmission process as an MDP and then devise a stealthy constraint in terms of the state–action pairs associated with the MDP. After that, the optimal malicious policy is derived by solving a constrained MDP. Attainability of perfect secrecy is analyzed for unstable systems based on the feasibility of the constrained MDP.

A. Markov Decision Process

As shown in Fig. 2, the sensor is controlled by the adversary after the hacking, and both η_k^e and η_k^s are known to the sensor. This enables the adversary to modify the transmission policy in (15) by taking into account the adversary's covariance P_k^e (equivalent to η_k^e) in the general form of

$$\mathbb{P}(\nu_{k+1}=1 \mid \eta_k^s=i, \eta_k^e=j) = \tilde{\tau}_{ij},\ \forall i,j\in\mathbb{N}. \tag{24}$$

Note from (14) and (16) that both η_k^s and η_k^e are Markovian. We can formulate an MDP to derive the optimal malicious transmission policy for the adversary. Define the pair (η_k^s, η_k^e) as the state S_k and the action as the transmission command $\nu_k \in \mathbb{A}$ with $\mathbb{A} = \{0,1\}$. Based on (3), (8), and (11), the state transition probabilities for $S_k = (i,j)$ are derived as follows:

$$\mathbb{P}(S_{k+1} \mid S_k, \nu_{k+1})$$

$$= \begin{cases} 1 & S_{k+1}=(i+1,j+1),\ \nu_{k+1}=0 \\ (1-\lambda\lambda_a)(1-\lambda_e) & S_{k+1}=(i+1,j+1),\ \nu_{k+1}=1 \\ \lambda\lambda_a(1-\lambda_e) & S_{k+1}=(0,j+1),\ \nu_{k+1}=1 \\ (1-\lambda\lambda_a)\lambda_e & S_{k+1}=(i+1,0),\ \nu_{k+1}=1 \\ \lambda\lambda_a\lambda_e & S_{k+1}=(0,0),\ \nu_{k+1}=1 \end{cases}. \tag{25}$$

In Problem 1, the action ν_k is determined by minimizing the AEEC at the adversary while satisfying a stealthy constraint.

Problem 1:

$$\min_{\nu_k} \quad J_e = \lim_{T\to\infty}\frac{1}{T}\sum_{k=1}^{T}\mathrm{tr}(\mathbb{E}(P_k^e))$$

$$\text{s.t.} \quad \text{stealthy constraint.}$$

Next, we detail the design of the stealthy constraint.

B. Stealthy Constraint

From (24), the transmission probability at η_k^s follows

$$\mathbb{P}(\nu_{k+1}=1 \mid \eta_k^s=i)=\sum_{j=0}^{\infty}\tilde{\tau}_{ij}\mathbb{P}(\eta_k^e=j)$$

which might significantly differ from the reference policy in (15). Being aware of the potential existence of the adversary, the legitimate estimator will proactively detect whether the transmission policy in (15) is modified or not based on its information set $\mathcal{I}_k$. This becomes a parameter estimation problem for a hidden Markov model (HMM) [38] if we take η_k^s as the hidden states and $\nu_k\gamma_k$ as the observations (emissions). The state transition probability is given in (17) and the emission probabilities can be derived from (3), (10), (15), and (16), as follows:

$$\begin{aligned}\mathbb{P}(\nu_k\gamma_k=1 \mid \eta_k^s=i+1)&=\frac{\mathbb{P}(\nu_k\gamma_k=1 \mid \eta_{k-1}^s=i)}{\mathbb{P}(\eta_k^s=i+1 \mid \eta_{k-1}^s=i)}\\&=\tau_i\lambda/(1-\tau_i\lambda\lambda_a)\\\mathbb{P}(\nu_k\gamma_k=0 \mid \eta_k^s=i+1)&=1-\tau_i\lambda/(1-\tau_i\lambda\lambda_a)\\\mathbb{P}(\nu_k\gamma_k=1 \mid \eta_k^s=0)&=1\\\mathbb{P}(\nu_k\gamma_k=0 \mid \eta_k^s=0)&=0.\end{aligned}\tag{26}$$

Both the transition probability and emission probability are determined by the transmission policy $\{\tau_i\}$, and thus the legitimate estimator can detect variations in the parameters of this HMM by observing the indicator variables $\nu_0\gamma_0,\ldots,\nu_k\gamma_k$. This HMM has infinite hidden states since η_k^s takes values from the set $\mathbb{N}$. It can be equivalently represented by a finite-state HMM by aggregating the state $\eta_k^s\geq N_o$ for any positive integer N_o. From Theorem 6 in [39], the transmission probability τ_i with $i\in\{0,1,\ldots,N_o\}$ is generically identifiable from the marginal distribution of N_o consecutive observations

$$o_{k+1:k+N_o}=(\nu_{k+1}\gamma_{k+1},\ldots,\nu_{k+N_o}\gamma_{k+N_o}).$$

This property motivates the legitimate estimator to formulate a Hypothesis test as follows.

Hypothesis test

> H_0: *The marginal distribution of $o_{k+1:k+N_o}$ follows the distribution $\mathcal{P}_0$.*
>
> H_1: *The marginal distribution of $o_{k+1:k+N_o}$ does not follow the distribution $\mathcal{P}_0$.*

Denote the distribution of $o_{k+1:k+N_o}$ after the intrusion as $\mathcal{P}_1$. To stay undetected, the adversary intends to have the observations $o_{k+1:k+N_o}$ follow $\mathcal{P}_1$ while keeping Hypothesis H_0 not rejected by the legitimate estimator. Consider that the Kullback–Leibler distance $\mathcal{KL}(\mathcal{P}_1||\mathcal{P}_0)$, defined as

$$\mathcal{KL}(\mathcal{P}_1||\mathcal{P}_0)=\sum_{x\in\Omega_s}\mathcal{P}_1(x)\log\frac{\mathcal{P}_1(x)}{\mathcal{P}_0(x)}\tag{27}$$

gives the expected log-likelihood with which Hypothesis H_0 can be rejected per event [40]. We formulate a stealthy constraint as

$$\mathcal{KL}(\mathcal{P}_1||\mathcal{P}_0)\leq\epsilon_{kl}\tag{28}$$

with $\epsilon_{kl}>0$ denoting a stealthy tolerance. A small ϵ_{kl} will make the intrusion less likely being detected.

Next, we study the connections among the detection horizon N_o, the stealthy tolerance ϵ_{kl}, the successful reception probability λ_a, and the reference policy (15) onto perfect secrecy. In Theorem 5, we show that if the ACK channel is reliable, i.e., $\lambda_a=1$, and N_o is large enough, then perfect secrecy can be achieved for unstable systems.

Theorem 5. (Attainability of "Perfect Secrecy"): Given that $\lambda_a=1$, $\lambda>1-\frac{1}{|\lambda_{\max}(A)|^2}$, $0<\lambda_e<1$, and $|\lambda_{\max}(A)|>1$, devise the reference transmission policy as

$$\mathbb{P}[\nu_{k+1}=1 \mid \eta_k^s]=\begin{cases}1 & \eta_k^s>\bar{t}\\0 & \text{else}\end{cases}\tag{29}$$

with $\bar{t}$ satisfying $\frac{1}{|\lambda_{\max}(A)|^{2(\bar{t}+1)}}<\lambda(1-\lambda_e)$. Then, J_u is ensured to be bounded. If $N_o>\bar{t}$, there is no malicious transmission policy in the form of (24) that can simultaneously make J_e bounded and fulfill the stealthy constraint in (28).

Proof: See Appendix D. ■

In the following section, we show an opposite conclusion when there are packet dropouts in the ACK channel. In this case, the state η_k and η_k^s cannot be synchronized, making perfect secrecy not attainable for any reference policy and any detection horizon.

C. Constrained MDP for an Unreliable ACK Channel

In this section, we transform the stealthy constraint in (28) into an l_1-norm constraint on the stationary distribution of a state–action pair, such that Problem 1 can be cast into a linear program [41]. Based on this, we prove the nonattainability of perfect secrecy by studying the feasibility of the constrained MDP.

Proposition 6: Define $\omega_s(i,a)$ as the stationary probability of the state–action pair $(\eta_k^s=i,\nu_{k+1}=a)$ before the intrusion and $\rho_s(i,a)$ as that after the intrusion. Given that $\lambda_a<1$, for any stealthy tolerance $\epsilon_{kl}>0$ and any detection horizon $N_o>0$, there exists a scalar $\epsilon_s>0$ such that if

$$\|\omega_s-\rho_s\|_1\leq\epsilon_s,\tag{30}$$

then the stealthy constraint in (28) is satisfied.

Proof: See Appendix E. ■

According to Proposition 6, we can take (30) as the stealthy constraint in Problem 1. Define a tensor ω such that its component $\omega(i,j,a)$ is the stationary probability of the appearance of the state–action pair $(S_k=(i,j),\nu_{k+1}=a)$ with $i,j\in\mathbb{N},a\in\mathbb{A}$ before the launch of the intrusion. Similarly, we can define ρ as the stationary distribution after the intrusion. Based on ω and ρ, we show that Problem 1 is equivalent to a linear program.

Let us look at ρ first. Note from [41] that ρ is referred to as an occupation measure in constrained MDP, which satisfies

$$\begin{aligned}&\sum_{a\in\mathbb{A}}\rho(i,j,a)-\sum_{i,'j'\in\mathbb{N},a\in\mathbb{A}}\rho(i,j,a)\mathcal{P}_{i,'j,'a,i,j}=0\\&\sum_{i,j\in\mathbb{N},a\in\mathbb{A}}\rho(i,j,a)=1\\&\rho(i,j,a)\geq 0,\ \forall i,j\in\mathbb{N}\ \forall a\in\mathbb{A}.\end{aligned}\tag{31}$$

Here $\mathcal{P}_{i,'j,'a,i,j}$ is a short form of the state transition probability $\mathbb{P}(S_{k+1}=(i,j)\mid S_k=(i,'j'),\nu_{k+1}=a)$ in (25). For ease of notation, we write (31) in a compact form as $\rho\in\Omega$. Moreover, we can express J_e and ρ_s as linear combinations of ρ, namely,

$$\begin{aligned}J_e&=\lim_{n\to\infty}\sum_{i\in\mathbb{N}}\sum_{a\in\mathbb{A}}\left(\sum_{j\leq n}\rho(i,j,a)\mathrm{tr}(f^j(\bar{P}))\right)\\\rho_s(i,a)&=\sum_{j\in\mathbb{N}}\rho(i,j,a).\end{aligned}\tag{32}$$

Similarly, we have $\omega \in \Omega$ and $\omega_s(i,a) = \sum_{j\in\mathbb{N}} \omega(i,j,a)$. In addition, to be accordance with (15), ω should satisfy that

$$\tau_i = \frac{\omega(i,j,a=1)}{\sum_{a\in\mathbb{A}} \omega(i,j,a)},\ \forall i,j \in \mathbb{N}.$$

If the transmission policy $\{\tau_i\}$ is fixed, the resulted Markov chain is ergodic and thus has a unique stationary distribution, indicating that ω, as well as ω_s, is uniquely determined. Accordingly, the optimal malicious policy can be derived from Problem 2 where the occupation measure ρ is taken as a decision variable.

Problem 2:

$$\begin{aligned} \min_{\boldsymbol{\rho}} \quad & J_e \\ \text{s.t.} \quad & \rho \in \Omega \\ & \sum_{i\in\mathbb{N},a\in\mathbb{A}} |\sum_{j\in\mathbb{N}} \rho(i,j,a) - \omega_s(i,a)| \le \epsilon_s. \end{aligned} \tag{33}$$

Equation (33) arises from (30). After introducing auxiliary variables $\epsilon_{i,a}$ with $i \in \mathbb{N}, a \in \mathbb{A}$, (33) can be further simplified into a set of linear equalities as

$$\begin{aligned} & -\epsilon_{i,a} \le \sum_{j\in\mathbb{N}} \rho(i,j,a) - \omega_s(i,a) \le \epsilon_{i,a} \\ & \sum_{i\in\mathbb{N},a\in\mathbb{A}} \epsilon_{i,a} \le \epsilon_s. \end{aligned} \tag{34}$$

Therefore, Problem 2 is a linear program.

If Problem 2 is feasible, which means there is a solution that can make J_e bounded and the constraints satisfied, for any ϵ_s and any reference policy $\{\tau_i\}$, then perfect secrecy is not attainable. Thus, the feasibility of this constrained linear program determines the attainability of perfect secrecy.

In the following section, we study the feasibility of Problem 2 by truncating the original MDP into a finite-state MDP. The truncation is also employed in the practical implementation of the malicious policy.

D. Finite-Dimensional Approximation

We truncate the MDP with $(N_t+1)^2$ states reserved by defining the state S_k as

$$S_k = \left(\min(\eta_k^s, N_t), \min(\eta_k^e, N_t)\right).$$

Here N_t is the truncation horizon. The transition probability corresponding to the truncated MDP is revised as (cf(25))

$$\mathbb{P}(S_{k+1} \mid S_k, \nu_{k+1}) =$$

$$\begin{cases} 1 & S_{k+1}=(\min(i+1,N_t),\min(j+1,N_t)) \\ & \nu_{k+1}=0 \\ (1-\lambda\lambda_a)(1-\lambda_e) & S_{k+1}=(\min(i+1,N_t),\min(j+1,N_t)) \\ & \nu_{k+1}=1 \\ \lambda\lambda_a(1-\lambda_e) & S_{k+1}=(0,\min(j+1,N_t)) \\ & \nu_{k+1}=1 \\ (1-\lambda\lambda_a)\lambda_e & S_{k+1}=(\min(i+1,N_t),0) \\ & \nu_{k+1}=1 \\ \lambda\lambda_a\lambda_e & S_{k+1}=(0,0),\ \nu_{k+1}=1 \end{cases} \tag{35}$$

Define a tensor $\rho_t \in \mathbb{R}^{(N_t+1)\times(N_t+1)\times 2}$ as the occupation measures for the states of the truncated MDP. Similar to (31), we have ρ_t satisfy that

$$\begin{aligned} & \sum_{a\in\mathbb{A}} \rho_t(i,j,a) - \sum_{0\le i,'j'\le N_t, a\in\mathbb{A}} \rho_t(i,j,a)\mathcal{P}_{i,'j,'a,i,j} = 0 \\ & \sum_{0\le i,j\le N_t, a\in\mathbb{A}} \rho_t(i,j,a) = 1 \\ & 0 \le \rho_t(i,j,a) \le 1,\ \forall\ 0 \le i,j \le N_t\ \forall a \in \mathbb{A}. \end{aligned} \tag{36}$$

Here $\mathcal{P}_{i,'j,'a,i,j}$ denotes the transition probability in (35). Denote (36) as $\rho_t \in \Omega_{N_t}$ for simplicity in notation. Meanwhile, we limit the number of design variables in the malicious policy as

$$\tau_{ij}^t = \begin{cases} \tilde{\tau}_{ij} & 0 \le i,j < N_t \\ 1 & i \ge N_t \text{ or } j \ge N_t \end{cases} \tag{37}$$

where $\tilde{\tau}_{i,j}$ with $0 \le i,j \le N_t$ are taken as free variables to be determined and the others are fixed to be 1. In accordance to (37), $\frac{\rho_t(i,j,a=1)}{\sum_{a\in\mathbb{A}}\rho_t(i,j,a)} = 1$ when $i = N_t$ or $j = N_t$, which gives

$$\rho_t(i,j,a=0) = 0, \quad i = N_t \text{ or } j = N_t. \tag{38}$$

Proposition 7, stated below, shows that J_e is a linear function of ρ_t and the policy (37) makes J_e bounded for any N_t.

Proposition 7: The averaged expected error covariance corresponding to the truncated policy in (37) can be expressed in terms of ρ_t as

$$\begin{aligned} J_e = & \sum_{i,j\le N_t,\ a\in\mathbb{A}} \rho_t(i,j,a)\text{tr}(f^j(\bar{P}))+ \\ & \sum_{i\le N_t} \rho_t(i,N_t,a=1)\sum_{j=0}^{\infty}\lambda_e(1-\lambda_e)^{j-N_t}\text{tr}f^j(\bar{P}) \end{aligned} \tag{39}$$

which is bounded for any $N_t \ge 0$ if $\lambda_e \in (1-\frac{1}{|\lambda_{\max}(A)|^2},1)$.

Proof: See Appendix F. ∎

This enables us to devise a linear program based on ρ_t as

Problem 3:

$$\begin{aligned} \min_{\boldsymbol{\rho}_t,\epsilon_{i,a}} \quad & J_e \\ \text{s.t.} \quad & (36),\ (38) \\ & \text{(Stealthy constraint):} \\ & -\epsilon_{i,a} \le \sum_{0\le j\le N_t} \rho_t(i,j,a) - \omega_s(i,a) \le \epsilon_{i,a} \qquad (40) \\ & -\epsilon_{N_t,a} \le \sum_{0\le j\le N_t} \rho_t(N_t,j,a) - \sum_{N_t}^{\infty}\omega_s(i,a) \le \epsilon_{N_t,a} \qquad (41) \\ & \sum_{0\le i\le N_t,\ a\in\mathbb{A}} \epsilon_{i,a} \le \epsilon_s. \qquad (42) \end{aligned}$$

Feasibility of Problem 3 is analyzed in the following theorem.

Theorem 8. (Feasibility): Given that $\lambda_a < 1$ and $\lambda_e \in (1-\frac{1}{|\lambda_{\max}(A)|^2},1)$, there exists an integer N_t such that Problem 3 is ensured to be feasible for any stealthy tolerance $\epsilon_s > 0$.

Proof: See Appendix G.

Denote the solution of Problem 3 as ρ_t^c. The associated transmission probability $\tilde{\tau}_{ij}$ in (37) can be determined as

$$\tilde{\tau}_{i,j} = \frac{\rho_t^c(i,j,a=1)}{\sum_{a\in\mathbb{A}}\rho_t^c(i,j,a)},\ \forall\ 0 \le i,j < N_t.$$

Next, we show that by tuning the truncation horizon N_t, the policy derived from the finite-dimension linear program in Problem 3 can be made arbitrarily close to that of the infinite-dimension linear program in Problem 2.

Proposition 9. (ϵ-Optimality of the Truncated Policy): Denote the optimal policy derived from the infinite dimension linear program in Problem 2 as $\boldsymbol{\tau}^\star$ and the optimal truncated policy derived from Problem 3 as $\boldsymbol{\tau}^c$. Then, we have

$$J_e(\boldsymbol{\tau}^c) \leq J_e(\boldsymbol{\tau}^\star) + \epsilon_g(N_t). \tag{43}$$

In addition, with $\boldsymbol{\tau}_c$ implemented, the stealthy constraint in (30) satisfies that

$$\|\omega_s - \rho_s\|_1 \leq \epsilon_s + \epsilon_\omega(N_t). \tag{44}$$

Here $\lim_{N_t\to\infty} \epsilon_g(N_t) = 0$ and $\lim_{N_t\to\infty} \epsilon_\omega(N_t) = 0$.

Proof: See Appendix H. ■

Combining Theorem 8 and Proposition 9, we can conclude the nonattainability of perfect secrecy as follows.

Corollary 10 (Nonattainability of "Perfect Secrecy"): Suppose that $\lambda_a < 1$ and $\lambda_e \in (1 - \frac{1}{|\lambda_{\max}(A)|^2}, 1)$. Then perfect secrecy cannot be attained for the legitimate estimator since for any reference policy, any detection horizon N_o, and any stealthy tolerance ϵ_{kl}, there exists a malicious policy that can satisfy the stealthy constraint and make J_e bounded.

Remark 2: Our analysis of perfect secrecy is mainly conducted for unstable systems since for stable systems, the AEECs of both the legitimate estimator and the adversary are always bounded, and therefore perfect secrecy can never be attained. Nonetheless, the design of the malicious transmission policy proposed in this section is still valid for stable systems in terms of maximizing the information overheard. Our previous work on privacy-preserving transmission scheduling for stable systems may shed a light on this point [42].

V. Synthesis of the Optimal Reference Policy

In this section, we look at the problem from the legitimate estimator's point of view and explore the design of the optimal reference transmission policy for privacy enhancement. In view of the negative result in Corollary 10, we propose a resilient transmission strategy for the legitimate estimator that can simultaneously optimize its own estimation accuracy and reduce the information leakage to the adversary.

A. Formulation of a Stackelberg Game

If we view the legitimate estimator and the adversary as two players of a game, we may notice that they have different objectives. The legitimate estimator would like to reduce the estimation error and information leakage, while the adversary intends to maximize the information overheard. The two decision-making problems are coupled via the stealthy constraint. Since the hacking occurs after the set up of the communication between the sensor and the legitimate estimator, the legitimate estimator has the priority to determine the reference policy before the hacking. Therefore, we formulate this interactive decision-making process as a Stackelberg game where the legitimate estimator acts as the leader and the adversary acts as the follower [43].

In particular, we define the estimator's performance index as J_c, which is a linear combination of the AEEC before and after the intrusion, i.e.,

$$J_c = \alpha\left(\beta_1\hat{J}_u - (1-\beta_1)\hat{J}_e\right) + (1-\alpha)\left(\beta_2 J_u - (1-\beta_2)J_e\right)$$

Here $\alpha, \beta_1, \beta_2 \in [0,1]$. J_u and J_e evaluate the estimation performance at the legitimate estimator and the adversary after the intrusion, while $\hat{J}_u$ and $\hat{J}_e$ evaluate the estimation performance before the intrusion. Hence, J_u and J_e are determined by the malicious policy, and $\hat{J}_u$ and $\hat{J}_e$ are determined by the reference policy. The two policies couple via the stealthy constraint. We outline the Stackelberg game as Problem 4.

Problem 4:

$$\begin{aligned}\min_{\text{Reference policy}} \quad & J_c \\ \text{s.t.} \quad & \text{malicious policy} = \arg\min \ J_e \\ & \qquad\qquad \text{s.t.} \quad \text{stealthy constraint.}\end{aligned}$$

Since, in practice, it is hard to design and implement a policy with parameters of infinite-dimension, we limit ourselves into a class of suboptimal policy in the form of

$$\mathbb{P}(\nu_{k+1} = 1 \mid \eta_k^s = i) = \begin{cases} \tau_i & 0 \leq i < N_r \\ 1 & N_r \leq i \leq N_t \end{cases}. \tag{45}$$

It can be verified from Proposition 4 that (45) can ensure perfect secrecy for unstable systems before the intrusion, provided that N_r is selected large enough.

Next, we detail Problem 4 as a bilevel program using the notations of occupation measure. As defined in Section IV-D, ρ_t denotes the occupation measure of the finite-dimension MDP after the intrusion. Similar to the derivation of J_e in (39), we can express J_u in terms of ρ_t as

$$\begin{aligned} J_u = & \sum_{i,j\leq N_t,\, a\in\mathbb{A}} \rho_t(i,j,a)\mathrm{tr}(f^i(\bar{P})) \\ & + \sum_{j\leq N_t} \rho_t(j,N_t,a=1)\sum_{i=0}^{\infty}\lambda\lambda_a(1-\lambda\lambda_a)^{i-N_t}\mathrm{tr}f^i(\bar{P}). \end{aligned} \tag{46}$$

Moreover, let the tensor $\omega_t \in \mathbb{R}^{(N_t+1)\times(N_t+1)\times 2}$ be the occupation measure of the MDP before the intrusion. Then, ω_t satisfies the general properties of occupation measure given in (36), i.e.,

$$\begin{aligned} & \omega_t \in \Omega_{N_t} \qquad \sum_{0\leq i,j\leq N_t, a\in\mathbb{A}} \omega_t(i,j,a) = 1 \\ & \omega_t(i,j,a=0) = 0, \quad i = N_t \text{ or } j = N_t \end{aligned} \tag{47}$$

and

$$0 \leq \omega_t(i,j,a) \leq 1. \tag{48}$$

Equation (45) further gives that

$$\begin{aligned} & \frac{\omega_t(i,j,a=1)}{\omega_t(i,j,a=0)+\omega_t(i,j,a=1)} = \tau_i \quad 0 \leq i < N_r \\ & \frac{\omega_t(i,j,a=1)}{\omega_t(i,j,a=0)+\omega_t(i,j,a=1)} = 1 \quad N_r \leq i < N_t \end{aligned} \tag{49}$$

for all $0 \leq i,j \leq N_t$. Now we are ready to express $\hat{J}_u$ and $\hat{J}_e$ with ω_t as

$$\begin{aligned} \hat{J}_u = & \sum_{i,j\leq N_t,\, a\in\mathbb{A}} \omega_t(i,j,a)\mathrm{tr}(f^i(\bar{P})) \\ & + \sum_{j\leq N_t} \omega_t(j,N_t,a=1)\sum_{i=0}^{\infty}\lambda\lambda_a(1-\lambda\lambda_a)^{i-N_t}\mathrm{tr}f^i(\bar{P}) \end{aligned} \tag{50}$$

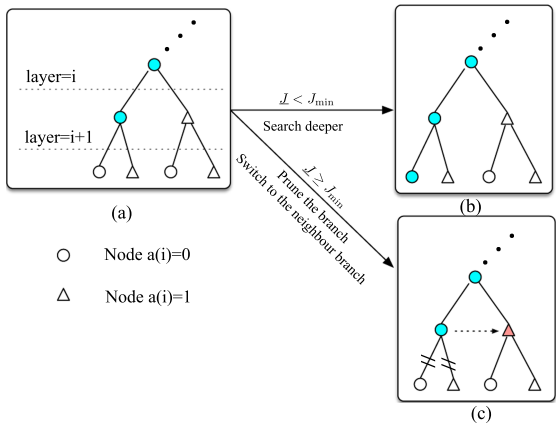


Fig. 4. An illustration of the depth-first branch-and-bound algorithm.

$$\hat{J}_e = \sum_{i,j\leq N_t,\, a\in\mathbb{A}} \omega_t(i,j,a)\mathrm{tr}(f^j(\bar{P})) + \sum_{i\leq N_t} \omega_t(i,N_t,a=1)\sum_{j=0}^{\infty}\lambda_e(1-\lambda_e)^{j-N_t}\mathrm{tr}f^j(\bar{P}). \tag{51}$$

In addition, we may notice that $\omega_s(i,a)$ in Problem 3 is the marginal probability of $\omega_t(i,j,a)$, i.e., $\sum_{0\leq j\leq N_t, a\in\mathbb{A}}\omega_t(i,j,a)=\omega_s(i,a)$. Hence, by replacing $\omega_s(i,a)$ in (40) and (41) with $\sum_{0\leq j\leq N_t,a\in\mathbb{A}}\omega_t(i,j,a)$, Problem 4 can be detailed as

Problem 5:

$$\min_{\tau,\omega_t,\rho_t}\ \alpha\left(\beta_1\hat{J}_u-(1-\beta_1)\hat{J}_e\right)+(1-\alpha)\left(\beta_2 J_u-(1-\beta_2)J_e\right)$$

$$\text{s.t. } (39),\ (46)-(51),$$

$$\rho_t = \arg\min_{\rho_t,\epsilon_{i,a},0\leq i\leq N_t,a\in\mathbb{A}} J_e$$

$$\text{s.t.} \quad (36),\ (38),\ (40)-(42).$$

B. A Depth-First Branch-and-Bound Algorithm

In this section, we present a BnB algorithm to derive the optimal solution of Problem 5. Before detailing the algorithm, we show that the optimal reference policy is a deterministic policy as follows.

Proposition 11 (Determinacy): The optimal solution of Problem 5 is at least one of the extreme points of the feasible region. Therefore, the optimal reference transmission policy is a deterministic policy with $\tau_i=0$ or $\tau_i=1$ for $\forall i\in[0,N_r-1]$. ■

Proof: See Appendix I. ■

This proposition shows that there are at most 2^{N_r} candidate solutions. Therefore, if N_r is small, we can obtain the optimal solution by enumerating all the candidate solutions. Next, we present a BnB algorithm to accelerate the computation for the case that N_r is relatively large.

We formulate a binary tree with N_r layers and 2^{N_r} leaf nodes to represent the set of the candidate solutions. In layer i, each node denotes a choice of the transmission probability τ_i. As exemplified in Fig. 4, for each layer i, the round nodes denote $\tau_i=0$ and the triangle nodes denote $\tau_i=1$. Hence, each path that connects the root node and the leaf node gives a feasible solution to Problem 5. With our proposed depth-first BnB algorithm, the nodes in the tree will be traversed from the left to the right while pruning redundant branches to accelerate the search. Specifically, we use l as an index of the depth of the search. Initialize $J_{\min}$ with a large value. When the search proceeds to $l+1$, $\tau_0,\ldots,\tau_l$ are fixed and $\tau_{l+1},\ldots,\tau_{N_r-1}$ are to be determined. To decide whether we should go deeper to visit the subsequent nodes, we need a lower bound on this specific branch [for example, the branch highlighted in blue in Fig. 4(a)]. Compare this lower bound, denoted as $\underline{J}$, with the candidate optimum $J_{\min}$. If $\underline{J}\geq J_{\min}$, there is no need to search deeper since no solution can outperform the candidate optimum. Otherwise, the subsequent nodes should be visited from the left branch to the right branch in turn. The algorithm terminates when the rightmost branch is either traversed or pruned. As long as $\underline{J}$ is a lower bound of the given branch, the derived solution is ensured to be a global optimum of Problem 5.

Next, we detail the derivation of $\underline{J}$. We relax the problem into two separate convex programs which together gives a lower bound of the optimal value. In layer $l+1$, fix $\tau_0,\ldots,\tau_l$. Denote the optimal value of Problem 5 as $J_c^\star$. Consider two reference policies $\mathcal{T}_1$ and $\mathcal{T}_2$ whose transmission probabilities are set as $[\tau_0,\ldots,\tau_l,1,\ldots,1]$ and $[\tau_0,\ldots,\tau_l,0,\ldots,0]$. Before the intrusion, the occupation measures of the corresponding MDPs are denoted as ω_t^1 and ω_t^0. When $\mathcal{T}_1$ is applied, the optimal malicious policy can be derived from Problem 3. Denote the occupation measure of the resulted MDP as ρ_t^1. Based upon these, a lower bound of $J_c^\star$ is provided in Theorem 12.

Theorem 12: Given $\tau_0,\ldots,\tau_l$, set

$$\zeta=\frac{\epsilon_s}{\|\sum_{j=0}^{N_t}\omega_t^0(\cdot,j,\cdot)-\sum_{j=0}^{N_t}\omega_t^1(\cdot,j,\cdot)\|_1+\epsilon_s}. \tag{52}$$

Denote $J_f^\diamond$ and $J_g^\diamond$ as the optimal value of the following two convex programs.

Problem 6:

$$\min_{\omega_t,\rho_t}\ J_g=(1-\alpha)\beta_2 J_u$$

$$\text{s.t. } (36),\ (38),\ (40)-(42)$$

$$(46)-(48),\ (50),\ (51),\ (53),\ (54).$$

Problem 7:

$$\min_{\omega_t,\rho_t}\ J_f=\alpha\left(\beta_1\hat{J}_u-(1-\beta_1)c_e\hat{J}_e\right)-(1-\alpha)(1-\beta_2)J_e$$

$$\text{s.t. } (39),\ (46)-(48),\ (50),\ (51)$$

$$\frac{\omega_t(i,j,a=1)}{\omega_t(i,j,a=0)+\omega_t(i,j,a=1)}=\tau_i\ 0\leq i\leq l \tag{53}$$

$$\frac{\omega_t(i,j,a=1)}{\omega_t(i,j,a=0)+\omega_t(i,j,a=1)}=1\ N_r\leq i<N_t \tag{54}$$

$$\rho_t=(1-\zeta)\omega_t+\zeta\rho_t^1. \tag{55}$$

Then, we have $J_f^\diamond+J_g^\diamond\leq J_c^\star$.

Proof: See Appendix J. ■

VI. Numerical Example

In this section, we verify the aforementioned results with the linearized Pendubot example of [9], where

$$A=\begin{bmatrix}1.0058 & 0.015 & -0.0016 & 0.0000\\ 0.7808 & 1.0058 & -0.2105 & -0.0016\\ -0.0060 & 0.0000 & 1.0077 & 0.0150\\ -0.7962 & -0.0060 & 1.0294 & 1.0077\end{bmatrix}$$

TABLE I
COMPUTATIONAL COMPLEXITY VERSUS OPTIMALITY

Optimization horizon N_r	5	10	15	20
Number of nodes visited (exhaustive search)	32	1028	32768	1.1×10^6
Number of nodes visited (the proposed BnB)	10	17	79	585
Optimal value J_c	-1.85	-19.95	-24.19	-24.19
Threshold	5	10	12	12

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad R = 0.001 \times I$$

$$Q = qq^\top, \quad q = [0.003 \; 1.0000 \; -0.0050 \; -2.150]^\top.$$

The packet reception probability $\lambda = 0.6$ and $\lambda_e = 0.6$. The reception probability of the ACK is set as $\lambda_a = 0.95$. The weight parameters in J_c are set as $\alpha = 0.1$, $\beta_1 = 0.95$, and $\beta_2 = 0.5$. The truncation horizon is taken as $N_t = 50$.

First, we verify the efficiency of the proposed BnB algorithm. As discussed in Proposition 11, the optimal τ_i is either 0 or 1. Therefore, the optimum can be derived by an exhaustive search among the 2^{N_r} leaf nodes. The proposed BnB algorithm searches the intermediate nodes while pruning redundant branches to reduce the computation time. Note that both methods solve convex programs to derive the optimal malicious policy at each node. Therefore, we demonstrate the computational efficiency by comparing the number of nodes visited by the two algorithms. In particular, we fix the stealthy tolerance as $\epsilon_s = 0.05$ and set the optimization horizon N_r as 5, 10, 15, and 20. According to the simulation, the optimal reference is in the form of the threshold-type structure as

$$\nu_{k+1} = \begin{cases} 0 & \eta_k^s < \text{threshold} \\ 1 & \text{else} \end{cases}. \tag{56}$$

As shown in Table I, the proposed BnB algorithm successfully reduces the number of nodes visited and thus significantly reduces the computation time. The results also show that with the increase in optimization horizon N_r, the optimal value J_c decreases but the number of nodes visited increases. From this perspective, N_r can be employed to balance the suboptimality gap and computation complexity.

Next, we examine the effects of the stealthy tolerance ϵ_s on the estimation accuracy at the legitimate estimator and at the adversary. We increase ϵ_s from 0 to 0.1 and derive the corresponding optimal value of $\hat{J}_u$, $\hat{J}_e$, J_u, and J_e by solving Problem 5. As shown in Fig. 5, with the increase of ϵ_s, all of $\hat{J}_u$, $\hat{J}_e$, J_u, and J_e get smaller. However, the improvements at the adversary are more significant after launching the attack. This leads to the increase of the overall performance index J_c. From this point of view, a smaller ϵ_s is helpful for the optimization of J_c. In addition, Fig. 5 shows that the legitimate estimator allows the sensor to transmit more often when ϵ_s increases. This can be interpreted with Problem 5, where the legitimate estimator regulates the information leakage via the stealthy constraint. When the stealthy constraint becomes loose, reducing the transmission cannot prevent information leakage. Therefore, the legitimate estimator will give up on preventing the information leakage and pay more effort to reduce its own estimation error.

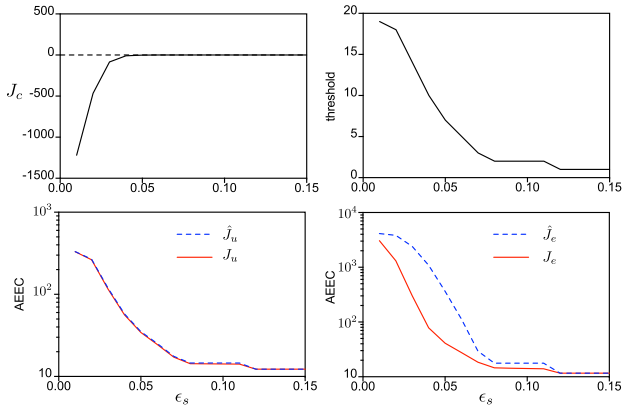


Fig. 5. Variations of J_c, $\hat{J}_u$, $\hat{J}_e$, J_u, J_e and the threshold with the stealthy tolerance ϵ_s.

VII. CONCLUSION

In this article, we study covariance-based transmission policies for remote state estimation, where an active adversary can hack the sensor, reprogram the transmission policy, and overhear the transmissions. From the adversary's perspective, we derive an optimal stealthy malicious policy to reschedule the transmission such that the estimation performance at the adversary is optimized. This is done by formulating the transmission process as a constrained MDP where an information-theoretic stealthy constraint is incorporated. We show that the feasibility of the constrained MDP depends on the reliability of the ACK channel. If the ACK channel is reliable, there exists a reference policy, making the adversary's AEEC unbounded. Otherwise, the constrained MDP is ensured to be feasible with any stealthy tolerance and any reference policy. To make the system resilient, from the legitimate estimator's perspective, we explore the design of the reference policy to maximally reduce information leakage while ensuring its estimation performance. A bilevel program is formulated for this purpose and a depth-first BnB algorithm with global optimality is devised to solve the problem. Numerical examples are presented to illustrate the efficacy of the transmission policies as well as the efficiency of the proposed optimization algorithm. Future works will include the study of the structural properties of the optimal solutions to further reduce computation cost and the detection algorithms for such hacking attacks.

APPENDIX A
PROOF OF LEMMA 2

From (6), we have

$$f^i(\bar{P}) = A^i \bar{P} (A^\top)^i + \sum_{j=0}^{i-1} A^j Q (A^\top)^j. \tag{57}$$

For any positive definite matrix $X \in \mathbb{R}^{n_s}$ and any positive integer i, according to Von Neumann's trace inequality, we have

$$\begin{aligned} \text{tr}\left(A^i X (A^\top)^i\right) &\le n_s \sigma_{\max}(X) \sigma_{\max}\left(A^i (A^\top)^i\right) \\ &= n_s \sigma_{\max}(X) \sigma_{\max}^2\left(A^i\right) \end{aligned} \tag{58}$$

$$\begin{aligned} \text{tr}\left(A^i X (A^\top)^i\right) &\ge \lambda_{\min}(X) \lambda_{\max}\left((A^\top)^i A^i\right) \\ &= \lambda_{\min}(X) \sigma_{\max}^2\left(A^i\right). \end{aligned} \tag{59}$$

Conduct an eigen-decomposition of matrix A such that $A = VDV^{-1}$. Matrix D is either a diagonal matrix or a Jordan Canonical form matrix. Denote the maximal dimension of the Jordan block as n_c. Note that $n_c \leq n_s$ and $n_c = 1$ if matrix A is diagonalizable.

First, according to Theorem 3.1 in [44], we have $\sigma_{\max}(A^i) \geq |\lambda_{\max}(A)|^i$. The lower bounds can be obtained from (59) by setting $c_l = \min\{\lambda_{\min}(\bar{P}), \lambda_{\min}(Q)\}$. Next, we derive the upper bound. Note that the matrix D is either a diagonal matrix or a Jordan matrix. From Theorem 3.12 in [44], we have $\sigma_{\max}(D^i) \leq n_s^2 i^{n_c} |\lambda_{\max}(A)|^i$. Since $\sigma_{\max}(A^i) \leq \sigma_{\max}(V)\sigma_{\max}(D^i)\sigma_{\max}(V^{-1})$, we have $\mathrm{tr}(A^i X (A^\top)^i) \leq n_s \sigma_{\max}(X)\sigma^2_{\max}(A^i) \leq n_s^5 \sigma^2_{\max}(V)\sigma^2_{\max}(V^{-1})\sigma_{\max}(X) i^{2n_c} |\lambda_{\max}(A)|^{2i}$. Take $c_u = n_s^5 \sigma^2_{\max}(V)\sigma^2_{\max}(V^{-1}) \max\{\sigma_{\max}(\bar{P}), \sigma_{\max}\bar{Q})\}$. The right-hand side of (21) is proved.

Appendix B
Proof of Proposition 3

The sufficient condition in (22) can be easily proved from Theorem 2 in [45]. Next, we detail the proof of the necessary condition in (23). From (18) and (19), J_u equals

$$\frac{\mathrm{tr}(f^0(\bar{P}))}{1 + \sum_{l=0}^{\infty} \prod_{i=0}^{l} (1 - \tau_i \lambda_a \lambda)} + \frac{\sum_{l=1}^{\infty} \prod_{i=0}^{l-1} (1 - \tau_i \lambda_a \lambda) \mathrm{tr}(f^l(\bar{P}))}{1 + \sum_{l=0}^{\infty} \prod_{i=0}^{l} (1 - \tau_i \lambda_a \lambda)}.$$

If J_u is bounded, each term in the equation above should be bounded. In the case $|\lambda_{\max}(A)| \geq 1$, Lemma 2 shows that $\mathrm{tr}(f^l(\bar{P}))$ increases either linearly or exponentially to infinity. To make the term $\sum_{l=1}^{\infty} \prod_{i=0}^{l-1} (1 - \tau_i \lambda) \mathrm{tr}(f^l(\bar{P}))$ bounded, $\prod_{i=0}^{l-1} (1 - \tau_i \lambda)$ must converge to 0, which proves (23).

Appendix C
Proof of Proposition 4

i) We prove the boundedness of J_e by analyzing the worst-case scenario at the adversary. Given that $|\lambda_{\max}(A)| = 1$, Proposition 3 ensures the existence of a positive integer N such that the sensor transmits with a probability greater than zero at least once between $k = mN$ and $k = (m+1)N$ for all $m \in \mathbb{N}$. To derive the upper bound of J_e, we address the worst scenario. In particular, we detail the transmission policy as for $k \in [mN, (m+1)N]$, the sensor transmits once with probability $\epsilon_t > 0$. According to this policy, the probability that all transmissions are failed at the adversary is $(1 - \lambda_e \epsilon_t)^{\lfloor k/N \rfloor}$. Meanwhile, (21) further gives that

$$\mathbb{P}(\mathrm{tr}\mathbb{E}(P_k^e) \geq c_u + c_u k^{2n_c+1}) \leq (1 - \lambda_e \epsilon_t)^{\lfloor k/N \rfloor}. \quad (60)$$

Using the tail sum formula, we have

$$\mathbb{E}\left((\mathrm{tr}\mathbb{E}(P_k^e) - c_u)/c_u \right)^{\frac{1}{(2n_c+1)}} \leq \sum_{k=0}^{\infty} (1 - \lambda_e \epsilon_t)^{\lfloor k/N \rfloor}. \quad (61)$$

Since $0 < 1 - \lambda_e \epsilon_t < 1$, $\mathbb{E}(\frac{\mathrm{tr}\mathbb{E}(P_k^e) - c_u}{c_u})$ is bounded. Thus, $\mathrm{tr}\mathbb{E}(P_k^e)$ is bounded. Denote this bound as $\bar{b}_e$. It can be easily proved that $J_e = \lim_{T \to \infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{tr}(\mathbb{E}(P_k^e)) < \bar{b}_e < \infty$.

Next, we devise a threshold-type transmission policy to show that J_e can be made arbitrarily large by increasing the threshold. Consider a threshold-type policy as

$$\mathbb{P}(\nu_{k+1} = 1 \mid \eta_k^s) = \begin{cases} 1 & \eta_k^s > \bar{t} \\ 0 & \text{else} \end{cases}. \quad (62)$$

The stationary probability of the event $\eta_k^s = i$ with $i \in [0, \bar{t}]$ equals $\frac{1}{2 + \bar{t} + \frac{1 - \lambda\lambda_a}{\lambda\lambda_a}}$ according to (18). Note that when $\lambda_e = 1$, all transmissions made by the sensor are successfully received by the adversary. This is an ideal scenario for the adversary that gives the minimum J_e upon the given transmission policy. Therefore, we can derive a lower bound of J_e according to (21) as

$$J_e \geq \frac{1}{2 + \bar{t} + \frac{1 - \lambda\lambda_a}{\lambda\lambda_a}} \sum_{i=0}^{\bar{t}} (c_l + c_l i) = \frac{(c_l + c_l \bar{t}/2)(1 + \bar{t})}{2 + \bar{t} + \frac{1 - \lambda\lambda_a}{\lambda\lambda_a}}.$$

Define $g(\bar{t}) = \frac{(c_l + c_l \bar{t}/2)(1 + \bar{t})}{2 + \bar{t} + \frac{1 - \lambda\lambda_a}{\lambda\lambda_a}}$. We may notice that $g(\bar{t})$ linearly increases with the threshold $\bar{t}$. For any given $\bar{b}$, we can select a large $\bar{t}$ such that $J_e \geq g(\bar{t}) > \bar{b}$. This shows that by increasing $\bar{t}$, we can make J_e arbitrarily large. In addition, note from (18) and (19) that to make the legitimate estimator's AEEC bounded, $\bar{t}$ should be finite, and as long as $\bar{t}$ is finite, J_e is finite according to (61).

ii) If the system is unstable, according to Theorem III.6 in [9], a threshold-type policy in the form of (62) can make J_e infinite if the threshold $\bar{t}$ satisfies that $\lambda_e < 1 - 1/(\lambda\lambda_a |\lambda_{\max}(A)|^{2(\bar{t}+1)})$. The existence of the threshold is ensured when $\lambda_e < 1$.

Appendix D
Proof of Theorem 5

The theorem is proved in three steps. First, from Lemma III.5 in [9], we can figure out that the proposed policy makes J_u bounded in the case that $\lambda > 1 - \frac{1}{|\lambda_{\max}(A)|^2}$. Second, we show that to satisfy the given stealthy constraint, the malicious policy must satisfy that

$$\tilde{\tau}_{ij} = 0, \quad i \leq \bar{t} \text{ and } \forall j \text{ with } \pi_{ij} > 0. \quad (63)$$

Here π_{ij} denotes the stationary probability of the state $s_k = (i, j)$ when the reference policy is applied and no intrusion is launched. Third, we show that any malicious policy that satisfies (63) will make J_e infinite.

We prove (63) by contradiction. Assume that there exists a malicious policy in the form of

$$\tilde{\tau}_{ij} = \begin{cases} 0 & i \leq \bar{t},\ i \neq i_0,\ j \neq j_0 \\ 1 & i = i_0,\ j = j_0 \\ 1 & i > \bar{t} \end{cases} \quad (64)$$

that can satisfy the stealthy constraint. Here $i_0 \leq \bar{t}$. i_0 and j_0 satisfy that $\pi_{i_0 j_0} > 0$. Given that $\lambda_a = 1$, we can prove $\eta_k = \eta_k^s$ from (8), (10), and (16). When the malicious policy (64) is applied, the estimator may observe $o_k = \{1, \underbrace{0, 0, \ldots, 0}_{i_0}, 1\}$. Denote observations in this form as $\tilde{o}$. The above statement is equivalent to $\mathcal{P}_1(\tilde{o}) > 0$. Note that in the case that no intrusion is launched, $N_o > \bar{t}$, and the reference policy is set as (29), the probability of the presence of $\tilde{o}$ should be zero, i.e., $\mathcal{P}_0(o_k = \tilde{o}) = 0$. According to (27), if $\mathcal{P}_1(o_k = \tilde{o}) \neq 0$,

the stealthy constraint will be violated, which contradicts the assumption. Therefore, (63) must hold. With this prerequisite, the minimal J_e will be achieved when the transmissions are made at all (i,j) with $i > \bar{t}$. Theorem III.6 in [9] has proved that J_e is unbounded in this case. Therefore, we can obtain the attainability of "perfect secrecy."

Appendix E
Proof of Proposition 6

The proposition is established in two steps. First, we prove that if $\lambda_a < 1$, then the Kullback–Leibler divergence in (28) is always well defined. We model the evolution of the pair (η_k, η_k^s) as a Markov chain. Define $s_k = (\eta_k, \eta_k^s)$. From (3), (8), (10), (15), and (16), the transition probability can be derived as

$$\mathbb{P}(s_{k+1} \mid s_k) = \begin{cases} \tau_j \lambda \lambda_a & s_{k+1} = (0,0) \\ \tau_j \lambda (1-\lambda_a) & s_{k+1} = (0, j+1) \\ 1 - \tau_j \lambda & s_{k+1} = (i+1, j+1) \end{cases} \tag{65}$$

with $s_k = (i,j)$ and $i,j \in \mathbb{N}$. Denote the stationary probability of the state $s_k = (i,j)$ as $\pi^c_{i,j}$. From (65), we have

$$\pi^c_{0,0} = \sum_{i,j \in \mathbb{N}} \pi^c_{i,j} \tau_j \lambda \lambda_a \quad \pi^c_{0,j+1} = \sum_{i \in \mathbb{N}} \pi^c_{i,j} \tau_j \lambda (1-\lambda_a)$$

$$\pi^c_{i+1,j+1} = \pi^c_{i,j}(1 - \tau_j \lambda) \tag{66}$$

which indicates that $\pi^c_{i,j} > 0$ for all $j \geq i \geq 0$. Then, we have $\mathbb{P}(\eta_k = i) = \sum_{j \in \mathbb{N}} \pi^c_{i,j} > 0$ for any $i \in \mathbb{N}$. Since $\mathbb{P}(\eta_k = i, \nu_{k+1}\gamma_{k+1} = 0) = \sum_{j=i}^{\infty} \pi^c_{i,j}(1-\tau_j\lambda)$ and $\mathbb{P}(\eta_k = i, \nu_{k+1}\gamma_{k+1} = 1) = \sum_{j=i}^{\infty} \pi^c_{i,j}\tau_j\lambda$, we have

$$\mathbb{P}(\eta_k = i, \nu_{k+1}\gamma_{k+1} = a) > 0, \quad a \in \mathbb{A}. \tag{67}$$

Note from (8) that

$$\begin{aligned} &\mathbb{P}(o_{k+1:k+N_o} = (i_1, \ldots, i_{N_o})) \\ &= \sum_{l=0}^{\infty} \mathbb{P}(\eta_k = l) \mathbb{P}(\nu_{k+1}\gamma_{k+1} = i_1 | \eta_k = l) \cdots \times \\ &\mathbb{P}\left(\nu_{k+N_o}\gamma_{k+N_o} = i_{N_o} | \eta_k = l, \nu_{k+j}\gamma_{k+j} = i_j, j \in [1, N_o)\right) \end{aligned} \tag{68}$$

with $i_1, \ldots, i_{N_o} \in \{0,1\}$. Combining (67) and (68), we have $\mathbb{P}(o_{k+1:k+N_o} = (i_1, \ldots, i_{N_o})) > 0$ for any $(i_1, \ldots, i_{N_o})$. This ensures that the Kullback–Leibler divergence is always well defined.

Based on this, we show that the stealthy constraint can be satisfied by limiting $\|\omega_s - \rho_s\|_1$. From (66), we have

$$\begin{aligned} &\mathbb{P}(\eta_k = i, \nu_{k+1}\gamma_{k+1} = 0) \\ &= \sum_{j \in \mathbb{N}} \omega_s(j,1)\lambda \left[\lambda_a \prod_{l=0}^{i} (1 - \tau_l \lambda) + (1-\lambda_a) \prod_{l=1}^{i+1} (1 - \tau_{j+l}\lambda) \right] \\ &\mathbb{P}(\eta_k = i, \nu_{k+1}\gamma_{k+1} = 1) = \sum_{j \in \mathbb{N}} \omega_s(j,1)\lambda \\ &\times \left[\lambda_a \prod_{l=0}^{i-1} (1 - \tau_l \lambda)\tau_i \lambda + (1-\lambda_a) \prod_{l=1}^{i} (1 - \tau_{j+l}\lambda)\tau_{j+i+1}\lambda \right] \end{aligned} \tag{69}$$

where $\omega_s(j,1)$ is the stationary probability of $(\eta_k^s = j, \nu_{k+1} = 1)$ and $\tau_l = \frac{\omega_s(l,1)}{\omega_s(l,0) + \omega_s(l,1)}$ for $\forall l \in \mathbb{N}$. With (69) and (68), we may note that the mapping between $\mathbb{P}(\eta_k, \nu_{k+1}\gamma_{k+1})$ and ω_s is continuously differentiable. Therefore, the mapping is locally Lipschitz continuous. Then, there exists a constant $\mathcal{L}$ such that $\|\mathbb{P}(o_k = (i_1, \ldots, i_{N_t})) - \mathbb{P}(o'_k = (i_1, \ldots, i_{N_t}))\|_1 \leq \mathcal{L}\|\omega_s - \rho_s\|_1$, where o'_k denotes the observations after the intrusion. Since $\mathbb{P}(o_k = (i_1, \ldots, i_{N_t})) > 0$, the Kullback–Leibler divergence can be made arbitrarily small by squeezing $\|\omega_s - \rho_s\|_1$, which completes the proof.

Appendix F
Proof of Proposition 7

According to the definition of ρ and ρ_t, we have

$$\begin{aligned} \rho_t(i,j,a) &= \rho(i,j,a) \quad 0 \leq i,j < N_t \\ \rho_t(i, N_t, a=1) &= \sum_{j=N_t}^{\infty} \rho(i,j,a=1), \quad 0 \leq i < N_t \\ \rho_t(N_t, j, a=1) &= \sum_{i=N_t}^{\infty} \rho(i,j,a=1), \quad 0 \leq j < N_t \\ \rho_t(N_t, N_t, a=1) &= \sum_{i=N_t}^{\infty} \sum_{j=N_t}^{\infty} \rho(i,j,a=1). \end{aligned} \tag{70}$$

Equation (31) gives that

$$\sum_{i=0}^{\infty} \sum_{a \in \mathbb{A}} \rho(i, j+1, a) = (1-\lambda_e) \sum_{i=0}^{\infty} \sum_{a \in \mathbb{A}} \rho(i,j,a), \ j \geq N_t$$

$$\sum_{i=0}^{N_t} \rho_t(i, N_t, a=1) = \sum_{i=0}^{\infty} \sum_{j=N_t}^{\infty} \sum_{a \in \mathbb{A}} \rho(i,j,a).$$

When $j \geq N_t$, it can be further derived from the above two equations that $\sum_{i=0}^{\infty} \sum_{a \in \mathbb{A}} \rho(i,j,a) = \lambda_e (1-\lambda_e)^{j-N_t} \sum_{i=0}^{N_t} \rho_t(i, N_t, a=1)$. Based on these, the expression of the AEEC at the adversary after the intrusion follows

$$\begin{aligned} \lim_{T \to \infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{tr}(\mathbb{E}(P_k^e)) &= \sum_{j=0}^{\infty} \sum_{i=0}^{\infty} \sum_{a \in \mathbb{A}} \rho(i,j,a) \mathrm{tr}(f^j(\bar{P})) \\ &= \sum_{j \in [0, N_t - 1]} \sum_{i \in [0, N_t]} \sum_{a \in \mathbb{A}} \rho_t(i,j,a) \\ &\quad \times \mathrm{tr}(f^j(\bar{P})) + \sum_{i \in [0, N_t]} \rho_t(i, N_t, a=1) \\ &\quad \times \sum_{j=0}^{\infty} \lambda_e (1-\lambda_e)^{j-N_t} \mathrm{tr} f^j(\bar{P}). \end{aligned}$$

Since $\lambda_e > 1 - \frac{1}{|\lambda_{\max}(A)|^2}$, the term $\sum_{j=0}^{\infty} \lambda_e (1-\lambda_e)^{j-N_t} \mathrm{tr} f^j(\bar{P})$ is bounded for any N_t from Lemma 2.

Appendix G
Proof of Theorem 8

We prove this theorem by devising a transmission policy in the form of

$$\tau^t_{ij} = \begin{cases} \tau_i & 0 \leq i,j < N_t \\ 1 & i \geq N_t \text{ or } j \geq N_t \end{cases} \tag{71}$$

and show that (71) is a feasible solution that can make J_e bounded and the stealthy constraint satisfied.

We may note from the comparison with (37) that (71) is a special form of (37) with $\tilde{\tau}_{ij}$ set the same as τ_i for $0 \leq i, j < N_t$. Note that τ_i is the transmission probability given by the reference policy. Following the proof of Proposition 7, it can be proved that the policy in (71) can make J_e bounded. We focus on the proof of the feasibility of the stealthy constraint.

Define a tensor $\omega_t \in \mathbb{R}^{(N_t+1)\times(N_t+1)\times 2}$ as the occupation measure of the truncated MDP when the reference policy in (15) is applied. Following the properties of occupation measure, we have

$$\omega_t \in \Omega_{N_t} \text{ and } \tau_i = \frac{\omega_t(i,j,a=1)}{\sum_{a\in\mathbb{A}} \omega_t(i,j,a)} \tag{72}$$

for all $0 \leq i, j < N_t$. Similar to (70), it can be derived that

$$\omega_t(i, N_t, a=0) = \sum_{j=N_t}^{\infty} \omega(i,j,a=0)$$

$$\omega_t(N_t, j, a=0) = \sum_{i=N_t}^{\infty} \omega(i,j,a=0) \tag{73}$$

for $0 \leq i, j \leq N_t$. For simplicity in notation, we rearrange the tensor ω_t into a vector ω_b such that

$$\omega_b\left(2(N_t+1)i + 2j + a\right) = \omega_t(i,j,a) \tag{74}$$

and rewrite the equalities in (72) and (73) as

$$M_c \omega_b = N_\omega. \tag{75}$$

Note that there are $(N_t+1)^2$ nonredundant equality constraints in Ω_{N_t}. Equations (72) and (73) provide another $(N_t+1)^2$ nonredundant equality constraints. We have $M_c \in \mathbb{R}^{2(N_t+1)^2\times 2(N_t+1)^2}$ being of full-rank and thus invertible. In addition, $N_\omega \in \mathbb{R}^{2(N_t+1)^2}$. Moreover, since ρ_t also denotes occupation measure, we have $\rho_t \in \Omega_{N_t}$. In view of the transmission policy in (71), ρ_t must satisfy that

$$\tau_i = \frac{\rho_t(i,j,a=1)}{\sum_{a\in\mathbb{A}} \rho_t(i,j,a)} \ \forall i,j < N_t \tag{76}$$

$$\rho_t(i, N_t, a=0) = 0 \quad \rho_t(N_t, j, a=0) = 0, \ i,j \leq N_t. \tag{77}$$

Define ρ_b as

$$\rho_b\left(2(N_t+1)i + 2j + a\right) = \rho_t(i,j,a). \tag{78}$$

Compare (76) and (77) with (72) and (73). We may notice that ρ_b should follow the equation $M_c\rho_b = N_\rho$, where N_ρ differs from N_ω at the elements corresponding to (77). If we can prove that $\sum_{j=N_t}^{\infty} \omega(i,j,a=0)$ and $\sum_{i=N_t}^{\infty} \omega(i,j,a=0)$ converge to 0 with N_t, then we have $\lim_{N_t\to\infty} \|N_\omega - N_\rho\|_1 = 0$. In view of the fact that M_c is invertible, we can prove that for any ϵ_s, there exists an N_t such that $\|\rho_b - \omega_b\|_1 = \|M_c^{-1}(N_\omega - N_\rho)\|_1 \leq \epsilon_s$.

Note that the convergence of $\sum_{i=N_t}^{\infty} \omega(i,j,a=0)$ can be easily obtained from (18). We focus on the proof of $\lim_{N_t\to\infty} \sum_{j=N_t}^{\infty} \omega(N_t,j,a=0) = 0$. Define the stationary distribution of the state $(\eta_k^s = i, \eta_k^e = j)$ with $i,j \in \mathbb{N}$ as $\pi_{i,j}$ before the intrusion. Since $\pi_{i,j} = \sum_{a\in\mathbb{A}} \omega(i,j,a)$, we have

$$\omega(i,j,a=0) \leq \pi_{i,j}, \ \forall i,j \in \mathbb{N}. \tag{79}$$

From (15) and (25), we have

$$\pi_{0,0} = \lambda\lambda_e \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} \tau_i \pi_{i,j}$$

$$\pi_{0,j+1} = \lambda(1-\lambda_e) \sum_{i=0}^{\infty} \tau_i \pi_{i,j}$$

$$\pi_{i+1,0} = (1-\lambda)\lambda_e \sum_{j=0}^{\infty} \tau_i \pi_{i,j}$$

$$\pi_{i+1,j+1} = [(1-\lambda)(1-\lambda_e)\tau_i + 1 - \tau_i]\pi_{i,j}. \tag{80}$$

Define $\pi_j^e = \sum_{i=0}^{\infty} \pi_{i,j}$, it can be proved from (80) that

$$\begin{aligned}\pi_{j+1}^e &= \pi_{0,j+1} + \sum_{i=0}^{\infty} \pi_{i+1,j+1} \\ &= \lambda\lambda_a(1-\lambda_e) \sum_{i=0}^{\infty} \tau_i \pi_{i,j} + \sum_{i=0}^{\infty} [(1-\lambda_a\lambda)(1-\lambda_e)\tau_i \\ &\quad + 1 - \tau_i]\pi_{i,j} \\ &= \underbrace{\sum_{i=0}^{\infty} \pi_{i,j}}_{=\pi_j^e} - \lambda_e \underbrace{\sum_{i=0}^{\infty} \tau_i \pi_{i,j}}_{=\frac{\pi_{0,j+1}}{\lambda_a\lambda(1-\lambda_e)}} = \pi_j^e - \frac{\lambda_e \pi_{0,j+1}}{\lambda\lambda_a(1-\lambda_e)}.\end{aligned} \tag{81}$$

Since $\pi_{0,j+1} \geq 0$, we have $\pi_j^e \geq \pi_{j+1}^e$. Considering that $\pi_j^e \geq 0$ and $\sum_{j=0}^{\infty} \pi_j^e = 1$, we may conclude that π_j^e is a Cauchy sequence and, thus, $\lim_{N_t\to\infty} \sum_{j=N_t}^{\infty} \pi_j^e = 0$. From (79), it can be further proved that $\lim_{N_t\to\infty} \sum_{j=N_t}^{\infty} \omega(N_t,j,a=0) \leq \lim_{N_t\to\infty} \sum_{j=N_t}^{\infty} \pi_j^e = 0$. The proof is completed. ■

APPENDIX H
PROOF OF PROPOSITION 9

First, we prove (44) assuming the convergence of $\sum_{a\in\mathbb{A}} \sum_{i=N_t}^{\infty} \omega_s(i,a)$ and $\sum_{N_t}^{\infty} \sum_{a\in\mathbb{A}} \rho_s(i,a)$. According to the definition of ρ_t and ω_s, the stealthy constraints in Problem 3 can be written as $\sum_{i=0}^{N_t-1} \|\omega_s(i,a) - \rho_s(i,a)\|_1 + \|\sum_{N_t}^{\infty} \omega_s(i,a) - \sum_{N_t}^{\infty} \rho_s(i,a)\|_1 \leq \epsilon_s$. Moreover, if $\lim_{i=N_t\to\infty} \sum_{a\in\mathbb{A}} \sum_{i=N_t}^{\infty} \omega_s(i,a) = 0$ and $\lim_{N_t\to\infty} \sum_{N_t}^{\infty} \sum_{a\in\mathbb{A}} \rho_s(i,a) = 0$, we have

$$\|\omega_s - \rho_s\|_1 \leq \underbrace{\sum_{i=0}^{N_t-1} \|\omega_s(i,a) - \rho_s(i,a)\|_1}_{\leq \epsilon_s} + \underbrace{\sum_{a\in\mathbb{A}} \sum_{N_t}^{\infty} \omega_s(i,a) + \rho_s(i,a)}_{\text{converge to 0 with } N_t} \tag{82}$$

such that (44) is proved. Next, we articulate the convergence of $\sum_{a\in\mathbb{A}} \sum_{N_t}^{\infty} \omega_s(i,a)$. For each i, from the definition of $\omega_s(i,a)$, we have $\sum_{a\in\mathbb{A}} \omega_s(i+1,a) \leq \sum_{a\in\mathbb{A}} \omega_s(i,a)$ and $0 \leq \sum_{a\in\mathbb{A}} \omega_s(i+1,a) \leq \sum_{i=0}^{\infty} \sum_{a\in\mathbb{A}} \omega_s(i,a) = 1$. Then, $\sum_{a\in\mathbb{A}} \omega_s(i,a)$ constitutes a Cauchy sequence and therefore its tail sum converges to 0. The convergence of $\sum_{i=N_t}^{\infty} \sum_{a\in\mathbb{A}} \rho_s(i,a)$ can be proved similarly.

Second, we prove (43) by devising a candidate policy τ^f in the form of

$$\tau^f_{ij} = \begin{cases} \tau^\star_{ij} & 0 \le i,j < N_t \\ 1 & i \ge N_t \text{ or } j \ge N_t \end{cases}. \tag{83}$$

We show that $J_e(\tau^f)$, which denotes the AEEC of the adversary when (83) is applied, gives that

$$|J_e(\tau^f) - J_e(\tau^\star)| \le \epsilon_a(N_t) \tag{84}$$

$$J_e(\tau^c) \le J_e(\tau^f) + \epsilon_b(N_t) \tag{85}$$

where $\lim_{N_t\to\infty} \epsilon_a(N_t) = 0$ and $\lim_{N_t\to\infty} \epsilon_b(N_t) = 0$. Set $\epsilon_g(N_t) = \epsilon_a(N_t) + \epsilon_b(N_t)$. The expression in (43) can be obtained. Note that the policy τ^f is obtained from $\tau^\star$ by setting all the values of τ_{ij} with i or j greater than N_t to 1. From Proposition 7 and Theorem 8, both τ^f and $\tau^\star$ give bounded AEECs. Then, the discrepancy between $J_e(\tau^f)$ and $J_e(\tau^\star)$ diminishes with N_t, which gives (84). Denote the value of $\sum_{i=0}^{N_t-1} \|\omega_s(i,a) - \rho_s(i,a)\|_1 + \|\sum_{N_t}^{\infty} \omega_s(i,a) - \sum_{N_t}^{\infty} \rho_s(i,a)\|_1$ as $\epsilon_u(N_t)$. From (82), we have $\lim_{N_t\to\infty} |\epsilon_u(N_t) - \epsilon_s| = 0$. Thus, the policy τ^f can be viewed as a feasible solution to Problem 2 with the stealthy tolerance ϵ_s perturbed with $|\epsilon_u(N_t) - \epsilon_s|$. Following the local sensitivity analysis in Section 5.6 of [46], we prove (85). Equations (84) and (85) together establish (43).

Appendix I
Proof of Proposition 11

We prove this proposition in three steps. First, we rearrange the constraints into linear equalities and inequalities. Second, we transform the bilevel program into a single-level nonlinear program based on the duality theorem. Third, we show that the optimum is one of the extreme points.

Define a vector $\omega_b \in \mathbb{R}^{2(N_t+1)^2}$ according to (74), such that we can express the constraints in (47) and (48) as linear equalities and inequalities in terms of ω_b, i.e.,

$$M_a\omega_b = m_a, \quad M_c\omega_b \le m_c. \tag{86}$$

Here $M_a \in \mathbb{R}^{(N_t+1)^2 \times 2(N_t+1)^2}$ and $M_c \in \mathbb{R}^{4(N_t+1)^2 \times 2(N_t+1)^2}$. Equation (49) is simplified as

$$M_b(\tau)\omega_b = m_b. \tag{87}$$

Here the coefficient matrix $M_b \in \mathbb{R}^{(N_t+1)^2}$ depends on the transmission probabilities. Moreover, $\hat{J}_u$ and $\hat{J}_e$ can be written as functions of ω_b as

$$\hat{J}_u = c_u\omega_b \quad \hat{J}_e = c_e\omega_b \tag{88}$$

where $c_u,\ c_e \in \mathbb{R}^{1\times 2(N_t+1)^2}$. Similarly, we can transform ρ_t to ρ_b according to (78). For any fixed ω_s, the lower level of Problem 5 can be simplified into a linear program as

Problem 8:

$$\min_{\rho_b,\epsilon} \quad c_e\rho_b$$

$$\text{s.t.} \quad M_1\rho_\epsilon \le m_1, \quad \rho_\epsilon = [\rho_b^\top,\ \epsilon^\top]^\top \tag{89}$$

$$M_{21}\rho_\epsilon + M_{22}\omega_b \le m_2$$

$$\epsilon = [\epsilon_{0,0},\ \epsilon_{0,1},\ \epsilon_{1,0},\ \epsilon_{1,1},\ \ldots, \epsilon_{N_t-1,0},\ \epsilon_{N_t-1,1}]^\top. \tag{90}$$

Here $M_1 \in \mathbb{R}^{6(N_t+1)^2+2(2N_t+1)\times 2(N_t+1)^2}$, $M_{21} \in \mathbb{R}^{(N_t+2)\times(2(N_t+1)^2+N_t+1)}$, and $M_{22} \in \mathbb{R}^{(N_t+2)\times 2(N_t+1)^2}$.

Next, we transform the bilevel program into a single-level nonlinear program. In particular, the dual of Problem 8 is in the form of

$$\max_{y} \quad y([\,m_1^\top\ m_2^\top\,]^\top - [\,\mathbf{0}^\top\ M_{22}^\top\,]^\top\omega_b)$$

$$\text{s.t.} \quad y\,[\,M_1^\top\ M_{21}^\top\,]^\top \ge [c_e\ \mathbf{0}]. \tag{91}$$

According to the duality theorem, the duality gap of this linear program should be zero, i.e.,

$$y([\,m_1^\top\ m_2^\top\,]^\top - [\,\mathbf{0}^\top\ M_1^\top\,]^\top\omega_b) = c_e\rho_b. \tag{92}$$

Based on this, we can replace the lower level of Problem 5 with inequalities (89), (90), and (92) such that Problem 5 is transformed into a single-level problem as

$$\min_{\omega_b,\tau,y,\rho_\epsilon} \quad J_c$$

$$\text{s.t.} \quad (86),\ (87),\ (89),\ (90),\ (92). \tag{93}$$

Equation (87), which is derived from (49), is bilinear with respect to the decision variables τ and ω_b. Equation (92) is also bilinear with respect to the decision variables y and ω_b. The objective function is linear in terms of the decision variables and the remaining constraints are convex in terms of the decision variables. Define two vectors $z_1 = [\tau^\top,\ y^\top]^\top$ and $z_2 = [\omega_b^\top,\ \rho_\epsilon^\top]^\top$. For any fixed z_2, the optimization in (93) is equivalent to minimizing a concave function. Hence, according to [47], the optimal value of z_1 must be among the extreme points of the feasible region. Since each τ_i is a component in z_1 and both $\tau_i = 0$ and $\tau_i = 1$ are attainable for all $0 \le i < N_o$, we can conclude that the optimal value of τ_i should be either 0 or 1. This property indicates that for each state i, the optimal reference policy will let the sensor either transmit or not transmit with a probability of 1. Therefore, the optimal reference policy is a deterministic policy.

Appendix J
Proof of Theorem 12

Briefly, we derive the lower bound by removing the bilinear constraints and replacing the lower level with a suboptimal solution which has a closed-form expression. We use $\star$ to mark the optimal solution of Problem 5 when $\tau_0, \ldots, \tau_l$ are fixed and $J_c^\star$ is the corresponding optimal value of Problem 5. First, we prove that $(\omega_t^\star, (1-\zeta)\omega_t^\star + \zeta\rho_t^1)$ is a feasible solution of Problem 7. For simplicity in notation, denote $(1-\zeta)\omega_t^\star + \zeta\rho_t^1$ as ρ_t^c. Compare Problem 7 with Problem 5. Problem 7 has a larger feasible region since the constraints (49) are removed for $i \in (l, N_o)$. Therefore, $\omega_t^\star$ can satisfy all the constraints and $(\omega_t^\star, \rho_t^c)$ is naturally a group of feasible solution to Problem 7. Denote $(\omega_t^\diamond, \rho_t^\diamond)$ as the optimal solution of Problem 7. According to its optimality, we have

$$J_f(\omega_t^\diamond, \rho_t^\diamond) \le J_f(\omega_t^\star, \rho_t^c). \tag{94}$$

Next, we prove that

$$J_f(\omega_t^\star, \rho_t^c) \le \alpha\left(\beta_1\hat{J}_u(\omega_t^\star) - (1-\beta_1)\hat{J}_e(\rho_t^\star)\right) - (1-\alpha)(1-\beta_2)J_e(\rho_t^\star) \tag{95}$$

by showing that ρ_t^c is feasible to the constraints in the lower level of Problem 5 when $\omega_t = \omega_t^\star$. The satisfaction of (36) and (38) can be easily checked from (47), (48), and the definition of ρ_t^1. We need to further check the satisfaction of (40)–(42). Note from the definition of ρ_t^c that $\| \sum_{j=0}^{N_t}(\rho_t^c(\cdot,j,\cdot) - \omega_t^\star(\cdot,j,\cdot))\|_1 \leq \zeta \| \sum_{j=0}^{N_t}(\omega_t^\star(\cdot,j,\cdot) - \rho_t^1(\cdot,j,\cdot))\|_1 \leq \zeta(\| \sum_{j=0}^{N_t}(\omega_t^\star(\cdot,j,\cdot) - \omega_t^1(\cdot,j,\cdot))\|_1 + \| \sum_{j=0}^{N_t}(\omega_t^1(\cdot,j,\cdot) - \rho_t^1(\cdot,j,\cdot))\|_1)$. Moreover, according to the definition of ρ_t^1, we have $\| \sum_{j=0}^{N_t}(\omega_t^1(\cdot,j,\cdot) - \rho_t^1(\cdot,j,\cdot))\|_1 = \epsilon_s$. It can be checked with the expressions of the stationary distribution given in (18) that for any ω_t satisfying the constraints in Problem 7, we have $\| \sum_{j=0}^{N_t}(\omega_t(\cdot,j,\cdot) - \omega_t^1(\cdot,j,\cdot))\|_1 \leq \| \sum_{j=0}^{N_t}(\omega_t^0(\cdot,j,\cdot) - \omega_t^1(\cdot,j,\cdot))\|_1$. Therefore, for ζ given in (52), we have $\| \sum_{j=0}^{N_t}(\rho_t^c(\cdot,j,\cdot) - \omega_t^\star(\cdot,j,\cdot))\|_1 \leq \epsilon_s$, which is equivalent to (40)–(42). Now we have proved that ρ_t^c is a feasible solution to the lower level of Problem 5. According to the optimality of $\rho_t^\star$, we have $J_e(\rho_t^c) \geq J_e(\rho_t^\star)$. Therefore, we have $J_f(\omega_t^\star, \rho_t^c) = \alpha(\beta_1 \hat{J}_u(\omega_t^\star) - (1-\beta_1)\hat{J}_e(\rho_t^c)) - (1-\alpha)(1-\beta_2)J_e^\star(\rho_t^c) \leq \alpha(\beta_1 \hat{J}_u(\omega_t^\star) - (1-\beta_1)\hat{J}_e(\rho_t^\star)) - (1-\alpha)(1-\beta_2)J_e^\star(\rho_t^\star)$, which proves (95).

Next, we prove that $J_g^\diamond \leq (1-\alpha)\beta_2 J_u^\star$. Compare Problem 6 with Problem 5. We may notice that the feasible region of Problem 5 is a subset of Problem 6. Therefore, $(\omega_t^\star, \rho_t^\star)$ should be a feasible solution of Problem 6. Then, with the optimality of $J_g^\diamond$, we have $J_g^\diamond \leq J_g(\omega_t^\star, \rho_t^\star) = (1-\alpha)\beta_2 J_u^\star$. This, together with (94) and (95), proves Theorem 12.

REFERENCES

[1] M. S. Chong, H. Sandberg, and A. M. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," in *Proc. 18th Eur. Control Conf.*, 2019, pp. 968–978.

[2] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy attack against redundant controller architecture of industrial cyber-physical system," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9783–9793, Dec. 2019.

[3] J.-M. Lee and S. Hong, "Keeping host sanity for security of the SCADA systems," *IEEE Access*, vol. 8, pp. 62 954–62968, 2020.

[4] D. Kushner, "The real story of Stuxnet," *IEEE Spectr.*, vol. 3, no. 50, pp. 48–53, Mar. 2013.

[5] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2015.

[6] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[7] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 226–231.

[8] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, 2011.

[9] 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 Trans. Autom. Control*, vol. 64, no. 9, pp. 3732–3739, Sep. 2018.

[10] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State-secrecy codes for networked linear systems," *IEEE Trans. Autom. Control*, vol. 65, no. 5, pp. 2001–2015, May 2020.

[11] L. Huang, K. Ding, A. S. Leong, D. E. Quevedo, and L. Shi, "Encryption scheduling for remote state estimation under an operation constraint," *Automatica*, vol. 127, 2021, Art. no. 109537.

[12] J. Kim and H. Shim, "Encrypted state estimation in networked control systems," in *Proc. IEEE 58th Conf. Decis. Control*, 2019, pp. 7190–7195.

[13] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun., Control, Comput.*, 2009, pp. 911–918.

[14] X. Ren, J. Yan, and Y. Mo, "Binary hypothesis testing with Byzantine sensors: Fundamental tradeoff between security and efficiency," *IEEE Trans. Signal Process.*, vol. 66, no. 6, pp. 1454–1468, Mar. 2018.

[15] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *Proc. 52nd IEEE Conf. Decis. Control*, 2013, pp. 1854–1859.

[16] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *Proc. 6th Int. Symp. Resilient Control Syst.*, 2013, pp. 54–59.

[17] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, Oct. 2015.

[18] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Trans. Ind. Inform.*, vol. 12, no. 5, pp. 1786–1794, Oct. 2016.

[19] A. S. Leong, A. Redder, D. E. Quevedo, and S. Dey, "On the use of artificial noise for secure state estimation in the presence of eavesdroppers," in *Proc. Eur. Control Conf.*, 2018, pp. 325–330.

[20] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Information bounds for state estimation in the presence of an eavesdropper," *IEEE Control Syst. Lett.*, vol. 3, no. 3, pp. 547–552, Jul. 2019.

[21] K. Ding, X. Ren, A. S. Leong, D. E. Quevedo, and L. Shi, "Remote state estimation in the presence of an active eavesdropper," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 229–244, Jan. 2021.

[22] W. Yang, D. Li, H. Zhang, Y. Tang, and W. X. Zheng, "An encoding mechanism for secrecy of remote state estimation," *Automatica*, vol. 120, 2020, Art. no. 109116.

[23] P. Cheng, Z. Yang, J. Chen, Y. Qi, and L. Shi, "An event-based stealthy attack on remote state estimation," *IEEE Trans. Autom. Control*, vol. 65, no. 10, pp. 4348–4355, Oct. 2020.

[24] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *Proc. Amer. Control Conf.*, 2015, pp. 195–200.

[25] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs," *Automatica*, vol. 82, pp. 251–260, 2017.

[26] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE Int. Symp. Inf. Theory*, 2013, pp. 2945–2949.

[27] A. S. Leong, D. E. Quevedo, and S. Dey, "A game-theoretic approach to covert communications," in *Proc. 31st Annu. IEEE Int. Symp. Personal, Indoor Mobile Radio Commun.*, 2020, pp. 1–6.

[28] A. Sinha, P. Malo, and K. Deb, "A review on bilevel optimization: From classical to evolutionary approaches and applications," *IEEE Trans. Evol. Comput.*, vol. 22, no. 2, pp. 276–295, Apr. 2018.

[29] O. Ben-Ayed and C. E. Blair, "Computational difficulties of bilevel linear programming," *Operations Res.*, vol. 38, no. 3, pp. 556–560, 1990.

[30] G. Anandalingam and D. White, "A solution method for the linear static Stackelberg problem using penalty functions," *IEEE Trans. Autom. Control*, vol. 35, no. 10, pp. 1170–1173, Oct. 1990.

[31] D. J. White and G. Anandalingam, "A penalty function approach for solving bi-level linear programs," *J. Global Optim.*, vol. 3, no. 4, pp. 397–419, 1993.

[32] T. Kailath, A. H. Sayed, and B. Hassibi, *Linear Estimation*. Englewood Cliffs, NJ, USA: Prentice Hall, 2000.

[33] J. Wu, X. Ren, D. Han, D. Shi, and L. Shi, "Finite-horizon Gaussianity-preserving event-based sensor scheduling in Kalman filter applications," *Automatica*, vol. 72, pp. 100–107, 2016.

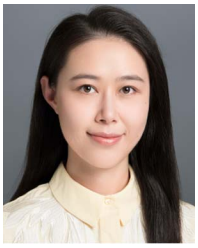
[34] L. Shi and H. Zhang, "Scheduling two Gauss–Markov systems: An optimal solution for remote state estimation under bandwidth constraint," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 2038–2042, Apr. 2012.

[35] S. Trimpe and R. D'Andrea, "Event-based state estimation with variance-based triggering," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3266–3281, Dec. 2014.

[36] Y. Li and T. Chen, "A randomized variance-based sensor scheduling for remote state estimation," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 6385–6390, 2017.

[37] K. Ding, X. Ren, D. E. Quevedo, S. Dey, and L. Shi, "DoS attacks on remote state estimation with asymmetric information," *IEEE Control Netw. Syst.*, vol. 6, no. 2, pp. 653–666, Jun. 2019.

[38] T. L. Molloy and J. J. Ford, "Minimax robust quickest change detection in systems and signals with unknown transients," *IEEE Trans. Autom. Control*, vol. 64, no. 7, pp. 2976–2982, Jul. 2019.
[39] E. S. Allman, C. Matias, and J. A. Rhodes, "Identifiability of parameters in latent structure models with many observed variables," *Ann. Statist.*, vol. 37, no. 6A, pp. 3099–3132, 2009.
[40] W. H. Press, S. A. Teukolsky, B. P. Flannery, and W. T. Vetterling, *Numerical Recipes in Fortran 77: Fortran Numerical Recipes: The Art of Scientific Computing*, vol. 1. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[41] E. Altman, *Constrained Markov Decision Processes*, vol. 7. Boca Raton, FL, USA: CRC Press, 1999.
[42] J. Lu, A. S. Leong, and D. E. Quevedo, "Optimal event-triggered transmission scheduling for privacy-preserving wireless state estimation," *Int. J. Robust Nonlinear Control*, vol. 30, no. 11, pp. 4205–4224, 2020.
[43] D. Kar *et al.*, "Trends and applications in Stackelberg security games" *Handbook of Dynamic Game Theory*, T. Basar and G. Zaccour Eds., Cham, Switzerland: Springer, 2017, doi: 10.1007/978-3-319-27335-8 27-1.
[44] D. A. Dowler, "Bounding the norm of matrix powers," Ph.D. dissertation, 2013. [Online]. Available: https://scholarsarchive.byu.edu/etd/3692
[45] L. Schenato, "Optimal estimation in networked control systems subject to random delay and packet drop," *IEEE Trans. Autom. Control*, vol. 53, no. 5, pp. 1311–1317, Jun. 2008.
[46] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[47] P. B. Zwart, "Global maximization of a convex function with linear inequality constraints," *Operations Res.*, vol. 22, no. 3, pp. 602–609, 1974.



Jingyi Lu (Member, IEEE) received the B.S. degree in automation from Zhejiang University, Hangzhou, China, in 2011, and the Ph.D. degree in chemical and biomolecular engineering from the Hong Kong University of Science and Technology, Clear Water Bay Peninsula, Hong Kong, in 2016.

She was a Research Associate with the Department of Chemical and Biological Engineering, Hong Kong University of Science and Technology from 2016 to 2019 and with the Department of Electrical Engineering, Paderborn University, Germany from 2019 to 2021, respectively. She is currently with the East China University of Science and Technology, Shanghai, China.

Daniel E. Quevedo (Fellow, IEEE) received the Ingeniero Civil Electronico and M.Sc. degrees in electronic engineering from Universidad Tecnica Federico Santa Maria, Valparaiso, Chile, in 2000, and the Ph.D. degree in electrical engineering and computer science from the University of Newcastle, Australia, in 2005.

He is currently a Professor with the School of Electrical Engineering and Robotics, Queensland University of Technology (QUT), Brisbane, QLD, Australia. He had established and led the Chair in Automatic Control, Paderborn University, Germany. His research interests include networked control systems, control of power converters, and cyberphysical systems security.

Dr. Quevedo is currently an Associate Editor for IEEE CONTROL SYSTEMS and is on the Editorial Board of the *International Journal of Robust and Nonlinear Control*. From 2015 to 2018, he was Chair of the IEEE Control Systems Society Technical Committee on Networks and Communication Systems. In 2003, he received the IEEE Conference on Decision and Control Best Student Paper Award and was also a finalist in 2002. He is a co-recipient of the 2018 IEEE TRANSACTIONS ON AUTOMATIC CONTROL George S. Axelby Outstanding Paper Award.

Vijay Gupta (Senior Member, IEEE) received the B.Tech. degree from the Indian Institute of Technology, Delhi, India, in 2001, and the M.S. and Ph.D. degrees from the California Institute of Technology, Pasadena, CA, USA, in 2002 and 2007, all in electrical engineering.

Since January 2008, he has been with the Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN, USA. His research and teaching interests include the interface of communication, control, distributed computation, and human decision-making.

Dr. Gupta has received the 2018 Antonio J. Ruberti Award from the IEEE Control Systems Society, the 2013 Donald P. Eckman Award from the American Automatic Control Council, and a 2009 National Science Foundation (NSF) CAREER Award.

Subhrakanti Dey (Senior Member, IEEE) received the Bachelor in Technology and the Master in Technology degrees from the Department of Electronics and Electrical Communication Engineering, Indian Institute of Technology, Kharagpur, India, in 1991 and 1993, respectively, and the Ph.D. degree from the Department of Systems Engineering, Research School of Information Sciences and Engineering, Australian National University, Canberra, ACT, Australia, in 1996.

He is currently a Professor with the Hamilton Institute, National University of Ireland, Maynooth, Ireland. He was a Professor with the Department of Engineering Sciences, Uppsala University, Sweden, from 2013 to 2017, Professor with the Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, Australia, from 2000 until early 2013, and a Professor of Telecommunications with the University of South Australia from 2017 to 2018. From September 1995 to September 1997, and September 1998 to February 2000, he was a Postdoctoral Research Fellow with the Department of Systems Engineering, Australian National University. From September 1997 to September 1998, he was a Postdoctoral Research Associate with the Institute for Systems Research, University of Maryland, College Park, MD, USA. His research interests include wireless communications and networks, signal processing for sensor networks, networked control systems, and molecular communication systems.

Dr. Dey is currently on the Editorial Board of IEEE CONTROL SYSTEMS LETTERS, IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, and IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He was an Associate Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING from 2007 to 2010 and 2014 to 2018, IEEE TRANSACTIONS ON AUTOMATIC CONTROL from 2004 to 2007, and *Elsevier Systems and Control Letters* from 2003 to 2013.