Data-Injection Attacks in Stochastic Control Systems: Detectability and Performance Tradeoffs

Cheng-Zong Bai\textsuperscript{a}, Fabio Pasqualetti\textsuperscript{b}, Vijay Gupta\textsuperscript{a}

\textsuperscript{a}Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN USA
\textsuperscript{b}Department of Mechanical Engineering, University of California, Riverside, CA USA

Abstract

Consider a stochastic process being controlled across a communication channel. The control signal that is transmitted across the control channel can be replaced by a malicious attacker. The controller is allowed to implement any arbitrary detection algorithm to detect if an attacker is present. This work characterizes some fundamental limitations of when such an attack can be detected, and quantifies the performance degradation that an attacker that seeks to be undetected or stealthy can introduce.

Key words: Cyberphysical system security, networked control systems, stochastic systems

1 Introduction

Using communication channels to inject malicious data that degrades the performance of a cyber-physical system has now been demonstrated both theoretically and practically Farwell & Rohozinski (2011), Kuvshinkova (2003), Mo et al. (2014), Pasqualetti et al. (2013), Richards (2008), Slay & Miller (2007). Intuitively, there is a tradeoff between the performance degradation an attacker can induce and how easy it is to detect the attack Teixeira et al. (2012). Quantifying this tradeoff is of great interest to operate and design secure cyber-physical systems (CPS).

As explained in more detail later, for noiseless systems, zero dynamics provide a fundamental notion of stealthiness of an attacker, which characterizes the ability of an attacker to stay undetected even if the controller can perform arbitrary tests on the data it receives. However, similar notions for stochastic systems have been lacking. In this work, we consider stochastic cyber-physical systems, propose a graded stealthiness notion, and characterize the performance degradation that an attacker with a given level of stealthiness can induce. The proposed notion is fundamental in the sense that we do not constraint the detection test that the controller can employ to detect the presence of an attack.

Related work Security of cyber-physical systems is a growing research area. Classic works in this area focus on the detection of sensor and actuator failures in control systems Patton et al. (1989), whereas more recent approaches consider the possibility of intentional attacks at different system layers; e.g., see Pasqualetti et al. (2015). Both simple attacks, such as jamming of communication channels Foroush & Martínez (2013), and more sophisticated attacks, such as replay and data injection attacks, have been considered Mo & Sinopoli (2010), Smith (2011).

One way to organize the literature in this area is based on the properties of the considered cyber-physical systems. While initial studies focused on static systems Dan & Sandberg (2010), Giani et al. (2011), Liu et al. (2009), Mohsenian-Rad & Leon-Garcia (2011), Teixeira et al. (2010), later works exploited the dynamics of the system either to design attacks or to improve the performance of the detector that a controller can employ to detect if an attack is present Bhattacharya & Başar (2013), Hamza et al. (2011), Maharjan et al. (2013),
Manshaei et al. (2011), Zhu & Martínez (2011), Zhu et al. (2013). For noiseless cyber-physical systems, the concept of stealthiness of an attack is closely related to the control-theoretic notion of zero dynamics (Basile & Marro 1991, Section 4). In particular, an attack is undetectable in noiseless systems if and only if it excites only the zero dynamics of an appropriately defined input-output system describing the system dynamics, the measurements available to the security monitor, and the variables compromised by the attacker Fawzi et al. (2014), Pasqualetti et al. (2013). For cyber-physical systems driven by noise, instead, the presence of process and measurements noise offers the attacker an additional possibility to tamper with sensor measurements and control inputs within acceptable uncertainty levels, thereby making the detection task more difficult.

Detectability of attacks in stochastic systems remains an open problem. Most works in this area consider detectability of attacks with respect to specific detection schemes employed by the controller, such as the classic bad data detection algorithm Cui et al. (2012), Mo & Sinopoli (2010). The trade-off between stealthiness and performance degradation induced by an attacker has also been characterized only for specific systems and detection mechanisms Kosut et al. (2011), Kwon et al. (2013), Liu et al. (2011), Mo et al. (2014), and a thorough analysis of resilience of stochastic control systems to arbitrary attacks is still missing. While convenient for analysis, the restriction to a specific class of detectors prevents the characterization of fundamental detection limitations. In our previous work Bai & Gupta (2014), we proposed the notion of $\epsilon$-marginal stealthiness to quantify the stealthiness level in an estimation problem with respect to the class of ergodic detectors. In this work, we remove the assumption of ergodicity and introduce a notion of stealthiness for stochastic control systems that is independent of the attack detection algorithm, and thus provides a fundamental measure of the stealthiness of attacks in stochastic control systems. Further, we also characterize the performance degradation that such a stealthy attack can induce.

We limit our analysis to linear, time-invariant plants with a controller based on the output of an asymptotic Kalman filter, and to injection attacks against the actuation channel only. Our choice of using controllers based on Kalman filters is not restrictive. In fact, while this is typically the case in practice, our results and analysis are valid for arbitrary control schemes. Our choice of focusing on attacks against the actuation channel only, instead, is motivated by two main reasons. First, actuation and measurements channels are equally likely to be compromised, especially in networked control systems where communication between sensors, actuators, plant, and controller takes place over wireless channels. Second, this case has received considerably less attention in the literature – perhaps due to its enhanced difficulty – where most works focus on attacks against the measurement channel only; e.g., see Fawzi et al. (2014), Teixeira et al. (2010). We remark also that our framework can be extended to the case of attacks against the measurement channel, as we show in Bai & Gupta (2014) for scalar systems and a different notion of stealthiness.

Finally, we remark that since the submission of this work, some recent literature has appeared that builds on it and uses a notion of attack detectability that is similar to what we propose in Bai & Gupta (2014), Bai et al. (2015) and in this paper. For instance, Kung et al. (2016) extends the notion of $\epsilon$-stealthiness of Bai et al. (2015) to higher order systems, and shows how the performance of the attacker may differ in the scalar and vector cases (in this paper we further extend the setup in Kung et al. (2016) by leveraging the notion of right-invertibility of a system to consider input and output matrices of arbitrary dimensions). In Zhang & Venkatasubramaniam (2016), the authors extend the setup in Bai et al. (2015) to vector and not necessarily stationary systems, but consider a finite horizon problem. In Guo et al. (2016), the degradation of remote state estimation is studied, for the case of an attacker that compromises the system measurements based on a linear strategy. Two other relevant recent works are Weerakkody et al. (2016) that uses the notion of Kullback-Liebler divergence as a causal measure of information flow to quantify the effect of attacks on the system output, while Chen et al. (2016) characterizes optimal attack strategies with respect to a linear quadratic cost that combines attackers control and undetectability goals.

Contributions The main contributions of this paper are threefold. First, we propose a notion of $\epsilon$-stealthiness to quantify detectability of attacks in stochastic cyber-physical systems. Our metric is motivated by the Chernoff-Stein Lemma in detection and information theories and is universal because it is independent of any specific detection mechanism employed by the controller. Second, we provide an information theoretic bound for the degradation of the minimum-mean-square estimation error caused by an $\epsilon$-stealthy attack as a function of the system parameters, noise statistics, and information available to the attacker. Third, we characterize optimal stealthy attacks, which achieve the maximal degradation of the estimation error covariance for a stealthy attack. For right-invertible systems (Basile & Marro 1991, Section 4.3.2), we provide a closed-form expression of optimal $\epsilon$-stealthy attacks. The case of single-input single-output systems considered in our conference paper Bai et al. (2015) is a special case of this analysis. For systems that are not right-invertible, we propose a sub-optimal $\epsilon$-stealthy attack with an analytical expression for the induced degradation of the system performance. We include a numerical study showing the effectiveness of our bounds. Our results provide a quantitative analysis of the trade-off between performance degradation that an attacker can induce versus a fundamental limit of the detectability of the attack.
Paper organization Section 2 contains the mathematical formulation of the problems considered in this paper. In Section 3, we propose a metric to quantify the stealthiness level of an attacker, and we characterize how this metric relates to the information theoretic notion of Kullback-Leibler Divergence. Section 4 contains the main results of this paper, including a characterization of the largest performance degradation caused by an $\epsilon$-stealthy attack, a closed-form expression of optimal $\epsilon$-stealthy attacks for right invertible systems, and a suboptimal class of attacks for not right-invertible systems. Section 5 presents illustrative examples and numerical results. Finally, Section 6 concludes the paper.

2 Problem Formulation

Notation: The sequence $\{x_n\}_{n=1}^j$ is denoted by $x^j$ (when clear from the context, the notation $x^j$ may also denote the corresponding vector obtained by stacking the appropriate entries in the sequence). This notation allows us to denote the probability density function of a stochastic sequence $x_i f_{x_i}$, and to define its differential entropy $h(x_i)$ as (Cover & Thomas 2006, Section 8.1)

$$h(x_i) \triangleq \int_{-\infty}^{\infty} f_{x_i}(t_i) \log f_{x_i}(t_i) dt_i.$$ 

Let $x^k_1$ and $y^k_1$ be two random sequences with probability density functions (pdf) $f_{x^k_1}$ and $f_{y^k_1}$, respectively. The Kullback-Leibler Divergence (KLD) (Cover & Thomas 2006, Section 8.5) between $x^k_1$ and $y^k_1$ is defined as

$$D(x^k_1 \| y^k_1) \triangleq \int_{-\infty}^{\infty} \log \frac{f_{x^k_1}(t_1^k)}{f_{y^k_1}(t_1^k)} f_{x^k_1}(t_1^k) dt_1.$$ 

(1)

The KLD is a non-negative quantity that gauges the dissimilarity between two probability density functions with $D(x^k_1 \| y^k_1) = 0$ if $f_{x^k_1} = f_{y^k_1}$. Also, the KLD is generally not symmetric, that is, $D(x^k_1 \| y^k_1) \neq D(y^k_1 \| x^k_1)$. A Gaussian random vector $x$ with mean $\mu_x$ and covariance matrix $\Sigma_x$ is denoted by $x \sim \mathcal{N}(\mu_x, \Sigma_x)$. We let $I$ and $O$ be the identity and zero matrices, respectively, with their dimensions clear from the context. We also let $\mathbb{S}^n_+$ and $\mathbb{S}^n_{++}$ denote the sets of $n \times n$ positive semidefinite and positive definite matrices, respectively. For a square matrix $M$, $\text{tr}(M)$ and $\text{det}(M)$ denote the trace and the determinant of $M$, respectively.

We consider the setup shown in Figure 1 with the following assumptions:

Process: The process is described by the following linear time-invariant (LTI) state-space representation:

$$x_k+1 = A x_k + B u_k + w_k,$$
$$y_k = C x_k + v_k.$$ 

(2)

where $x_k \in \mathbb{R}^{N_x}$ is the process state, $u_k \in \mathbb{R}^{N_u}$ is the control input, $y_k \in \mathbb{R}^{N_y}$ is the output measured by the sensor, and the sequences $w_k^\infty$ and $v_k^\infty$ represent process and measurement noises, respectively.

Assumption 1 The noise random processes are independent and identically distributed (i.i.d.) sequences of Gaussian random vectors with $w_k \sim \mathcal{N}(0, \Sigma_w)$, $v_k \sim \mathcal{N}(0, \Sigma_v)$, $\Sigma_w \in \mathbb{S}^{N_w}_{++}$, and $\Sigma_v \in \mathbb{S}^{N_v}_{++}$.

Assumption 2 The state-space realization $(A, B, C)$ has no invariant zeros (Basile & Marro 1991, Section 4.4). In particular, this assumption implies that the system $(A, B, C)$ is both controllable and observable.

Assumption 3 The controller uses a Kalman filter to estimate and monitor the process state. Note that the control input itself may be calculated using an arbitrary control law. The Kalman filter, which calculates the Minimum-Mean-Squared-Error (MMSE) estimate $\hat{x}_k$ of $x_k$ from the measurements $y_{1:k}^k$, is described as

$$\hat{x}_{k+1} = A \hat{x}_k + K_k (y_k - C \hat{x}_k) + B u_k,$$ 

(3)

where the Kalman gain $K_k$ and the error covariance matrix $P_{k+1} \triangleq \mathbb{E}[(\hat{x}_{k+1} - x_{k+1})(\hat{x}_{k+1} - x_{k+1})^T]$ are calculated through the recursions

$$K_k = A P_k C^T (C P_k C^T + \Sigma_w)^{-1},$$
$$P_{k+1} = A P_k A^T - A P_k C^T (C P_k C^T + \Sigma_v)^{-1} C P_k A^T + \Sigma_w,$$

with initial conditions $\hat{x}_1 = \mathbb{E}[x_1] = 0$ and $P_1 = \mathbb{E}[x_1 x_1^T]$.

Assumption 4 Given Assumption 2, $\lim_{k \to \infty} P_k = P$, where $P$ is the unique solution of a discrete-time algebraic Riccati equation. For ease of presentation, we assume that $P_1 = P$, although the results can be generalized to the general case at the expense of more involved notation. Accordingly, we drop the time index and let $K_k = K$ and $P_k = P$ at every time step $k$. Notice that this assumption also implies that the innovation sequence $z_k \triangleq y_k - C \hat{x}_k$ is an i.i.d. Gaussian process with $z_k \sim \mathcal{N}(0, \Sigma_z)$, where $\Sigma_z = CP C^T + \Sigma_v \in \mathbb{S}^{N_y}_{++}$.

Let $G(Z)$ denote the $N_u \times N_y$ matrix transfer function of the system $(A, B, C)$. We say that the system $(A, B, C)$ is...
right invertible if there exists an \( N_u \times N_y \) matrix transfer function \( G_{RI}(Z) \) such that \( G(Z)G_{RI}(Z) = I_{N_y} \).

**Attack model:** An attacker can replace the input sequence \( u_k^\infty \) with an arbitrary sequence \( \tilde{u}_k^\infty \). Thus, in the presence of an attack, the system dynamics are given by

\[
\begin{align*}
\dot{x}_{k+1} &= A\tilde{x}_k + Bu_k + w_k, \\
\hat{y}_k &= C\tilde{x}_k + v_k.
\end{align*}
\]  

Note that the sequence \( \hat{y}_1^\infty \) generated by the sensor in the presence of an attack \( \hat{u}_1^\infty \) is different from the nominal measurement sequence \( y_1^\infty \). We assume that the attacker knows the system parameters, including the matrices \( A, B, C, \Sigma_w, \) and \( \Sigma_v \). The attack input \( \tilde{u}_1^\infty \) is constructed based on the system parameters and the information pattern \( I_k \) of the attacker. We make the following assumptions on the attacker’s information pattern:

**Assumption 5** The attacker knows the control input \( u_k \); thus \( u_k \in I_k \) at all times \( k \). Additionally, the attacker does not know the noise vectors for any time.

**Assumption 6** The attacker has perfect memory; thus, \( I_k \subseteq I_{k+1} \) at all times \( k \).

**Assumption 7** The attacker has causal information; in particular, \( I_k \) is independent of \( w_k^\infty \) and \( v_{k+1}^\infty \) for all \( k \).

**Example 1 (Attack scenarios)** Attack scenarios satisfying Assumptions 5-7 include the cases when:

(i) the attacker knows the control input exactly, that is, \( I_k = \{ u_k^i \} \).

(ii) the attacker knows the control input and the state, that is, \( I_k = \{ u_k^i, x_k^i \} \).

(iii) the attacker knows the control input and delayed measurements from the sensor, that is, \( I_k = \{ u_k^i, \hat{y}_k^{i-d} \} \) for some \( d \geq 1 \).

**Stealthiness of an attacker:** The attacker is constrained in the input \( \hat{u}_1^\infty \) it replaces since it seeks to be stealthy or undetected by the controller. If the controller is aware that an attacker has replaced the correct control sequence \( u_k^\infty \) by a different sequence \( \hat{u}_k^\infty \), it can presumably switch to a safer mode of operation. Notions of stealthiness have been proposed in the literature before. As an example, for noiseless systems, Pasqualetti et al. (2013) showed that stealthiness of an attacker is equivalent to the existence of zero dynamics for the system driven by the attack. Similar to Pasqualetti et al. (2013), we seek to define the notion of stealthiness without placing any restrictions on the attacker or the controller behavior. However, we need to define a similar notion for stochastic systems when zero dynamics may not exist. To this end, we pose the problem of detecting an attacker by the controller as a (sequential) hypothesis testing problem. Specifically, the controller relies on the received measurements to decide the following binary hypothesis testing problem:

\[
H_0 : \text{No attack is in progress (the controller receives } y_1^k); \quad H_1 : \text{Attack is in progress (the controller receives } \hat{y}_1^k).
\]

For a given detector employed at the controller to select one of the two hypotheses, denote the probability of false alarm (i.e., the probability of deciding \( H_1 \) when \( H_0 \) is true) at time \( k \) by \( p_F^0 \), and the probability of correct detection (i.e., the probability of deciding \( H_1 \) when \( H_1 \) is true) at time \( k + 1 \) by \( p_D^0 \).

One may envisage that stealthiness of an attacker implies \( p_D^0 = 0 \). However, as is standard in detection theory, we need to consider both \( p_F^0 \) and \( p_D^0 \) simultaneously. For instance, a detector that always declares \( H_1 \) to be true will achieve \( p_D^0 = 1 \). However, it will not be a good detector because \( p_F^0 = 1 \). Intuitively, an attack is harder to detect if the performance of any detector is independent of the received measurements. In other words, we define an attacker to be stealthy if there exists no detector that can perform better (in the sense of simultaneously achieving higher \( p_F^0 \) and lower \( p_D^0 \)) than a detector that makes a decision by ignoring all the measurements and making a random guess to decide between the hypotheses. We formalize this intuition in the following definition.

**Definition (Stealthy attacks)** Consider the problem formulation stated in Section 2. An attack \( \hat{u}_1^\infty \) is

(i) strictly stealthy, if there exists no detector such that \( p_F^0 < p_D^0 \) for any \( k > 0 \).

(ii) \( \epsilon \)-stealthy, if, given \( \epsilon > 0 \) and for any \( 0 < \delta < 1 \), for any detector for which \( 0 < 1 - p_D^0 < \delta \) for all times \( k \), it holds that \( \limsup_{k \to \infty} -\frac{1}{k} \log p_F^k \leq \epsilon \).

Intuitively, an attack is strictly stealthy if no detector can perform better than a random guess in deciding whether an attack is in progress. Further, an attack is \( \epsilon \)-stealthy if there exists no detector such that \( 0 < 1 - p_D^0 < \delta \) for all time \( k \) and \( p_F^k \) converges to zero exponentially fast with rate greater than \( \epsilon \) as \( k \to \infty \).

**Performance metric:** The requirement to stay stealthy clearly curtails the performance degradation that an attacker can cause. The central problem that we consider is to characterize the worst performance degradation that an attacker can achieve for a specified level of stealthiness. In the presence of an attack (and if the controller is unaware of the attack), it uses the corrupted measurements \( \hat{y}_1^\infty \) in the Kalman filter. Let \( \hat{x}_1^\infty \) be the estimate of the Kalman filter (3) in the presence of the attack \( \hat{u}_1^\infty \), which is obtained from the recursion

\[
\hat{x}_{k+1} = A\hat{x}_k + K\hat{z}_k + Bu_k,
\]
where the innovation is $\hat{z}_k = y_k - C\hat{x}_k$. Note that the estimate $\hat{x}_{k+1}$ is a sub-optimal MMSE estimate of the state $x_k$ since it is obtained by assuming the nominal control input $u_k$, whereas the system is driven by the attack input $\tilde{u}_k$. Also, note that the random sequence $\tilde{z}_1^\infty$ need neither be zero mean, nor white or Gaussian.

Since the Kalman filter estimate depends on the measurement sequence received, as a performance metric, we consider the covariance of the error in the predicted measurement $\hat{y}_k$ as compared to true value $y_k$. Further, to normalize the relative impact of the degradation induced by the attacker among different components of this error vector, we weight each component of the error vector by an amount corresponding to how accurate the estimate of this component was without attacks. Thus, we consider the performance index

$$E \left[ \left( \hat{y}_k - y_k \right)^T \Sigma_{z}^{-1} \left( \hat{y}_k - y_k \right) \right] = \text{Tr}(\hat{P}_k W),$$

where $\hat{P}_k$ is the error covariance matrix in the presence of an attack, $\hat{P}_k = E[(\hat{x}_k - x_k)(\hat{x}_k - x_k)^T]$, and $W = C^T \Sigma_{z}^{-1} C$.

To obtain a metric independent of time and focus on the long term effect of the attack, we consider the limit superior of the arithmetic mean of the $\{\text{Tr}(\hat{P}_k W)\}_{k=1}^\infty$ and define $\hat{P}_W \triangleq \limsup_{k \to \infty} \frac{1}{k} \sum_{n=1}^{k} \text{Tr}(\hat{P}_n W)$. If $\{\text{Tr}(\hat{P}_k W)\}_{k=1}^\infty$ is convergent, then $\lim_{k \to \infty} \text{Tr}(\hat{P}_k W) = \hat{P}_W$, which equals the Cesàro mean of $\hat{P}_k W$.

**Problems considered in the paper:** We assume that the attacker is interested in staying stealthy or undetected for as long as possible while maximizing the error covariance $\hat{P}_W$. We consider two problems:

(i) What is a suitable metric for stealthiness of an attacker in stochastic systems where Assumption 2 holds? We consider this problem in Section 3.

(ii) For a specified level of stealthiness, what is the worst performance degradation that an attacker can achieve? We consider this problem in Section 4.

3 **Stealthiness in Stochastic systems**

Our first result provides conditions that can be used to verify if an attack is stealthy or not.

**Theorem 1 (KLD and stealthy attacks)** Consider the problem formulation in Section 2. An attack $\tilde{u}_1^\infty$ is

(i) strictly stealthy if and only if $D(\hat{y}_1^k \mid y_1^k) = 0 \forall k > 0$.

(ii) $\epsilon$-stealthy if the corresponding observation sequence $\hat{y}_1^\infty$ is ergodic and satisfies

$$\lim_{k \to \infty} \frac{1}{k} D(\hat{y}_1^k \mid y_1^k) \leq \epsilon. \quad (5)$$

**Proof.** Presented in Appendix A. \qed

The following result provides a characterization of $D(\hat{y}_1^k \mid y_1^k)$ that contains additional insight into the meaning of stealthiness of an attacker.

**Proposition 2 (KLD and differential entropy)** The quantity $D(\hat{y}_1^k \mid y_1^k)$ can be calculated as

$$\frac{1}{k} D(\hat{y}_1^k \mid y_1^k) = \frac{1}{k} \sum_{n=1}^{k} \left( I(\tilde{z}_1^{n-1} \mid \tilde{z}_n) + D(\tilde{z}_n \mid z_n) \right), \quad (6)$$

where $I(\tilde{z}_1^{n-1} \mid \tilde{z}_n)$ denotes the mutual information between $\tilde{z}_1^{n-1}$ and $\tilde{z}_n$ (Cover & Thomas 2006, Section 8.5).

**Proof.** Due to the invariance property of the Kullback-Leibler divergence Kullback (1997), we have $D(\hat{y}_1^k \mid y_1^k) = D(\tilde{z}_1^k \mid z_1^k)$, for every $k > 0$. Further, note that $z_1^\infty$ is an i.i.d. sequence of Gaussian random vectors with $z_k \sim \mathcal{N}(0, \Sigma_z)$. From (1), we obtain

$$\frac{1}{k} D(\tilde{z}_1^k \mid z_1^k) = (a) \frac{1}{k} h(\tilde{z}_1^k) - \frac{1}{k} \sum_{n=1}^{k} \mathbb{E} \left[ \log f_{z_n}(z_n) \right]$$

$$\triangleq (b) \frac{1}{k} \sum_{n=1}^{k} \left( - h(\tilde{z}_n \mid z_1^{n-1}) + h(\tilde{z}_n) - h(\tilde{z}_n) - \mathbb{E} \left[ \log f_{z_n}(z_n) \right] \right)$$

$$= \frac{1}{k} \sum_{n=1}^{k} \left( I(\tilde{z}_1^{n-1} \mid \tilde{z}_n) + D(\tilde{z}_n \mid z_n) \right),$$

where $I(\tilde{z}_1^{n-1} \mid \tilde{z}_n)$ denotes the mutual information between $\tilde{z}_1^{n-1}$ and $\tilde{z}_n$. Equality (a) holds because $z_1^\infty$ is an independent random sequence, while (b) follows by applying the chain rule of differential entropy (Cover & Thomas 2006, Theorem 8.6.2) on the term $- \frac{1}{k} h(\hat{z}_1^k)$ to obtain $\frac{1}{k} \sum_{n=1}^{k} - h(\tilde{z}_n \mid \tilde{z}_1^{n-1})$, and adding and subtracting $h(\tilde{z}_n)$.

Intuitively, the mutual information $I(\tilde{z}_1^{n-1} \mid \tilde{z}_n)$ measures how much information about $\tilde{z}_n$ can be obtained from $\tilde{z}_1^{n-1}$, that is, it characterizes the memory of the sequence $\tilde{z}_1^\infty$. Similarly, the Kullback-Leibler divergence $D(\tilde{z}_n \mid z_n)$ measures the dissimilarity between the marginal distributions of $\tilde{z}_n$ and $z_n$. Proposition 2 thus states that the stealthiness level of an ergodic attacker can be degraded in two ways: (i) if the sequence $\tilde{z}_1^\infty$...
becomes autocorrelated, and (ii) if the marginal distributions of the random variables $\tilde{z}(k)$ in the sequence $\tilde{z}_1^\infty$ deviate from $\mathcal{N}(0, \Sigma_z)$.

4 Fundamental Performance Limitations

We are interested in the maximal performance degradation $P_W$ that an $\epsilon$-stealthy attacker may induce. We begin by proving a converse statement that gives an upper bound for $P_W$ induced by an $\epsilon$-stealthy attacker in Section 4.1. In Section 4.2 we prove a tight achievability result that provides an attack that achieves the upper bound when the system $(A, B, C)$ is right-invertible. In Section 4.3 we prove a looser achievability result that gives a lower bound on the performance degradation for non right-invertible systems.

We will use a series of preliminary technical results to present the main results of the paper. The following result is immediate.

Lemma 3 Define the function $\bar{\delta} : [0, \infty) \rightarrow [1, \infty)$ as $\delta(x) = 2x + 1 + \log \delta(x)$. Then, for any $\gamma > 0$, $\delta(\gamma) = \arg \max_{x \in \mathbb{R}} x$, subject to $\frac{1}{2}x - \gamma - \frac{1}{2} \leq \frac{1}{2} \log x$.

The following result is proved in the appendix B.

Lemma 4 Consider the problem setup above. We have

$$\frac{1}{2k} \sum_{n=1}^{k} \text{tr}\left(\mathbb{E}[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}\right) \leq \frac{N_y}{2} + \frac{1}{k} D(\tilde{z}_1^k \| z_1^k) + \frac{N_y}{2} \log \left(\frac{1}{N_y k} \sum_{n=1}^{k} \text{tr}\left(\mathbb{E}[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}\right)\right).$$

(7)

Further, if the sequence $\tilde{z}_1^\infty$ is a sequence of independent and identically distributed (i.i.d.) Gaussian random variables, $\tilde{z}_k$, each with mean zero and covariance matrix $\mathbb{E}[\tilde{z}_k \tilde{z}_k^T] = \alpha \Sigma_z$, for some scalar $\alpha$, then (7) is satisfied with equality.

Combining Lemmas 3 and 4 leads to the following result.

Lemma 5 Consider the problem setup above. We have

$$\frac{1}{N_y k} \sum_{n=1}^{k} \text{tr}\left(\mathbb{E}[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}\right) \leq \tilde{\delta}\left(\frac{1}{N_y k} \text{tr}(\tilde{z}_1^k \| z_1^k)\right).$$

(8)

where $\tilde{\delta}(\cdot)$ is as defined in Lemma 3.

The following result relates the covariance of the innovation and the observation sequence.

Lemma 6 Consider the problem setup above. We have

$$CP_k C^T = \mathbb{E}[\tilde{z}_k \tilde{z}_k^T] - \Sigma_v$$

(9)

$$CP_k C^T = \mathbb{E}[\tilde{z}_k \tilde{z}_k^T] - \Sigma_v.$$  

(10)

PROOF. By definition, $z_k = y_k - C\hat{x}_k = C(x_k - \hat{x}_k) + v_k$, and similarly $\tilde{z}_k = C(\hat{x}_k - \tilde{x}_k) + v_k$. Since $(x_k - \tilde{x}_k)$ and $(\hat{x}_k - \tilde{x}_k)$ are independent of the measurement noise $v_k$ due to Assumptions 1 and 7, the result follows. □

4.1 Converse

We now present an upper bound of the weighted MSE induced by an $\epsilon$-stealthy attack.

Theorem 7 (Converse) Consider the problem setup above. For any $\epsilon$-stealthy attack $\tilde{w}_1^\infty$ generated by an information pattern $\tilde{I}_1^\infty$ that satisfies Assumptions 5-7,

$$\tilde{P}_W = \text{tr}(PW) + \tilde{\delta}\left(\frac{\epsilon}{N_y}\right) - 1 N_y,$$

(11)

where $N_y$ is the number of outputs of the system, the function $\tilde{\delta}$ is defined in Lemma 3, and $\text{tr}(PW)$ is the weighted MSE in the absence of the attacker.

PROOF. We begin by writing

$$\tilde{P}_W = \limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{n=1}^{k} \text{tr}(\tilde{P}_n C^T \Sigma_z^{-1} C)$$

$$= \limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{n=1}^{k} \text{tr}(C \tilde{P}_n C^T \Sigma_z^{-1})$$

$$= \limsup_{k \rightarrow \infty} \frac{1}{k} \sum_{n=1}^{k} \text{tr}\left((\mathbb{E}[\tilde{z}_n \tilde{z}_n^T] - \Sigma_v) \Sigma_z^{-1}\right),$$

where we have used the invariance of trace operator under cyclic permutations and the relation in (10), respectively. The right hand side has two terms. The first term can be upper bounded using Lemma 5, so that we obtain

$$\tilde{P}_W \leq \limsup_{k \rightarrow \infty} N_y \tilde{\delta}\left(\frac{1}{N_y} \text{tr}(\tilde{z}_1^k \| z_1^k)\right) - \text{tr}(\Sigma_v \Sigma_z^{-1}).$$

Since the function $\tilde{\delta}(\cdot)$ is continuous and monotonic, we can rewrite the above bound as

$$\tilde{P}_W \leq N_y \tilde{\delta}\left(\limsup_{k \rightarrow \infty} \frac{1}{N_y} \text{tr}(\tilde{z}_1^k \| z_1^k)\right) - \text{tr}(\Sigma_v \Sigma_z^{-1}).$$

Since the attack is $\epsilon$-stealthy, we use Theorem 1 to bound the Kullback-Leibler divergence $D(\tilde{z}_1^k \| z_1^k)$ to
obtain \( \hat{P}_W \leq N_y \delta \left( \frac{c}{N_y} \right) - \text{tr}(\Sigma_y \Sigma_z^{-1}) \). Finally, substituting for \( \Sigma_z \) from (9) on the right hand side and using \( W = C^T \Sigma_z^{-1} C \) completes the proof. □

**Remark 8 (Stealthiness vs induced error)** Theorem 7 provides an upper bound for the performance degradation \( P_W \) for \( \epsilon \)-stealthy attacks. Since \( \delta \left( \frac{c}{N_y} \right) \) is a monotonically increasing function of \( \epsilon \), the upper bound (11) characterizes a trade-off between the induced error and the stealthiness level of an attack.

To further understand this result, we consider two extreme cases, namely, \( \epsilon = 0 \), which implies strictly stealthiness, and \( \epsilon \to \infty \), that is, no stealthiness level.

**Corollary 9** A strictly stealthy attacker cannot induce any performance degradation. Further, for an \( \epsilon \)-stealthy attacker, the upper bound in (11) increases linearly with \( \epsilon \) as \( \epsilon \to \infty \).

**PROOF.** A strictly stealthy attacker corresponds to \( \epsilon = 0 \). Using the fact that \( \delta(0) = 1 \) in Theorem 7 yields that \( \text{tr}(\hat{P}W) \leq \text{tr}(PW) \). The second statement follows by noting that the first order derivative of the function \( \delta(x) \to 2 \) from the right as \( x \) tends to infinity. □

### 4.2 Achievability for Right Invertible Systems

We now show that the bound presented in Theorem 7 is achievable if the system \( (A, B, C) \) is right invertible. We begin with the following preliminary result.

**Lemma 10** Let the system \( (A, B, C) \) be right invertible. Then, the system \( (A - KC, B, C) \) is also right invertible.

Let \( G_{RL}^* \) be the right inverse of the system \( (A - KC, B, C) \). We consider the following attack.

**Attack \( A_1 \):** The attack sequence is generated in three steps. In the first step, a sequence \( \zeta_k^\infty \) is generated, such that each vector \( \zeta_k \) is independent and identically distributed and independent of the information pattern \( I_k \) of the attacker, with probability density function \( \zeta_k \sim \mathcal{N}(0, (\delta(\frac{c}{N_y}) - 1) \Sigma_z) \). In the second step, the sequence \( \phi_k^\infty \) is generated as the output of the system \( G_{RL}^* \) with \( \zeta_k^\infty \) as the input sequence. Finally, the attack sequence \( \alpha_k^\infty \) is generated as \( \alpha_k = u_k + \phi_k \).

**Remark 11 (Information pattern of attack \( A_1 \))** The attack \( A_1 \) can be generated by an attacker with any information pattern satisfying Assumptions 5–7.

We note the following property of the attack \( A_1 \).

**Lemma 12** Consider the attack \( A_1 \). With this attack, the innovation sequence \( \tilde{z}_k^\infty \) is as calculated at the controller, is a sequence of independent and identically distributed Gaussian random vectors with mean zero and covariance matrix \( E[\tilde{z}_k \tilde{z}_k^T] = \delta \left( \frac{c}{N_y} \right) \Sigma_z \).

**PROOF.** Consider an auxiliary Kalman filter that is implemented as the recursion

\[
\tilde{x}_{k+1}^a = A\tilde{x}_k^a + K\tilde{z}_k + B\tilde{u}_k, \tag{12}
\]

with the initial condition \( \tilde{x}_0^a = 0 \) and the innovation \( \tilde{z}_k^a = y_k - C\tilde{x}_k^a \). The innovation sequence is independent and identically distributed with each \( \tilde{z}_k^a \sim \mathcal{N}(0, \Sigma_z) \).

Now, we express \( \tilde{z}_k = z_k^a - C\tilde{e}_k \), where \( \tilde{e}_k \equiv \tilde{x}_k - \tilde{x}_k^a \). Further, \( \tilde{e}_k \) evolves according to the recursion

\[
\tilde{e}_{k+1} = (A\tilde{x}_k + K\tilde{z}_k + B\tilde{u}_k) - (A\tilde{x}_k^a + K\tilde{z}_k^a + B\tilde{u}_k) = (A - KC)\tilde{e}_k - B\phi_k, \tag{13}
\]

with the initial condition \( \tilde{e}_0 = 0 \). Together, \( \tilde{z}_k \) and (13) define a system of the form

\[
\tilde{e}_{k+1} = (A - KC)\tilde{e}_k + B(-\phi) \tag{14}
\]

We now note that (i) the above system is \( (A - KC, B, C) \), (ii) \( \phi_k^\infty \) is the output of the right inverse system of \( (A - KC, B, C) \) with input \( \zeta_k^\infty \), and (iii) the system in equation (14) is linear. These three facts together imply that the output of (14), i.e., \( \{z_k^a - \tilde{z}_k\}_{k=1}^\infty \) is a sequence of independent and identically distributed random variables with each random variable distributed as \( \mathcal{N}(0, (\delta(\frac{c}{N_y}) - 1) \Sigma_z) \). Now since \( z_k^a \) is independent of \( e_k^a \), we obtain that \( z_k^\infty \) is an independent and identically distributed sequence with each random variable \( z_k \) as Gaussian with mean zero and covariance matrix

\[
E[\tilde{z}_k \tilde{z}_k^T ] = \delta \left( \frac{c}{N_y} \right) - 1 \Sigma_z = \delta \left( \frac{c}{N_y} \right) \Sigma_z. \tag{15}
\]

**Theorem 13 (Achievability for right invertible systems)** Suppose that the LTI system \( (A, B, C) \) is right invertible. The attack \( A_1 \) is \( \epsilon \)-stealthy and achieves

\[
\hat{P}_W = \text{tr}(PW) + N_y \left( \delta \left( \frac{c}{N_y} \right) - 1 \right),
\]

where \( W = C^T \Sigma_z^{-1} C \).

**PROOF.** For the attack \( A_1 \), Lemma 12 states that \( z_k^\infty \) is a sequence of independent and identically distributed (i.i.d.) Gaussian random variables \( z_k \) each with mean zero and covariance matrix \( E[\tilde{z}_k \tilde{z}_k^T] = \alpha \Sigma_z \), with \( \alpha = \delta \left( \frac{c}{N_y} \right) \). Lemma 4, thus, implies that (7) holds with
equality. Further, following the proof of Theorem 7, if (7) holds with equality, then (11) also holds with equality. Thus, the attack $A_1$ achieves the converse in terms of performance degradation.

Next we show that the attack is $\epsilon$-stealthy. Once again, from Lemma 4 and the expression for the covariance matrix of $\tilde{z}_k$, we have for every $k > 0$,

$$
\frac{1}{k} D(\tilde{z}_k \parallel \tilde{z}_1) = \frac{1}{2k} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T \Sigma_z^{-1}]) - \frac{N_y}{2} \log \left( \frac{1}{N_y} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T \Sigma_z^{-1}]) \right)
$$

$$
= \frac{1}{2k} \sum_{n=1}^{k} \text{tr}(\delta(\frac{\epsilon}{N_y}) \Sigma_z \Sigma_z^{-1}) - \frac{N_y}{2} \log \left( \frac{1}{N_y} \sum_{n=1}^{k} \delta(\frac{\epsilon}{N_y}) \Sigma_z \Sigma_z^{-1} \right)
$$

$$
= \frac{N_y}{2} \delta(\frac{\epsilon}{N_y}) - \frac{N_y}{2} \log \delta(\frac{\epsilon}{N_y}) = \epsilon.
$$

Now with this attack, $\tilde{z}_k^w$ is an independent and identically distributed sequence and the measurement sequence $\tilde{y}_k^w$ is ergodic. Thus, from Theorem 1, the attack $A_1$ is $\epsilon$-stealthy. □

**Remark 14 (Attacker information pattern)** Intuitively, we may expect that the more information about the state variables that an attacker has, larger the performance degradation it can induce. However, Theorem 7 and Theorem 13 imply that the only critical piece of information for the attacker to launch an optimal attack is the nominal control input $u_1^w$.

### 4.3 Achievability if System is not Right Invertible

If the system is not right invertible, the converse result in Theorem 7 may not be achieved. We now construct a heuristic attack $A_2$ that allows us to derive a lower bound for the performance degradation $P_w$ induced by $\epsilon$-stealthy attacks against such systems.

**Attack $A_2$:** The attack sequence is generated as $\tilde{u}_k = u_k + L \tilde{e}_k - \tilde{\zeta}_k$, where $\tilde{e}_k = \hat{e}_k - \hat{x}_k^w$ as in (14), and the sequence $\tilde{\zeta}_k^w$ is generated such that each vector $\tilde{\zeta}_k$ is independent and identically distributed with probability density function $\tilde{\zeta}_k \sim N(0, \Sigma_\zeta)$ and independent of the information pattern $I_k$ of the attacker. The feedback matrix $L$ and the covariance matrix $\Sigma_\zeta$ are determined in three steps, which are detailed next.

**Step 1 (Limiting the memory of the innovation sequence $\tilde{z}_k^w$):** Notice that, with the attack $A_2$ and the notation in (12), the dynamics of $\tilde{e}_k$ and $\tilde{\zeta}_k$ are given by

$$
\tilde{e}_{k+1} = (A - KC - BL)\tilde{e}_k + B \tilde{\zeta}_k
$$

$$
\tilde{\zeta}_k = C \tilde{e}_k + z_k^w.
$$

The feedback matrix $L$ should be selected to eliminate the memory of the innovation sequence computed at the controller. One way to achieve this aim is to set $A - KC - BL = 0$. In other words, if $A - KC - BL = 0$, then $\tilde{z}_k^w$ is independent and identically distributed. It may not be possible to select $L$ to achieve this aim exactly. Thus, we propose the following heuristic. Note that if $A - KC - BL = 0$, then the cost function $\lim_{k \to \infty} \frac{1}{k} \sum_{n=1}^{k} \text{tr}(E[\tilde{e}_n \tilde{e}_n^T]W)$, is minimized, with $W = C^T \Sigma_{\zeta}^{-1} C$. Since $\sum_{n=1}^{k} \text{tr}(E[\tilde{e}_n \tilde{e}_n^T]W) = E \left[ \sum_{n=1}^{k} \tilde{e}_n^T W \tilde{e}_n \right]$, selecting $L$ to satisfy the constraint $A - KC - BL = 0$ is equivalent to selecting $L$ to solve a cheap Linear Quadratic Gaussian (LQG) problem (Hesthammer 2009, Section VI). Thus, heuristically, we select the attack matrix $L$ as the solution to this cheap LQG problem and, specifically, as

$$
L = \lim_{\eta \to 0} (B^T T_\eta B + \eta I)^{-1} B^T T_\eta (A - KC),
$$

where $T_\eta$ is the solution to the discrete algebraic Riccati equation

$$
T_\eta = (A - KC)^T (T_\eta - T_\eta B (B^T T_\eta B + \eta I)^{-1} B^T T_\eta) (A - KC) + W.
$$

**Step 2 (Selection of the covariance matrix $\Sigma_\zeta$):** Notice that the selection of the feedback matrix $L$ in Step 1 is independent of the covariance matrix $\Sigma_\zeta$. As the second step, we select the covariance matrix $\Sigma_\zeta$ such that $C \Sigma_\zeta C^T$ is close to a scalar multiplication of $\Sigma_z$, say $\alpha^2 \Sigma_z$. From (15), notice that $\lim_{k \to \infty} E[\tilde{z}_k \tilde{z}_k^T] = C \Sigma_z C^T + \Sigma_{\zeta}$, where $\Sigma_{\zeta} \in S_{+}^n$ is the positive semi-definite solution to the equation

$$
\Sigma_{\zeta} = (A - KC - BL) \Sigma_{\zeta} (A - KC - BL)^T + B \Sigma_{\zeta} B^T.
$$

We derive an expression for $\Sigma_\zeta$ from (17) by using the pseudoinverse matrices of $B$ and $C$, i.e.,

$$
\Sigma_\zeta = \alpha^2 B^T \left( C^T \Sigma_z (C^T)^T \right)^+ - (A - KC - BL) C^T \Sigma_z (C^T)^+ (A - KC - BL)^T (B^T)^+, \tag{18}
$$

where $^+$ denotes the pseudoinverse operation. It should be noted that the right-hand side of (18) may not be positive semidefinite. Many choices are possible to construct a positive semi-definite $\Sigma_\zeta$. We propose that if the right-hand side is indefinite, we set its negative eigenvalues to zero without altering its eigenvectors.
Step 3 (Enforcing the stealthiness level): The covariance matrix $\Sigma_\zeta$ obtained in Step 2 depends on the parameter $\alpha$. We now select $\alpha$ so as to make the attack $A_2$ $\epsilon$-stealthy. To this aim, we first compute an explicit expression for the stealthiness level and the error induced by $A_2$. For the entropy rate of $\hat{z}_{1}^\infty$, since $\hat{z}_{1}^\infty$ is Gaussian, we obtain

$$\lim_{k \to \infty} \frac{1}{k} h(\hat{z}_{1}^k) = \lim_{k \to \infty} h(\hat{z}_{k+1} | \hat{z}_{1}^k) = \frac{1}{2} \log \left( 2 \pi e^{N_y} \det \left( (\hat{z}_{k+1} - g_k(\hat{z}_{1}^k))^T \right) \right)$$

where $g_k(\hat{z}_{1}^k)$ is the minimum mean square estimate of $\hat{z}_{k+1}$ from $\hat{z}_{1}^k$, which can be obtained from Kalman filtering, and $S \in \mathbb{S}_+^{N_y}$ is the positive semidefinite solution to the following discrete algebraic Riccati equation

$$S = (A - KC - BL)(S - SC^T(CSC^T + \Sigma_z)^{-1}CS)\times (A - KC - BL)^T + BS\Sigma_z B^T + \Sigma_z.$$  \hspace{1cm} \text{(22)}

Note that the equality (19) is due to (Cover & Thomas 2006, Theorem 4.2.1); (20) is a consequence of the maximum differential entropy lemma (Gamal & Kim 2011, Section 2.2); the positive semidefinite matrix $S$ that solves (22) represents the steady-state error covariance matrix of the Kalman filter that estimates $\hat{z}_{k+1}$ from $\hat{z}_{1}^k$. Thus, the level of stealthiness for the attack $A_2$ is

$$\lim_{k \to \infty} \frac{1}{k} D(\hat{z}_{1}^k || \hat{z}_{1}^k) = \epsilon = -\frac{1}{2} \log \left( 2 \pi e^{N_y} \det(CSC^T + \Sigma_z) \right) + \frac{1}{2} \log \left( \left( 2 \pi e^{N_y} \det(\Sigma_z) \right) + \frac{1}{2} \text{tr}\left( (C\Sigma_z C^T + \Sigma_z)^{-1} \right) \right) - \frac{1}{2} \log \text{det}(I + SW) + \frac{1}{2} \text{tr}(\Sigma_z W) + \frac{1}{2} N_y,$$ \hspace{1cm} \text{(23)}

where $W = C^T \Sigma_z^{-1} C$. To conclude our design of the attack $A_2$, we use (23) to solve for the desired value of $\alpha$, and compute the error induced by $A_2$ as

$$\hat{P}_W = \lim_{k \to \infty} \frac{1}{k} \sum_{n=1}^{k} \text{tr}(E[\hat{z}_{n} \hat{z}_{n}^T | \hat{z}_{1}^k]) - \text{tr}(\Sigma_w \Sigma_z^{-1}) \hspace{1cm} \text{(24)}$$

where $\Sigma_w$ is the solution to the Lyapunov equation (17).

5 Numerical Results

Example 1 Consider a right invertible system $(A, B, C)$

$$A = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 10 \\ 0 \\ 10 \\ 02 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 \end{bmatrix}^T.$$

and let $\Sigma_w = 0.5I$ and $\Sigma_v = I$. Figure 2 plots the upper bound (11) of performance degradation achievable for an attacker versus the attacker’s stealthiness level $\epsilon$. From Theorem 13, the upper bound can be achieved by a suitably designed $\epsilon$-stealthy attack. Thus, Fig. 2 represents a fundamental limitation for the performance degradation that can be induced by any $\epsilon$-stealthy attack. Observe that plot is approximately linear as $\epsilon$ becomes large, as predicted by Corollary 9.

Example 2 Consider the system $(A, B, C)$

$$A = \begin{bmatrix} 2 & -1 & 0 & 0 & 0 \\ 1 & -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -10 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 01 \\ 10 \end{bmatrix}, \quad C = \begin{bmatrix} 20 \\ 01 \\ 11 \end{bmatrix}.$$
6 Conclusion

This work characterizes fundamental limitations and achievability results for performance degradation induced by an attacker in a stochastic control system. The attacker is assumed to know the system parameters and noise statistics, and is able to hijack and replace the nominal control input. We propose a notion of ε-stealthiness to quantify the difficulty of detecting an attack from the measurements, and we characterize the largest degradation of Kalman filtering induced by an ε-stealthy attack. For right invertible systems, our study reveals that the nominal control input is the only critical piece of information to induce the largest performance degradation. For systems that are not right invertible, we provide an achievability result that lower bounds the performance degradation that an optimal ε-stealthy attack can achieve.

A Proof of Theorem 1

The first statement follows directly from the Neyman-Pearson Lemma Poor (1998).

For the second statement, we apply the Chernoff-Stein Lemma for ergodic measurements (see Polyanyskij & Wu (2012–2013)) that states that for any given attack sequence \( \tilde{u}_k \), for a given \( 0 < 1 - p_k^D \leq \delta \) where \( 0 < \delta < 1 \), the best achievable decay exponent of \( p_k^D \) is given by \( \lim_{k \to \infty} \frac{1}{k} D(\hat{y}_k^i \| y_k^i) \). For this attack sequence and with any detector, we obtain

\[
\limsup_{k \to \infty} -\frac{1}{k} \log p_k^D \leq \lim_{k \to \infty} \frac{1}{k} D(\hat{y}_k^i \| y_k^i) \leq \epsilon.
\]

Thus, by Definition 1, the attack is ε-stealthy.

Finally, the proof for the third statement follows by contradiction. Assume that (5) does not hold and there exists an ε-stealthy attack \( \tilde{u}_k \) such that \( \limsup_{k \to \infty} \frac{1}{k} D(\hat{y}_k^i \| y_k^i) > \epsilon \). Suppose that the detector employs the standard log-likelihood ratio test with threshold \( \lambda_k \) at every time \( k + 1 \). Thus, the test is \( L_k(\eta_k^i) \leq \lambda_k \), where \( L_k(\eta_k^i) = \log \frac{f_k(\eta_k^i)}{f_k(\eta_k^i)} \) is the log-likelihood ratio and \( \eta_k^i = y_k^i \) (resp. \( \eta_k^i = \tilde{y}_k^i \)) if \( H_0 \) (resp. \( H_1 \)) is true. Define the conditional cumulant generating function for the log-likelihood ratio to be \( g_{k|0}(s) = \log \mathbb{E}[e^{sL_k} | H_0] \) and \( g_{k|1}(s) = \log \mathbb{E}[e^{sL_k} | H_1] \). Note that \( g_{k|0}(s) = g_{k|1}(s - 1) \). Let \( \lambda_k \) be chosen to ensure that \( 0 < 1 - p_k^D \leq \delta \) for every \( k > 0 \) (notice that such \( \lambda_k \) always exists, because \( p_k^D \) increases to one as \( \lambda_k \) decreases to zero). Then, for any \( s_k > 0 \), Chernoff’s inequality yields

\[
\begin{align*}
p_k^D = \mathbb{P}[L_k \geq \lambda_k | H_0] &\leq e^{-s_k \lambda_k + g_{k|0}(s_k)} \\
&\Rightarrow -\log p_k^D \geq s_k \lambda_k - g_{k|0}(s_k) \\
&\geq s_k \lambda_k - g_{k|1}(s_k - 1) \\
&= s_k \lambda_k - \log \mathbb{E}[e^{(s_k - 1)L_k} | H_1].
\end{align*}
\]

Now, by applying Jensen’s inequality twice we obtain

\[
-\log p_k^D \geq s_k \lambda_k + \log \mathbb{E}[e^{-(s_k - 1)L_k} | H_1] \\
\geq s_k \lambda_k + \log \mathbb{E}[-(s_k - 1)L_k | H_1].
\]

Finally, using \( \mathbb{E}[L_k | H_1] = D(\hat{y}_k^i \| y_k^i) \) implies

\[
-\log p_k^D \geq D(\hat{y}_k^i \| y_k^i) + s_k \left( \lambda_k - D(\hat{y}_k^i \| y_k^i) \right).
\]

(A.1)

Now, for any time index \( k \) such that \( \frac{1}{k} D(\hat{y}_k^i \| y_k^i) > \epsilon \), let

\[
s_k = \frac{D(\hat{y}_k^i \| y_k^i) - \lambda_k}{2(D(\hat{y}_k^i \| y_k^i) - \lambda_k)}.
\]

(A.2)

Using (A.1), (A.2) and \( \lim sup_{k \to \infty} \frac{1}{k} D(\hat{y}_k^i \| y_k^i) > \epsilon \), we obtain \( \lim sup_{k \to \infty} -\frac{1}{k} \log p_k^D > \epsilon \), which contradicts the definition of ε-stealthiness. Hence, the attack cannot be stealthy, and the condition stated in (5) must be true.

B Proof of Lemma 4

By definition, we can write Kullback-Leibler divergence

\[
D(z_k^i \| \tilde{z}_k^i) = \int_{-\infty}^{\infty} f_{z_k^i} (t_k^i) \log f_{z_k^i} (t_k^i) dt_k^i - \int_{-\infty}^{\infty} f_{\tilde{z}_k^i} (t_k^i) \log f_{\tilde{z}_k^i} (t_k^i) dt_k^i
\]

Now, \( z_k^i \) is the innovation sequence without any attack and is thus an independent and identically distributed...
sequence of Gaussian random variables with mean 0 and covariance $\Sigma_z$. Plugging into the above equation yields

$$D(\tilde{z}^k \mid z^k) = -h(\tilde{z}^k) + \frac{k}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{2} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}),$$

which we can rewrite as

$$\frac{1}{2k} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}) = \frac{1}{k} D(\tilde{z}_1 \mid z_1) - \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{k} h(\tilde{z}_1). \quad \text{(B.1)}$$

We can upper-bound the right hand side by first using the sub-additivity property of differential entropy (Cover & Thomas 2006, Corollary 8.6.1), and then further bounding the entropy $h(\tilde{z}_n)$ using the maximum differential entropy lemma (Gamal & Kim 2011, Section 2.2) for multivariate random variables. Thus, we obtain

$$\frac{1}{2k} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}) \leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) - \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{k} \sum_{n=1}^{k} h(\tilde{z}_n)$$

$$\leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) - \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{k} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi e)^{N_y} \det(E[\tilde{z}_n \tilde{z}_n^T])\right).$$

with equality if the sequence $\tilde{z}_n$ is an independent sequence of random variables with each random variable $\tilde{z}_n$ as Gaussian distributed with mean zero for all $n$. Straight-forward algebraic manipulation yields

$$\frac{1}{2k} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}) \leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) - \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{k} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi e)^{N_y} \det(E[\tilde{z}_n \tilde{z}_n^T])\right)$$

$$\leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) - \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) + \frac{1}{k} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi e)^{N_y} \det(E[\tilde{z}_n \tilde{z}_n^T])\right) + \frac{1}{k} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right) \leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) + \frac{N_y}{2} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi)^{N_y} \det(E[\tilde{z}_n \tilde{z}_n^T])\right)$$

$$= \frac{1}{k} D(\tilde{z}_1 \mid z_1) + \frac{N_y}{2} \sum_{n=1}^{k} \frac{1}{2} \log \left((2\pi)^{N_y} \det(\Sigma_z)\right)(\det(\Sigma_z)^{-1}).$$

We can further bound

$$\det(E[\tilde{z}_n \tilde{z}_n^T])((\det(\Sigma_z))^{-1} \leq \left(\frac{1}{N_y} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1})\right)^{N_y}$$

$$\Rightarrow \frac{1}{2k} \sum_{n=1}^{k} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1}) \leq \frac{1}{k} D(\tilde{z}_1 \mid z_1) + \frac{N_y}{2} \sum_{n=1}^{k} \log \left((\frac{1}{N_y} \text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1})\right),$$

with equality if the matrix $E[\tilde{z}_n \tilde{z}_n^T]$ is a scalar multiplication of $\Sigma_z$ for all $n$. Finally, using the Arithmetic Mean and Geometric Mean (AM-GM) inequality yields the desired result (7). For the AM-GM inequality to hold with equality we need that $\text{tr}(E[\tilde{z}_n \tilde{z}_n^T] \Sigma_z^{-1})$ is constant for every $n$. Collecting all the above conditions for equality at various steps, (7) holds with equality if $E[\tilde{z}_k \tilde{z}_k^T] = \alpha \Sigma_z$ for some scalar $\alpha$.

References


Dan, G. & Sandberg, H. (2010), Stealth attacks and protection schemes for state estimators in power systems, in ‘IEEE Int. Conf. on Smart Grid Communications’, Gaithersburg, MD, USA, pp. 214–219.


adversarial attacks’, *IEEE Transactions on Automatic Control* 59(6), 1454–1467.


Richards, G. (2008), ‘Hackers vs slackers’, *Engineering & Technology* 3(19), 40–43.


