UNIVERSITY OF CALIFORNIA SAN DIEGO

Communication and security in cyber-physical systems

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Electrical Engineering
(Intelligent Systems, Robotics, and Control)

by

Mohammad Javad Khojasteh

Committee in charge:

Professor Massimo Franceschetti, Chair
Professor Jorge Cortés
Professor Tara Javidi
Professor Sonia Martínez
Professor Alon Orlitsky

2019

The dissertation of Mohammad Javad Khojasteh is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____

_____

_____

Chair

University of California San Diego

2019

DEDICATION

To Sogoli

EPIGRAPH

Dr. Ford: You think it's sabotage? Imagine someone's been diddling with our creations?

Bernard: It's the simplest solution.

Dr. Ford: Ah, Mr. Occam's razor. The problem, Bernard, is that what you and I do is so complicated. We practice witchcraft. We speak the right words. Then we create life itself out of chaos. William of Occam was a 13th century monk. He can't help us now, Bernard. He would have us burned at the stake.

Westworld, Chestnut

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my inspiring advisor, Prof. Massimo Franceschetti, who always listened to me carefully and provided his priceless feedback about my research and many other things. Massimo was the one who instilled in me the appreciation for mathematical rigor. He taught me how to be the most severe critic of my work and present exciting results in the most attainable fashion.

I am thankful to Prof. Jorge Cortés, who has always made time for me in his busy schedule. Jorge's hard work and interest in research has always been a source of inspiration for me.

I am grateful to Prof. Tara Javidi for her unwavering confidence in my capabilities to conduct fundamental research. Tara helped by showing me amusing research directions and always encouraging me to integrate multi-disciplinary ideas.

I would like to acknowledge Prof. Alon Orlitsky and Prof. Sonia Martínez for their willingness to serve on my thesis committee, and for their insightful and honest feedback. I would also like to thank Alon for his outstanding teaching skills and Sonia for allowing me to participate in her joint weekly group meetings with Jorge.

I met Prof. Nikolay A. Atanasov when I was almost graduating, but our ongoing collaboration is beneficial and joyful for me. I am grateful to Nikolay because he taught me how to apply machine learning in robotics and control.

I would like to thank my lovely wife, Sogoli Sadraeinouri, to whom I have dedicated this dissertation, for her unconditional love, support, and understanding.

I want to thank my father, mother, sister, and brother for their endless love. I did not see them in person for more than four years to write this dissertation, but they always supported and encouraged me to do more. I would also like to thank my caring parents-in-law for their encouragement.

I am thankful to my awesome friend Mojtaba Hedayatpour for always being there for me. I would also like to thank Amir Valibeygi, Moein Falahatgar, Arman Fazeli, Shubhanshu Shekhar,

Hamed Omidvar, and Vinnu Bhardwaj for their friendship and support.

Chapter 2, in part, is a reprint of the material as it appears in M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "The value of timing information in event-triggered control," *IEEE Transactions on Automatic Control*, in press, and M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "Time-triggering versus event-triggering control over communication channels," In *Proc. IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017. The dissertation author was the primary investigator and author of these papers.

Chapter 3, in part, is a reprint of the material as it appears in M. J. Khojasteh, M. Hedayatpour, J. Cortés, M. Franceschetti, "Event-triggered stabilization over digital channels of linear systems with disturbances," submitted for publication in *Automatica*, and M. J. Khojasteh, M. Hedayatpour, M. Franceschetti, "Theory and implementation of event-triggered stabilization over digital channels," In *Proc. IEEE 58th Annual Conference on Decision and Control (CDC)*, 2019. The dissertation author was the primary investigator and author of these papers.

Chapter 4, in full, is a reprint of the material in M. J. Khojasteh, M. Franceschetti, G. Ranade, "Stabilizing a linear system using phone calls: when time is information," being prepared for publication. The dissertation author was the primary investigator and author of this paper.

Chapter 5, in part, is a reprint of the material in M. J. Khojasteh, A. Khina, M. Franceschetti, T. Javidi, "Learning-based attacks in cyber-physical systems," being prepared for publication. The dissertation author was the primary investigator and author of this paper. The last part of this chapter, in part, is a reprint of the material in A. Rangi, M. J. Khojasteh, M. Franceschetti, "Learning-based attacks in cyber-physical systems: exploration vs. exploitation," being prepared for publication. The dissertation author was the co-primary investigator and co-author of this paper.

VITA

2015	B.Sc. in Electrical Engineering, Sharif University of Technology.
2015	B.Sc. in Mathematics, Sharif University of Technology.
2017	M.Sc. in Electrical Engineering, University of California, San Diego.
2019	Ph.D. in Electrical Engineering (Intelligent Systems, Robotics, and Control), University of California, San Diego.

PUBLICATIONS

M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "The value of timing information in event-triggered control," *IEEE Transactions on Automatic Control*, 2019, in press.

M. J. Khojasteh, M. Hedayatpour, J. Cortés, M. Franceschetti, "Event-triggered stabilization over digital channels of linear systems with disturbances," arXiv:1805.01969, 2018, submitted for publication in *Automatica*.

M. J. Khojasteh, M. Franceschetti, G. Ranade, "Stabilizing a linear system using phone calls: when time is information" arXiv:1804.00351, 2018, being prepared for publication.

M. J. Khojasteh, A. Khina, M. Franceschetti, T. Javidi, "Learning-based attacks in cyber-physical systems," arXiv:1809.06023, 2018, being prepared for publication.

M. J. Khojasteh, M. Hedayatpour, M. Franceschetti, "Theory and implementation of event-triggered stabilization over digital channels," In *Proc. IEEE 58th Annual Conference on Decision and Control (CDC)*, 2019.

M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "Time-triggering versus event-triggering control over communication channels," In *Proc. IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017.

A. Rangi, M. J. Khojasteh, M. Franceschetti, "Learning-based attacks in cyber-physical systems: exploration vs. exploitation,", 2019, being prepared for publication.

ABSTRACT OF THE DISSERTATION

Communication and security in cyber-physical systems

by

Mohammad Javad Khojasteh

Doctor of Philosophy in Electrical Engineering
(Intelligent Systems, Robotics, and Control)

University of California San Diego, 2019

Professor Massimo Franceschetti, Chair

Recent technological advances in networking, communication, and computation technologies have enabled the development of cyber-physical systems and cloud robotics, where computing, communication, and control are tightly coupled and integrated into a single distributed platform. These systems open the door to a myriad of new and exciting applications in transportation, health care, agriculture, energy, and many others. The need for the tight integration of different components, requirements, and time scales means that the modeling, analysis, and design of these systems present new challenges. We focus on two aspects of emerging systems architecture. Firstly, we investigate the presence of finite-rate, digital communication channels

with delays in the feedback loop. In this context, we study event-triggering strategies that utilize timing information by transmitting in a state-dependent fashion. The proposed event-triggering strategies utilize the available communication resources more efficiently compared to existed time-triggering setups. Secondly, the distributed nature of cyber-physical systems and cloud robotics is their Achilles' heel, as it is a source of vulnerability to cyber-attacks. In this regard, we introduce the problem of learning-based attacks in these systems, and we show how the controller can impede these attacks by superimposing a carefully crafted privacy-enhancing signal upon its control policy.

Chapter 1

Introduction

Cyber-physical systems (CPS) are engineering systems that integrate computing, communication, and control; see Figure 1.1. They arise in a wide range of areas such as energy, civil infrastructure, manufacturing, transportation, and robotics [97, 136]. In particular, CPS are closely tied to cloud robotics, an emerging field in robotics and automation systems. The cloud enables robots to utilize wireless networking, powerful cloud computing and storage, machine learning, big data, and many other shared resources to enhance their performances [7, 29, 81, 195]; see Figure 1.2. Using the cloud resources is of specific interest for mobile robots [180], where strong on-board computation resources reduce the operating duration, restrict robot mobility, and

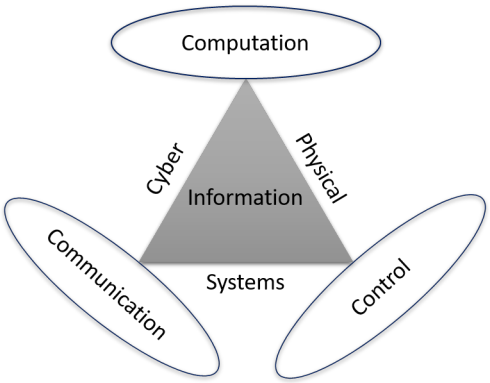


Figure 1.1: Recent technological advances in networking, communication, and computation technologies have enabled the development of cyber-physical systems.

Figure 1.2: Cloud robots and automation systems

increase costs.

The need for tight integration of different components, requirements, and time scales means that the modeling, analysis, and design of these systems present new challenges. We focus on two aspects of these emerging systems architectures, described next.

1.1 Communication

The first issue that we address in these networks of interacting elements is the presences of digital communication channels in the feedback loop, as demonstrated in Figure 1.3.

To use the available resources efficiently, the event-triggering control techniques have emerged as a way of trading computation and decision-making for other services, such as communication, sensing, and actuation. In the context of communication, event-triggered control seeks to prescribe information exchange between the controller and the plant in an opportunistic manner. In this way, communication occurs only when needed for the task at hand (e.g., stabilization, tracking), and the primary focus is on minimizing the number of transmissions while guaranteeing the control objectives and the feasibility of the resulting real-time implementation.

In the same way that subsequent pauses in spoken language are used to convey information,

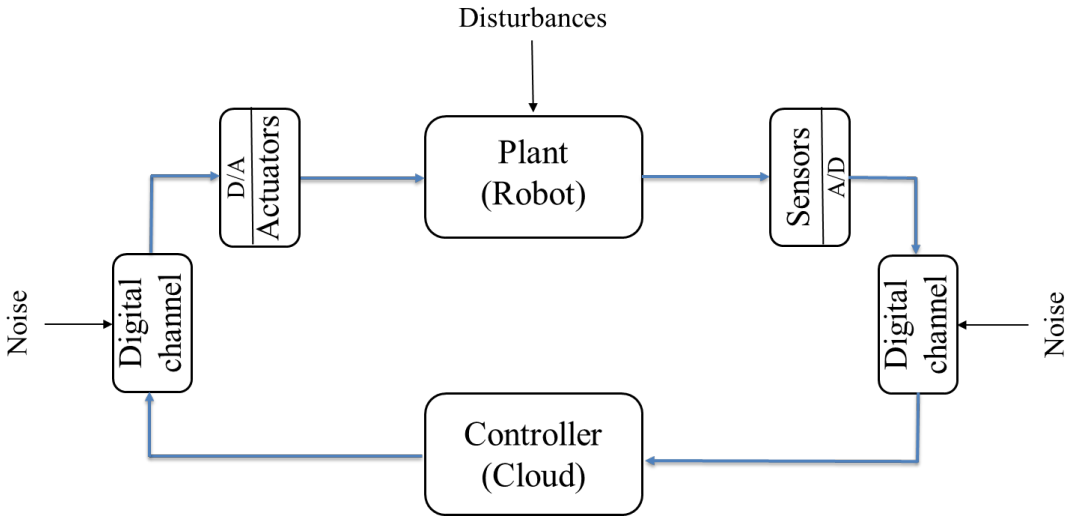


Figure 1.3: Dynamical system abstraction of CPS and cloud robots

it is also possible to transmit information in communication systems not only by message content (data payload), but also with its timing. In this context, the encoding process consists of choosing the timing and data payload of the packet, as shown in Figure 1.4. In other words, in the sensor block, the quantized version of the state is encoded in a packet containing data payload as well as its timing. In Chapters 2 and 3 we investigate event-triggering strategies that utilize timing information by transmitting in a state-dependent fashion. We show that using intrinsic timing information in communication in an event-triggered design; our design can outperform the traditional existed time-triggered control.

To develop theoretical results, we first start with low-complexity models; continuous-time scalar systems without disturbances. Then, to make the results more practical, we escalate the

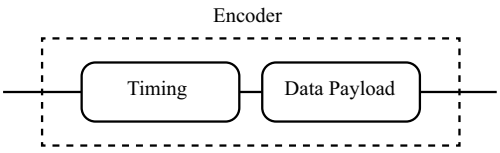


Figure 1.4: Representation of information transmission using data payload and transmission time of the packet in a digital channel. The encoding process consists of choosing the data payloads and their transmission times. Here, the sensor determines the transmission time using our event-triggering strategy in a state-dependent manner.

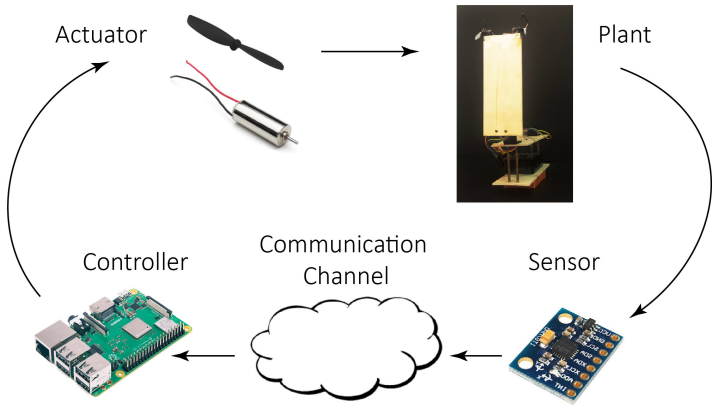


Figure 1.5: Architecture and components of the prototype.

complexity of the model by studying the effect of system disturbances, vector, and nonlinear systems. Eventually, we implement the proposed event-triggering control design and demonstrate the utilization of timing information to stabilize a laboratory-scale inverted pendulum over a digital communication channel with bounded unknown delay. Figure 1.5 depicts the different components of the system.

Finally, in Chapter 4 we extend these results from an information-theoretic perspective, as we explicitly quantify the value of the timing information independent of any transmission strategy.

1.2 Security

The distributed nature of cyber-physical systems is their Achilles' heel, as it is a source of vulnerability to cyber-attacks [22, 134, 165]. Also, the connectivity inherent in the cloud makes the cloud robotics systems vulnerable to these attacks [81]. These cyber-attacks can have catastrophic consequences ranging from hampering the economy through financial scams, to possible losses of human lives through hijacking autonomous vehicles and drones, and all the way to terrorist acts by manipulating large industrial infrastructures [19, 25, 67, 100, 129]. Real-world examples of security breaches in these systems include the revenge sewage attack in Maroochy

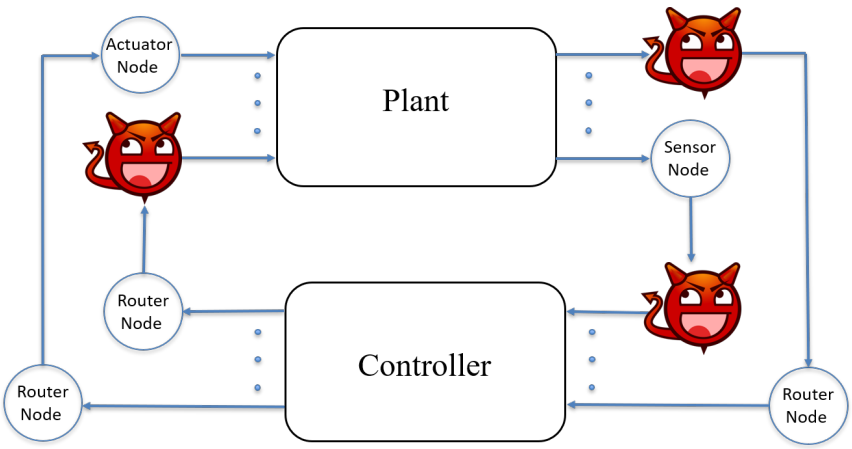


Figure 1.6: Ensuring physical security in CPS requires safe operation in the presence of malicious agents that might have compromised some sensor and actuation signals.

Shire, Australia [181], the Ukraine power attack [111], the German steel mill cyber-attack [106], the Davis-Besse nuclear power plant Slammer worm attack in Ohio, USA [20], and the Iranian uranium enrichment facility attack via the Stuxnet malware [26, 52, 57, 104, 126]. In all of these cases, physical damage has been performed by hackers tampering with the CPS. Despite studying and preventing security breaches via control-theoretic methods has received considerable attention in recent years [1, 11, 18, 21, 24, 47, 55, 59, 133, 146, 170, 178, 179], providing enhanced security remains a critical open problem, which is made particularly challenging by the complexity of the interconnections and the dynamical nature of the system.

We will concentrate on an important and widely used class of attacks called the "man-in-the-middle" (MITM) [8]. In this setting, an attacker takes over the physical plant's control and sensor signals and acts as a malicious controller for the plant and fictitious plant for the controller, see Figure 1.7. The MITM attack has been extensively studied in two special cases [127, 135,

Figure 1.7: The man in the middle attack: the attacker acts as a malicious controller for the plant and a fictitious plant for the controller

169, 182, 216]. The first case is the *replay attack*, in which the attacker observes and records the legitimate system behavior for a given time window and then replays this recording periodically at the controller's input [127, 135, 216]. This attack is reminiscent of the notorious attack of video surveillance systems, in which previously recorded surveillance footage is replayed during a heist. A well-known example is that of the Stuxnet malware, which used an operating system vulnerability to enable a replay attack during which the attacker has driven the speed of the centrifuges at a uranium enrichment facility toward excessively high and destructive speed levels [105]. The second case is the *statistical-duplicate attack*, which assumes that the attacker has acquired complete knowledge of the dynamics and parameters of the system, and can construct arbitrarily long fictitious sensor readings that are statistically identical to the actual signals [169, 182]. The replay attack assumes no knowledge of the system parameters—and as a consequence, it is relatively easy to detect it. The statistical-duplicate attack assumes full knowledge of the system dynamics—and as a consequence, it requires a more sophisticated detection procedure, as well as additional assumptions on the attacker or controller behavior to ensure it can be detected.

In many practical situations, the attacker does not have full knowledge of the system and cannot simulate a statistically indistinguishable copy of the system. On the other hand, the attacker can carry out more sophisticated attacks simply replaying previous sensor readings, by attempting to "learn" the system dynamics from the observations. For this reason, in Chapter 5, we study *learning-based attacks* and show that they can outperform replay attacks by analyzing the performance using a specific learning algorithm. By utilizing tools from information theory and statistics, we bound the asymptotic detection and deception probabilities for *any measurable* control policy when the attacker uses *an arbitrary* learning algorithm to estimate the dynamic of the plant. We also show how the controller can impede the learning process of the attacker by superimposing a carefully crafted *privacy-enhancing signal* upon its control policy. Since both the attacker and the controller need to perform optimal on-line decision making in a feedback

loop fashion, in the last part of Chapter 5, we use active decision theory to study the interplay between control and attacker.

1.3 Dissertation Overview

The rest of this dissertation is organized as follows.

In Chapter 2, we study event-triggered control for stabilization of unstable linear plants over rate-limited communication channels subject to unknown, bounded delay. On one hand, the timing of event triggering carries implicit information about the state of the plant. On the other hand, the delay in the communication channel causes information loss, as it makes the state information available at the controller out of date. Combining these two effects, we show a *phase transition* behavior in the transmission rate required for stabilization using a given event-triggering strategy. For small values of the delay, the timing information carried by the triggering events is substantial, and the system can be stabilized with any positive rate. When the delay exceeds a critical threshold, the timing information alone is not enough to achieve stabilization, and the required rate grows. When the delay equals the inverse of the *entropy rate* of the plant, the implicit information carried by the triggering events perfectly compensates the loss of information due to the communication delay, and we recover the rate requirement prescribed by the *data-rate theorem*. We also provide an explicit construction yielding a sufficient rate for stabilization, as well as results for vector systems. Finally results for event triggering strategies are presented are compared with the data-rate theorem for time-triggered control, that is extended here to a setting with unknown delay. Finally, the developed results for event triggering strategies are compared with the data-rate theorem for time-triggered control, which is extended here to a setting with unknown delay.

In Chapter 3, we study to what extent the implicit timing information in the triggering events, which is studied in Chapter 2, is still useful in the presence of plant disturbances. Beyond

the uncertainty due to the unknown delay in communication, disturbances add an additional degree of uncertainty to the state estimation process, whose effect needs to be properly accounted for. We then demonstrate this in the context of stabilization of a laboratory-scale inverted pendulum around its equilibrium point over a digital communication channel with bounded unknown delay. Through experimental results, we show that as the delay in the communication channel increases, a higher data payload transmission rate is required to fulfill the proposed event-triggering policy requirements. This confirms the theoretical intuition that a larger delay brings a larger uncertainty about the value of the state at the controller, as less timing information is carried in the communication. Our results also provide a novel encoding-decoding scheme to achieve input-to-state practically stability (ISpS) for nonlinear continuous-time systems under appropriate assumptions.

In Chapter 4, we consider the problem of stabilizing an undisturbed, scalar, linear system over a "timing" channel, namely a channel where information is communicated through the timestamps of the transmitted symbols. Each symbol transmitted from a sensor to a controller in a closed-loop system is received subject to some to random delay. The sensor can encode messages in the waiting times between successive transmissions and the controller must decode them from the inter-reception times of successive symbols. This set-up is analogous to a telephone system where a transmitter signals a phone call to a receiver through a "ring" and, after the random delay required to establish the connection, the receiver is aware of the "ring" being received. Since there is no data payload exchange between the sensor and the controller, the set-up provides an abstraction for performing event-triggering control with zero-payload rate. We show the following requirement for stabilization: for the state of the system to converge to zero in probability, the *timing capacity* of the channel should be at least as large as the *entropy rate* of the system. Conversely, in the case the symbol delays are exponentially distributed, we show a tight sufficient condition using a coding strategy that refines the estimate of the decoded message every time a new symbol is received. Our results generalize previous zero-payload event-triggering control

strategies, revealing a fundamental limit in using timing information for stabilization, independent of any transmission strategy.

In Chapter 5, we study the problem of learning-based attacks in a abstraction of cyber-physical systems— the case of a discrete-time, linear, time-invariant plant that may be subject to an attack that overrides the sensor readings and the controller actions. The attacker attempts to learn the dynamics of the plant and subsequently override the controller's actuation signal, to destroy the plant without being detected. The attacker can feed fictitious sensor readings to the controller using its estimate of the plant dynamics and mimic the legitimate plant operation. The controller, on the other hand, is constantly on the lookout for an attack; once the controller detects an attack, it immediately shuts the plant off. For this setting, we derive impossibility bounds on the asymptotic detection and deception probabilities for *any measurable* control policy when the attacker uses *an arbitrary* learning algorithm to estimate the system dynamics. We further derive achievability bounds by proposing a specific authentication test that inspects the empirical variance of the system disturbance. We also show how the controller can impede the learning process of the attacker by superimposing a carefully crafted *privacy-enhancing signal* on top of the nominal control policy. Finally, we study the trade-off between the performance of the learning algorithm, and the performance of arbitrary detection and control strategies adopted by the controller, providing a tight bound on the scaling of the expected time required to detect the attack, as the probability of detection tends to one.

1.4 Notation

The notation used in this thesis is aimed to be as intuitive as possible. One may skip this section and refer back to it, if any notation is confusing.

Let $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the set of real numbers, integers, and positive integers, respectively. We denote by $\mathcal{B}(r)$ the ball centered at 0 of radius r. We let $\log$ and $\ln$ denote the logarithm with

bases 2 and e, respectively. We let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x, and $\lceil x \rceil$ denote the smallest integer greater than or equal to x. We denote by $\mathrm{mod}(x, y)$ the modulo function, whose value is the remainder left after dividing x by y. We let $\mathrm{sign}(x)$ be 1, -1, or 0 when x is positive, negative, or zero, respectively. We let m denote the Lebesgue measure on $\mathbb{R}^n$, which for $n = 2$ and $n = 3$ can be interpreted as area and volume, respectively.

We let $M_{n,m}(\mathbb{R})$ be the set of $n \times m$ matrices over the field of real numbers. Given $A = [a_{i,j}]_{1 \leq i,j \leq n} \in M_{n,n}(\mathbb{R})$, we let $\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{ii}$ and $\det(A)$ denote its trace and determinant, respectively. We use the $\dagger$ sign to represent the transpose of a matrix. $A \succeq B$ means that $A - B$ is a positive semidefinite matrix, namely $\succeq$ is the Loewner order of Hermitian matrices. $\lambda_{max}(A)$ denotes the largest eigenvalue of the matrix A. We consider the two-norm, which is denoted by $\| \cdot \|$, for the vector spaces, and we denote the operator norm induced by it with $\| \cdot \|_{op}$. We also use $\|.\|$ to denote complex absolute value. Any $Q \in \mathbb{C}$ can be written as $Q = \mathrm{Re}(Q) + i\,\mathrm{Im}(Q) = \|Q\| e^{i\phi_Q}$, and for any $y \in \mathbb{R}$ we have $\|e^{Qy}\| = e^{\mathrm{Re}(Q)y}$.

An event happens almost surely (a.s.) if it occurs with probability one. We write $X_n \xrightarrow{P} X$ if X_n converges in probability to X. Similarly, we write $X_n \xrightarrow{a.s.} X$ if X_n converges almost surely to X. We use $H(X)$ to denote the Shannon entropy of a discrete random variable X and $h(X)$ to denote the differential entropy of a continuous random variable X. For real numbers a and b, $a \ll b$ means a is much less than b, in some numerical sense, while for probability distributions $\mathbb{P}$ and $\mathbb{Q}$, $\mathbb{P} \ll \mathbb{Q}$ means $\mathbb{P}$ is absolutely continuous w.r.t. $\mathbb{Q}$. $d\mathbb{P}/d\mathbb{Q}$ denotes the Radon–Nikodym derivative of $\mathbb{P}$ w.r.t. $\mathbb{Q}$. The Kullback–Leibler (KL) divergence between probability distributions $\mathbb{P}_X$ and $\mathbb{P}_Y$ is defined as

$$D(\mathbb{P}_X \| \mathbb{P}_Y) \triangleq \begin{cases} \mathbb{E}_{\mathbb{P}_X}\left[\log \dfrac{d\mathbb{P}_X}{d\mathbb{P}_Y}\right], & \mathbb{P}_X \ll \mathbb{P}_Y; \\ \infty, & \text{otherwise}, \end{cases}$$

where $E_{\mathbb{P}_X}$ denotes the expectation w.r.t. probability measure $\mathbb{P}_X$. The conditional KL di-

vergence between probability distributions $\mathbb{P}_{Y|X}$ and $\mathbb{Q}_{Y|X}$ averaged over $\mathbb{P}_X$ is defined as $D\left(\mathbb{P}_{X|Y}\middle\|\mathbb{Q}_{Y|X}\middle|\mathbb{P}_X\right) \triangleq \mathbb{E}_{\mathbb{P}_{\tilde{X}}}\left[D\left(\mathbb{P}_{Y|X=\tilde{X}}\middle\|\mathbb{Q}_{Y|X=\tilde{X}}\right)\right]$, where $(X, \tilde{X})$ are independent and identically distributed (i.i.d.). The mutual information between random variables X and Y is defined as $I(X;Y) \triangleq D\left(\mathbb{P}_{XY}\|\mathbb{P}_X\mathbb{P}_Y\right)$. The conditional mutual information between random variables X and Y given random variable Z is defined as $I(X;Y|Z) \triangleq \mathbb{E}_{\mathbb{P}_{\tilde{Z}}}\left[I(X;Y|Z=\tilde{Z})\right]$, where $(Z, \tilde{Z})$ are i.i.d.

For a function $f : \mathbb{R} \to \mathbb{R}^n$ and $t \in \mathbb{R}$, we let $f(t^+)$ denote the limit from the right, namely $\lim_{s\downarrow t} f(s)$. For two real valued functions g and h, $g(x) = O\left(h(x)\right)$ as $x \to x_0$ means $\limsup_{x\to x_0} |g(x)/h(x)| < \infty$, and $g(x) = o\left(h(x)\right)$ as $x \to x_0$ means $\lim_{x\to x_0} |g(x)/h(x)| = 0$. For any set $\mathscr{X}$ and any $n \in \mathbb{N}$ we let $\pi_n : \mathscr{X}^{\mathbb{N}} \to \mathscr{X}^n$ be the truncation operator, namely the projection of a sequence in $\mathscr{X}^{\mathbb{N}}$ into its first n symbols. For a scalar continuous-time signal $w(t)$, we define

$$|w|_t = \sup_{s\in[0,t]} |w_1(s)|.$$

Finally, to formulate the stability properties, for non-negative constants d and d' we define

$\mathcal{K}(d) := \{f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} | f \text{ continuous, strictly increasing, and } f(0) = d\}$,

$\mathcal{K}_\infty(d) := \{f \in \mathcal{K}(d) |\ f \text{ unbounded}\}$,

$\mathcal{K}^2_\infty(0, d') := \{f : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} |\ \forall t \geq 0,\ f(.,t) \in \mathcal{K}_\infty(0), \text{ and } \forall r > 0\ f(r,.) \in \mathcal{K}_\infty(d')\}$

$\mathcal{L} := \{f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} |\ f \text{ continuous, strictly decreasing, and } \lim_{s\to\infty} f(s) = 0\}$,

$\mathcal{KL} := \{f : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} |\ f \text{ continuous}, \forall t \geq 0, f(.,t) \in \mathcal{K}(0), \text{ and } \forall r > 0\ f(r,.) \in \mathcal{L}\}$.

Chapter 2

The value of timing information in event-triggered control

2.1 Introduction

One key aspect in the modeling, analysis, and design of CPS is the presence of finite-rate, digital communication channels in the feedback loop. Data-rate theorems quantify the effect that communication has on stabilization by stating that the communication rate available in the feedback loop should be at least as large as the *intrinsic entropy rate* of the system (corresponding to the sum of the logarithms of the unstable modes). In this way, the controller can compensate for the expansion of the state occurring during the communication process. Early formulations of data-rate theorems appeared in [12, 40, 206], followed by the key contributions in [141, 191]. More recent extensions include time-varying rate, Markovian, erasure, additive white and colored Gaussian, and multiplicative noise feedback communication channels [5, 46, 84, 86, 121, 128, 130, 132, 184], formulations for nonlinear systems [36, 113, 142], for optimal control [83, 101, 192], for systems with random parameters [140, 156], and for switching systems [114, 208]. Connections with information theory are highlighted in [123, 131, 138, 142, 164]. Extended surveys of the

literature appear in [60, 139] and in the book [212].

Another key aspect of CPS to which we pay special attention here is the need to efficiently use the available resources. Event-triggering control techniques [9, 68, 96, 145, 186, 188, 203, 211] have emerged as a way of trading computation and decision-making for other services, such as communication, sensing, and actuation. In the context of communication, event-triggered control seeks to prescribe information exchange between the controller and the plant in an opportunistic manner. In this way, communication occurs only when needed for the task at hand (e.g., stabilization, tracking), and the primary focus is on minimizing the number of transmissions while guaranteeing the control objectives and the feasibility of the resulting real-time implementation. While the majority of this literature relies on the assumption of continuous availability and infinite precision of the communication channel, recent works also explore event-triggered implementations in the presence of data-rate constraints [99, 107, 109, 147, 187, 210], and packet drops [41, 154, 189]. In this context, one important observation raised in [99] is that using event-triggering it is possible to "beat" the data-rate theorem. Namely, if the channel does not introduce any delay and the controller knows the triggering mechanism, then an event-triggering strategy can achieve stabilization for any positive rate of transmission. This apparent contradiction can be explained by noting that the timing of the triggering events carries information, revealing the state of the system. When communication occurs without delay, the controller can track the state with arbitrary precision, and transmitting a single data payload bit at every triggering event is enough to compute the appropriate control action. The works [99] take advantage of this observation to show that any positive rate of transmission is sufficient for stabilization when the delay is sufficiently small. In contrast, the work in [187] studies the problem of stabilization using an event-triggered strategy, but it does not exploit the implicit timing information carried by the triggering events. The recent work in [119] studies the required information transmission rate for containability [206] of scalar systems, when the delay in the communication channel is at most the inverse of the intrinsic system's entropy rate. Finally, [88] compares the results

presented here with those of a time-triggered implementation.

The main contribution of this chapter is the precise quantification of the amount of information implicit in the timing of the triggering events across the whole spectrum of possible communication delay values, and the use of both timing information and data payload for stabilization. For a given event-triggering strategy, we derive necessary and sufficient conditions for the exponential convergence of the state estimation error and the stabilization of the plant, revealing a *phase transition* behavior of the transmission rate as a function of the delay. Key to our analysis is the distinction between the *information access rate*, that is the rate at which the controller needs to receive information, conveyed by both data payload and timing information and regulated by the classic data-rate theorem; and the *information transmission rate*, that is the rate at which the sensor needs to send data payload, that is affected by channel delays, as well as design choices such as event-triggering or time-triggering strategies. We show that for sufficiently low values of the delay, the timing information carried by the triggering events is large enough and the system can be stabilized with any positive information transmission rate. At a critical value of the delay, the timing information carried by the triggering events is not enough for stabilization, and the required information transmission rate begins to grow. When the delay reaches the inverse of the entropy rate of the plant, the timing information becomes completely obsolete, and the required information transmission rate becomes larger than the information access rate imposed by the data-rate theorem. We also provide necessary conditions on the information access rate for asymptotic stabilizability and observability with exponential convergence guarantees; necessary conditions on the information transmission rate for asymptotic observability with exponential convergence guarantees; as well as a sufficient condition with the same asymptotic behavior. We consider both scalar and vector linear systems without disturbances.

2.2 Problem formulation

Here we describe the system evolution, the model for the communication channel, and the event-triggering strategy.

2.2.1 System model

We consider the standard networked control system model composed of the plant-sensor-channel-controller tuple depicted in Figure 2.1. We start with a scalar, continuous-time, linear time-invariant (LTI) system, and then extend the model to the vector case.

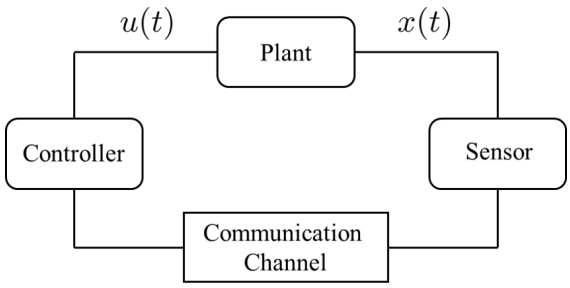


Figure 2.1: System model. The sensor can measure the full state of the system and the controller applies the input with infinite precision and without delay. The communication channel only supports a finite rate and is subject to delay.

The plant dynamics are described by

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{2.1}$$

where $x(t) \in \mathbb{R}$ and $u(t) \in \mathbb{R}$ for $t \in [0, \infty)$ are the system state and control input, respectively. Here, A is a positive real number, B is a nonzero real number, and $|x(0)| < L$ is any bounded initial condition, where L is known to both sensor and controller. The sensor can measure the state of the system perfectly, and the controller can apply the control input with infinite precision and without delay. However, the sensor and the controller communicate through a channel that can support only a finite communication rate and is subject to delay. At each triggering event, the

sensor can transmit a packet composed of a finite number of bits, representing a quantized version of the state, through the communication channel, which is received by the controller entirely and without error, after an unknown, bounded delay, as described next.

2.2.2 Triggering strategy and controller dynamics

We denote by $\{t_s^k\}_{k\in\mathbb{N}}$ the sequence of times at which the sensor transmits to the controller a packet composed of $g(t_s^k)$ bits representing the state of the plant. For every $k \in \mathbb{N}$, we let t_c^k be the time at which the controller receives the packet that the sensor transmitted at time t_s^k. We assume a uniform upper bound, known to both the sensor and the controller, on the unknown *communication delays*

$$\Delta_k = t_c^k - t_s^k \leq \gamma, \tag{2.2}$$

and denote the k^{th} *triggering interval* by

$$\Delta_k' = t_s^{k+1} - t_s^k.$$

We assume the upper bound on the communication delays in (2.2) to be independent of the packet size. When referring to a generic triggering time or reception time, for notational convenience we omit the superscript k in t_s^k and t_c^k. Our model does not assume any a priori probability distribution for the delay, and our results hold for any random communication delay with bounded support.

From the data received from the sensor, and from the timing at which the data is received, the controller maintains an estimate $\hat{x}$ of the plant state, which starting from $\hat{x}(t_c^{k+})$ evolves during

the inter-reception times as

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t), \quad t \in [t_c^k, t_c^{k+1}]. \tag{2.3}$$

The controller then computes the control input $u(t)$ based on this estimate. The sensor can compute the same estimate $\hat{x}(t)$ for the plant state at the controller via *communication through the control input* [164]. Namely, assuming that the input has been computed by the controller as $u(t) = \mu(\hat{x}(t))$, where μ an *invertible* function known to both parties, the sensor can first compute $u(t) = (\dot{x}(t) - Ax(t))/B$ and then compute $\hat{x}(t)$ by inversion.

The *state estimation error* computed at the sensor is then

$$z(t) = x(t) - \hat{x}(t).$$

Initially, we let $x(0) - \hat{x}_0 = z(0)$. Without updated information from the sensor, this error grows, and the system can potentially become unstable. The sensor should, therefore, select the sequence of transmission times $\{t_s^k\}_{k\in\mathbb{N}}$, the packet sizes $\{g(t_s^k)\}_{k\in\mathbb{N}}$ and the corresponding quantization strategy used to determine the data payload, so that the controller can ensure stability. This choice requires a certain communication rate available in the channel, which we wish to characterize.

To select the transmission times, we adopt an event-triggering approach. Consider the *event-triggering function* known to both sensor and controller

$$v(t) = v_0 e^{-\sigma t}, \tag{2.4}$$

where v_0 and σ are positive real numbers. A transmission occurs whenever

$$|z(t)| = v(t). \tag{2.5}$$

Upon reception of the packet, the controller updates the estimate of the state according to the *jump strategy*

$$\hat{x}(t_c^+) = \bar{z}(t_c) + \hat{x}(t_c), \tag{2.6}$$

where $\bar{z}(t_c)$ is an estimate of $z(t_c)$ constructed by the controller knowing that $|z(t_s)| = v(t_s)$, the bound (2.2), and the decoded packet received through the communication channel. It follows that

$$|z(t_c^+)| = |x(t_c) - \hat{x}(t_c^+)| = |z(t_c) - \bar{z}(t_c)|.$$

We also point out that if the control law is not invertible, the sensor can perform the same computation of the controller to obtain $\hat{x}(t_c^+)$, provided that it can infer the reception times from jumps in the control input.

By transmitting when the state estimation error $|z(t)|$ reaches the threshold $|v(t)|$, the sensor effectively encodes information in timing using the event-triggering rule (2.5). On the other hand, the data payload of the transmissions also carries information, and the sensor can choose any arbitrary, finite-precision quantization of the state to construct the data payload as long as it ensures that, for all $t_c \in [t_s, t_s + \gamma]$,

$$|z(t_c^+)| = |z(t_c) - \bar{z}(t_c)| \leq \rho(t_s) := \rho_0 e^{-\sigma\gamma} v(t_s), \tag{2.7}$$

where $0 < \rho_0 < 1$ is a given design parameter. Note that $v(t_c) = v_0 e^{-\sigma t_c} \geq v_0 e^{-\sigma t_s} e^{-\sigma\gamma} = v(t_s) e^{-\sigma\gamma}$, and hence (2.7) ensures that at each triggering event the estimation error drops below the triggering function, namely

$$|z(t_c^+)| \leq \rho_0 v(t_c).$$

Consequently, the sequence of transmission times $\{t_s^k\}_{k\in\mathbb{N}}$ is monotonically increasing, i.e., $\Delta_k' > 0$ for all $k \in \mathbb{N}$. Moreover, based on $\dot{z} = Az$ and (2.5), a new transmission occurs only after the previous packet has been delivered to the controller, that is $t_s^{k+1} > t_c^k$. Additionally, using $\dot{z} = Az$ and (2.2), we deduce

$$\begin{aligned} |z(t_c)| &\leq v(t_s)e^{A\gamma} \leq v_0 e^{-\sigma(t_c-\gamma)}e^{A\gamma} \\ &= v_0 e^{(A+\sigma)\gamma}e^{-\sigma t_c}. \end{aligned} \tag{2.8}$$

From (2.7) and (2.8), it follows that the described triggering strategy ensures an exponentially decaying estimation error. The design parameter ρ_0 regulates the resolution of the quantization, and hence the size of the transmitted packets; as well as the magnitude of the jumps below the triggering function, and hence the triggering rate. These also depend on the delay, which governs the amount of overshoot of the estimation error above the triggering function, see Figure 2.2.

The design parameter v_0 determines the initial condition of the estimation error when the first triggering event occurs. For any given $0 < \rho_0 < 1$, and $0 < v_0 < \infty$, our objective is to determine the rate required to achieve these exponential bounds for all possible delay realizations, and then provide an explicit quantization strategy that satisfies these bounds.

2.2.3 Information transmission rate

To define the transmission rate, we take the viewpoint of the sensor and examine the amount of information that it needs to transmit so that the controller is able to stabilize the system. Let $b_s(t)$ be the number of bits in the data payload transmitted by the sensor up to time t, and define the *information transmission rate* as

$$R_s = \limsup_{t\to\infty} \frac{b_s(t)}{t}.$$

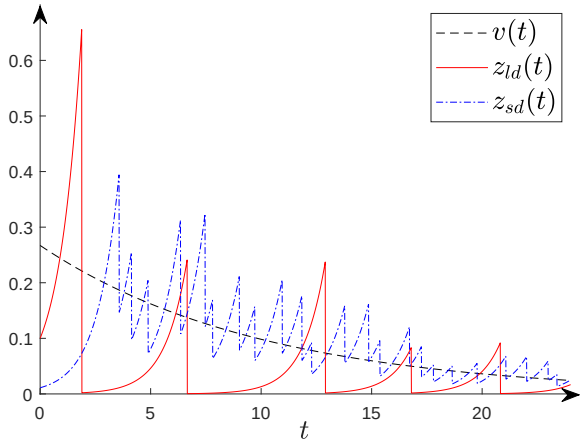


Figure 2.2: Evolution of the state estimation error $|z_{ld}(t)|$ for a larger delay upper bound $\gamma = 1.2$, and $|z_{sd}(t)|$ for a smaller delay upper bound $\gamma = 0.9$. Here, $A = 1$, $\sigma = 0.1$, and $\rho_0 = 0.1$. The dashed exponential decaying curve represents the triggering function $v(t) = 0.27e^{-\sigma t}$. A larger delay corresponds to a larger overshoot of the estimation error above the triggering function and higher uncertainty about the state at the controller. Since γ regulates the resolution of the quantization (2.7) in an exponential manner, larger delay corresponds to larger jumps under the triggering function upon reception of the packet.

Since at every triggering time, t_s^k the sensor sends $g(t_s^k)$ data payload bits, we have

$$R_s = \limsup_{N\to\infty} \frac{\sum_{k=1}^{N} g(t_s^k)}{\sum_{k=1}^{N} \Delta_k'}. \tag{2.9}$$

We now make two key observations. First, in the presence of unknown communication delays, the state estimate received by the controller might be out of date so that the sensor might need to send data at a *higher rate* than what is needed on a channel without delay. Second, in the presence of event-triggered transmissions, the timing of the triggering events carries implicit information. For example, if the communication channel does not introduce any delay, and assuming that the sensor and the controller can keep track of time with infinite precision, then the time of a triggering event reveals the system state up to a sign, since according to (2.5),

$$x(t) = \hat{x}(t) \pm v(t).$$

It follows that in this case, the controller can stabilize the system even if the sensor uses the channel very sparingly, transmitting a single data payload bit at a triggering event, that is at a much *smaller rate* than what needed in any time-triggered implementation. In general, there is a trade-off between the information gain due to triggering timing, and the information loss due to the delay. As we shall see below, this leads to a *phase transition* in the minimum rate required to satisfy (2.7) and as a consequence (2.8).

Finally, it is worth pointing out that the exponential convergence of the state estimation error to zero implies the asymptotic stabilizability of the system.

2.2.4 Information access rate

We now consider the viewpoint of the controller and examine the amount of information that it needs to receive from the plant to be able to stabilize the system. We define $b_c(t)$ to be the amount of information, measured in bits, conveyed by both data payload and timing information, received by the controller up to time t. We define the *information access rate* as

$$R_c = \limsup_{t\to\infty} \frac{b_c(t)}{t}.$$

Remark 1. We do not consider the bounded delays (2.2) to be chosen from any specific distribution. Thus, the information that can be gained about the triggering time t_s from the reception time t_c may be quantified by the Rényi 0th-order information functional I_0 [138, 177]. Assuming the controller has received N packet by time t, we deduce $b_c(t) = \sum_{k=1}^{N} \big(g(t_s^k) + I_0(t_s^k; t_c^k)\big)$. •

Classic data-rate theorems describe the information access rate required to stabilize the system. They are generally stated for discrete-time systems, albeit similar results hold in continuous time as well, see e.g. [70]. They are based on the fundamental observation that there is an inherent

entropy rate

$$h = \frac{A}{\ln 2},$$

at which the system generates information. It follows that for the system to be stabilizable the controller must have access to state information at a rate

$$R_c \geq h. \tag{2.10}$$

This result indicates what is required by the controller, and it does not depend on the feedback structure — including aspects such as communication delays, information pattern at the sensor and the controller, and whether the times at which transmissions occur are state-dependent, as in event-triggered control, or periodic, as in time-triggered control.

2.3 Necessary condition on the access rate

In this section, we quantify the amount of information that the controller needs to ensure exponential convergence of the state estimation error or the state to zero, independently of the feedback structure used by the sensor to decide when to transmit. The result obtained here generalizes (2.10) and establishes a common ground to compare later against the results for the information transmission rate, which depend on the given policy adopted by the sensor. The proof follows, with minor modifications, the argument in [191, Propositions 3.1 and 3.2] for discrete-time systems.

Theorem 1. *Consider the plant-sensor-channel-controller model described in Section 2.2.1, with plant dynamics* (2.1)*, and state estimation error* $z(t)$*, and let* $\sigma > 0$*. The following necessary conditions hold:*

1. *If the state estimation error satisfies*

$$|z(t)| \leq |z(0)|\, e^{-\sigma t},$$

then

$$b_c(t) \geq t\, \frac{A+\sigma}{\ln 2} + \ \log \frac{L}{|z(0)|}. \tag{2.11}$$

2. *If the system is stabilizable and*

$$|x(t)| \leq |x(0)|\, e^{-\sigma t},$$

then

$$b_c(t) \geq t\, \frac{A+\sigma}{\ln 2}. \tag{2.12}$$

In both cases, the necessary information access rate is

$$R_c \geq \frac{A+\sigma}{\ln 2}. \tag{2.13}$$

Proof. From (2.1), we have

$$x(t) = e^{At}x(0) + \alpha(t), \tag{2.14a}$$

$$\alpha(t) = e^{At} \int_0^t e^{-A\tau} B u(\tau) d\tau. \tag{2.14b}$$

Using (2.14a) we define the uncertainty set at time t

$$\Gamma_t = \{x \in \mathbb{R} : x = e^{At}x(0) + \alpha(t) \text{ and } x(0) \in \mathcal{B}(L)\}.$$

The state of the system can be any point in this uncertainty set. Letting $\epsilon(t) = |z(0)|\, e^{-\sigma t}$, we can then find a lower bound on $b_c(t)$ by counting the number of one-dimensional balls of radius $\epsilon(t)$ that cover Γ_t. Specifically,

$$\begin{aligned} b_c(t) &\geq \log \frac{m(\Gamma_t)}{m(\mathcal{B}(\epsilon(t)))} = \log \frac{e^{At} m(\mathcal{B}(L))}{2|z(0)|\, e^{-\sigma t}} \\ &= t\ \log e^{A+\sigma} + \log \frac{L}{|z(0)|}, \end{aligned}$$

which proves (i).

To prove (ii), for any given control trajectory $\{u(\tau)\}_{\tau\in[0,t]}$, define the set of initial conditions for which the plant state $x(t)$ tends to zero exponentially with rate σ, i.e.,

$$\Pi_{\{u(\tau)\}_{\tau\in[0,t]}} = \{x(0) \in \mathcal{B}(L) : |x(t)| \leq |x(0)|\, e^{-\sigma t}\}.$$

By (2.14b) $x(t)$ depends linearly on $\{u(\tau)\}_{\tau\in[0,t]}$, so that all the sets $\Pi_{\{u(\tau)\}_{\tau\in[0,t]}}$ are linear transformations of each other. The measure of $\Pi_{\{u(\tau)=0\}_{\tau\in[0,t]}}$ is $2|x(0)|e^{-At}e^{-\sigma t}$, which is upper bounded by $2Le^{-At}e^{-\sigma t}$. Hence, this quantity also upper bounds the measure of each $\Pi_{\{u(\tau)\}_{\tau\in[0,t]}}$. It follows that we can determine a lower bound for $b_c(t)$ by counting the number of sets of measure $2Le^{-At}e^{-\sigma t}$ required to cover the ball $|x(0)| \leq L$, and we have

$$b_c(t) \geq \log \frac{2L}{2Le^{-(A+\sigma)t}} = t\ \frac{A+\sigma}{\ln 2},$$

showing (ii). Finally, (2.13) follows by dividing (2.11) and (2.12) by t and taking the limit for $t \to \infty$. ∎

Remark 2. Theorem 1 is valid for any control scheme, and the controller does not necessarily have to compute the state estimate following (2.3). This result can be viewed as an extension of the data-rate theorem with exponential convergence guarantees. It states that to have exponential convergence of the estimation error and the state, the access rate should be larger than the estimation entropy, the latter concept having been recently introduced in [116]. A similar result for continuous-time systems appears in [187], but only for linear feedback controllers. In fact, this work shows that the bound in (2.13) is also sufficient for scalar systems when the controller does not use any timing information about the triggering events. The classic formula of the data-rate theorem (2.10) [141, 191], can be derived as a special case of Theorem 1 by taking $\sigma \to 0$ and using continuity. •

2.4 Necessary and sufficient conditions on the transmission rate

In this section, we determine necessary and sufficient conditions on the transmission rate for the exponential convergence of the estimation error under the event-triggered control strategy described in Section 2.2.1. We start by observing that in an event-triggering implementation, the transmission times and the packet sizes are state-dependent. Thus, there may be some initial conditions and delay realizations for which both the necessary and sufficient transmission rates are arbitrarily small. For this reason, we provide results that hold in worst-case conditions, namely accounting for all possible realizations of the delay and initial conditions, without assuming any a priori distribution on these realizations.

2.4.1 Necessary condition on the transmission rate

Here we quantify the necessary rate at which the sensor needs to transmit to ensure the exponential convergence of the estimation error to zero under the given event-triggering strategy. This rate depends on the number of bits that the sensor transmits at each triggering event, as well as the frequency with which transmission events occur, according to the triggering rule. Our strategy to obtain a necessary rate consists of appropriately bounding each of these quantities.

To obtain a lower bound on the number of bits transmitted at each triggering event, consider the uncertainty set of the sensor about the estimation error at the controller, $z(t_c)$, given t_s

$$\Omega(z(t_c)|t_s) = \{y : y = \pm v(t_s)e^{A(t_c - t_s)},\ t_c \in [t_s, t_s + \gamma]\}.$$

On the other hand, consider the uncertainty from the point of view of the controller about $z(t_c)$, given t_c

$$\Omega(z(t_c)|t_c) = \{y : y = \pm v(\bar{t}_r)e^{A(t_c - \bar{t}_r)},\ \bar{t}_r \in [t_c - \gamma, t_c]\}.$$

Clearly, for any $t_c \in [t_s, t_s + \gamma]$, we have $\Omega(z(t_c)|t_c) \neq \Omega(z(t_c)|t_s)$, namely there is a *mismatch* between the uncertainties at the controller and at the sensor. The next result shows that the uncertainty at the sensor is always smaller than the one at the controller.

Lemma 1. *Consider the plant-sensor-channel-controller model described in Section 2.2.1, with plant dynamics* (2.1)*, estimator dynamics* (2.3)*, event-triggering function* (2.4)*, triggering strategy* (2.5)*, and jump strategy* (2.6)*. Then,* $\Omega(z(t_c)|t_s) \subseteq \Omega(z(t_c)|t_c)$.

Proof. The uncertainty set of the sensor can be expressed as

$$\Omega(z(t_c)|t_s) = [v(t_s), v(t_s)e^{A\gamma}] \cup [-v(t_s)e^{A\gamma}, -v(t_s)].$$

Noting that for any $t_c \in [t_s, t_s + \gamma]$, $v(\bar{t}_r)e^{A(t_c - \bar{t}_r)}$ is a decreasing function of $\bar{t}_r$, we have

$$\Omega(z(t_c)|t_c) = \\ [v(t_c), v(t_c)e^{(A+\sigma)\gamma}] \cup [-v(t_c)e^{(A+\sigma)\gamma}, -v(t_c)].$$

The result now follows by noting that, since v is a decreasing function, for all $t_c \in [t_s, t_s + \gamma]$ we have $v(t_s) \geq v(t_c)$ and $v(t_s)e^{A\gamma} \leq v(t_c)e^{(A+\sigma)\gamma}$. ∎

To ensure that (2.7) holds, the controller needs to reduce the state estimation error $z(t_c)$ to within an interval of radius $\rho(t_s)$. From Lemma 1, this implies that the sensor needs to cover at least the uncertainty set $\Omega(z(t_c)|t_s)$ with one-dimensional balls of radius $\rho(t_s)$. This observation leads us to the following lower bound on the number of bits that the sensor must transmit at every triggering event.

Lemma 2. *Under the assumptions of Lemma 1, if* (2.7) *holds for all* $k \in \mathbb{N}$*, then the packet size at every triggering event must satisfy*

$$g(t_s^k) \geq \max\left\{0, \log \frac{(e^{A\gamma} - 1)}{\rho_0 e^{-\sigma\gamma}}\right\}. \tag{2.15}$$

Proof. We compute the number of bits that must be transmitted to guarantee that the sensor uncertainty set $\Omega(z(t_c)|t_s)$ is covered by balls of radius $\rho(t_s)$. Define $\chi_\gamma = \{y : y = e^{At}, t \in [0, \gamma]\}$. Since $g(t_s)$ is the packet size, it is non-negative. Hence, $g(t_s) \geq \max\left\{0, H_{\rho(t_s)}\right\}$, where

$$\begin{aligned} H_{\rho(t_s)} &:= \log \frac{m(\Omega(z(t_c)|t_s))}{m(\mathcal{B}(\rho(t_s)))} \\ &= \log \frac{2v(t_s)m(\chi_\gamma)}{2\rho_0 e^{-\sigma\gamma} v(t_s)} \\ &= \log \frac{2v(t_s)(e^{A\gamma} - 1)}{2\rho_0 e^{-\sigma\gamma} v(t_s)}, \end{aligned} \tag{2.16}$$

and the result follows. ∎

Our next goal is to characterize the frequency with which transmission events are triggered. We define the triggering rate

$$R_{tr} = \limsup_{N\to\infty} \frac{N}{\sum_{k=1}^{N} \Delta_k'}. \tag{2.17}$$

First, we provide an upper bound on the triggering rate that holds for all initial conditions and possible communication delays upper bounded by γ.

Lemma 3. *Under the assumptions of Lemma 1, if* (2.7) *holds for all* $k \in \mathbb{N}$*, then the triggering rate is upper bounded as*

$$R_{tr} \leq \frac{A+\sigma}{-\ln(\rho_0 e^{-\sigma\gamma})}. \tag{2.18}$$

Proof. Consider two successive triggering times t_s^k and t_s^{k+1} and the reception time t_c^k. We have $t_s^k \leq t_c^k \leq t_s^{k+1}$. From (2.1) and (2.3), we have $\dot{z}(t) = A(x(t) - \hat{x}(t)) = Az(t)$. The triggering time t_s^{k+1} is defined by

$$|z(t_c^{k+})e^{A(t_s^{k+1}-t_c^k)}| = v(t_s^{k+1}). \tag{2.19}$$

From (2.7), we have

$$\rho_0 e^{-\sigma\gamma} v(t_s^k) e^{A(t_s^{k+1}-t_c^k)} \geq v(t_s^{k+1}).$$

Using (2.4) and $t_s^k \leq t_c^k$, it follows that

$$\rho_0 e^{-\sigma\gamma} v_0 e^{-\sigma t_s^k} e^{A(t_s^{k+1}-t_s^k)} \geq v_0 e^{-\sigma t_s^{k+1}},$$

and after some algebra we obtain

$$(A+\sigma)(t_s^{k+1}-t_s^k) \geq -\ln(\rho_0 e^{-\sigma\gamma}).$$

We then have the uniform lower bound for all $k \in \mathbb{N}$

$$\Delta_k' = t_s^{k+1}-t_s^k \geq \frac{-\ln(\rho_0 e^{-\sigma\gamma})}{A+\sigma}, \tag{2.20}$$

which substituted into (2.17) leads to the desired upper bound on the triggering rate. ∎

Remark 3. In addition to providing an upper bound on the triggering rate, Lemma 3 also shows that our event-triggered scheme does not exhibit "Zeno behavior" [79], namely the occurrence of infinitely many triggering events in a finite time interval. This follows from the uniform lower bound for all $k \in \mathbb{N}$ on the size of triggering interval in (2.20). •

If $\Delta_k = 0$ and $|z(t_c^{k+})| = \rho_0 e^{-\sigma\gamma} v(t_s)$ for all $k \in \mathbb{N}$, then the upper bound on the triggering rate in Lemma 3 is tight. Our next goal is to provide a lower bound on the triggering rate that holds for a given initial condition and delay value. To obtain a nontrivial lower bound, we need to restrict the class of allowed quantization policies used to construct the data payload. We assume that, at each triggering event, there exists a delay such that the sensor can reduce the estimation error at the controller to at most a fraction of the maximum value $\rho(t_s)$ required by (2.7). This is a natural assumption, and in practice corresponds to assuming an upper bound on the size of the packet that the sensor can transmit at every triggering event and hence on the precision of the quantization strategy. Without such a bound, a packet may carry an unlimited amount of information, the quantization error may become arbitrary small, and $|z(t_c^+)|$ may become arbitrarily close to zero for all delay values, resulting in a triggering rate arbitrarily close to zero. The next assumption precludes such an unrealistic scenario.

Assumption 1 *The controller can only achieve ν-precision quantization. Formally, letting*

$\beta = \frac{1}{A}\ln(1 + 2\rho_0 e^{-\sigma\gamma})$, *we assume there exists a delay realization* $\{\Delta_k \leq \beta\}_{k\in\mathbb{N}}$, *an initial condition* $x(0)$, *and a real number* $\nu \geq 1$, *such that for all* $k \in \mathbb{N}$

$$|z(t_c^k) - \bar{z}(t_c^k)| \geq \frac{\rho(t_s^k)}{\nu}. \tag{2.21}$$

The upper bound β on the delay in Assumption 1 corresponds to the time required for the state estimation error to grow from $z(t_s)$ to $z(t_s) + 2\rho(t_s)$. In fact,

$$z(t_c) = z(t_s)e^{A\beta} = z(t_s)(1 + 2\rho_0 e^{-\sigma\gamma}),$$

from which it follows that

$$z(t_c) - z(t_s) = 2z(t_s)\rho_0 e^{-\sigma\gamma},$$

and since $z(t_s) = \pm v(t_s)$, we have

$$|z(t_c) - z(t_s)| = 2\rho(t_s).$$

To ensure (2.7), the size of the quantization cell should be at most $2\rho(t_s)$. As the delay takes values in $[0, \beta]$, the value of $z(t_c)$ sweeps an area of measure $2\rho(t_s)$. It follows that Assumption 1 corresponds to the existence of a value of the communication delay for which the uncertainty ball about the state shrinks from having a radius at most $\rho(t_s)$ to having a radius at least $\rho(t_s)/\nu$. With this assumption in place, we can now compute the desired lower bound on the triggering rate.

Lemma 4. *Under the assumptions of Lemma 1, if* (2.7) *holds with* ν*-precision for all* $k \in \mathbb{N}$, *then there exists a delay realization* $\{\Delta_k\}_{k\in\mathbb{N}}$ *and an initial condition such that*

$$R_{tr} \geq \frac{A + \sigma}{\ln \nu + \ln(2 + \frac{e^{\sigma\gamma}}{\rho_0})}.$$

Proof. By Assumption 1, for all $k \in \mathbb{N}$ there exists a delay $\Delta_k \leq \beta$ such that

$$|z(t_c^{k+})| \geq (1/\nu)\rho_0 v(t_s^k) e^{-\sigma\gamma}.$$

From the definition of the triggering time t_s^{k+1} in (2.19), we also have

$$(1/\nu)\rho_0 e^{-\sigma\gamma} v(t_s^k) e^{A(t_s^{k+1} - t_s^k - \Delta_k)} \leq v(t_s^{k+1}).$$

Noting that for all $k \in \mathbb{N}$, $\Delta_k \leq \beta$, we have

$$(1/\nu)\rho_0 e^{-\sigma\gamma} v(t_s^k) e^{A(t_s^{k+1} - t_s^k - \beta)} \leq v(t_s^{k+1}).$$

By dividing both sides by $(1/\nu)\rho_0 e^{-\sigma\gamma}$ and using the definition of triggering function, we obtain

$$e^{(A+\sigma)(t_s^{k+1} - t_s^k)} \leq \frac{1}{(1/\nu)\rho_0 e^{-\sigma\gamma} e^{-A\beta}}.$$

Taking the logarithm, we get

$$\Delta_k' = t_s^{k+1} - t_s^k \leq \frac{-\ln((1/\nu)\rho_0 e^{-\sigma\gamma}) + A\beta}{A + \sigma}. \tag{2.22}$$

By substituting (2.22) into (2.17), we finally have

$$\begin{aligned} R_{tr} &\geq \lim_{N\to\infty} \frac{1}{\frac{-\ln((1/\nu)\rho_0 e^{-\sigma\gamma})}{A+\sigma} + \frac{A}{A+\sigma}\beta} \\ &= \frac{A+\sigma}{\ln\nu - \ln(\rho_0 e^{-\sigma\gamma}) + \ln(1 + 2\rho_0 e^{-\sigma\gamma})} \\ &= \frac{A+\sigma}{\ln\nu + \ln(2 + \frac{e^{\sigma\gamma}}{\rho_0})}. \quad \blacksquare \end{aligned}$$

We can now combine Lemma 2 and Lemma 4 to obtain a lower bound on the information transmission rate.

Theorem 2. *Under the assumptions of Lemma 1, if* (2.7) *holds with* ν*-precision for all* $k \in \mathbb{N}$*, then there exists a delay realization* $\{\Delta_k\}_{k\in\mathbb{N}}$ *and an initial condition such that*

$$R_s \geq \frac{A+\sigma}{\ln\nu + \ln(2+\frac{e^{\sigma\gamma}}{\rho_0})} \max\left\{0, \log\frac{(e^{A\gamma}-1)}{\rho_0 e^{-\sigma\gamma}}\right\}. \tag{2.23}$$

Remark 4. Theorem 2 provides a necessary transmission rate for the exponential convergence of the estimation error to zero using our event-triggering strategy. By noting that the lower bound in (2.23) does not depend on v_0, it is easy to check that as $\sigma \to 0$, this result also gives a necessary condition for asymptotic stability, although it does not provide an exponential convergence guarantee of the state. •

2.4.2 Phase transition behavior

We now show a phase transition for the rate required for stabilization expressed in Theorem 2. By combining Lemmas 3 and 4, we have

$$\frac{A+\sigma}{\ln\nu + \ln(2+\frac{1}{\rho_0 e^{-\sigma\gamma}})} \leq R_{tr} \leq \frac{A+\sigma}{-\ln(\rho_0 e^{-\sigma\gamma})}.$$

It follows that if $\rho_0 \ll e^{\sigma\gamma}/\max\{2,\nu\}$, we can neglect the value of 2 inside the logarithm in the left-hand side, as well as $\ln\nu$, and we have

$$R_{tr} \approx \frac{A+\sigma}{-\ln(\rho_0 e^{-\sigma\gamma})}.$$

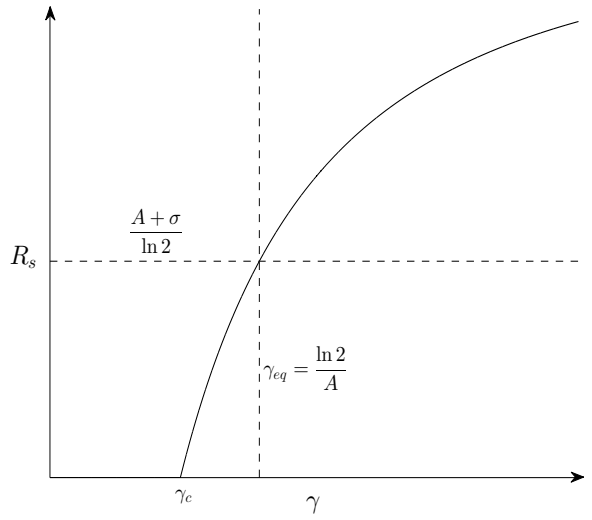


Figure 2.3: Illustration of the phase transition behavior in (2.24). R_s is measured in bits/sec, and γ is measured in sec. The plot is valid for a generic system and design parameters. In this specific example, we have chosen $A = 5$, $\sigma = 3$, and $\rho_0 = 0.7$. Consequently, $(A + \sigma)/\ln 2 = 11.5416$, $\ln 2/A = 0.1386$, and $\gamma_c = 0.0864$.

In this case, the necessary condition on the transmission rate can be approximated as

$$R_s \geq \frac{A+\sigma}{\ln 2} \max\left\{0, 1 + \frac{\log(e^{A\gamma} - 1)}{-\log(\rho_0 e^{-\sigma\gamma})}\right\}. \tag{2.24}$$

We use this approximation to discuss the phase transition behavior. The approximation clearly holds for large values of the delay upper bound γ. It also holds for small values of γ, since in this case both (2.23) and (2.24) tend to zero. For intermediate values of γ, the approximation holds for large values of the convergence rate σ. The phase transition is illustrated in Figure 2.3.

We make the following observations. For small values of γ, the amount of timing information carried by the triggering events is higher than what is needed to stabilize the system and the value of R_s is zero. This means that if the delay is sufficiently small, then only a positive transmission rate is required to track the state of the system and the controller can successfully stabilize the system by receiving a single bit of information at every triggering event. This situation persists until a critical value $\gamma = \gamma_c$ is reached. This critical value is the solution of the

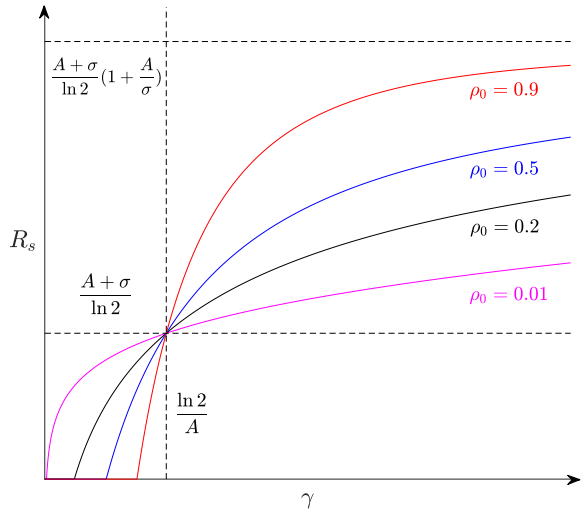


Figure 2.4: Illustration of the phase transition behavior in (2.24) for different values of ρ_0. R_s is measured in bits/sec, and γ is measured in sec. The plots are valid for a generic system and design parameters. In this specific example, we have chosen $A = 1$, and $\sigma = 0.5$. Therefore, $(A+\sigma)/\ln 2 = 2.1640$, $\ln 2/A = 0.6931$, $\frac{A+\sigma}{\ln 2}(1+\frac{A}{\sigma}) = 6.4921$.

equation

$$e^{A\gamma} - \rho_0 e^{-\sigma\gamma} = 1.$$

For this level of delay, the timing information of the triggering events becomes so much out of date that the transmission rate must begin to increase.

When γ reaches the equilibrium point $\gamma_{eq} = \ln 2/A$, which equals the inverse of the intrinsic entropy rate of the system, the timing information carried by the triggering events compensates exactly the loss of information due to the delay introduced by the communication channel. This situation is analogous to having no delay, but also no timing information. It follows that in this case the required transmission rate matches the access rate in Theorem 1, and we have $R_s = (A+\sigma)/\ln 2$.

When γ is increased even further, then the timing information carried by event triggering

is excessively out of date and cannot fully compensate for the channel's delay. The required transmission rate then exceeds the access rate imposed by the data-rate theorem. In this case, a more precise estimate of the state must be sent at every triggering time to compensate for the larger delay. Another interpretation of this behavior follows by considering the definition $H_{\rho(t_s)}$ in (2.16). The value $\gamma = \gamma_{eq} = \ln 2/A$ marks a transition point for $H_{\rho(t_s)}$ from negative to positive values. For $\gamma > \gamma_{eq}$ event triggering does not supply enough information and $H_{\rho(t_s)}$ presents a positive information balance in terms of the number of bits required to cover the uncertainty set. On the other hand, for $\gamma < \gamma_{eq}$, event triggering supplies more than enough information, and $H_{\rho(t_s)}$ presents a negative information balance. We can then think of event triggering as a "source" supplying information, the controller as a "sink" consuming information, and $H_{\rho(t_s)}$ as measuring the balance between the two, indicating whether additional information is needed in terms of quantized observations sent through the channel.

Finally, Figure 2.4 illustrates the phase transition for different values of ρ_0. For $\gamma < \gamma_{eq}$, since according to (2.18) smaller values of ρ_0 imply fewer triggering events, it follows that curves associated to smaller values of ρ_0 must have larger transmission rates to compensate for the lack of timing information. On the other hand, for $\gamma > \gamma_{eq}$ the situation is reversed. The timing information carried by the triggering events is now completely exhausted by the delay, and the controller relies only on the state information contained in the quantized packets. Since, according to (2.15), smaller values of ρ_0 imply larger packets sent through the channel and, for each value of the delay, the information in the larger packets becomes out of date at a slower rate than that in the smaller packets, it follows that in this case curves associated to smaller values of ρ_0 correspond to smaller transmission rates. Finally, we observe that all curves have the same asymptotic behavior for large values of γ, which is independent of ρ_0. This occurs because as γ increases, more information needs to be sent through the channel and also the triggering rate decreases. Taking both effects into account yields the asymptotic value of the transmission rate $\frac{A+\sigma}{\ln 2}(1 + \frac{A}{\sigma})$.

Remark 5. The value of γ_c is a threshold distinguishing whether (2.23) is zero or strictly positive.

This threshold tends to $\gamma_{eq} = \ln 2/A$ as $\sigma \to 0$ and $\rho_0 \to 1$. This is consistent with the fact that in this case there is only an asymptotic convergence guarantee (not an exponential one), and when the delay upper bound γ is at most the inverse of entropy rate of the system only a positive transmission rate is necessary for stabilization. •

2.4.3 Sufficient condition on the transmission rate

We now determine a sufficient transmission rate for the exponential convergence of the state estimation error using the event-triggering strategy described in Section 2.2.2.

In our strategy, we let the sensor send a packet consisting of the sign of $z(t_s)$ and a quantized version of t_s to the controller. Using the bound (2.2), and the decoded packet, the controller constructs $q(t_s)$, a quantized version of t_s. The controller then estimates $z(t_c)$ as follows

$$\bar{z}(t_c) = \text{sign}(z(t_s))v(q(t_s))e^{A(t_c - q(t_s))}. \tag{2.25}$$

The next result provides a bound on the error in the time quantization that guarantees that the requirements of the design are satisfied.

Lemma 5. *Under the assumptions of Lemma 1, using* (2.25)*, if*

$$|t_s - q(t_s)| \leq \frac{1}{A+\sigma} \ln(1 + \rho_0 e^{-(\sigma+A)\gamma}) \tag{2.26}$$

then (2.7) *holds.*

Proof. Using (2.25), it follows that

$$
\begin{aligned}
&|z(t_c)-\bar{z}(t_c)| \qquad (2.27)\\
&\quad = v(t_s)e^{A(t_c-t_s)}\left|1-\frac{v(q(t_s))}{v(t_s)}e^{A(t_s-q(t_s))}\right|\\
&\quad = v(t_s)e^{A(t_c-t_s)}\left|1-\frac{v_0e^{-\sigma q(t_s)}}{v_0e^{-\sigma t_s}}e^{A(t_s-q(t_s))}\right|\\
&\quad = v(t_s)e^{A(t_c-t_s)}\left|1-e^{(A+\sigma)(t_s-q(t_s))}\right|.
\end{aligned}
$$

As a consequence, (2.7) may be expressed as

$$|1-e^{(A+\sigma)(t_s-q(t_s))}| \leq \rho_0 e^{-\sigma\gamma}e^{-A(t_c-t_s)}.$$

The smallest possible value of $e^{-A(t_c-t_s)}$ for $(t_c-t_s)\in[0,\gamma]$ is $e^{-A\gamma}$. Therefore, by ensuring

$$\left|1-e^{(A+\sigma)(t_s-q(t_s))}\right| \leq \rho_0 e^{-(\sigma+A)\gamma}, \qquad (2.28)$$

we can also ensure (2.7). The condition in (2.28) can be rewritten as

$$1-\rho_0 e^{-(\sigma+A)\gamma} \leq e^{(A+\sigma)(t_s-q(t_s))} \leq 1+\rho_0 e^{-(\sigma+A)\gamma}.$$

Taking logarithms and dividing by $(A+\sigma)$, we obtain

$$\frac{1}{A+\sigma}\ln(1-x') \leq t_s-q(t_s) \leq \frac{1}{A+\sigma}\ln(1+x'),$$

where $x'=\rho_0 e^{-(\sigma+A)\gamma}$. It follows that to satisfy (2.7) for all delay values it is enough that

$$|t_s-q(t_s)| \leq \min\{|\frac{1}{A+\sigma}\ln(1-x')|, |\frac{1}{A+\sigma}\ln(1+x')|\}.$$

The result now follows. ∎

The next result presents a sufficient transmission rate, along with the design that meets it.

Theorem 3. *Under the assumptions of Lemma 1, if the state estimation error satisfies* $|z(0)| < v_0$, *then for any information transmission rate*

$$R_s \geq \frac{A+\sigma}{-\ln(\rho_0 e^{-\sigma\gamma})} \max\left\{0, 1+\log\frac{b\gamma(A+\sigma)}{\ln(1+\rho_0 e^{-(\sigma+A)\gamma})}\right\}, \tag{2.29}$$

where $b > 1$, *there exists a quantization policy that achieves* (2.7) *for all* $k \in \mathbb{N}$ *(and consequently* $|z(t)| \leq v_0 e^{(A+\sigma)\gamma} e^{-\sigma t}$*).*

Proof. Our proof strategy is as follows. We design a quantizer to construct a packet of length $g(t_s)$ that the sensor sends to the controller. Using this packet, the decoder reconstructs the quantized version $q(t_s)$ of t_s satisfying (2.26). The result then follows from Lemma 5 and quantifying the associated transmission rate.

In our construction, the first bit of the packet determines the sign of $z(t_s)$, i.e., whether $z(t_s) = +v(t_s)$ or $z(t_s) = -v(t_s)$. For quantizing t_s, we first divide the whole positive time line in sub-intervals of length $b\gamma$. Recall that the controller receives a packet at time t_c, and $t_s \in [t_c - \gamma, t_c]$. Noting that $b\gamma > \gamma$, upon the reception of the packet at time t_c the decoder identifies two consecutive sub-intervals of length $b\gamma$ that t_s can belong to — the second bit of the packet is mod $\left(\lfloor \frac{t_s}{b\gamma} \rfloor, 2\right)$, which informs the decoder that $t_s \in [\iota b\gamma, (\iota+1)b\gamma]$ for some fixed ι. The encoder divides this interval uniformly into $2^{g(t_s)-2}$ sub-intervals, one of which contains t_s. After receiving the packet, the decoder determines the correct sub-interval and chooses $q(t_s)$ as the middle point of it. With this strategy, we have

$$|t_s - q(t_s)| \leq \frac{b\gamma}{2^{g(t_s)-1}}. \tag{2.30}$$

Hence, from Lemma 5, it is enough to ensure

$$\frac{b\gamma}{2^{g(t_s)-1}} \leq \frac{1}{A+\sigma}\ln(1+\rho_0 e^{-(\sigma+A)\gamma}),$$

to guarantee that (2.7) holds. This is equivalent to

$$g(t_s) \geq \max\left\{0, 1+\log\frac{b\gamma(A+\sigma)}{\ln(1+\rho_0 e^{-(\sigma+A)\gamma})}\right\}. \tag{2.31}$$

The characterization (2.29) of the transmission rate now follows from using this bound and the uniform upper bound on the triggering rate (2.18). ∎

Theorem 3 ensures the exponential convergence of the state estimation error. The following result shows that (2.29) is sufficient for asymptotic stabilizability when employing a linear controller.

Corollary 1. *Under the assumptions of Theorem 3,* (2.29) *is also a sufficient condition for asymptotic stabilizability.*

Proof. With $u(t) = -K\hat{x}(t)$, we can rewrite (2.1) as

$$\dot{x}(t) = (A-BK)x(t) + BKz(t).$$

As a consequence, we have

$$x(t) = e^{(A-BK)t}x(0) + e^{(A-BK)t}\int_0^t e^{-(A-BK)\tau}BKz(\tau)d\tau.$$

According to Theorem 3, (2.29) is sufficient to guarantee $\lim_{t\to\infty} z(t) = 0$. Since $B \neq 0$ one can choose K such that $A - BK < 0$, and it follows that criterion (2.29) is also sufficient for $\lim_{t\to\infty} x(t) = 0$. Stability can also be guaranteed from the above expression. ∎

It should be clear that if the quantization policy designed for establishing Theorem 3

satisfies Assumption 1, then the number of bits transmitted at each triggering time is finite. We conclude this section by providing a condition under which the designed policy satisfies Assumption 1.

Theorem 4. *Under the assumptions of Lemma 1, let $\nu \geq 2$, and let the number of bits in each transmitted packet be a constant $g(t_s^k) = g$. If g satisfies the lower bound* (2.31) *and the upper bound*

$$g \leq \log \frac{b\gamma(A+\sigma)}{\left| \ln \left(1 - \frac{1}{(\nu-1)\left(2+\frac{1}{\rho_0 e^{-\sigma\gamma}}\right)} \right) \right|}, \tag{2.32}$$

and

$$\frac{1 - e^{-(A+\sigma)\frac{\delta}{2}}}{1 - e^{-(A+\sigma)\frac{\delta}{4}}} \geq e^{(A+\sigma)\frac{3\delta}{4}}, \tag{2.33}$$

where $\delta = b\gamma/2^{g-2}$, then the quantization policy used in Theorem 3 satisfies Assumption 1 at every triggering time.

Proof. The proof follows from the following two claims.

Claim (a): For all $k \in \mathbb{N}$, if t_s^k satisfies

$$-\frac{\delta}{2} = -\frac{b\gamma}{2^{g-1}} \leq t_s^k - q(t_s^k) \leq -\frac{b\gamma}{2^g} = -\frac{\delta}{4}, \tag{2.34}$$

then there exists a delay $\Delta_k \leq \beta$ such that (2.21) is satisfied.

Claim (b): The sequence of transmission times $\{t_s^k\}$ is uniquely determined by the initial condition $z(0)$ and there exists a $z(0)$ such that for each $k \in \mathbb{N}$, t_s^k satisfies (2.34).

We first prove Claim (a). Note that when the sensor transmits g bits, lower bounded by (2.31), the upper bound on the quantization error (2.30) holds and thus (2.34) is well defined.

From (2.34) and (2.32), we have

$$t_s^k - q(t_s^k) \leq \frac{1}{A+\sigma} \ln\left(1 - \frac{1}{(\nu-1)(2+\frac{1}{\rho_0 e^{-\sigma\gamma}})}\right),$$

where we have used the fact that $\nu \geq 2$ to simplify the absolute value. We rewrite this inequality as

$$1 - e^{(A+\sigma)(t_s^k - q(t_s^k))} \geq \frac{\rho_0 e^{-\sigma\gamma}}{(\nu-1)(1+2\rho_0 e^{-\sigma\gamma})} > 0.$$

Thus, from (2.27), we see that

$$\begin{aligned}
|z(t_c^k) - \bar{z}(t_c^k)| &\geq v(t_s^k) e^{A\Delta_k} \frac{\rho_0 e^{-\sigma\gamma}}{(\nu-1)(1+2\rho_0 e^{-\sigma\gamma})} \\
&\geq \frac{\rho(t_s^k)}{\nu} e^{A(\Delta_k - \beta + \ln(\frac{\nu}{\nu-1}))} \\
&\geq \frac{\rho(t_s^k)}{\nu}, \quad \forall \Delta_k \in \left[\beta - \ln\left(\frac{\nu}{\nu-1}\right), \beta\right],
\end{aligned}$$

where in the second inequality, we have used the definition of $\rho(t_s^k)$ in (2.7). This proves Claim (a).

We now prove Claim (b). First, we need to determine the dependence of t_s^{k+1} on t_s^k and Δ_k. Recall the triggering rule (2.5), which we express as $v(t_s^k)e^{-\sigma\Delta_k'} = |z(t_c^{k+})|e^{A(\Delta_k' - \Delta_k)} = v(t_s^k)|1 - e^{(A+\sigma)(t_s^k - q(t_s^k))}|e^{A\Delta_k'}$, where we have used the fact $\Delta_k' = t_s^{k+1} - t_s^k$ and (2.27). On simplification, we obtain

$$\Delta_k' = \mathfrak{h}(t_s^k - q(t_s^k)), \tag{2.35}$$

where, for convenience, we have defined $\mathfrak{h}(t) := -\frac{1}{A+\sigma}\ln(|1-e^{(A+\sigma)t}|)$. Notice that t_s^{k+1} depends only on t_s^k and not on Δ_k and. We show next that $t_s^k - q(t_s^k)$ uniquely determines $t_s^{k+1} - q(t_s^{k+1})$.

To show this, recall that according to the proof of Theorem 3, the quantization policy has the encoder divide the interval $[\iota b\gamma, (\iota+1)b\gamma]$ for some fixed ι uniformly into 2^{g-2} sub-intervals,

one of which includes t_s^k. The decoder chooses as $q(t_s^k)$ the middle point of the sub-interval that contains t_s^k. Thus, we have

$$q(t) = \left\lfloor \frac{t}{\delta} \right\rfloor \delta + \frac{\delta}{2}, \quad \delta = \frac{b\gamma}{2^{g-2}}. \tag{2.36}$$

Letting $y_k = t_s^k - q(t_s^k)$, we obtain

$$\begin{aligned} y_{k+1} &= t_s^k + \Delta_k' - q(t_s^k + \Delta_k') \\ &= y_k + \left\lfloor \frac{t_s^k}{\delta} \right\rfloor \delta + \Delta_k' - \left\lfloor \frac{y_k + \left\lfloor \frac{t_s^k}{\delta} \right\rfloor \delta + \frac{\delta}{2} + \Delta_k'}{\delta} \right\rfloor \delta \\ &= y_k + \mathfrak{h}(y_k) - \left\lfloor \frac{y_k + \frac{\delta}{2} + \mathfrak{h}(y_k)}{\delta} \right\rfloor \delta =: \mathcal{H}(y_k), \end{aligned}$$

where in the second step we have used $t_s^k = y_k + q(t_s^k)$ and (2.36), and in the third step we have used (2.35). From the conditions on g, we know that (2.30) is satisfied and hence $\mathcal{H}$ is a map from the interval $[-\frac{\delta}{2}, \frac{\delta}{2}]$ onto itself. We also notice that $\mathcal{H}$ is a piecewise continuous function. In fact, it is easy to verify that on $[-\frac{\delta}{2}, 0)$, the function is piecewise strictly increasing. Further, note that if $\mathcal{H}$ is discontinuous at $w < 0$, then the left limit of $\mathcal{H}$ at w is $\delta/2$ while the right limit of $\mathcal{H}$ at w is $-\delta/2$.

Next, (2.33) implies that

$$\ln(1 - e^{-(A+\sigma)\frac{\delta}{2}}) - \ln(1 - e^{-(A+\sigma)\frac{\delta}{4}}) \geq (A+\sigma)\frac{3\delta}{4},$$

which, after rearranging the terms, we see that it implies

$$-\frac{\delta}{4} + \mathfrak{h}\left(-\frac{\delta}{4}\right) \geq -\frac{\delta}{2} + \mathfrak{h}\left(-\frac{\delta}{2}\right) + \delta.$$

Now, observe that if $w_1, w_2 \in [-\frac{\delta}{2}, \frac{\delta}{2}]$ are such that $w_2 + \mathfrak{h}(w_2) = w_1 + \mathfrak{h}(w_1) + n\delta$ for some $n \in \mathbb{Z}$, then $\mathcal{H}(w_1) = \mathcal{H}(w_2)$. As a result, we conclude that there exists an interval $I \in [-\frac{\delta}{2}, -\frac{\delta}{4}]$

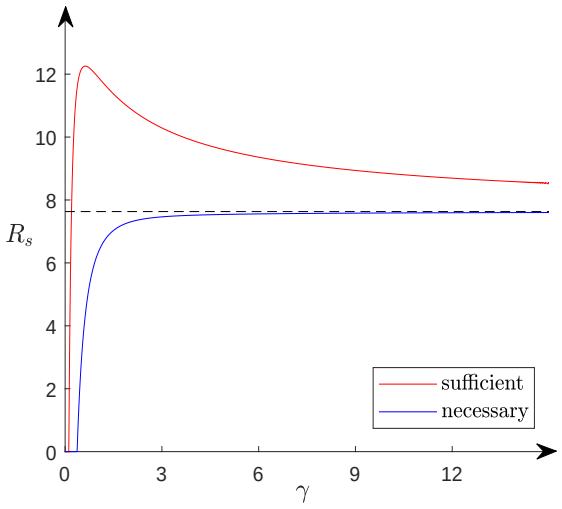


Figure 2.5: Comparison between the sufficient and necessary conditions. R_s is measured in bits/sec, and γ is measure in sec. Here, $A = 1.3$, $\sigma = 1$, $b = 1.0001$, and $\rho_0 = 0.9$. The dashed line represents the asymptote $((A+\sigma)/\ln 2)(1+A/\sigma) = 7.6319$.

such that the restriction $\mathcal{H} : I \to [-\frac{\delta}{2}, \frac{\delta}{2}]$ is continuous, one-to-one and onto. Hence the inverse mapping of this restriction is continuous and is a contraction and hence using the Banach contraction principle [153], there exists a fixed point of the original map $\mathcal{H}$ in I. Finally, note that as we sweep $z(0)$ through $(0, v(0)]$, t_s^1 varies continuously from ∞ to 0. Thus, there exists a $z(0)$ such that $y_1 = t_s^1 - q(t_s^1)$ is the fixed point in I. This proves Claim (b). ∎

Remark 6. We use the assumption in (2.33) in the proof of Theorem 4 to be able to apply the Banach contraction principle in establishing the existence of a suitable initial condition. We use the assumption $\nu \geq 2$ to ensure that the upper bound in (2.32) is well defined. •

Remark 7. Figure 2.5 illustrates the gap between the sufficient conditiont (2.29) and the supremum over σ of the necessary condition (2.23). For small values of γ, both conditions reduce to $R_s > 0$. As γ grows to infinity, both conditions converge to the same asymptote with value $\frac{A+\sigma}{\ln 2}(1 + \frac{A}{\sigma})$. While (2.24) reaches the asymptote monotonically increasing for all ρ_0 values, the sufficient condition has an overshoot behavior for larger values of ρ_0 as depicted in Figure 2.6.

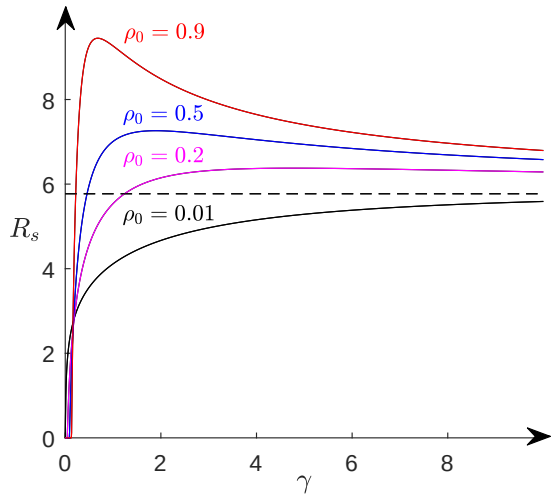


Figure 2.6: Illustration of the sufficient transmission rate for asymptotic observability versus the upper bound of delay for different values of ρ_0. R_s is measured in bits/sec, and γ is measure in sec. Here, $A = 1$, $\sigma = 1$, and $b = 1.0001$. The dashed line represents the asymptote $\mathrm{n}((A+\sigma)/\ln 2)(1 + A/\sigma) = 5.7708$.

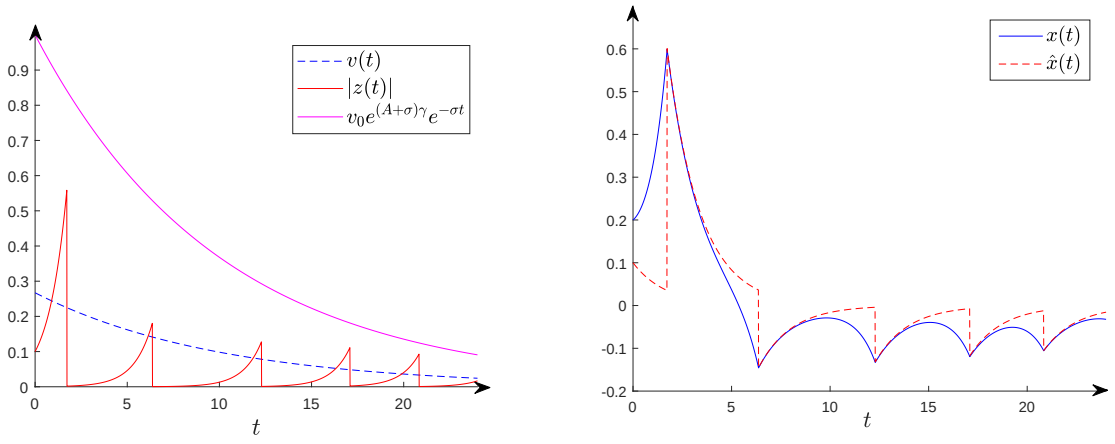
For intermediate values of γ, the gap can be explained noticing that the exact value of the communication delay is unknown to the sensor and the controller, and hence there can be a mismatch between the uncertainty sets at the controller and the sensor. In addition, the sensor and the controller lack a common reference frame for the quantization of the transmission time. •

2.4.4 Simulation

In this section, we illustrate an execution of our design for deriving the sufficient condition on the transmission rate. Using Theorem 3, we choose the size of the packet to be

$$g(t_s) = \max\left\{1, \lceil 1 + \log \frac{b\gamma(A+\sigma)}{\ln(1+\rho_0 e^{-(\sigma+A)\gamma})} \rceil \right\}, \tag{2.37}$$

where the ceiling operator ensures that the packet size is an integer number (we take the maximum between this quantity and 1 to make sure to send at least one bit of data payload at each



(a) (b)

Figure 2.7: An example realization of our design. (a) shows the evolution of the absolute value of the state estimation error, the value of the event-triggering function, and the upper bound on the state estimation error. (b) shows the corresponding evolution of the state and state estimation. The continuous-time dynamics is discretized with step size 0.0002. Because of this, a triggering happens when $z(t)$ becomes larger than the triggering function and there is no packet in the communication channel. In fact, since the sampling time is small, a triggering happens when $z(t)$ becomes approximately equal $v(t)$.

transmission).

We illustrate the execution of our design for the system

$$\dot{x}(t) = x(t) + 0.2u(t), \qquad u(t) = -8\hat{x}(t).$$

The event-triggering function is $v(t) = 0.2671e^{-0.1t}$. The upper bound on the communication delay is $\gamma = 1.2$. The design parameter are $b = 1.0001$, $\rho_0 = 0.1$, and the initial condition $x(0) = 0.2$, and $\hat{x}(0) = 0.1$. Figure 2.7(a) shows the evolution of the state estimation error. The triggering strategy ensures that the state estimation error $z(t)$ converges exponentially to zero and triggering occurs every time the state estimation error crosses the triggering function $v(t)$. The overshoots observed in the plot are due to the unknown delay in the communication channel. Clearly, $|z(t)|$ is upper bounded by $v_0 e^{(A+\sigma)\gamma} e^{-\sigma t} = e^{-0.1t}$. Figure 2.7(b) shows the corresponding

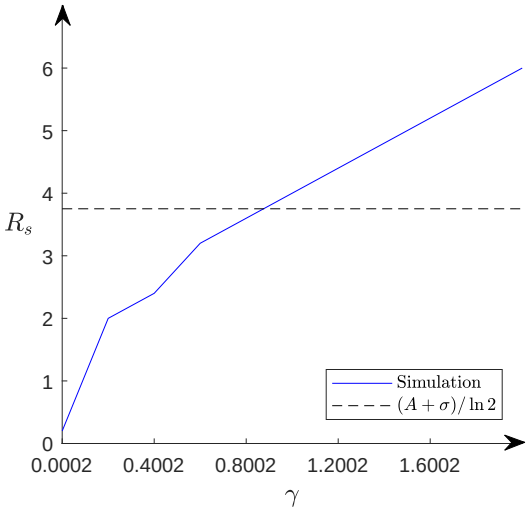


Figure 2.8: Information transmission rate versus the upper bound of the delay in the communication channel. R_s is measured in bits/sec, and γ is measured in sec. Here, $A = 2.4$, $B = 1$, $u(t) = -8\hat{x}(t)$, $\sigma = 0.2$, $b = 1.0001$, $\rho_0 = 0.1$, $v_0 = 0.0442$, $x(0) = 0.201$, and $\hat{x}(0) = 0.2$. The value of γ ranges from 0.0005 to 2.0005, in steps of 0.2. For each value of γ, we compute the transmission rate over an interval of 7 seconds of simulation.

evolution of $x(t)$ and $\hat{x}(t)$. The values of $x(t)$ and $\hat{x}(t)$ become close to each other at the reception times because of the jump strategy, while the distance between $x(t)$ and $\hat{x}(t)$ grows during the inter-reception interval.

Finally, Figure 2.8 shows the information transmission rate of a simulation versus the delay upper bound γ in the channel. The packet size is chosen according to (2.37). We calculate the information transmission rate by multiplying the packet size and the number of triggering events in the simulation time interval divided by its length. One can observe from the plot that, for small delay upper bound γ, the system is stabilized with an information transmission rate smaller than the data-rate theorem (3.75 bits/sec in this example). Instead, for larger γ, the transmission rate becomes greater than the threshold determined by the data-rate theorem.

2.5 Extension to vector systems

We generalize here our results to vector systems, building on the scalar case. Consider the plant-sensor-channel-controller tuple in Figure 2.1, and let the plant dynamics be described by a continuous-time, linear time-invariant (LTI) system

$$\dot{x} = Ax(t) + Bu(t), \tag{2.38}$$

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^m$ for $t \in [0, \infty)$ are the plant state and the control input, respectively. Here, $A \in M_{n,n}(\mathbb{R})$, $B \in M_{n,m}(\mathbb{R})$, and $\|x(0)\| < L$, where L is known to both sensor and controller. We assume all the eigenvalues of A are real. Without loss of generality, we also assume that they are positive (since stable modes do not need any actuation and we can disregard them). In this setting, the intrinsic entropy rate of the plant is

$$h_v = \frac{\mathrm{Tr}(A)}{\ln 2} = \frac{\sum_{i=1}^{n} \lambda_i}{\ln 2}. \tag{2.39}$$

Hence, to guarantee stability it is necessary for the controller to have access to state information at a rate

$$R_c \geq h_v.$$

Using the Jordan block decomposition [152], we can write the matrix $A \in M_{n,n}(\mathbb{R})$ as $\Phi\Psi\Phi^{-1}$, where Φ is a real-valued invertible matrix and $\Psi = \mathrm{diag}[J_1, \ldots, J_q]$, where each J_j is a Jordan block corresponding to the real-valued eigenvalue λ_j of A. We let p_j indicate the order of each Jordan block. For simplicity of exposition, we assume from here on that A is equal to its Jordan block decomposition, that is, $A = \mathrm{diag}[J_1, \ldots, J_q]$.

In the following, we deal with each state coordinate separately. This corresponds to treating the n-dimensional system as n scalar, coupled systems. When a triggering occurs for

one of the coordinates, the controller should be aware of which coordinate the received packet corresponds to. Accordingly, we assume there are n parallel finite-rate digital communication channels between each coordinate of the system and the controller, each subject to unknown, bounded delay.

We use the same notation of Section 2.2.1, but add subindex i and superindex j to specify the i^{th} coordinate of the j^{th} Jordan block. So, for instance, $\{t_{s,i}^{k,j}\}_{k\in\mathbb{N}}$, $\{t_{c,i}^{k,j}\}_{k\in\mathbb{N}}$, $g(t_{s,i}^{k,j})$ denote the sequences of transmission times, reception times, and number of bits that the sensor transmits at each triggering time. Similarly, the k^{th} *communication delay* $\Delta_{k,i}^{j}$ and k^{th} *triggering interval* $\Delta'^{j}_{k,i}$ can be specified for each coordinate. The communication delays for all coordinates are uniformly upper-bounded by γ, a non-negative real number known to both the sensor and the controller. The transmission rate for each coordinate is then

$$R_{s,i}^{j} = \limsup_{N_i^j\to\infty} \frac{\sum_{k=1}^{N_i^j} g(t_{s,i}^{k,j})}{\sum_{k=1}^{N_i^j} \Delta'^{j}_{k,i}}.$$

Assuming n parallel communication channels between the plant and the controller, each devoted to a coordinate separately, we have

$$R_s = \sum_{j=1}^{q}\sum_{i=1}^{p_j} R_{s,i}^{j}.$$

Using the same notation of Section 2.2.1, when referring to a generic triggering or reception time, we omit the superscript k.

The controller maintains an estimate $\hat{x}$ of the state, which evolves according to

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t), \tag{2.40}$$

during the inter-reception times. The *state estimation error* is $z(t) = x(t) - \hat{x}(t)$, which initially is set to $z(0) = x(0) - x_0$. For the i^{th} coordinate of the j^{th} Jordan block, we consider an

event-triggering function as in (2.4) with different initial values v_0^j for each coordinate, namely

$$v_i^j(t) = v_{0,i}^j e^{-\sigma t}. \tag{2.41}$$

For each coordinate, we employ the triggering rule (2.5) and the jump strategy (2.6). When a triggering occurs for the i^{th} coordinate of the j^{th} Jordan block, we assume that the sensor sends a packet large enough to ensure

$$|z_i^j(t_{c,i}^{j+})| \leq \rho_0 e^{-\sigma\gamma} v(t_{s,i}^j). \tag{2.42}$$

When referring to a generic Jordan block, we omit the superscript and subscript j.

Although each Jordan block is effectively independent of each other, the vector case is not an immediate extension of the scalar one. Specifically, from (2.38) and (2.40), we have that

$$\begin{aligned} \dot{z}_1(t) &= \lambda z_1(t) + z_2(t) \\ &\vdots \\ \dot{z}_{p-1}(t) &= \lambda z_{p-1}(t) + z_p(t) \\ \dot{z}_p(t) &= \lambda z_p(t), \end{aligned} \tag{2.43}$$

where p denotes the order of the Jordan block. This shows that the evolution of the coordinates is coupled and hence, even assuming parallel communication channels, care must be taken in generalizing the results for the scalar case.

Our first result generalizes Theorem 1 on the necessary condition for the information access rate.

Theorem 5. *Consider the plant-sensor-channel-controller model described in Section 2.2.1, with plant dynamics* (2.38)*, and state estimation error $z(t)$. Let $\sigma \in \mathbb{R}$ be positive, then the following*

necessary conditions hold:

1. *If the state estimation error satisfies*

$$\|z(t)\| \leq \|z(0)\| \, e^{-\sigma t},$$

then

$$b_c(t) \geq t \, \frac{\mathrm{Tr}(A) + n\sigma}{\ln 2} + n \, \log \frac{L}{\|z(0)\|}. \tag{2.44}$$

2. *If the system in* (2.38) *is stabilizable and*

$$\|x(t)\| \leq \|x(0)\| \, e^{-\sigma t},$$

then

$$b_c(t) \geq t \, \frac{\mathrm{Tr}(A) + n\sigma}{\ln 2}. \tag{2.45}$$

In both cases, the information access rate is

$$R_c > \frac{\mathrm{Tr}(A) + n\sigma}{\ln 2}. \tag{2.46}$$

Proof. Note that (2.46) immediately follows by dividing (2.44) and (2.45) by t and taking the limit for $t \to \infty$. Regarding (i), let us write the solution to (2.38) as

$$x(t) = e^{At}x(0) + \alpha(t), \quad \alpha(t) = e^{At} \int_0^t e^{-A\tau} B u(\tau) d\tau. \tag{2.47}$$

We then define,

$$\Gamma_t = \{x(t) : x(t) = e^{At}x(0) + \alpha(t)\ ;\ \|x(0)\| \leq L\}, \tag{2.48}$$

that is a set which represents the uncertainty at time t given the bound L on the norm of the initial condition $x(0)$ and $\alpha(t)$. The state of the system can be any point in this uncertainty set. We can find a lower bound on $b_c(t)$ by counting the number of balls of radius $\epsilon(t)$, that cover Γ_t, where $\epsilon(t) = \|z(0)\|\ e^{-\sigma t}$. The Lebesgue measure of a sphere of radius ϵ in $\mathbb{R}^n$ is $k_n\epsilon^n$ where k_n is a constant that changes with dimension. Therefore $b_c(t)$, the number of bits of information that the controller must have access to by time t, should satisfy

$$\begin{aligned} b_c(t) &\geq \log \frac{m(\Gamma_t)}{m(\mathcal{B}(\epsilon(t)))} \\ &= \log \frac{|\det((e^A)^t)| m(\|x(0)\| \leq L)}{k_d \|z(0)\|^n\ e^{-n\sigma t}} \\ &= t\ \log|\det(e^A)e^{n\sigma}| + \log \frac{L^n}{\|z(0)\|^n} \\ &= t\ \log|e^{\mathrm{Tr}(A)+n\sigma}| + n \log \frac{L}{\|z(0)\|}. \end{aligned}$$

With access to $b_c(t)$ bits of information, the controller can at best identify $x(t)$ up to a ball of radius $\epsilon(t)$. Consequently, (i) follows.

Recall that $\|x(0)\| \leq L$. For any given control trajectory $\{u(\tau)\}_{\tau=0}^{\tau=t}$ define

$$\Pi_{\{u(\tau)\}_{\tau=0}^{\tau=t}} = \{x(0) : \|x(t)\| < \epsilon(t)\},$$

where $\epsilon(t) = \|x(0)\|\ e^{-\sigma t}$. These are the sets of all initial conditions for which by choosing the control trajectory $\{u(\tau)\}_{\tau=0}^{\tau=t}$, the plant state at time t, $x(t)$, will be in a ball of radius $\epsilon(t)$. $x(t)$ depends linearly on $\{u(\tau)\}_{\tau=0}^{\tau=t}$. As a consequence, all of the sets $\Pi_{\{u(\tau)\}_{\tau=0}^{\tau=t}}$, are linear transformation of each other. So, the measure of all of them are upper bounded by

$|\det(e^{-At})k_n\|x(0)\|^n e^{-n\sigma t}| = k_n\|x(0)\|^n e^{-(\mathrm{Tr}(A)+n\sigma)t}$. We can then determine a lower bound for $b_c(t)$ by counting the number of Π sets (for different control trajectories $\{u(\tau)\}_{\tau=0}^{\tau=t}$) which takes to cover the ball $\|x(0)\| \leq L$.

Thus, the controller must have access to at least $b_c(t)$ bits by time t, where

$$\begin{aligned} b_c(t) &\geq \log \frac{m(\|x(0)\| \leq L)}{m(\Pi)} \\ &= \log \frac{k_n L^n}{k_n\|x(0)\|^n e^{-(\mathrm{Tr}(A)+n\sigma)t}} \\ &= t\ \frac{\mathrm{Tr}(A)+n\sigma}{\ln 2} + n\ \log \frac{L}{\|x(0)\|}, \end{aligned}$$

and this proves (ii). ∎

We next generalize the necessary condition on the information transmission rate. If A is diagonalizable, then the necessary and sufficient bit rate for the vector system is equal to the sum of the necessary and sufficient bit rates that we provide in Section 2.4 for each coordinate of the system. We now generalize this idea to any matrix with real eigenvalues.

Theorem 6. *Consider the plant-sensor-channel-controller model with plant dynamics* (2.38)*, where all eigenvalues of A are real, estimator dynamics* (2.40)*, event-triggering strategy* (2.5)*, event-triggering function* (2.41)*, and packet sizes such that $z_i^j(t_{c,i}^{k,j})$ is determined at the controller within a ball of radius $\rho(t_{s,i}^{k,j}) = \rho_0 e^{-\sigma\gamma} v(t_{s,i}^{k,j})$ with ν-precision, ensuring* (2.42) *via the jump strategy* (2.6) *for all $k \in \mathbb{N}$, $i = 1, \ldots, p_j$, and $j = 1, \ldots, q$. Then, there exists a delay realization and initial condition, such that*

$$R_s \geq \sum_{j=1}^{q} \frac{p_j(\lambda_j + \sigma)}{\ln \nu + \ln(2 + \frac{e^{\sigma\gamma}}{\rho_0})} \max\left\{0, \log \frac{(e^{\lambda_j \gamma} - 1)}{\rho_0 e^{-\sigma\gamma}}\right\}.$$

Proof. Since there is no coupling across different Jordan blocks in (2.38), the inherent entropy

rate (2.39) is

$$h_v(A) = h_v(J_1) + \cdots + h_v(J_q).$$

Therefore, it is enough to prove the result for one of the Jordan blocks. Let J be a Jordan block of order p with associated eigenvalue λ. Note that the part of the vector $z(t)$ which corresponds to J is governed by (2.43). The solution of the first differential equation in (2.43) is

$$z_1(t) = e^{\lambda t} z_1(0) + e^{\lambda t} \int_0^t e^{-\lambda \tau} z_2(\tau) d\tau.$$

If for the first coordinate a triggering event occurs at time $t_{s,1}$, then $z_1(t_{c,1})$ belongs to the set

$$\begin{aligned}\Omega(z(t_{c,1})|t_{s,1}) = \{y = y_1 + y_2 : y_1 = \pm v_1(t_{s,1}) e^{\lambda(t_{c,1} - t_{s,1})},\\ y_2 = \int_{t_{s,1}}^{t_{c,1}} e^{\lambda(t_{c,1}-\tau)} z_2(\tau) d\tau;\ t_{c,1} \in [t_{s,1}, t_{s,1} + \gamma],\\ z_2(\tau) \in \zeta_\tau^{s,2} \ \text{ for } \tau \in [t_{s,1}, t_{c,1}]\},\end{aligned}$$

where $\zeta_\tau^{s,2}$ is the uncertainty set for $z_2(\tau)$ at the sensor. We define

$$Y_1 = \{y_1 : y_1 = \pm v(t_{s,1}) e^{\lambda(t_{c,1} - t_{s,1})}, t_{c,1} \in [t_{s,1}, t_{s,1} + \gamma]\},$$

which is the uncertainty set of $z_1(t_{c,1})$ given $t_{s,1}$ for the differential equation $\dot{z}_1 = \lambda z_1$. By comparing the definitions of the sets $\Omega(z(t_{c,1})|t_{s,1})$ and Y_1, we have

$$m(\Omega(z(t_{c,1})|t_{s,1})) \geq m(Y_1).$$

Finally, we apply Lemmas 2 and 4 for each coordinate separately, so that the necessary bit rate

for each must satisfy

$$R_{s,i} \geq \frac{\lambda + \sigma}{\ln \nu + \ln(2 + \frac{e^{\sigma\gamma}}{\rho_0})} \max \left\{ 0, \log \frac{(e^{\lambda\gamma} - 1)}{\rho_0 e^{-\sigma\gamma}} \right\}$$

for $i = 1, \ldots, p$. The result now follows. ∎

Note that, when $\rho_0 \ll e^{\sigma\gamma} / \max\{2, \nu\}$, the result in Theorem 6 can be simplified to

$$R_s \geq \sum_{j=1}^{q} \frac{p_j(\lambda_j + \sigma)}{\ln 2} \max \left\{ 0, 1 + \frac{\log(e^{\lambda_j\gamma} - 1)}{-\log(\rho_0 e^{-\sigma\gamma})} \right\}.$$

Our next result generalizes the sufficient condition of Theorem 3 to vector systems.

Theorem 7. *Consider the plant-sensor-channel-controller model with plant dynamics* (2.38)*, where all eigenvalues of A are real, estimator dynamics* (2.40)*, event-triggering strategy* (2.5)*, and event-triggering function* (2.41)*. For the j^{th} Jordan block choose the following sequence of design parameters*

$$0 < \rho_1^j < \ldots < \rho_{p_j - 1}^j < \rho_{p_j}^j = \rho_0 < 1.$$

If the state estimation error satisfies $|z_i^j(0)| \leq v_{0,i}^j$, then we can achieve (2.42) *and*

$$|z_i^j(t)| \leq v_{0,i}^j((\rho_0 - \rho_i^j) + e^{(\lambda_j + \sigma)\gamma}) e^{-\sigma t}$$

for $i = 1, \ldots, p_j$ and $j = 1, \ldots, q$, with an information transmission rate, R_s, at least equal to

$$\sum_{j=1}^{j=q} \sum_{i=1}^{i=p_j} \frac{(\lambda_j + \sigma)}{-\ln(\rho_0 e^{-\sigma\gamma})} \max \left(0, 1 + \log \frac{b\gamma(\lambda_j + \sigma)}{\ln(1 + \rho_i^j e^{-(\sigma + \lambda_j)\gamma})} \right),$$

where

$$0 < v_{0,i}^j \leq \frac{v_{0,i-1}^j(\lambda_j+\sigma)(\rho_0-\rho_i^j)}{((\rho_0-\rho_i^j)+e^{(\lambda_j+\sigma)\gamma})(e^{(\lambda_j+\sigma)\gamma}-1)}, \tag{2.49}$$

for $i = 2, \ldots, p_j$ *and* $j = 1, \ldots, q$, *and* $b > 1$.

Proof. It is enough to prove the result for one Jordan block. The solution of the last two equations in (2.43) is

$$\begin{aligned} z_{p-1}(t) &= e^{\lambda t} z_{p-1}(0) + e^{\lambda t} \int_0^t e^{-\lambda\tau} z_p(\tau) d\tau, \\ z_p(t) &= e^{\lambda t} z_p(0). \end{aligned} \tag{2.50}$$

The differential equation that governs $z_p(t)$ is similar to what we considered in Theorem 3. It follows that if the transmission rate for coordinate p is lower bounded as (2.29) and $|z_p(0)| \leq v_{0,p}$, then we can ensure $|z_p(t)| \leq v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\lambda t}$.

Assume now that a triggering happens for coordinate $p-1$ at time $t_{s,p-1}$, namely $|z_{p-1}(t_{s,p-1})| = v(t_{s,p-1})$, and the controller receives the packet related to coordinate $p-1$ at time $t_{c,p-1}$. Then the uncertainty set for $z_{p-1}(t_{c,p-1})$ at the controller is

$$\begin{aligned} \Omega(z(t_{c,p-1})|t_{c,p-1}) = \{ & w_{p-1} = w_{p-1}^{(1)} + w_{p-1}^{(2)} : \\ & w_{p-1}^{(1)} = \pm v_{p-1}(\bar{t}_{r,p-1}) e^{\lambda(t_{c,p-1}-\bar{t}_{r,p-1})}, \\ & w_{p-1}^{(2)} = \int_{\bar{t}_{r,p-1}}^{t_{c,p-1}} e^{\lambda(t_{c,p-1}-\tau)} z_p(\tau) d\tau; \\ & \bar{t}_{r,p-1} \in [t_{c,p} - \gamma, t_{c,p-1}], \\ & z_p(\tau) \in \zeta_\tau^{c,p} \text{ for } \tau \in [\bar{t}_{r,p-1}, t_{c,p-1}] \}, \end{aligned} \tag{2.51}$$

where $\zeta_\tau^{c,p}$ is the uncertainty set for $z_p(\tau)$ at the controller. Clearly, the measure of $\Omega(z(t_{c,p-1})|t_{c,p-1})$

is larger when $w_{p-1}^{(1)}$ and $w_{p-1}^{(2)}$ in (2.51) have the same sign. Hence, we can assume that $z_{p-1}(\bar{t}_{r,p-1})$ and $z_p(\tau)$ for $\tau \in [\bar{t}_{r,p-1}, t_{c,p-1}]$ and $\bar{t}_{r,p-1} \in [t_{c,p-1} - \gamma, t_{c,p-1}]$ are positive. Define

$$\begin{aligned} W_{p-1} = \{w_{p-1} = w_{p-1}^{(1)} + w_{p-1}^{(2)} : \\ w_{p-1}^{(1)} = \pm v_{p-1}(\bar{t}_{r,p-1}) e^{A(t_{c,p-1} - \bar{t}_{r,p-1})}, \\ w_{p-1}^{(2)} = \int_{\bar{t}_{r,p-1}}^{t_{c,p-1}} e^{\lambda(t_{c,p-1} - \tau)} z_p(\tau) d\tau; \\ \bar{t}_{r,p-1} \in [t_{c,p} - \gamma, t_{c,p-1}], \\ |z_p(\tau)| \leq v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\sigma\tau} \text{ for } \tau \in [\bar{t}_{r,p-1}, t_{c,p-1}]\}. \end{aligned}$$

Clearly, we have

$$m(\Omega(z(t_{c,p-1})|t_{c,p-1})) \leq m(W_{p-1}). \tag{2.52}$$

Hence, a sufficient condition for W_{p-1} will also be a sufficient condition for $\Omega(z(t_{c,p-1})|t_{c,p-1})$. We note that W_{p-1} is the Brunn-Minkowski sum of the following sets

$$\begin{aligned} W_{p-1}^{(1)} = \{w_{p-1}^{(1)} : w_{p-1}^{(1)} = \pm v_{p-1}(\bar{t}_{r,p-1}) e^{A(t_{c,p-1} - \bar{t}_{r,p-1})}, \\ \bar{t}_{r,p-1} \in [t_{c,p} - \gamma, t_{c,p-1}]\} \\ W_{p-1}^{(2)} = \{w_{p-1}^{(2)} : w_{p-1}^{(2)} = \int_{\bar{t}_{r,p-1}}^{t_{c,p-1}} e^{\lambda(t_{c,p-1} - \tau)} z_p(\tau) d\tau; \\ |z_p(\tau)| \leq v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\sigma\tau} \text{ for } \tau \in [\bar{t}_{r,p-1}, t_{c,p-1}], \\ \bar{t}_{r,p-1} \in [t_{c,p} - \gamma, t_{c,p-1}]\}. \end{aligned}$$

By the Brunn-Minkowski inequality [62], we have

$$m(W_{p-1}) \geq m(W_{p-1}^{(1)}) + m(W_{p-1}^{(2)}).$$

The operators in the definition of $W_{p-1}^{(1)}$ and $W_{p-1}^{(2)}$ are continuous and the operator in the definition of $W_{p-1}^{(2)}$ is integral. Hence, even if during the time interval $[\bar{t}_{r,p-1}, t_{c,p-1}]$ the value of $z_p(\tau)$ jumps according to (2.6), $W_{p-1}^{(2)}$ remains a connected compact set. Therefore, $W_{p-1}^{(1)}$ and $W_{p-1}^{(2)}$ are closed intervals that are translation and dilation of each other. In this case, the inequality (2.5) is tight [98], and by (2.52) we have

$$m(\Omega(z(t_{c,p-1})|t_{c,p-1})) \leq m(W_{p-1}^{(1)}) + m(W_{p-1}^{(2)}). \tag{2.53}$$

This allows us to deal with each coordinate, $p-1$ and p, separately as follows. If there is no coupling in the differential equation that governs $z_{p-1}(t)$, we have

$$\dot{z}_{p-1}(t) = \lambda z_{p-1}(t).$$

Using Theorem 3, and equation (2.53) with the rate

$$R_{s,p-1} \geq \tag{2.54}$$
$$\frac{\lambda+\sigma}{-\ln(\rho_{p-1}e^{-\sigma\gamma})} \max\left\{0, 1+\log\frac{b\gamma(\lambda+\sigma)}{\ln(1+\rho_{p-1}e^{-(\sigma+\lambda)\gamma})}\right\},$$

we can ensure

$$\Upsilon^c_{t^+_{c,p-1}} \leq \rho_{p-1} v_{p-1}(t_{c,p-1}) + m(W_{p-1}^{(2)}), \tag{2.55}$$

where $\Upsilon^c_{t^+_{c,p-1}}$ is the uncertainty set for $z_{p-1}(t^+_{c,p-1})$ at the controller.

We now find an upper bound for $m(W_{p-1}^{(2)})$ as follows. Since, $R_{s,p}$ is lower bounded

as (2.29), we can ensure $|z_p(t)| \leq v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\sigma t}$, and

$$\begin{aligned} m(W_{p-1}^{(2)}) &= \int_{t_{c,p-1}-\gamma}^{t_{c,p-1}} e^{\lambda(t_{c,p-1}-\tau)} z_p(\tau) d\tau \\ &\leq v_{0,p} e^{(\sigma+\lambda)\gamma} e^{\lambda t_{c,p-1}} \int_{t_{c,p-1}-\gamma}^{t_{c,p-1}} e^{-(\lambda+\sigma)\tau} d\tau \\ &= \frac{v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\sigma t_{c,p-1}}}{\lambda+\sigma} (e^{(\lambda+\sigma)\gamma} - 1). \end{aligned} \tag{2.56}$$

From (2.49), we have

$$v_{0,p} \leq \frac{v_{0,p-1}(\lambda+\sigma)(\rho_0 - \rho_{p-1})}{e^{(\lambda+\sigma)\gamma}(e^{(\lambda+\sigma)\gamma} - 1)}.$$

Hence,

$$\begin{aligned} \frac{v_{0,p} e^{(\sigma+\lambda)\gamma} e^{-\sigma t_{c,p-1}}}{\lambda+\sigma} (e^{(\lambda+\sigma)\gamma} - 1) &\leq (\rho_0 - \rho_{p-1}) v_{0,p-1} e^{-\sigma t_{c,p-1}} \\ &= (\rho_0 - \rho_{p-1}) v_{p-1}(t_{c,p-1}). \end{aligned}$$

Consequently, from (2.56) we have

$$m(W_{p-1}^{(2)}) \leq (\rho_0 - \rho_{p-1}) v_{p-1}(t). \tag{2.57}$$

Therefore, using (2.55) and (2.57) we have $m(\Upsilon_{t_{c,p-1}^+}^c) \leq \rho_0 v_{p-1}(t_{c,p-1})$ and $|z_{p-1}(t_c^+)| \leq \rho_0 v_{p-1}(t_{c,p-1})$. When $R_{s,p}$ is lower bounded as (2.29) and $R_{s,p-1}$ is lower bounded as (2.54), we can ensure

$$|z_{p-1}(t)| \leq ((\rho_0 - \rho_{p-1}) + e^{(\lambda+\sigma)\gamma}) v_{p-1}(t_{c,p-1})$$

because the solution of the differential equation that governs z_{p-1} is given in (2.50), and us-

ing (2.57) we have

$$
\begin{aligned}
&|z(t_{c,p-1})| \leq \\
&v_{p-1}(t_{c,p-1}-\gamma)e^{\lambda\gamma} + (\rho_0 - \rho_{p-1})v_{p-1}(t_{c,p-1}) \\
&= ((\rho_0 - \rho_{p-1}) + e^{(\lambda+\sigma)\gamma})v_{p-1}(t_{c,p-1}).
\end{aligned}
$$

With the same procedure we can find the sufficient rate $R_{s,i}$ for $i = p-2, \ldots, 1$, and this concludes the proof. ∎

Remark 8. In a Jordan block of order p_j, the inequality (2.49) provides an upper bound on the value of the triggering function for coordinate i using the value of the triggering function for coordinate $i-1$, where $i = 2, \ldots, p_j$. This is a natural consequence of the coupling among the coordinates in a Jordan block, cf. (2.43), which makes the error in coordinate i affect the error in coordinates 1 to $i-1$, for each $i = 2, \ldots, p_j$. •

Corollary 1 can be generalized, provided (A, B) is stabilizable, using a linear control $u(t) = -K\hat{x}(t)$ with $A - BK$ Hurwitz. This is a consequence of Theorem 7 which guarantees that, using the stated communication rate, the state estimation error for each coordinate converges to zero exponentially fast.

Remark 9. In our discussion, we have assumed that $\hat{x}(t)$ is known to both controller and sensor. Since the sensor has access to the state, using the system dynamics, it can deduce $u(t)$, and then obtain $\hat{x}(t)$, cf. [164]. Note that the controller design for our sufficient condition is linear $u(t) = -K\hat{x}(t)$, and thus the sensor can deduce $\hat{x}(t)$ assuming that BK is invertible. Alternatively, the controller can directly signal the acknowledgment of the reception of the packet (and as a result t_c^k) to the sensor by applying a control input to the system that excites a specific frequency of the state each time a symbol has been received, and the sensor can construct $\hat{x}(t)$ at all time t if it knows the decoding rule at the controller. On the other hand, assuming knowledge

of $\hat{x}(t)$ at the sensor does not affect the generality of the necessary condition. •

2.6 Time-triggering versus event-triggering control over communication channels

In this section, we compare the presented event-triggered results with those of a time-triggered implementation, for which we provide a formulation of the data-rate theorem for continuous-time systems in the presence of delay. This comparison leads to additional insights on the value of information in event triggering.

We now derive a data-rate theorem for the information transmission rate in two different time-triggered scenarios and in the presence of unknown communication delays.

In the first scenario, we assume the following time-triggered implementation: the sensor transmits at all times $\{t_s^k\}_{k\in\mathbb{N}}$, where

$$t_s^k = kT, \tag{2.58}$$

and T denotes the transmission period. Note that in this setting, the sensor transmits without considering whether the previous packets have been received and decoded or not. Consequently, the communication delay is upper bounded as (2.2) only when there is not another packet in the communication channel. In this setting, we have the following theorem.

Theorem 8. *Consider the plant-sensor-channel-controller model described in Section 2.2.1 with plant dynamics* (2.1)*. Assume that the communication delays upper bounded as* (2.2) *when there is no other packet in the channel, and assuming that the packets are received and decoded by the controller in the order they are transmitted by the sensor. Then, there exists a delay realization*

$\{\Delta_k\}_{k\in\mathbb{Z}}$ *such that a rate*

$$R_s > \begin{cases} \dfrac{\mathrm{Tr}(A)}{\ln 2} & \text{if } \gamma < T, \\ \dfrac{\mathrm{Tr}(A)\frac{\gamma}{T}}{\ln 2} & \text{if } \gamma \geq T. \end{cases}$$

is necessary for asymptotic observability and asymptotic stabilizability.

Proof. Consider an observer that can receive the packets transmitted by the sensor without any delay, and that has the same knowledge about the system as the controller. Let ζ_t^o and ζ_t^c be the uncertainty sets for the state $x(t)$, at the observer and controller, respectively. We have $\zeta_0^o = \zeta_0^c$.

We write the solution to (2.1) as As a consequence, we have

$$m(\zeta^o_{t_s^{(k+1)-}}) = e^{\mathrm{Tr}(A)T} m(\zeta^o_{t_s^k}).$$

Since the observer receives packets without delay, we have

$$m(\zeta^o_{t_s^{k+1}}) \geq \frac{1}{2^{g(t_s^k)}} m(\zeta^o_{t_s^{(k+1)-}}) = \frac{1}{2^{g(t_s^k)}} e^{\mathrm{Tr}(A)T} m(\zeta^o_{t_s^k}).$$

By iterating from $k = 1$ to $k = \eta$, we have

$$m(\zeta^o_{t_s^{\eta-}}) \geq \frac{1}{2^{\sum_{k=1}^{k=\eta-1} g(t_s^k)}} e^{\mathrm{Tr}(A)\eta T} m(\zeta_0^o).$$

However, the controller does not necessarily receive packets immediately. Indeed, in the worst case, if $\gamma > T$ the controller receives packets that have been sent in the time interval $[0, \eta T)$ by

the time $\eta T + \eta(\gamma - T) = \eta\gamma$. While, for $T > \gamma$ we have

$$m(\zeta^c_{t_c^{\eta-}}) \geq m(\zeta^o_{t_s^{\eta-}}), \tag{2.59}$$

for $T \leq \gamma$ we have

$$\sup_{\{\Delta_k\}\leq\gamma} m(\zeta^c_{t_c^{\eta-}}) \geq m(\zeta^o_{t_s^{\eta-}}) e^{\mathrm{Tr}(A)\eta(\gamma-T)}. \tag{2.60}$$

It follows that the right-hand side of (2.59) and (2.60) tends to infinity as $\eta \to \infty$, making it impossible to stabilize or track the state, if

$$\begin{aligned}\infty &= \lim_{\eta\to\infty} \frac{1}{2^{\sum_{k=1}^{k=\eta-1} g(t_s^k)}} e^{\mathrm{Tr}(A)\eta T} \\ &= \lim_{\eta\to\infty} \exp\left\{ T\eta \left(\mathrm{Tr}(A) - \ln 2 \frac{\sum_{k=1}^{k=\eta-1} g(t_s^k)}{T\eta} \right) \right\}\end{aligned}$$

for $T > \gamma$, and

$$\begin{aligned}\infty &= \lim_{\eta\to\infty} \frac{1}{2^{\sum_{k=1}^{k=\eta-1} g(t_s^k)}} e^{\mathrm{Tr}(A)\eta\gamma} \\ &= \lim_{\eta\to\infty} \exp\left\{ T\eta \left(\mathrm{Tr}(A)\frac{\gamma}{T} - \ln 2 \frac{\sum_{k=1}^{k=\eta-1} g(t_s^k)}{T\eta} \right) \right\}\end{aligned}$$

for $T < \gamma$. The result now follows. ∎

Remark 10. *Theorem 8 provides a data-rate theorem for the information transmission rate without imposing exponential convergence guarantees. It shows the existence of a critical delay value $\gamma = T$, at which the rate begins to increase linearly with the delay.* •

We next consider a different time-triggered scenario. Let

$$t_s^0 = 0, \quad t_s^{k+1} = t_s^k + (\lfloor \Delta_k/T \rfloor + 1)T, \tag{2.61}$$

where T is a fixed non-negative real number. In this case, the sensor transmits only at integer multiples of the period T, after the previous packet is received. It follows that there is no delay accumulation, and for all packets the delay satisfies (2.2). In this setting, we have the following result for exponential convergence of the estimation error to zero.

Theorem 9. *Consider the plant-sensor-channel-controller model described in Section 2.2.1 with plant dynamics* (2.1)*, and state estimation error $z(t)$. Let $\sigma \in \mathbb{R}$ be positive. If using the time-triggered implementation* (2.61) *the state estimation error satisfies*

$$\|z(t_s^k)\| \leq \|z(0)\| \, e^{-\sigma t_s^k}, \tag{2.62}$$

for all $k \in \mathbb{Z}$, then there exists a delay realization $\{\Delta_k\}_{k\in\mathbb{Z}}$ which requires

$$R_s \geq \frac{(\mathrm{Tr}(A) + n\sigma)(\lfloor \frac{\gamma}{T} \rfloor + 1)}{\ln 2}. \tag{2.63}$$

Proof. Using (2.47) we know the state of the system can be any point in Γ_t, cf. (2.48), then, we have

$$m(\Gamma_{t_c^k}) = e^{\mathrm{Tr}(A)\Delta_k} m(\Gamma_{t_s^k}),$$

and

$$m(\Gamma_{t_s^{k+1}}) \geq m(\Gamma_{t_c^k}) e^{\mathrm{Tr}(A)\left((\lfloor \frac{\Delta_k}{T} \rfloor + 1)T - \Delta_k\right)}.$$

Iterating from $k = 0$ to $k = \eta$, we have

$$m(\Gamma_{t_s^{\eta-}}) \geq e^{\sum_{k=0}^{k=\eta-1} \mathrm{Tr}(A)(\lfloor \frac{\Delta_k}{T} \rfloor + 1)T} m(\zeta_0) = e^{\mathrm{Tr}(A) t_s^\eta} m(\zeta_0).$$

We can now obtain a lower bound on $\sum_{k=0}^{k=\eta-1} g(t_s^k)$ by counting the number of balls of radius $\|z(0)\|\, e^{-\sigma t_s^\eta}$, that cover $\Gamma_{t_s^{\eta-}}$. Recall that the Lebesgue measure of a sphere of radius r in $\mathbb{R}^n$ is $k_n r^n$ where k_n is a constant that depends on the dimension. We have

$$\begin{aligned}\sum_{k=0}^{k=\eta-1} g(t_s^k) &\geq \log \frac{e^{\mathrm{Tr}(A)t_s^\eta} m(\zeta_0)}{k_n \|z(0)\|^n\, e^{-n\sigma t_s^\eta}} \\ &= \log \frac{e^{(\mathrm{Tr}(A)+n\sigma)t_s^\eta} m(\zeta_0)}{k_n \|z(0)\|^n}.\end{aligned}$$

Hence,

$$\sum_{k=0}^{k=\eta-1} g(t_s^k) \geq \log \frac{e^{(\mathrm{Tr}(A)+n\sigma)\eta(\lfloor \frac{\gamma}{T} \rfloor+1)T} m(\zeta_0)}{k_n \|z(0)\|^n},$$

because the sensor, not having any fore-knowledge of the delay, must send at least the number of bits required when $\Delta_k = \gamma$ for all $k \in \mathbb{Z}$, to ensure that (2.62) holds. However, the actual realization of the delay may be $\Delta_k = 0$ for all $k \in \mathbb{Z}$, so that we have

$$R_s \geq \lim_{\eta\to\infty} \frac{1}{\eta T} \log \frac{e^{(\mathrm{Tr}(A)+n\sigma)\eta(\lfloor \frac{\gamma}{T} \rfloor+1)T} m(\zeta_0)}{k_n \|z(0)\|^n},$$

and the result follows. ∎

Remark 11. *In the time-triggered setting governed by* (2.58)*, a packet is transmitted without considering whether the previous packets have been received and decoded. On the other hand, in the time-triggered setting governed by* (2.61) *a packet is transmitted only after the previous packet is received. Letting $\sigma \to 0$, for $\gamma < T$ both Theorems 8 and 9 reduce to $R_s \geq \mathrm{Tr}(A)/\ln 2$. Namely, for low values of the delay, and without imposing exponential convergence guarantees, we recover the critical value of the data-rate theorem for the access rate in Theorem 1.* •

Figure 2.9 compares the results of Theorem 9 and Theorem 2. For small values of γ, the necessary

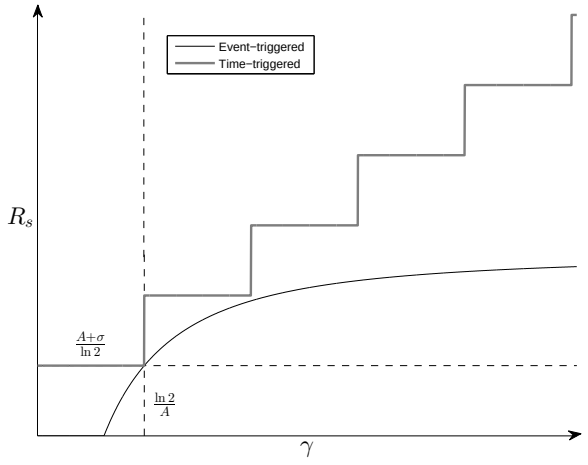


Figure 2.9: Illustration of the necessary bit rate for time-triggering control of a scalar plant (2.63) and approximation of the necessary bit rate for event-triggering control of a scalar plant (2.24) versus the worst-case delay in the communication channel. For the time-triggered scheme, $T = \ln 2/A$.

transmission rate in Theorem 4 becomes,

$$R_s \geq 0. \tag{2.64}$$

On the other hand, the result of Theorem 9 in the scalar case and for small values of γ can be written as

$$R_s \geq \frac{A+\sigma}{\ln 2}. \tag{2.65}$$

Comparing (2.64) and (2.65), the value of the intrinsic timing information in communication in an event-triggered design becomes evident. When the delay is small, the timing information carried by the triggering events is substantial and ensures that controller can stabilize the system. In contrast, for small values of the delay the information transmission rate required by a time-triggered implementation equals the information access rate required by the classic data-rate theorem.

For large delay values, it can be easily shown that while both the necessary and sufficient conditions for the event-triggered design in Theorems 2 and 3 converge to the asymptote $((A+\sigma)/\ln 2)(1+A/\sigma)$ as $\gamma \to \infty$, the time-triggered result in Theorem 9 for grows linearly as $\gamma \to \infty$. The reason for this difference is that the time-triggered design (2.61) depends only on the delay while the event-triggered scheme depends on both state and delay. In both time-triggered and event-triggered schemes the sensor does not have fore-knowledge of the delay, and the sensor needs to send larger packets when the worst-case delay is larger. On the other hand, the triggering rate in the event-triggering case tends to zero as γ tends to infinity. More precisely, using Lemma 3 in the event-triggering setting for all of the possible realizations we have

$$t_s^{k+1} - t_s^k \geq \frac{-\ln(\rho_0 e^{-\sigma\gamma})}{A+\sigma},$$

which tends to infinity as $\gamma \to \infty$. In contrast, in the time-triggered case for delay realization $\Delta_k = 0$ for all $k \in \mathbb{Z}$ we have

$$t_s^{k+1} - t_s^k = T,$$

and in this case the rate increases linearly with the delay.

2.7 Conclusions

In this chapter, we have studied event-triggered control strategies for stabilization and exponential observability of linear plants in the presence of unknown bounded delay in the communication channel between the sensor and the controller. Our study has been centered on quantifying the value of the timing information implicit in the triggering events. We have identified a necessary and a sufficient condition on the transmission rate required to guarantee stabilizability and observability of the system for a given event triggering strategy. Our results

reveal a phase transition behavior as a function of the maximum delay in the communication channel, where for small delays, a positive transmission rate ensures the control objective is met, while for large delays, the necessary transmission rate is larger than that of classical data-rate theorems with periodic communication and no delay. We also compared our event-triggered results with two time-triggered designs.

Future research will consider additional errors in the communication channel not caused by quantization, extensions to the case when the communication delay is a function of thepacket size, replacing the Assumption 1 with packet size constraints, and the study of other event-triggering strategies.

Chapter 2, in full, is a reprint of the material as it appears in M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "The value of timing information in event-triggered control," *IEEE Transactions on Automatic Control*, in press, and M. J. Khojasteh, P. Tallapragada, J. Cortés, M. Franceschetti, "Time-triggering versus event-triggering control over communication channels," In *Proc. IEEE 56th Annual Conference on Decision and Control (CDC)*, 2017. The dissertation author was the primary investigator and author of this paper.

Chapter 3

Event-triggered stabilization over digital channels of systems with disturbances

3.1 Introduction

For many cyber-physical systems, the feedback loop is closed over a communication channel [97]. In this context, data-rate theorems state that the minimum communication rate to achieve stabilization is equal to the *entropy rate* of the plant, expressed by the sum of the unstable modes in nats (one nat corresponds to $1/\ln 2$ bits.) Key contributions by [191], [141], and [112] consider a "bit-pipe" communication channel, capable of noiseless transmission of a finite number of bits per unit time evolution of the plant. Extensions to noisy communication channels are considered in [123, 164, 212]. Stabilization over time-varying bit-pipe channels, including the erasure channel as a special case, are studied by [132]. Additional formulations include stabilization of switched linear systems [114], uncertain systems [156], multiplicative noise [46], optimal control [83, 101], and stabilization using event-triggered strategies [42, 87, 91, 92, 95, 108, 119, 147, 189].

A similar data-rate theorem formulation also holds for nonlinear systems. The works [36,

115, 142] for nonlinear systems are restricted to plants without disturbances and with a bit-pipe communication channel. The work [142] uses the entropy of topological dynamical systems to elegantly determine necessary and sufficient bit rates for local uniform asymptotic stability. Consequently, the results are only local and derived under restrictive assumptions. Under appropriate assumptions, the work [115] extends to nonlinear but locally Lipschitz systems, the zoom-in/zoom-out strategy of [112]. The sufficient condition proposed in this work is, however, conservative, and does not match the necessary condition proposed in [142]. The work [174] further extend the results in [115] to linear systems with uncertainty and under appropriate assumptions to nonlinear systems with disturbances. Inspired by the Jordan block decomposition employed in [191] to design an encoder/decoder pair of a vector system, the work [36] provides a sufficient design for feed-forward dynamics that matches the necessary condition proposed in [142]. The recent work in [166] studies the estimation of a nonlinear system over noisy communication channels, providing a necessary condition over memoryless communication channels and a sufficient condition in case of additive white Gaussian noise channel.

While the majority of communication systems transmit information by adjusting the content of the message, it is also possible to communicate information by adjusting the transmission time of a symbol [2]. In Chapter 4 we will study the fundamental limitations of using timing information for stabilization and show that it is possible to stabilize a plant using inherent information in the timing of the transmissions. In fact, it is known that event-triggering control techniques encode information in the timing in a state-dependent fashion. The work [99] shows that, in the absence of delay in the communication process, without plant disturbances, and assuming the controller has knowledge of the triggering strategy, one can stabilize the plant with any positive data payload transmission rate. Building upon this observation, Chapter 1 considers transmission delays in the communication channel and quantifies the information contained in the timing of the triggering events for the stabilization of scalar plants without disturbances. For small values of the delay, we show that stability can be achieved with any positive information

transmission rate (the rate at which sensor transmits data payload). However, as the delay increases to values larger than a critical threshold, the timing information contained in the triggering action itself may not be enough to stabilize the plant and the information transmission rate must be increased. Chapter 1 also extends the treatment to the vector case, but the analysis is limited to plants with only real eigenvalues of the open-loop gain matrix. Furthermore, the required exponential convergence guarantees lead to a mismatch between sensor and controller about the possible values of the state estimation error, which requires an additional layer of complexity in the sensor's transmission policy of the event-triggered control design. In contrast, in this chapter we consider the weaker stability notion of input-to-state practical stability (ISpS) [78, 174], and this allows us to simplify the treatment and design a simpler event-triggered control strategy. The literature has not considered to what extent the implicit timing information in the triggering events is still useful in the presence of plant disturbances. Beyond the uncertainty due to the unknown delay in communication, disturbances add an additional degree of uncertainty to the state estimation process, whose effect needs to be properly accounted for. With this in mind, we study ISpS of a linear, time-invariant plant subject to bounded disturbance over a communication channel with bounded delay.

Our contributions are fivefold. First, for scalar real plants with disturbances, we derive a sufficient condition on the information transmission rate for the whole spectrum of possible communication delay values. Specifically, we design an encoding-decoding scheme that, together with the proposed event-triggering strategy, rules out Zeno behavior and ensures that there exists a control policy which renders the plant ISpS. We show that for small values of the delay, our event-triggering strategy achieves ISpS using only implicit timing information and transmitting data payload at a rate arbitrarily close to zero. On the other hand, since larger values of the delay imply that the information transmitted has become excessively outdated and corrupted by the disturbance, increasingly higher communication rates are required as the delay becomes larger. Our second contribution pertains to the generalization of the sufficient condition to complex

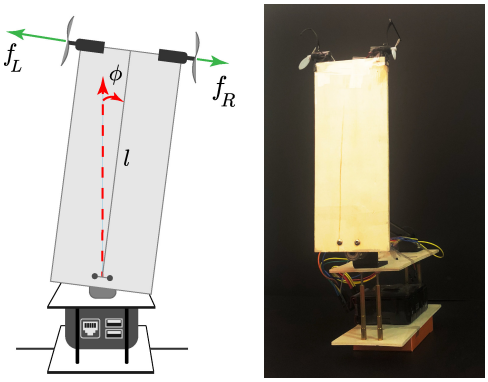


Figure 3.1: An inverted pendulum controlled by thrust force of two propellers. The pendulum is a plywood sheet of length l. The angle ϕ of the pendulum from the vertical line and its rate of change, measured by the sensor and transmitted to the controller over a digital channel with bounded unknown delay, are used to determine the left and right thrust forces f_L and f_R of the propellers.

plants with complex open-loop gain subject to disturbances. This result sets the basis for the generalization of event-triggered control strategies that meet the bounds on the information transmission rate for the ISpS of vector systems under disturbances and with any real open-loop gain matrix (with complex eigenvalues). Our third contribution is a necessary condition on the information transmission rate for scalar real plants, assuming that at each triggering time the sensor transmits the smallest possible packet size to achieve the triggering goal for all realizations of the delay and plant disturbance. The majority of results on control under communication constraints are restricted to theoretical works. Here for the first time, we examine data-rate theorems in a practical setting, using an inverted pendulum, a classic example of an inherently unstable nonlinear plant with numerous practical applications. Our fourth contribution is to implement our event-triggering control design, and demonstrate the utilization of timing information to stabilize a laboratory-scale inverted pendulum over a digital communication channel with bounded unknown delay, see Figure 3.1. The results of our experiments show that using the sufficient packet size on a linearized model of the inverted pendulum around its unstable equilibrium point, the state estimation error is sufficiently small and we can stabilize the system. We show that for small values of the delay the experimental data payload transmission rate is

lower than the entropy rate of the plant. On the other hand, by increasing the upper bound on the delay in the communication channel, higher data payload transmission rates are required to satisfy the requirements of the proposed control strategy. This event-triggering policy can only stabilize the pendulum *locally* around its equilibrium point, where linearization is possible. Our final contribution is to address nonlinear systems directly, and develop a novel event-triggering scheme that exploits timing information to render a class of continuous-time nonlinear systems subject to disturbances ISpS.

3.2 Problem formulation

We consider a networked control system described by a plant-sensor-channel-controller tuple, cf. Figure 2.1. The plant is described by a scalar, continuous-time, linear time-invariant model,

$$\dot{x} = Ax(t) + Bu(t) + w(t), \tag{3.1}$$

where $x(t) \in \mathbb{R}$ and $u(t) \in \mathbb{R}$ for $t \in [0, \infty)$ are the plant state and control input, respectively, and $w(t) \in \mathbb{R}$ represents the plant disturbance. The latter is a Lebesgue-measurable function of time, and *upper bounded* as

$$|w(t)| \leq M, \tag{3.2}$$

where $M \in \mathbb{R}_{\geq 0}$. In (3.1), $A \in \mathbb{R}$ is positive (i.e., the plant is unstable), $B \in \mathbb{R} \setminus \{0\}$, and the initial condition $x(0)$ is bounded. We assume the sensor measurements are exact and there is no delay in the control action, which is executed with infinite precision. However, measurements are transmitted from sensor to controller over a communication channel subject to a finite data rate and bounded unknown delay. We denote by $\{t_s^k\}_{k \in \mathbb{Z}}$ the sequence of times when the sensor

transmits a packet of length $g(t_s^k)$ bits containing a quantized version of the encoded state. We let $\Delta'_k = t_s^{k+1} - t_s^k$ be the k^{th} *triggering interval*. The packets are delivered to the controller without error and entirely but with unknown upper bounded delay. Let $\{t_c^k\}_{k\in\mathbb{Z}}$ be the sequence of times where the controller receives the packets transmitted at times $\{t_s^k\}_{k\in\mathbb{Z}}$. We assume the *communication delays* $\Delta_k = t_c^k - t_s^k$, for all $k \in \mathbb{Z}$, satisfy

$$\Delta_k \leq \gamma, \tag{3.3}$$

where $\gamma \in \mathbb{R}_{\geq 0}$. When referring to a generic triggering or reception time, for convenience we skip the super-script k in t_s^k and t_c^k, and the sub-script k in Δ_k and Δ'_k.

Remark 12. In our model clocks are synchronized at the sensor and the controller. In case of using a time stamp, due to the communication constraints, only a quantized version of it can be encoded in the packet $g(t_s)$. •

At the controller, the estimated state is represented by $\hat{x}$ and evolves during the inter-reception times as

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t), \quad t \in (t_c^k, t_c^{k+1}), \tag{3.4}$$

starting from $\hat{x}(t_c^{k+})$, which represents the state estimate of the controller with the information received up to time t_c^k with initial condition $\hat{x}(0)$ (the exact way to construct $\hat{x}(t_c^{k+})$ is explained later in Section 3.3).

Assumption 1 *The sensor can compute $\hat{x}(t)$ for all time $t \geq 0$.*

Remark 13. We show in Section 3.4.1 that Assumption 1 is valid for our controller design, provided the sensor knows $\hat{x}(0)$ and the times the actuator performs the control action. In practice, this corresponds to assuming an instantaneous acknowledgment from the actuator to the sensor

via the control input, known as *communication through the control input* [123, 164]. To obtain such causal knowledge, one can monitor the output of the actuator provided that the control input changes at each reception time. In case the sensor has only access to the plant state, since the system disturbance is bounded (3.2), assuming that the control input is continuous during inter-reception times and jumps in the reception times such that $B|u(t_c^-) - u(t_c)| > M$, the controller can signal the reception time of the packet to the sensor via $\dot{x}(t)$ (other specific constructions are provided in [190]). Finally, we note that any necessary condition on the information transmission rate obtained with Assumption 1 in place remains necessary without it too. •

Under Assumption 1, the *state estimation error* at the sensor is

$$z(t) = x(t) - \hat{x}(t), \tag{3.5}$$

and we rely on this error to determine when a triggering event occurs in our controller design. We next define a modified version of input-to-state practical stability (ISpS) [78, 174], which is suitable for our event-triggering setup with unknown but bounded delay.

Definition 1 *The plant* (3.1) *is ISpS if there exist* $\beta \in \mathcal{KL}$, $\psi \in \mathcal{K}_\infty(0)$, $d \in \mathbb{R}_{\geq 0}$, $\chi \in \mathcal{K}_\infty(d)$, $d' \in \mathbb{R}_{\geq 0}$ *and* $\zeta \in \mathcal{K}^2_\infty(0, d')$ *such that for all* $t \geq 0$

$$|x(t)| \leq \beta\left(|x(0)|, t\right) + \psi\left(|w|_t\right) + \chi(\gamma) + \zeta(|w|_t, \gamma).$$

Note that, for a fixed γ, this definition reduces to the standard notion of ISpS. Given that the initial condition, delay, and system disturbances are bounded, ISpS implies that the state must be bounded at all times beyond a fixed horizon.

Our objective is to ensure the dynamics (3.1) is ISpS given the constraints posed by the system model of Figure 2.1. In this chapter we also use the definitions of *information transmission rate* and *information access rate* defined in Chapter 2.

According to the data-rate theorem, if $R_c < A/\ln 2$, the value of the state in (3.1) becomes unbounded as $t \to \infty$ (the result for plants evolving in continuous time stated in [70, Theorem 1] does not consider disturbances, but can readily be generalized to account for them), and hence (3.1) is not ISpS. The data-rate theorem characterizes what is needed by the controller, and does not depend on the specific feedback structure (including aspects such as information pattern at the sensor/controller, communication delays, and whether transmission times are state-dependent, as in event-triggered control, or periodic, as in time-triggered control). In our discussion below, the bound $R_c = A/\ln 2$ serves as a baseline for our results on the information transmission rate R_s to understand the amount of timing information contained in event-triggered control designs in the presence of unknown communication delays.

We do not consider delays, plant disturbances, and initial condition to be chosen from any specific distribution. Therefore, our results are valid for any arbitrary delay, plant disturbances, and initial condition with finite support. In particular, our goal is to find upper and lower bounds on R_s, where the *lower bound* is necessary at least for *a realization* of the initial condition, delay, and disturbances, and the *upper bound* is sufficient for *all realizations* of the initial condition, delay, and disturbances. In addition, our lower bound is necessary for any control policy $u(t)$ to render the plant (3.1) ISpS under the class of event-triggering strategies described next.

3.3 Event-triggered design

Here we introduce the general class of event-triggered policies considered for plant 3.1 in this chapter. Consider the following class of triggers: for $J \in \mathbb{R}$ positive, the sensor sends a message to the controller at t_s^{k+1} if

$$|z(t_s^{k+1})| = J, \tag{3.6}$$

provided $t_c^k \leq t_s^{k+1}$ for $k \in \mathbb{N}$ and $t_s^1 \geq 0$. A new transmission happens only after the previous packet has been received by the controller. Since the triggering time t_s is a real number, its knowledge can reveal an unbounded amount of information to the controller. However, due to the unknown delay in the channel, the controller does not have perfect knowledge of it. In fact, both the finite data rate and the delay mean that the controller may not be able to compute the exact value of $x(t_c)$. To address this, let $\bar{z}(t_c)$ be an estimated version of $z(t_c)$ reconstructed by the controller knowing $|z(t_s)| = J$, the bound (3.3) on the delay, and the packet received through the channel. Using $\bar{z}(t_c)$, the controller updates the state estimate via the *jump strategy*,

$$\hat{x}(t_c^+) = \bar{z}(t_c) + \hat{x}(t_c). \tag{3.7}$$

Note that $|z(t_c^+)| = |x(t_c) - \hat{x}(t_c^+)| = |z(t_c) - \bar{z}(t_c)|$.

We assume the packet size $g(t_s)$ calculated at the sensor is so that

$$|z(t_c^+)| = |z(t_c) - \bar{z}(t_c)| \leq J, \tag{3.8}$$

is satisfied for all $t_c \in [t_s, t_s + \gamma]$. This property plays a critical role in our forthcoming developments. In particular, we will show later that our controller design for the sufficient characterization on the transmission rate builds on identifying a particular encoding-decoding strategy and a packet size to make (3.8) hold true. Likewise, our necessary characterization builds on identifying the minimal packet sizes necessary to ensure (3.8).

The importance of (3.8) starts to become apparent in the following result: if this inequality holds at each reception time, the state estimation error (3.5) is bounded for all time.

Lemma 6. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.1)*, estimator dynamics* (3.4)*, triggering strategy* (3.6)*, and jump strategy* (3.7)*. Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$ *and* (3.8) *holds at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$*. Then, for all* $t \geq 0$*,*

$$|z(t)| \leq Je^{A\gamma} + \frac{|w|_t}{A}\left(e^{A\gamma} - 1\right). \tag{3.9}$$

Proof. At the reception time, $z(t_c^{k+})$ satisfies (3.8), hence using the triggering rule (3.6), we deduce $|z(t)| \leq J$ for all $t \in (t_c^k, t_s^{k+1}]$. Since J is smaller than the upper bound in (3.9), and $z(t_c^{(k+1)+})$ satisfies (3.8), it remains to prove (3.9) for $t \in (t_s^{k+1}, t_c^{k+1})$. From (3.1), (3.4), and (3.5), we have $\dot{z}(t) = Az(t) + w(t)$ during inter-reception time intervals (t_c^k, t_c^{k+1}). Also, from (3.6) it follows $(t_s^{k+1}, t_c^{k+1}) \subseteq (t_c^k, t_c^{k+1})$. Thus, for all $t \in (t_s^{k+1}, t_c^{k+1})$, we have

$$z(t) = e^{A(t-t_s^{k+1})} z(t_s^{k+1}) + \int_{t_s^{k+1}}^{t} e^{A(t-\tau)} w(\tau) d\tau. \tag{3.10}$$

When a triggering occurs $|z(t_s^{k+1})| = J$, hence the absolute value of the first addend in (3.10) is upper bounded by $Je^{A(t-t_s^{k+1})}$. Also, for the second addend in (3.10) we have

$$\begin{aligned} &\left| \int_{t_s^{k+1}}^{t} e^{A(t-\tau)} w(\tau) d\tau \right| \\ &\quad \leq |w|_t \int_{t_s^{k+1}}^{t} |e^{A(t-\tau)}| d\tau = \frac{|w|_t}{A}\left(e^{A(t-t_s^{k+1})} - 1\right). \end{aligned} \tag{3.11}$$

By (3.3), we have $t - t_s^{k+1} \leq t_c^{k+1} - t_s^{k+1} \leq \gamma$, and the result follows. ∎

Using (3.2), we deduce from Lemma 6 that $|z(t)| \leq Je^{A\gamma} + \frac{M}{A}\left(e^{A\gamma} - 1\right)$ for all $t \geq 0$. Next, we rule out Zeno behavior (an infinite amount of triggering events in a finite time interval) for our our event-triggered control design. To do this, let $0 < \rho_0 < 1$ be a design parameter, and assume the packet size $g(t_s)$ is selected at the sensor to ensure a stronger version of (3.8),

$$|z(t_c^+)| = |z(t_c) - \bar{z}(t_c)| \leq \rho_0 J. \tag{3.12}$$

Clearly, (3.12) implies (3.8). The following result shows that given (3.12) the time between

consecutive triggers is uniformly lower bounded.

Lemma7. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.1)*, estimator dynamics* (3.4)*, triggering strategy* (3.6)*, and jump strategy* (3.7)*. Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$ *and* (3.12) *holds at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$*. Then for all* $k \in \mathbb{N}$

$$t_s^{k+1} - t_s^k \geq \ln\Big(\frac{JA+M}{\rho_0 JA+M}\Big)\Big/A.$$

Proof. By considering two successive triggering times t_s^k and t_s^{k+1} and the reception time t_c^k, from (3.6) it follows $t_s^k \leq t_c^k \leq t_s^{k+1}$. From (3.1), (3.4), and (3.5), we have $\dot{z}(t) = Az(t) + w(t)$ during inter-reception time intervals (t_c^k, t_c^{k+1}), consequently using the definition of the triggering time t_s^{k+1} (3.6) it follows

$$|z(t_c^{k+})e^{A(t_s^{k+1}-t_c^k)}| + |\int_{t_c^k}^{t_s^{k+1}} e^{A(t_s^{k+1}-\tau)}w(\tau)d\tau| \geq J.$$

Using (3.12) and (3.11), we have

$$\rho_0 J e^{A(t_s^{k+1}-t_c^k)} + (M/A)(e^{A(t_s^{k+1}-t_c^k)} - 1) \geq J,$$

which is equivalent to $t_s^{k+1} - t_c^k \geq \frac{1}{A}\ln(\frac{J+\frac{M}{A}}{\rho_0 J+\frac{M}{A}})$. The result follows from using $t_s^k \leq t_c^k$ in this inequality. ∎

Given the uniform lower bound on the inter-event time obtained in Lemma 7, we deduce that the event-triggered control design does not exhibit Zeno behavior. Using Lemma 7, we deduce that the triggering rate (2.17), the frequency with which transmission events are triggered, is uniformly upper bounded under the event-triggered control design, i.e., for *all* initial conditions,

possible delay and plant noise values, we have

$$R_{tr} \leq \frac{A}{\ln(\frac{J+\frac{M}{A}}{\rho_0 J+\frac{M}{A}})}. \tag{3.13}$$

3.4 Sufficient and necessary conditions on the information transmission rate

Here we derive sufficient and necessary conditions on the information transmission rate (2.9) to ensure (3.1) is ISpS. As mentioned above, our approach is based on the characterization of the transmission rate required to ensure that (3.8) holds at all reception times. Section 3.4.1 introduces a quantization policy that, together with the event-triggered scheme, provides a complete control design to guarantee (3.1) is ISpS and rules out Zeno behavior. Section 3.4.2 presents lower bounds on the packet size and triggering rate required to guarantee (3.1) is ISpS, leading to our bound on the necessary information transmission rate. We conclude the section by comparing the sufficient and necessary bounds, and discussing their gap.

3.4.1 Sufficient information transmission rate

We start by showing that, if (3.8) holds at each reception time $\{t_c^k\}_{k\in\mathbb{N}}$, then a linear controller renders the plant (3.1) ISpS. We note that similar results exist in the literature (e.g., [65, 68, 69, 148, 150]) and we here extend them to our event-triggering setup with quantization and unknown delays.

Proposition 1 *Under the assumptions of Lemma 6, the controller* $u(t) = -K\hat{x}(t)$ *renders* (3.1) *ISpS, provided* $A - BK < 0$.

Proof. By letting $u(t) = -K(x(t) - z(t))$, we rewrite (3.1) as $\dot{x}(t) = (A-BK)x(t)+BKz(t)+w(t)$. Consequently, we have

$$|x(t)| \leq e^{(A-BK)t}|x(0)| + e^{(A-BK)t}\int_0^t e^{-(A-BK)\tau}(BK|z(\tau)| + |w(\tau)|)d\tau. \tag{3.14}$$

since $A - BK < 0$, the first summand in (3.14) is a $\mathcal{KL}$ function of $|x(0)|$ and time. Thus, it remains to prove the second summand in (3.14) is upper bounded by summation of a $\mathcal{K}_\infty(0)$ function of $|w|_t$, a $\mathcal{K}_\infty(d)$ function of γ, and a $\mathcal{K}^2_\infty(0,0)$ function of $|w|_t$ and γ. The second summand in (3.14) is upper bounded by $-(1 - e^{(A-BK)t})(BK|z|_t + |w|_t)/(A - BK)$. Since $1 - e^{(A-BK)t} < 1$, using Lemma 6 we deduce the second summand in (3.14) is upper bounded by $\psi(|w|_t) + \iota(\gamma) + \vartheta(|w|_t, \gamma)$, where $\psi(|w|_t) = (|w|_t/-(A - BK))$ which is a $\mathcal{K}_\infty(0)$ function of $|w|_t$, $\iota(\gamma) = ((BKJe^{A\gamma})/-(A - BK))$ which is a $\mathcal{K}_\infty(d)$ function of γ with $d = \iota(0)$, and $\vartheta(|w|_t, \gamma) = ((BK|w|_t)/-A(A - BK))(e^{A\gamma} - 1)$ which is a $\mathcal{K}^2_\infty(0,0)$ function of γ and $|w|_t$.

∎

Design of quantization policy

The result in Proposition 1 justifies our strategy to obtain a sufficient condition on the transmission rate to guarantee (3.1) is ISpS, which consists of finding conditions to achieve (3.8) for all reception times. Here we specify a quantization policy and determine the resulting estimation error as a function of the number of bits transmitted. This allows us to determine the packet size that ensures (3.12) (and consequently (3.8)) holds, thereby leading to a complete control design which ensures (3.1) is ISpS and rules out Zeno behavior. In turn, this also yields a sufficient condition on the information transmission rate. In our sufficient design the controller

estimates $z(t_c)$ as

$$\bar{z}(t_c) = \text{sign}(z(t_s))Je^{A(t_c - q(t_s))}, \tag{3.15}$$

where $q(t_s)$ is an estimation of the triggering time t_s constructed at the controller as described next. According to (3.6), at every triggering event, the sensor encodes t_s and transmits a packet $p(t_s)$. The packet $p(t_s)$ consists of $g(t_s)$ bits of information and is generated according to the following quantization policy. The first bit $p(t_s)[1]$ denotes the sign of $z(t_s)$. As shown in

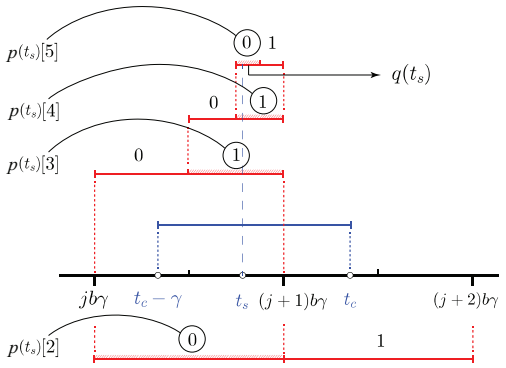


Figure 3.2: The encoding-decoding algorithms in the proposed event-triggered control scheme. In this example, we assume $g(t_s) = 5$ and j is an even natural number. The packet $p(t_s)$ of length 5 can be generated and sent to the controller. Recall that $p(t_s)[1]$ encode the sign of $z(t_s)$. After reception and decoding the controller choose the center of the smallest sub-interval as its estimation of t_s, denoted by $q(t_s)$.

Figure 3.2, the reception time t_c provides information to the controller that t_s could fall anywhere between $t_c - \gamma$ and t_c. Let $b > 1$. To determine the time interval of the triggering event, we break the positive time line into intervals of length $b\gamma$. Consequently, t_s falls into $[jb\gamma, (j+1)b\gamma]$ or $[(j+1)b\gamma, (j+2)b\gamma]$, with j being a natural number. We use the second bit of the packet to determine the correct interval of t_s. This bit is zero if the nearest integer less than or equal to the beginning number of the interval is an even number and is 1 otherwise. This can be written mathematically as $p(t_s)[2] = \text{mod}\big(\lfloor \frac{t_s}{b\gamma} \rfloor, 2\big)$. For the remaining bits of the packet, the encoder breaks the interval containing t_s into $2^{g(t_s)-2}$ equal sub-intervals. Once the packet is complete, it

is transmitted to the controller, where it is decoded and the center point of the smallest sub-interval is selected as the best estimate of t_s. Thus,

$$|t_s - q(t_s)| \leq b\gamma/2^{g(t_s)-1}. \tag{3.16}$$

We have employed this quantization policy in our previous work [95] and analyzed its behavior in the case with no disturbances. Next, we extend our analysis to scenarios with both unknown delays and plant disturbances. As discussed in Remark 13, we start by showing that under the proposed encoding-decoding scheme, provided the sensor knows $\hat{x}(0)$ and has causal knowledge of the delay (i.e., the controller acknowledges the packet reception times), then Assumption 1 holds.

Proposition 2 *Under the assumptions of Lemma 7, using the estimation* (3.15) *and the quantization policy described in Figure 3.2, if the sensor knows* $\hat{x}(0)$ *and has causal knowledge of delay, then it can calculate* $\hat{x}(t)$ *for all time* $t \geq 0$.

Proof. The proof is based on induction. Using $\hat{x}(0)$ sensor can construct the value of $\hat{x}(t)$ for $t \in (0, t_c^1)$ according to (3.4). Note that we are using the proposed quantizer in Figure 3.2, hence given t_s^1, $q(t_s^1)$ gets identified deterministically. Consequently, given t_c^1 and using (3.15), the sensor constructs the value of $z(t_c^{1+})$ and it determines the value of $\hat{x}(t_c^{1+})$.

Now assuming that the sensor is aware of the value of $\hat{x}(t_c^{k+})$ we will prove that the sensor can find the value of $\hat{x}(t_c^{(k+1)+})$ too. Since the sensor is aware of the $\hat{x}(t_c^{k+})$ and it knows that $\hat{x}(t)$ evolves according to (3.4) for $t \in (t_c^k, t_c^{k+1})$ starting from $\hat{x}(t_c^{k+})$ sensor can calculate all the values of $\hat{x}(t)$ until t_c^{k+1}. Using our proposed quantizer and given t_s^{k+1}, $q(t_s^{k+1})$ can be identified deterministically, therefore by knowing the value of $(k+1)^{th}$ delay the sensor can calculate the value of $\bar{z}(t_c^{(k+1)+})$ from (3.15). Then using the jump strategy (3.7) it can calculate $\hat{x}(t_c^{(k+1)+})$. So the result follows. ∎

Sufficient packet size

Our next result bounds the difference $|t_s - q(t_s)|$ between the triggering time and its quantized version so that (3.12) holds at all reception times.

Lemma 8. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.1)*, estimator dynamics* (3.4)*, triggering strategy* (3.6)*, and jump strategy* (3.7)*. Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$ *Using the estimation* (3.15) *and the quantization policy described in Figure 3.2, if*

$$|t_s - q(t_s)| \leq \frac{1}{A} \ln(1 + \frac{\rho_0 - \frac{M}{JA}(e^{A\gamma} - 1)}{e^{A\gamma}}),$$

then (3.12) *holds for all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *if* $J > \frac{M}{A\rho_0}(e^{A\gamma} - 1)$.

Proof. Using (3.10), (3.15), and the triangular inequality, we deduce

$$\begin{aligned} &|z(t_c) - \bar{z}(t_c)| \leq \\ &Je^{A(t_c - t_s)}|(1 - e^{A(t_s - q(t_s))})| + |\int_{t_s}^{t_c} e^{A(t_c - \tau)} w(\tau) d\tau|. \end{aligned}$$

By applying the bounds (3.3), (3.2), and (3.11) on first and second addend respectively it follows

$$\begin{aligned} &|z(t_c) - \bar{z}(t_c)| \leq \\ &|Je^{A\gamma}(1 - e^{A(t_s - q(t_s))})| + \frac{M}{A}\left(e^{A\gamma} - 1\right). \end{aligned}$$

Therefore, ensuring (3.12) reduce to

$$|1 - e^{A(t_s - q(t_s))}| \leq \eta, \tag{3.17}$$

where $\eta = e^{-A\gamma}(\rho_0 - \frac{M}{AJ}(e^{A\gamma}-1))$. Since $J > \frac{M}{A\rho_0}(e^{A\gamma}-1)$, we have $0 \leq \eta < 1$. Consequently, using (3.17), we deduce

$$\frac{\ln(1-\eta)}{A} \leq t_s - q(t_s) \leq \frac{\ln(\eta+1)}{A}$$

It follows that to satisfy (3.12) for all delay values, requiring

$$|t_s - q(t_s)| \leq \min\{\frac{|\ln(1-\eta)|}{A}, \frac{\ln(\eta+1)}{A}\}$$

suffices, and the result now follows. ∎

The next result provides a lower bound on the packet size so that (3.12) is ensured at all reception times.

Theorem 10 *Consider the plant-sensor-channel-controller model with plant dynamics* (3.1)*, estimator dynamics* (3.4)*, triggering strategy* (3.6)*, and jump strategy* (3.7)*. Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$*, Then there exists a quantization policy that achieves* (3.12) *for all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *with any packet size*

$$g(t_s^k) \geq \max\left\{0, 1 + \log \frac{Ab\gamma}{\ln(1 + \frac{\rho_0 - (M/(JA))(e^{A\gamma}-1)}{e^{A\gamma}})}\right\} \tag{3.18}$$

where $b > 1$ *and* $J > \frac{M}{A\rho_0}(e^{A\gamma}-1)$.

The proof is a direct consequence of (3.16) and Lemma 8. The combination of the upper bound (3.13) obtained for the triggering rate and Theorem 10 yields a sufficient bound on the information transmission rate. To sum it up, we conclude that there exist a information

transmission rate

$$R_s \leq \frac{A}{\ln(\frac{JA+M}{\rho_0 JA+M})} \max\left\{0, 1+\log \frac{Ab\gamma}{\ln(1+\frac{\rho_0-(M/(JA))(e^{A\gamma}-1)}{e^{A\gamma}})}\right\}, \tag{3.19}$$

that is sufficient to ensure (3.12) and, as a consequence (3.8), for all reception times $\{t_c^k\}_{k\in\mathbb{N}}$. Therefore, from Proposition 1, the bound (3.19) is sufficient to ensure the plant (3.1) is ISpS.

Remark 14. The lower bound given on the packet size in (3.18) might not be a natural number or might even be zero. If $g(t_s) = 0$, this means that there is no need to put any data payload in the packet and the plant can be stabilized using only timing information. However, in this case, the sensor still needs to inform the controller about the occurrence of a triggering event. Thus, when $g(t_s) = 0$ is sufficient, the sensor can stabilize the system by transmitting a fixed symbol from a unitary alphabet (see chapter 4 and [89, 90]). In practice, the packet size should be a natural number or zero, so if we do not want to use the fixed symbol from a unitary alphabet, the packet size

$$g(t_s) = \max\left\{1, \left\lceil 1+\log \frac{Ab\gamma}{\ln(1+\frac{\rho_0-(M/(JA))(e^{A\gamma}-1)}{e^{A\gamma}})}\right\rceil\right\}, \tag{3.20}$$

is sufficient for stabilization (the latter is the one used in our simulations of Section 3.6). •

3.4.2 Necessary information transmission rate

Here, we present a necessary condition on the information transmission rate required by any control policy to render plant (3.1) ISpS under the class of event-triggering strategies described in Section 3.3. In Section 3.4.1, to derive a sufficient bound that guarantees (3.1) is ISpS, our focus has been on identifying *a* quantization policy that could handle *any* realization of initial condition, delay, and disturbance. Instead, the treatment here switches gears to focus on

any quantization policy, for which we identify at least *a* realization of initial condition, delay, and disturbance that requires the necessary bound on the information transmission rate.

We start our discussion by making the following observation about the property (3.8). If this property is not satisfied at an arbitrary reception time t_c^k, i.e., $z(t_c^k) > J$, and $w(t) > 0$ or $w(t) < 0$ for all $t \geq t_c^k$, then t_c^k will be the last triggering time. In this case, after t_c^k, the controller needs to estimate the inherently unstable plant in open loop. In this case, there exists a realization of the initial condition, system disturbances, and delay for which the absolute value of the state estimation error grows exponentially with time. Thus, for any given control policy, there exists a realization for which the absolute value of the state tends to infinity with time and (3.1) is not ISpS.

As a consequence of this observation, our strategy to provide a necessary condition for (3.1) to be ISpS consists of identifying a necessary condition on the information transmission rate R_s to have (3.8) at all reception times $\{t_c^k\}_{k\in\mathbb{N}}$. In turn, we do this by finding lower bounds on the packet size $g(t_s)$ and the triggering rate R_{tr}. We do this in two steps: first, we find a lower bound on the number of bits transmitted at each triggering event which holds irrespective of the triggering rate. Then, we find a lower bound on the triggering rate, and the combination leads us to the necessary condition on R_s.

Necessary packet size

We rely on (3.10) to define the uncertainty set of the sensor about the estimation error at the controller $z(t_c)$ given t_s as follows

$$\Omega(z(t_c)|t_s) = \{y : y = \pm Je^{A(t_r-t_s)} + \int_{t_s}^{t_r} e^{A(t_r-\tau)}w(\tau)d\tau,$$
$$t_r \in [t_s, t_s+\gamma],\ |w(\tau)| \leq M \ \text{ for } \tau \in [t_s, t_r]\}.$$

Additionally, we define the uncertainty of the controller about $z(t_c)$ given t_c, as follows

$$\Omega(z(t_c)|t_c) = \{y : y = \pm Je^{A(t_c-t_r)} + \int_{t_r}^{t_c} e^{A(t_c-\tau)}w(\tau)d\tau,$$
$$t_r \in [t_c - \gamma, t_c],\ |w(\tau)| \leq M \ \text{ for } \tau \in [t_r, t_c]\}.$$

We next show the relationship between these uncertainty sets.

Lemma 9. *Assume the plant-sensor-channel-controller model described in Section 3.2, with plant dynamics* (3.1)*, estimator dynamics* (3.4)*, triggering strategy* (3.6)*, and jump strategy* (3.7)*. Moreover, assume* $M \leq AJ$*. Then* $\Omega(z(t_c)|t_s) = \Omega(z(t_c)|t_c)$ *and* $m\left(\Omega(z(t_c)|t_c)\right) = 2(M/A + J)(e^{A\gamma} - 1)$.

Proof. Due to symmetry, it is not difficult to show that $\Omega(z(t_c)|t_s)$ is the same as $\Omega(z(t_c)|t_c)$. We characterize the set $\Omega(z(t_c)|t_s)$ as follows. We reason for the case when $z(t_s) = J$ (the argument for the case $z(t_s) = -J$ is analogous). Clearly, $z(t_c)$ takes its largest value when $t_c = t_s + \gamma$ and $w(\tau) = M$ for $\tau \in [t_s, t_c]$, which is equal to $z(t_c) = Je^{A\gamma} + (M/A)(e^{A\gamma} - 1)$. On the other hand, finding the smallest value of $z(t_c)$ is more challenging. First, when $t_c = t_s$ we have

$$z(t_c) = J. \tag{3.21}$$

Second, by setting $w(\tau) = -M$ for $\tau \in [t_s, t_c]$ and $t_c = t_s + \Delta$,

$$z(t_c) = Je^{A\Delta} - (M/A)(e^{A\Delta} - 1). \tag{3.22}$$

Taking the derivative of (3.22) with respect to Δ results in

$$dz(t_c)/d\Delta = AJe^{A\Delta} - Me^{A\Delta} = e^{A\Delta}(AJ - M). \tag{3.23}$$

If $M \leq AJ$ and the derivative in (3.23) is non-negative, $z(t_c)$ in (3.22) would be a non-decreasing function of Δ. Hence, the smallest value of $z(t_c)$ in (3.22) occurs for $\Delta = 0$ which is equal to the value of $z(t_c)$ in (3.21). Hence, $\Omega(z(t_c)|t_s) = [J, Je^{A\gamma} + (M/A)(e^{A\gamma} - 1)]$, and the result follows. ∎

Lemma 9 allows us to find a lower bound on the packet size $g(t_s)$ which is valid irrespective of the triggering rate.

Lemma 10. *Under the assumptions of Lemma 9, if* (3.8) *holds for all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$*, then the packet size at every triggering event must satisfy*

$$g(t_s^k) \geq \max\left\{0, \log\left(\left(\frac{M}{AJ} + 1\right)\left(e^{A\gamma} - 1\right)\right)\right\}. \tag{3.24}$$

Proof. To ensure (3.8) for all reception times, we calculate a lower bound on the number of bits to be transmitted to ensure the sensor uncertainty set $\Omega(z(t_c)|t_s)$ is covered by quantization cells of measure $2J$. Therefore, we have

$$g(t_s) \geq \max\left\{0, \log\frac{m(\Omega(z(t_c)|t_s))}{m(\mathcal{B}(J))}\right\},$$

where $\mathcal{B}(J)$ is a ball centered at 0 of radius J, and we have incorporated the fact that the packet size $g(t_s)$ must be non-negative. From Lemma 9 we have

$$\log\frac{m(\Omega(z(t_c)|t_s))}{m(\mathcal{B}(J))} \geq \log\frac{2(M/A + J)(e^{A\gamma} - 1)}{2J}. \quad ∎$$

Lower bound on the triggering rate

Having found a lower bound on the packet size, our next step is to determine a lower bound on the triggering rate.

Lemma 11. *Under the assumptions of Lemma 9, for all the quantization policies which ensure* (3.8) *at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$*, if there exists a delay realization* $\{\Delta_k \leq \alpha\}_{k\in\mathbb{N}}$*, a disturbance realization, and an initial condition such that*

$$|z(t_c^{k+})| = |z(t_c^k) - \bar{z}(t_c^k)| \geq \Upsilon, \tag{3.25}$$

for all $k \in \mathbb{N}$*, then there exists a delay realization, a disturbance realization, and an initial condition such that*

$$R_{tr} \geq A\left(\ln\left(e^{A\alpha}(JA+M)\big/(\Upsilon A+M)\right)\right)^{-1}. \tag{3.26}$$

Proof. Using the definition of the triggering time (3.6), (3.25), $t_c^k = t_s^k + \Delta_k$, and (3.10), we have $\Upsilon e^{A(t_s^{k+1}-t_s^k-\Delta_k)} + (M/A)\big(e^{A(t_s^{k+1}-t_s^k-\Delta_k)} - 1\big) \leq J$, which is equivalent to

$$e^{A(t_s^{k+1}-t_s^k)} \leq e^{A\Delta_k}(JA+M)\big/(\Upsilon A+M). \tag{3.27}$$

By hypothesis, (3.25) occurs for all $k \in \mathbb{N}$ when $\Delta_k \leq \alpha$. Hence, by (3.27), we upper bound the triggering intervals as

$$\Delta_k' = t_s^{k+1} - t_s^k \leq A^{-1}\ln\left(e^{A\alpha}(JA+M)\big/(\Upsilon A+M)\right). \tag{3.28}$$

The result follows by substituting (3.28) into (2.17). ∎

If we do not limit the collection of permissible quantization policies, a packet may carry an unbounded amount of information, which can bring the state estimation error arbitrarily close to zero at all reception times and for all delay and disturbance values. This would give rise to a conservative lower bound on the transmission rate. Specifically, using $\Delta_k \leq \gamma$, cf. (3.3), putting $\Upsilon = 0$, and combining (3.26) and (3.24) we deduce there exists a delay realization, disturbance

realization, and initial condition such that

$$R_s \geq A \frac{\max\left\{0, \log\left(\left(\frac{M}{AJ}+1\right)\left(e^{A\gamma}-1\right)\right)\right\}}{\ln\left(e^{A\gamma}\frac{JA+M}{M}\right)}, \tag{3.29}$$

is necessary for all quantization policies. To find a tighter necessary condition we instead limit the collection of permissible quantization policies. Since ensuring (3.8) at each reception time is equivalent to dividing the uncertainty set at the controller $\Omega(z(t_c)|t_c)$ by quantization cells of measure of at most $2J$, our approach is to restrict the class of quantization policies to those that use the minimum possible number of bits to ensure (3.8).

Assumption 2 *We assume at each triggering time the sensor transmits the smallest possible packet size (data payload) to ensure* (3.8) *at each reception time for all initial conditions and all possible realizations of the delay and plant disturbance. Moreover, to simplify our analysis in the encoding-decoding scheme, we choose the center of each quantization cell as* $\bar{z}(t_c)$.

Based on this assumption, the sensor brings the uncertainty about $z(t_c)$ at the controller down to a quantization cell of measure at most $2J$, using the smallest possible packet size. The following result, shows that, for this class of quantization policies, there exists a delay realization such that the sensor can only shrink the estimation error for the controller to at most half of the largest value of J dictated by (3.8).

Lemma 12. *Let* $\beta = \ln\left(1 + 2AJ/(AJ+M)\right)/A \leq \gamma$.

$$\beta = \frac{1}{A}\ln\left(1 + \frac{2}{1+\frac{M}{AJ}}\right) \leq \gamma.$$

Under the assumptions of Lemma 9, for all the quantization policies ensuring (3.8) *at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *with Assumption 2 in place, there exists a delay realization* $\{\Delta_k \leq \beta\}_{k\in\mathbb{N}}$, *initial*

condition, and plant disturbance such that

$$|z(t_c^{k+})| = |z(t_c^k) - \bar{z}(t_c^k)| \geq J/2. \tag{3.30}$$

Proof. Without loss of generality assume that $z(t_s) = J$ throughout this proof. We also consider the realization of $w(t) = M$ for all time t. We first show β is the time needed for the state estimation error to grow from $z(t_s)$ to $z(t_s) + 2J$. From (3.10), we deduce at delay β we have

$$z(t_c) = e^{A\beta}J + (M/A)\left(e^{A\beta} - 1\right). \tag{3.31}$$

By combining (3.31), the bound on β, and $z(t_s) = J$ it follows $z(t_c) = z(t_s) + 2J$. Hence, the value of $z(t_c)$ sweeps an area of measure $2J$ when the delay takes values in $[0, \beta]$.

We continue by distinguishing between two classes of quantization cells. We call a quantization cell *perfect*, if its measure is equal to $2J$, and when the measure of a quantization cell is less than $2J$ we call it *defective*. Using these definitions we now prove the occurrence of (3.30) with delay of at most β, in three different cases. First, when $z(t_s)$ is in a perfect cell, clearly for a delay of at most β we have $|z(t_c^k) - \bar{z}(t_c^k)| \geq J$, and (3.30) follows. Second, when $z(t_s)$ is in a defective cell which is adjacent to a perfect cell, for a delay of at most β the value of $z(t_c)$ sweeps the area of the defective cell and $z(t_c)$ inters the adjacent perfect cell. Thus, with delay at most β we have $|z(t_c^k) - \bar{z}(t_c^k)| \geq J/2$, where $\bar{z}(t_c^k)$ is the center of the adjacent perfect cell with radius J, and (3.30) follows. It remains to check the assertion when $z(t_s)$ is in a defective quantization cell which is adjacent to another defective quantization cell. Due to the restriction on the quantization policies as in Assumption 2, the sensor transmits the minimum required bits to divide the uncertainty set at the controller to quantization cell of measure of at most $2J$. If the measure of union of two adjacent cells is at most $2J$, these two balls could be replaced by one quantization cell to reduce the number of quantization cells. As a consequence, under Assumption 2, the measure of union of two adjacent quantization cells is greater than $2J$.

Assume the defective quantization cell that contain $z(t_s)$ is of the measure μ_1 and the measure of the adjacent defective cell is μ_2. As a result, we have $\mu_1 + \mu_2 > 2J$. Therefore, at least one of the μ_1 or μ_2 is at least J, thus with a delay of at most β, we have $|z(t_c^k) - \bar{z}(t_c^k)| \geq J/2$, and (3.30) follows. ∎

Combining Lemmas 11 and 12, we deduce there exists a delay realization, disturbance realization, and initial condition such that

$$R_{tr} \geq A \left(\ln \left(\left(1 + \frac{2AJ}{AJ + M} \right) \frac{JA + M}{0.5JA + M} \right) \right)^{-1} \tag{3.32}$$

is valid for all quantization policies that use the minimum required packet size according to Assumption 2. Finally, the combination of the bounds on the packet size (cf. Lemma 10) and on the triggering rate (cf. (3.32)) yields the next result.

Theorem 11. *Under the assumptions of Lemma 9, for all the quantization policies which ensure* (3.8) *at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *with Assumption 2 in place, there exists a delay realization* $\{\Delta_k \leq \beta\}_{k\in\mathbb{N}}$*, a disturbance realization, and an initial condition such that*

$$R_s \geq A \frac{\max\left\{0, \log\left((M/(AJ) + 1)\left(e^{A\gamma} - 1\right)\right)\right\}}{\ln\left(\left(1 + \frac{2AJ}{AJ+M}\right)\frac{JA+M}{0.5JA+M}\right)}. \tag{3.33}$$

Note that the bound (3.33) is tighter than the bound in (3.29). Figure 3.3 compares our bounds on the sufficient (3.19) and necessary (3.33) information transmission rates for (3.1) to be ISpS. We attribute the gap between them to the fact that, while the necessary condition employs quantization policies with the minimum possible packet size according to Assumption 2, the encoding-decoding scheme proposed in the sufficient design does not generally satisfy this assumption. Also, the fact that we bound the triggering rate and the packet size independently in our analysis might further contribute to the gap.

As depicted in Figure 3.3, for sufficiently small delay values the timing information is

substantial, and the plant can be ISpS in the presence of bounded system disturbances when the sensor transmits data payload at a rate smaller than the one indicated by the data-rate theorem. On the other hand, as the communication delay increases, the timing information becomes less useful and the uncertainty about the state increases at the controller. Since in our design the state estimation error is smaller than the triggering threshold at each reception time (3.8), for larger values of delay R_s exceeds the access rate prescribed by the data-rate theorem.

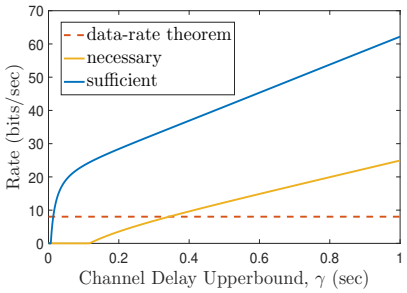


Figure 3.3: Illustration of the sufficient (3.19) and necessary (3.33) transmission rates as functions of the delay upper bound γ. Here, $A = 5.5651$, $\rho_0 = 0.1$, $b = 1.0001$, $M = 0.4$, and $J = \frac{M}{A\rho_0}(e^{A\gamma} - 1) + 0.1$. The rate dictated by the data-rate theorem is $R_c \geq A/\ln 2 = 8.02874$.

3.5 Extension to complex linear systems

In this section, we generalize our treatment to complex linear plants with disturbances. The results presented here can be readily applied to multivariate linear plants with disturbance and diagonalizable open loop-gain matrix (possibly, with complex eigenvalues). This corresponds to handling the n-dimensional real plant as n scalar (and possibly complex) plants, and derive a sufficient condition for them. We consider a plant, sensor, communication channel and controller described by the following continuous linear time-invariant system

$$\dot{x} = Ax(t) + Bu(t) + w(t), \tag{3.34}$$

where $x(t)$ and $u(t)$ belong to $\mathbb{C}$ for $t \in [0, \infty)$. Here $w(t) \in \mathbb{C}$ represents a plant disturbance, which is upper bounded as $\|w(t)\| \leq M$, with $M \in \mathbb{R}_{\geq 0}$. Also, $A \in \mathbb{C}$ with $\mathrm{Re}(A) \geq 0$ (since we are only interested in unstable plants) and $B \in \mathbb{C}$ is nonzero. The model for the communication channel is the same as in Section 3.2. To establish a baseline for comparison of the bounds on the information transmission rate, we start by stating a generalization of the classical data-rate theorem for the complex plant (3.34).

Theorem 12. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.34)*. If* $x(t)$ *remains bounded as* $t \to \infty$*, then*

$$R_c \geq \frac{2\,\mathrm{Re}(A)}{\ln 2}.$$

Proof. It is enough to prove the assertion when $w(t) = 0$. By rewriting (3.34) when $w(t) = 0$ we have $\mathrm{Re}\dot{(x)} + i\mathrm{Im}\dot{(x)} = \mathrm{Re}(A)\,\mathrm{Re}(x) - \mathrm{Im}(A)\,\mathrm{Im}(x) + i(\mathrm{Re}(A)\,\mathrm{Im}(x) + \mathrm{Im}(A)\,\mathrm{Re}(X))$, which is equivalent to

$$\begin{bmatrix} \mathrm{Re}\dot{(x)} \\ \mathrm{Im}\dot{(x)} \end{bmatrix} = \begin{bmatrix} \mathrm{Re}(A) & -\mathrm{Im}(A) \\ \mathrm{Im}(A) & \mathrm{Re}(A) \end{bmatrix} \begin{bmatrix} \mathrm{Re}(x)(t) \\ \mathrm{Im}(x)(t) \end{bmatrix}.$$

Since $\|x\| = \sqrt{\mathrm{Re}(x)^2 + \mathrm{Im}(x)^2}$, if $\mathrm{Re}(x)$ or $\mathrm{Im}(x)$ becomes unbounded, $\|x\|$ becomes unbounded. Consequently, using [70, Theorem 1], we need to have

$$R_c \geq \mathrm{Tr}\left(\begin{bmatrix} \mathrm{Re}(A) & -\mathrm{Im}(A) \\ \mathrm{Im}(A) & \mathrm{Re}(A) \end{bmatrix} \right) / \ln 2. \quad \blacksquare$$

3.5.1 Event-triggered control for complex linear systems

The state estimate $\hat{x}$ evolves according to the dynamics (3.4) along the inter-reception time intervals starting from $\hat{x}(t_c^{k+})$ with initial condition $\hat{x}(0)$. We use the *state estimation error* defined as (3.5) with initial condition $z(0) = x(0) - \hat{x}(0)$. A triggering event happens at t_s^{k+1} if

$$\|z(t_s^{k+1})\| = J, \tag{3.35}$$

provided $t_c^k \leq t_s^{k+1}$ for $k \in \mathbb{N}$ and $t_s^1 \geq 0$, and the triggering radius $J \in \mathbb{R}$ is positive. At each triggering time, the packet $p(t_s)$ of size $g(t_s)$ is transmitted from the sensor to the controller. The packet $p(t_s)$ consists of a quantized version of the phase of $z(t_s)$, denoted $\phi_{q(z(t_s))}$, and a quantized version of the triggering time t_s. By (3.35), we have

$$z(t_s) = Je^{i\phi_{z(t_s)}}.$$

We construct a quantized version, denoted $q(z(t_s))$, of $z(t_s)$ at the controller as

$$q\left(z(t_s)\right) = Je^{i\phi_{q(z(t_s))}}.$$

Additionally, using the bound (3.3) and the packet at the controller, the quantized version of t_s is reconstructed and denoted by $q(t_s)$. Hence, at the controller, $z(t_c)$ is estimated as follows

$$\bar{z}(t_c) = e^{A(t_c - q(t_s))} q\left(z(t_s)\right). \tag{3.36}$$

We use the jump strategy (3.7) to update the value of $\hat{x}(t_c^+)$. Hence, $\|z(t_c^+)\| = \|z(t_c) - \bar{z}(t_c)\|$ holds. At the sensor, the packet size $g(t_s)$ is chosen to be large enough such that

$$\|z(t_c^+)\| = \|z(t_c) - \bar{z}(t_c)\| \leq \rho_0 J, \tag{3.37}$$

(where $0 < \rho_0 < 1$ is a design parameter) is satisfied for all $t_c \in [t_s, t_s + \gamma]$. Figure 3.4 shows a typical realization of $z(t)$ under the proposed event-triggered strategy before and after one event. The notion of ISpS remains the same as in Definition 1 by replacing absolute value with complex absolute value.

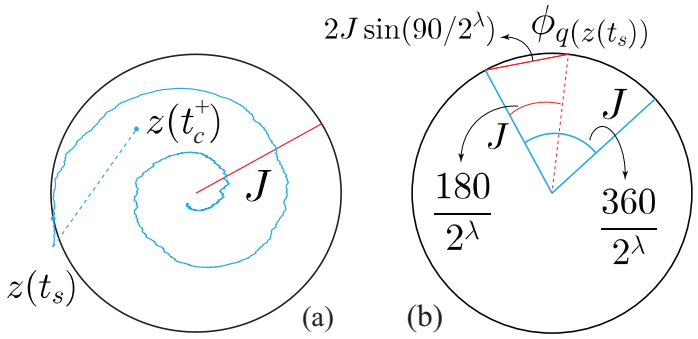


Figure 3.4: (a) The blue curve shows the evolution of the state estimation error before and after an event. The trajectory starts with an initial state inside a circle of radius J, and continues spiraling (due to the imaginary part of A) until it hits the triggering threshold radius J. Then it jumps back inside the circle after the update according to (3.36) and jump strategy (3.7). During inter-reception time intervals, $\dot{z}(t) = Az(t) + w(t)$, and the observed overshoot beyond the circle is due to the delay in the communication channel. Here, $A = 0.3 + 2i$, $B = 0.2$, $u(t) = -8\hat{x}(t)$, $M = 0.2$, $\gamma = 0.05$ sec, $\rho_0 = 0.9$ and $J = 0.0173$. (b) Estimation of the phase angle after event and transmission of λ bits.

Remark 15. Similarly to Proposition 1, one can show that if (3.37) occurs at all reception times and (A, B) is a stabilizable pair, then under the control rule $u(t) = -K\hat{x}(t)$, the plant (3.34) is ISpS, provided the real part of $A - BK$ is negative. As a consequence of this observation, our analysis focues on ensuring (3.37) at each reception time. The lower bound on the inter-event time of Lemma 7 and the upper bound on the triggering rate (3.13) also holds replacing A by $\mathrm{Re}(A)$ for the complex plant. •

3.5.2 Sufficient information transmission rate

In this section, we design a quantization policy that, using the event-triggered controller of Section 3.5.1, ensures the plant (3.34) is ISpS. We rely on this design to establish a sufficient

bound on the information transmission rate.

Design of quantization policy

We devote the first λ bits of the packet $p(t_s)$ for quantizing the phase of $z(t_s)$. The proposed encoding algorithm uniformly quantizes the circle into 2^λ pieces of $2\pi/2^\lambda$ radians. After reception, the decoder finds the correct phase quantization cell and selects its center point as $\phi_{q(z(t_s))}$. By letting $\omega = \phi_{z(t_s)} - \phi_{q(z(t_s))}$, as depicted in Figure 3.4, geometrically we deduce $|\omega| \leq \pi/2^\lambda$. Furthermore, we use the encoding scheme proposed in Figure 3.2 to append a quantized version of triggering time t_s of length $g(t_s) - \lambda$ to the packet $p(t_s)$. Hence, we have $p(t_s)[\lambda+1] = \text{mod}\big(\lfloor \frac{t_s}{b\gamma} \rfloor, 2\big)$. For the remaining bits of the packet, the encoder breaks the interval containing t_s into $2^{g(t_s)-\lambda-1}$ equal sub-intervals. Once the packet is complete, it is transmitted to the controller, where it is decoded and the center point of the smallest sub-interval is selected as the best estimate of t_s. Therefore,

$$|t_s - q(t_s)| \leq b\gamma/2^{g(t_s)-\lambda}. \tag{3.38}$$

Note that, given t_s^{k+1}, one can identify $q(t_s^{k+1})$ deterministically. Also, using the first λ bits of the packet, the sensor can find the value of $\phi_{q(z(t_s))}$. Consequently, similar to Proposition 2, if the sensor has a causal knowledge of the delay in the communication channel, it can calculate the state estimation $\hat{x}(t)$ for all time t.

Sufficient packet size

Here we show that with a sufficiently large packet size, we can achieve (3.37) at all reception times $\{t_c^k\}_{k\in\mathbb{N}}$ using the quantization policy designed in Section 3.5.2.

Theorem 13. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.34)*, estimator dynamics* (3.4)*, triggering strategy* (3.35)*, and jump strategy* (3.7)*. Assume* $\|z(0)\| =$

$\|x(0) - \hat{x}(0)\| < J$, *then the quantization policy designed above achieves* (3.37) *for all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *with any packet size lower bounded by*

$$g(t_s) \geq \bar{g} := \tag{3.39}$$
$$\max\left\{0, \lambda + \log \frac{\mathrm{Re}(A) b\gamma}{\ln\left(\frac{1+e^{-\mathrm{Re}(A)\gamma}\left(\rho_0 - \frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma}-1\right)\right)}{2\sin(\pi/2^{\lambda+1})+1+\sqrt{2\zeta}}\right)}\right\},$$

provided $\cos\Big(\mathrm{Im}(A)\big(t_s - q(t_s)\big)\Big) = 1-\zeta$, $b > 1$,

$$\rho_0 \geq \frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma} - 1\right) + e^{\mathrm{Re}(A)\gamma}\left(2\sin(\pi/2^{\lambda+1}) + \sqrt{2\zeta}\right), \tag{3.40a}$$
$$J \geq \frac{M}{\mathrm{Re}(A)\chi}\left(e^{\mathrm{Re}(A)\gamma} - 1\right), \quad \sqrt{2\zeta}e^{\mathrm{Re}(A)\gamma} \leq \chi', \tag{3.40b}$$
$$\lambda > \log\left(\pi \Big/ \arcsin\left(\frac{1-\chi-\chi'}{2e^{\mathrm{Re}(A)\gamma}}\right)\right) - 1, \tag{3.40c}$$

where $0 < \chi + \chi' < 1$.

Proof. In our design, the controller estimates $z(t_c)$ as in (3.36), and the encoding-decoding scheme is as depicted in Figures 3.2 and 3.4. Using (3.10), (3.36), and the triangle inequality, it follows

$$\|z(t_c) - \bar{z}(t_c)\| \leq \tag{3.41}$$
$$\left\|\left(e^{A(t_c-t_s)}z(t_s) - e^{A(t_c-q(t_s))}q\left(z(t_s)\right)\right)\right\| + \left\|\int_{t_s}^{t_c} e^{A(t_c-\tau)}w(\tau)d\tau\right\|.$$

Similarly to (3.11), since $\|w(t)\| \leq M$, the second summand in (3.41) is upper bounded as

$$\left\|\int_{t_s}^{t_c} e^{A(t_c-\tau)}w(\tau)d\tau\right\| \leq \frac{M}{\mathrm{Re}(A)}\left(e^{\mathrm{Re}(A)\gamma} - 1\right). \tag{3.42}$$

To find a proper upper bound on the first summand in (3.41), assuming $q\left(z(t_s)\right) = z(t_s) - v_1$ and $q(t_s) = t_s - v_2$, we have

$$\begin{aligned} &\left\| e^{At_c} \left(e^{-At_s} z(t_s) - e^{Aq(t_s)} q\left(z(t_s)\right) \right) \right\| = \\ &\left\| e^{A(t_c - t_s)} \left(z(t_s) - e^{Av_2} \left(z(t_s) - v_1 \right) \right) \right\| \leq \\ &e^{\mathrm{Re}(A)\gamma} \left(J \| 1 - e^{Av_2} \| + e^{\mathrm{Re}(A)v_2} \| v_1 \| \right). \end{aligned} \tag{3.43}$$

Next, we find an upper bound of $\|v_1\|$. Since the sensor devotes λ bits to transmit a quantized version of the phase of $z(t_s)$ to the controller, we have the upper bound $|\omega| \leq \pi/2^{\lambda}$ on the difference of the phases of $z(t_s)$ and $q(z(t_s))$. Also, over $[-\pi, \pi]$, the cosine function is concave, with global maximum at 0. Hence, as depicted in Figure 3.4, from the law of cosines, we have

$$\begin{aligned} &\| v_1 \| = \| z(t_s) - q\left(z(t_s)\right) \| \leq \\ &\sqrt{2J^2(1 - \cos(\pi/2^{\lambda}))} = 2J \sin(\pi/2^{\lambda+1}). \end{aligned} \tag{3.44}$$

Combining this with (3.43), the first summand in (3.41) is upper bounded by

$$J e^{\mathrm{Re}(A)\gamma} \left(\| 1 - e^{Av_2} \| + 2 e^{\mathrm{Re}(A)v_2} \sin(\pi/2^{\lambda+1}) \right).$$

Note that $\|1 - e^{Av_2}\|^2 = (1 - e^{\mathrm{Re}(A)v_2})^2 + 2e^{\mathrm{Re}(A)v_2}\zeta$, where $\cos(\mathrm{Im}(A)v_2) = 1 - \zeta$, and $0 \leq \zeta \leq 2$. Thus, the first summand in (3.41) is upper bounded by

$$J e^{\mathrm{Re}(A)\gamma} \Big(|1 - e^{\mathrm{Re}(A)v_2}| + \sqrt{2e^{\mathrm{Re}(A)v_2}\zeta} + 2 e^{\mathrm{Re}(A)v_2} \sin(\pi/2^{\lambda+1}) \Big).$$

For any positive real number ϵ we know $\epsilon + 1/\epsilon \geq 2$, hence, $e^{\mathrm{Re}(A)v_2} - 1 \geq 1 - e^{-\mathrm{Re}(A)v_2}$. Therefore, for the rest of the proof, and without loss of generality, we assume $v_2 \geq 0$, and the

first summand in (3.41) is upper bounded by

$$Je^{\mathrm{Re}(A)\gamma}\Big(e^{\mathrm{Re}(A)v_2}-1+\sqrt{2\zeta}e^{\mathrm{Re}(A)v_2}+2e^{\mathrm{Re}(A)v_2}\sin(\pi/2^{\lambda+1})\Big). \tag{3.45}$$

Combining (3.41), (3.42), and (3.45) we deduce

$$e^{\mathrm{Re}(A)v_2}\leq\frac{1+e^{-\mathrm{Re}(A)\gamma}\left(\rho_0-\frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma}-1\right)\right)}{2\sin(\pi/2^{\lambda+1})+1+\sqrt{2\zeta}} \tag{3.46}$$

which suffices to ensure (3.37). Recalling $v_2=t_s-q(t_s)$, using (3.38) and by setting

$$\frac{b\gamma}{2^{g(t_s)-\lambda}}\leq\frac{1}{\mathrm{Re}(A)}\ln\left(\frac{1+e^{-\mathrm{Re}(A)\gamma}\left(\rho_0-\frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma}-1\right)\right)}{2\sin(\pi/2^{\lambda+1})+1+\sqrt{2\zeta}}\right),$$

(3.46) is ensured. Consequently, the packet size in (3.39) is sufficient to ensure (3.37) for all reception times. However, (3.46) is well defined only when the upper bound in (3.46) is at least one, namely

$$e^{-\mathrm{Re}(A)\gamma}\left(\rho_0-\frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma}-1\right)\right)\geq 2\sin(\pi/2^{\lambda+1})+\sqrt{2\zeta},$$

which holds because of (3.40a). Moreover, the design parameter ρ_0 in (3.37) should be in the open interval $(0,1)$. Therefore, the lower bound in (3.40a) should be smaller than 1, namely

$$\frac{M}{\mathrm{Re}(A)J}\left(e^{\mathrm{Re}(A)\gamma}-1\right)+e^{\mathrm{Re}(A)\gamma}(2\sin(\pi/2^{\lambda+1})+\sqrt{2\zeta})<1.$$

The result now follows by noting that (3.40b), and (3.40c) ensure this inequality holds. ∎

Combining the bound on the triggering rate from Remark 15 with Theorem 13, it follows

that there exists an information transmission rate with

$$R_s \geq \frac{\mathrm{Re}(A)}{\ln\left(\frac{J+\frac{M}{\mathrm{Re}(A)}}{\rho_0 J+\frac{M}{\mathrm{Re}(A)}}\right)}\bar{g}, \tag{3.47}$$

that achieves (3.37) for all reception times $\{t_c^k\}_{k\in\mathbb{N}}$, and is therefore, sufficient to ensure (3.34) is ISpS. Figure 3.5 shows the sufficient information transmission rate in (3.47) as a function of the upper bound γ on the channel delay. One can observe that for small values of the delay, the sufficient information transmission rate is smaller than the rate required by the data-rate result in Theorem 12, and as the delay upper bound γ increases, the sufficient information transmission rate increases accordingly.

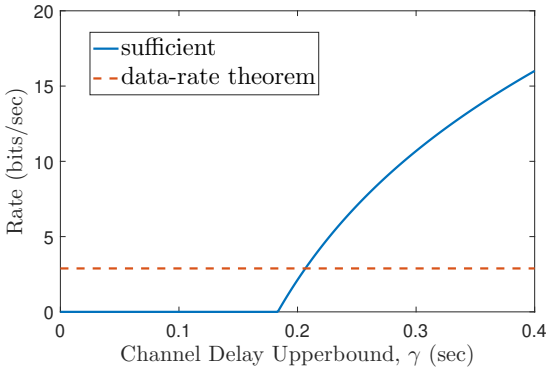


Figure 3.5: Sufficient information transmission rate (3.47) as a function of channel delay upper bound γ. Here $A = 1 + i$, $B = 0.5$, $M = 0.1$, $\rho_0 = 0.9$ and $b = 1.0001$. Also $\lambda = \log\left(\pi/2\arcsin(\frac{7}{8})e^{\mathrm{Re}(A)\gamma}\right)$ and $J = \frac{8M}{\mathrm{Re}(A)}\left(e^{\mathrm{Re}(A)\gamma}-1\right)+0.002$. The rate dictated by the data-rate theorem (cf. Theorem 12) is $2\,\mathrm{Re}(A)/\ln 2 = 2.885$.

Remark 16. Depending on whether the system is real or complex, the corresponding triggering criterion is based on the real or complex absolute value, resp., cf. (3.6) and (3.35). The controller needs to approximate the phase at which the state estimation error $z(t_s)$ hits the triggering radius. The real case is a particular case of our complex results, since the phase of $z(t_s)$ is then either 0 or π. Thus, for the real case, in our sufficient design, only the first bits of the packet $p(t_s)$ denote the sign of $z(t_s)$. On the other hand, in the complex case, we devote the first λ bits of the packet $p(t_s)$

for quantizing the phase of $z(t_s)$. By putting $A = \mathrm{Re}(A)$, $\lambda = 1$, and $\mathrm{Im}(A) = 0$ (or $\zeta = 0$), our sufficient condition for complex systems (3.47), becomes equal to (3.19) except a factor $1 + \sqrt{2}$, which makes (3.47) larger than (3.19). The reason for the difference is (3.44), where we find an upper bound on the estimation error of the phase of $z(t_s)$. In the real case, the controller deduces $z(t_s) = J$ or $z(t_s) = -J$, and the estimation error of the phase of $z(t_s)$ is zero. •

3.6 Simulations

This section presents simulation results validating the proposed event-triggered control schemes for both real and complex systems.

While our analysis is for continuous-time plants, we perform the simulations in discrete time with a small sampling time $\delta' > 0$. Thus, the minimum upper bound for the channel delay is equal to two sampling times in the digital environment (this is because a delay of at most one sampling time might occur from the time that triggering occurs to the time that the sensor took a sample from the plant state and another delay of at most one sampling time might occur from the time that the packet is received to the time the control input is applied to the plant).

3.6.1 Event-triggered control of diagonalizable systems with real eigenvalues

We consider a linearized version of the two-dimensional problem of balancing an inverted pendulum mounted on a cart, where the motion of the pendulum is constrained in a plane and its position can be measured by an angle θ as shown in Figure 3.6. The inverted pendulum has mass m_1, length l, and moment of inertia I. Also, the pendulum is mounted on top of a cart of mass m_2, constrained to move in y direction. The nonlinear equations governing the motion of the cart

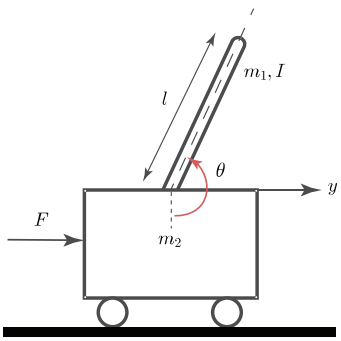


Figure 3.6: A pendulum mounted on a cart.

and pendulum are

$$(m_1 + m_2)\ddot{y} + \nu\dot{y} + m_1 l\ddot{\theta}\cos\theta - m_1 l\dot{\theta}^2 sin\theta = F$$
$$(I + m_1 l^2)\ddot{\theta} + m_1 g_0 l sin\theta = -m_1 l\ddot{y} cos\theta,$$

where ν is the damping coefficient between the pendulum and the cart and g_0 is the gravitational acceleration. We define $\theta = \pi$ as the equilibrium position of the pendulum and ϕ as small deviations from θ. We derive the linearized equations of motion using small angle approximation, noting that this linearizion is only valid for sufficiently small values of the delay upper bound γ. Define the state variable $s = [y, \dot{y}, \phi, \dot{\phi}]^T$, where y and $\dot{y}$ are the position and velocity of the cart respectively. Assuming $m_1 = 0.2$ kg, $m_2 = 0.5$ kg, $\nu = 0.1$ N/m/s, $l = 0.3$ m, $I = 0.006$ kg/m^2, one can write the evolution of s in time as

$$\dot{s} = As(t) + Bu(t) + w(t), \tag{3.48}$$

where

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -0.1818 & 2.6730 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & -0.4545 & 31.1800 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 \\ 1.8180 \\ 0 \\ 4.5450 \end{bmatrix}.$$

In addition, we add the plant noise $w(t) \in \mathbb{R}^4$ to the linearized plant model, and we assume that all of its elements are upper bounded by M. A simple feedback control law can be derived for (3.48) as $u = -Ks$, where $K = [-1.00 \; -2.04 \; 20.36 \; 3.93]$. is chosen such that $A - BK$ is Hurwitz.

The eigenvalues of the open-loop gain of the plant A are $e = [0 \; -5.6041 \; -0.1428 \; 5.5651]$. Thus, the open-loop gain of the plant A is diagonalizable (all eigenvalues of A are distinct). Using the eigenvector matrix P, we diagonalize the plant to obtain

$$\dot{\tilde{s}} = \tilde{A}\tilde{s}(t) + \tilde{B}\tilde{u}(t) + \tilde{w}(t), \tag{3.49}$$

where

$$\tilde{A} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -5.6041 & 0 & 0 \\ 0 & 0 & -0.1428 & 0 \\ 0 & 0 & 0 & 5.5651 \end{bmatrix}, \; \tilde{B} = \begin{bmatrix} 10.0000 \\ -2.3865 \\ 10.0979 \\ 2.2513 \end{bmatrix},$$

where $\tilde{s}(t) = P^{-1}s(t)$ and $\tilde{w}(t) = P^{-1}w(t)$. Also, $\tilde{u}(t) = -\tilde{K}\tilde{s}(t)$ where $\tilde{K} = KP$.

For the first three coordinates of the diagonalized plant in (3.49) the state estimation $\hat{s}$ at the controller simply constructs as $\dot{\hat{s}}_i = \tilde{A}_i\hat{s}(t) + \tilde{B}_i\tilde{u}(t)$, starting from $\hat{s}_i(0)$ for $i \in \{1, 2, 3\}$, where $\tilde{A}_i$ and $\tilde{B}_i$ denote the i^{th} row of $\tilde{A}$ and $\tilde{B}$. Since the first three eigenvalues of A are

non-positive, they are inherently stable. Thus, by the data theorem [174] there is no need to use the communication channel for them, and since $\tilde{A} - \tilde{B}\tilde{K}$ is Hurwitz, $\tilde{u}(t) = -\tilde{K}\tilde{s}(t)$ renders them ISS with respect to system disturbances. Now we apply Theorem 10 to the fourth mode of the plant, which is unstable, to make the whole plant ISpS. In fact, we use the packet size given in (3.20) for the simulations. Using the problem formulation in Section 3.2, the estimated state for the unstable mode $\hat{s}_4$ evolves during the inter-reception times as

$$\dot{\hat{s}}_4(t) = 5.5651\hat{s}_4(t) + 2.2513\tilde{u}(t), \quad t \in (t_c^k, t_c^{k+1}), \tag{3.50}$$

starting from $\hat{s}_4(t_c^{k+})$ and $\hat{s}_4(0)$. Also, a triggering occurs when $|\tilde{z}_4(t)| = |\tilde{s}_4(t) - \hat{s}_4(t)| = J$, where $|\tilde{z}_4(t)|$ is the estate estimation error for the unstable mode, and assuming the previous packet is already delivered to the controller. In the simulation environment, since the sampling time is small, a triggering happens as soon as $|\tilde{z}_4(t)|$ is equal or greater than J and the previous packet has been recived by the controller. Let $\lambda_4 = 5.5651$ be the eigenvalue corresponding to the unstable mode. By Theorem 10, we choose $J = (M/(\lambda_4\rho_0))(e^{\lambda_4\gamma} - 1) + 0.005$, and the size of the packet for all t_s to be (3.20), where $b = 1.0001$ and $\rho_0 = 0.9$.

A set of two simulations are carried out as follows. In simulation (a) the plant disturbance is upper bounded by $M = 0.05$ and channel delay is upper bounded by the two sampling time $2\delta'$. In simulation (b), the plant disturbance is upper bounded by $M = 0.05$ and channel delay is upper bounded by $\gamma = 0.1$. Each row in Figure 3.7 presents a different simulation. The first column shows the triggering function for $\tilde{s}_4$ in (3.49) and the absolute value of the state estimation error for the unstable coordinate, that is, $|\tilde{z}_4(t)| = |\tilde{s}_4(t) - \hat{s}_4(t)|$. As soon as the absolute value of this error is equal or greater than the triggering function, the sensor transmits a packet, and the jumping strategy adjusts $\hat{s}_4$ at the reception time to ensure the plant is practically stable. Note that the amount this error exceeds the triggering function depends on the random channel delay upper bounded by γ. Since γ in simulation (b) is larger than in simulation (a), the absolute value of the

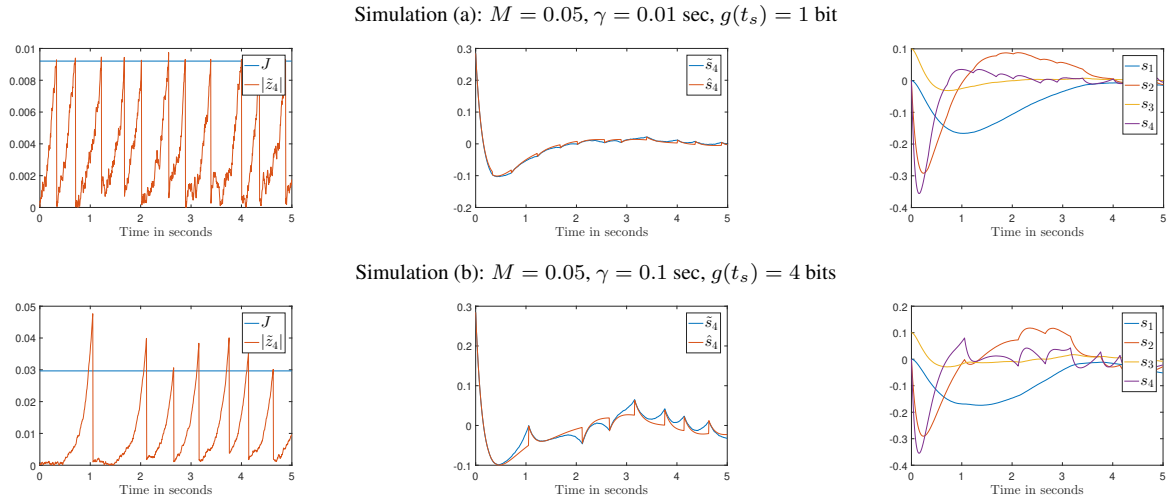


Figure 3.7: Simulation results: The following simulation parameters are chosen for the system: simulation time $T = 5$ seconds, sampling time $\delta' = 0.005$ seconds, $\tilde{s}(0) = P^{-1}[0, 0, 0, 0.1001]^T$, and $\hat{s}(0) = P^{-1}[0, 0, 0, 0.10]^T$. The first column represents the evolution of the absolute value of state estimation error for the unstable mode of the plant in (3.49). The second column represents the evolution of the unstable state in (3.49), and its estimate in (3.50). Finally, and the last column represents the evolution of all the actual states of the plant given in (3.48) in time.

state estimation error grows beyond the triggering function depending on the random delay in the communication channel. The second column of Figure 3.7 presents the evolution of the unstable state in (3.49) and its estimation in (3.50). The last column in Figure 3.7 represents the evolution of all the actual states of the linearized plant (3.48) in time. In the second and third columns, as expected, when γ increases, the controller performance deteriorate significantly. However, all the states of the plant remain bounded and the plant is ISPS.

Finally, Figure 3.8 presents the simulation of information transmission rate versus the delay upper bound γ in the communication channel for stabilizing the linearized model of the inverted pendulum. It can be seen that for small γ, the plant is ISpS with an information transmission rate smaller than the one prescribed by the data-rate theorem.

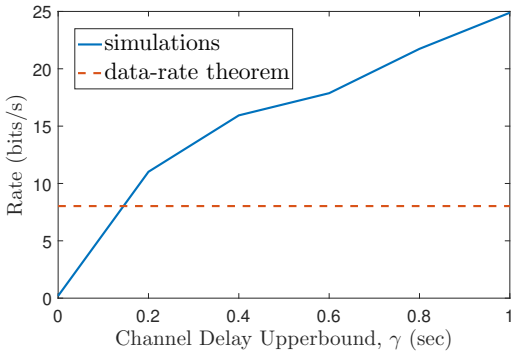


Figure 3.8: Information transmission rate in simulations compared to the data-rate theorem. Note that the rate calculated from simulations does not start at $\gamma = 0$ because the minimum channel delay upper bound is equal to two sampling time (0.005 seconds in this example). M is chosen to be 0.2 in these simulations, and simulation time is $T = 5$ seconds.

3.6.2 Event-triggered control of complex systems

We consider the state and state estimation as in (3.34) and (3.4) where $A = 2 + 0.5i$, $B = 0.5$, and the control input is chosen as $u(t) = -8\hat{x}(t)$. Using (3.40b), triggering radius J in (3.35) can be found as follows:

$$J = \frac{8M(e^{\mathrm{Re}(A)\gamma} - 1)}{\mathrm{Re}(A)} + \delta',$$

Also, to quantize the phase, using (3.40c) we calculate λ as follows:

$$\lambda = \left\lceil \log \left(\frac{\pi}{\arcsin\left(\frac{7/8}{2e^{\mathrm{Re}(A)\gamma}}\right)} \right) \right\rceil$$

We carry out a set of two different simulations. In *simulation (a)*, we assume the plant disturbance is upper bounded by $M = 0.1$ and the channel delay is upper bounded by two sampling times. For *simulation (b)*, we assume the plant disturbance is upper bounded by $M = 2$ and the channel delay is upper bounded by $\gamma = 1.2$ seconds.

Simulation results are presented in Figure 3.9, where the first column represents norm of

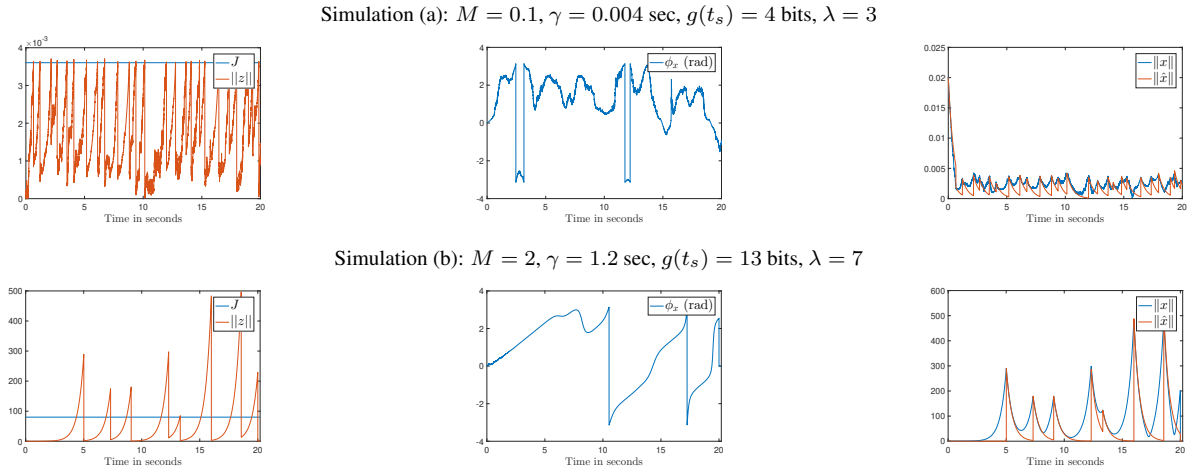


Figure 3.9: The first column represents norm of state estimation error. The second column represents variations of phase angle of the complex state x, and the last column represents evolution of the real component of x and $\hat{x}$ in time. In these simulations $A = 2.5 + 0.5i$, $B = 0.5$, $\rho_0 = 0.9$, $b = 1.0001$, $x_0 = 0.2001$, $\hat{x}_0 = 0.2000$, $\delta' = 0.002$ second, and simulation time $T = 20$ seconds.

the error $\|z(t)\|$, and triggering radius J, the second column represents the evolution of $\phi_{x(t)}$ and the third column represents the evolution of $\|x(t)\|$ in time. In the simulation (b), despite having large delays and large disturbances, the controller is able to stabilize the plant. As we can see in the plot, the estimate of the state at the controller tracks the norm and phase of the state. In the first column, sudden changes in the norm of the state estimation error represent reception of the transmitted packet at the controller.

3.7 Implementation

The majority of results on control under communication constraints are restricted to theoretical works. Here for the first time, we examine data-rate theorems in a practical setting, using an inverted pendulum. We implement the event-triggering control design introduced in Section 3.4.1, and demonstrate the utilization of timing information to stabilize a laboratory-scale inverted pendulum over a digital communication channel with bounded unknown delay,

see Figure 3.1.

3.7.1 Plant Dynamics

We consider a linearized version of the two-dimensional problem of balancing an inverted pendulum with two propellers, where the motion of the pendulum is constrained in a plane and its position can be measured by an angle ϕ representing small deviations from the upright position of the pendulum, as depicted in Figure 3.1. The inverted pendulum has mass m_1 and length l. The propellers are identical and are attached to two motors of mass m_2. m and I respectively represent the total mass of the system and its moment of inertia. Therefore, a nonlinear equation of the system can be written as follows

$$I\ddot{\phi} = mgl \sin \phi(t) + \xi(t)l + \text{noise}, \tag{3.51}$$

where g is the gravitational acceleration, and $\xi(t)$ is the resultant thrust force of the propellers (f_L and f_R as shown in Figure 3.1) generating a moment about the axis of rotation of the pendulum. Note that in this nonlinear equation the effect of the friction is included in the additive noise. The force $\xi(t)$ can be estimated as a linear function of the control input $\tilde{u}(t)$, applied to the motors, with some proportionality constant k_ξ (found from experiments), namely $\xi(t) = k_\xi \tilde{u}(t)$.

We derive the linearized equations of motion using a small angle approximation. This linearization is only valid for sufficiently small values of the delay upper bound γ in the communication channel. Linearizing (3.51) around the equilibrium point results in the following dynamics

$$I\ddot{\phi} = mgl\phi(t) + k_\xi l\tilde{u}(t) + \text{noise}.$$

By defining the state variable $\tilde{\boldsymbol{x}} = (\phi, \dot{\phi})^T$, the state-space equations can be written as follows

$$\dot{\tilde{\boldsymbol{x}}} = \tilde{\mathbf{A}}\tilde{\boldsymbol{x}} + \tilde{\mathbf{B}}\tilde{u}(t) + \tilde{\boldsymbol{w}}(t), \tag{3.52}$$

where

$$\tilde{\mathbf{A}} = \begin{bmatrix} 0 & 1 \\ \frac{mgl}{I} & 0 \end{bmatrix}, \tilde{\mathbf{B}} = \begin{bmatrix} 0 \\ \frac{k_\xi l}{I} \end{bmatrix}.$$

In our prototype shown in Figure 3.1, the pendulum is a plywood sheet of size $0.18 \times 0.073 \times 0.005$ m and mass $m_1 = 0.030$ kg. The motors are of mass $m_2 = 0.010$ kg. Also, $l = 0.180$ m, and $g = 9.81$ m/s^2. Using first principles, one can find the moment of inertia of the pendulum about its axis of rotation to be $I = 3.57 \times 10^{-4}$ kg/m^2. By experiments, we approximate $k_\xi = 0.001$. Therefore, the system (3.52) can be rewritten as follows

$$\dot{\tilde{\boldsymbol{x}}} = \begin{bmatrix} 0 & 1 \\ 53.58 & 0 \end{bmatrix} \tilde{\boldsymbol{x}} + \begin{bmatrix} 0 \\ 0.50 \end{bmatrix} \tilde{u}(t) + \tilde{\boldsymbol{w}}(t). \tag{3.53}$$

Using (3.52) it follows $\tilde{w}_1(t) = 0$. Also, by experiments we deduce $|w_2(t)|$ is upper bounded by 0.02.

Now using the eigenvector matrix

$$\mathbf{P} = \begin{bmatrix} 0.1354 & -0.1354 \\ 0.9908 & 0.9908 \end{bmatrix}$$

of matrix $\tilde{\mathbf{A}}$ we consider a canonical transformation to diagonalize the system (3.53) as follows

$$\dot{\boldsymbol{x}} = \mathbf{A}\boldsymbol{x}(t) + \mathbf{B}u(t) + \boldsymbol{w}(t), \tag{3.54}$$

where $\mathbf{A} = \mathbf{P}^{-1}\tilde{\mathbf{A}}\mathbf{P}$, $\mathbf{B} = \mathbf{P}^{-1}\tilde{\mathbf{B}}$, $\boldsymbol{x}(t) = \mathbf{P}^{-1}\tilde{\boldsymbol{x}}(t)$ and $\boldsymbol{w}(t) = \mathbf{P}^{-1}\tilde{\boldsymbol{w}}(t)$. Therefore, for the

diagonalized system (3.54) we have

$$\mathbf{A} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} = \begin{bmatrix} 7.3198 & 0 \\ 0 & -7.3198 \end{bmatrix},$$
$$\mathbf{B} = \begin{bmatrix} 0.2523 \\ 0.2523 \end{bmatrix},\ \boldsymbol{x} = \begin{bmatrix} 3.6940\phi + 0.5046\dot{\phi} \\ 0.5046\dot{\phi} - 3.6940\phi \end{bmatrix},$$
$$|w_i(t)| \leq M = 0.0470 \ \text{ for } i \in \{1, 2\},$$

where the upper bound M on the $|w_i(t)|$ for $i \in \{1, 2\}$ is found by taking the maximum of upper bounds of all the elements in $\boldsymbol{w}(t)$.

Since λ_2 in (3.54) is negative, the second coordinate is inherently stable, and we do not need to transmit updates about the second coordinate to the controller via the communication channel. However, since λ_1 is positive, the uncertainty about the first coordinate grows exponentially at the controller, hence the sensor needs to communicate information to the controller about the state of the first coordinate to render the plant ISpS.

3.7.2 Implementation and System Architecture

We now present the details of the implementation of the proposed event-triggered control scheme on a real system, along with experimental results validating the theory. The prototype used is an inverted pendulum system built using off-the-shelf components. The body of the system is made of plywood sheets, as depicted in Figure 3.1. For sensors, we use InvenSense MPU6050 MEMS sensor which has a 3-axis accelerometer and a 3-axis gyroscope, and we use a complementary filter to read the angle and angular velocity of the pendulum. We choose Raspberry Pi Model 3 for the computation unit and the controller in the system. For actuation, we use two small DC motors equipped with two identical propellers. Figure 1.5 depicts the different components of the system.

Using the plant dynamics introduced in (3.54), we implement the event-triggered control scheme proposed in Section 3.4.1 on the prototype system. While our theory is developed for continuous-time plants, the experiments are performed on digital systems and in discrete-time domain with small enough sampling time δ to make the discrete-time model as close to the continuous-time model as possible. Because of this discretization, the minimum upper bound for the channel delay is equal to two sampling times. A delay of at most one sampling time exists from the time that a triggering occurs to the time that the sensor takes a sample from the plant state and another delay of at most one sampling time exists from the time that the packet is received to the time the control input is applied to the plant. In the experiments, a triggering occurs as soon as z_1 is equal or greater than J and the controller has received the previous packet, in this way since the sampling time is small, at the triggering time, equation (3.6) will be valid approximately.

To simulate the digital channel between the sensor and the controller, we send packets composed of a finite number of bits from the sensor to the controller with a delay, that is a multiple of the sampling time δ, upper bounded by γ.

3.7.3 Experimental results

In this section, experimental results for various scenarios are presented. In all the experiments, the sampling time δ is 0.003 seconds, which is the smallest sampling time that the measurements from our sensors permit. Also we set $\rho_0 = 0.01$, $b = 1.00001$, and $J = \frac{M}{\lambda_1 \rho_0}(e^{\lambda_1 \gamma} - 1) + 0.1$. In the first set of experiments, we evaluate the performance of the controller for different values of γ. In Figure 3.11, the first row presents the results when $\gamma = 0.006$ seconds or two sampling times and the second row presents the results when $\gamma = 0.015$ seconds or five sampling times. The first column is the evolution of the absolute value of the state estimation error (3.5) (red) in time along with the triggering threshold (blue). As the absolute value of this error is greater than or equal to the triggering function, a triggering occurs and the sensor transmits a packet to

the controller. However, due to the random delay (upper bounded by γ) in the communication channel, this error could grow beyond the triggering function. This growth, of course, can become larger as γ increases which is shown in the first column of Figure 3.11. The first column also shows, more triggering occurred when the channel delay is upper bounded with five sampling times.

The second column in Figure 3.11 presents the evolution of the state x_1 (blue) corresponding to the unstable pole in the diagonalized system (3.54) and its estimate $\hat{x}_1$ (red) in time. The last column shows the evolution of the actual states of the system, namely the angle of the pendulum in radians and its rate of change in radians/sec. It can be seen that $|\phi|$ remains less than 0.2 radians which ensures the linearization of (3.51) remains valid and is a good approximation.

We repeat the experiments for different values of γ and calculate the sufficient transmission rate using (2.9). According to the data-rate theorem, to stabilize the plant, the information rate communicated over the channel in data payload and timing should be larger than the entropy rate of the plant (see chapter [88]). In our experiments, when $\gamma = 2\delta$ the timing information is substantial, therefore, the information transmission rate becomes smaller than the entropy rate of the plant which is shown in Figure 3.10. Furthermore, according to the theory developed in Section 3.4.1 as γ increases, more information has to be sent via data payload for stabilization since larger delay corresponds to more uncertainties about the value of the states at the controller and less timing information.

Finally, the robustness of the controller is evaluated against additional disturbances and the results are shown in Figure 3.12. The additional disturbances are applied to the system at time $t = 2$ seconds and the evolution of $|z_1|$, x_1 and $\hat{x}_1$ in time are presented. It can be seen that even in presence of additional disturbances which are quite large, the event-triggered control policy is able to stabilize the system.

Remark 17. Similar to our analysis in Section 3.4.1, we assume the plant disturbance is random but bounded. In most of our experiments, we successfully stabilized inverted pendulum around

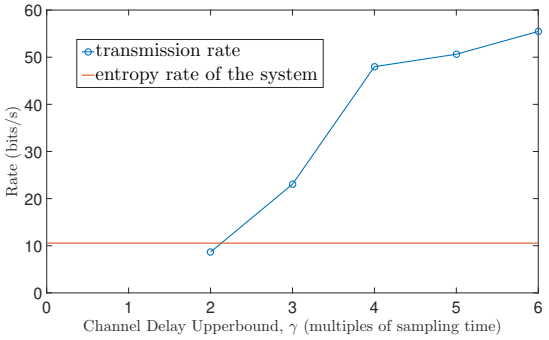


Figure 3.10: Information transmission rate in experiments compared with the entropy rate of the system. Note that the rate calculated from experiments does not start at zero worst-case delay because the minimum channel delay upper bound is equal to two sampling times (0.006 seconds). The entropy rate of the system is equal to $\lambda_1/\ln 2 = 10.56$ bits/sec while the minimum transmission rate for worst-case delay equal to two sampling time in the experiments is equal to 8.66 bits/sec.

its equilibrium point. Disturbances outside the prescribed limits occur rarely, but can still happen occasionally. Assuming that the disturbances are unbounded one might be able to extend the second-moment stability results of [141] to our setup. Similarly, the case where the delay in the communication channel becomes unbounded with a positive probability is another interesting research problem. •

3.8 Extension to nonlinear systems

The results developed in Section 3.4.1 are restricted to linear systems, and they can only stabilize the pendulum (3.51) locally, where the linear approximation is valid. Thus, now we develop a novel event-triggering scheme that encodes information in timing and under appropriate assumptions renders a continuous-time nonlinear system with disturbances ISpS. Clearly, the results of this section compare to the results of Section 3.4.1 are more sophisticated to analyze and implement. From the system's perspective, our set-up is closest to the one in [115, 174], as we consider locally Lipschitz nonlinear systems that can be made input-to-state stable (ISS) [183] with respect to the state estimation error and system disturbances. Using our encoding-decoding

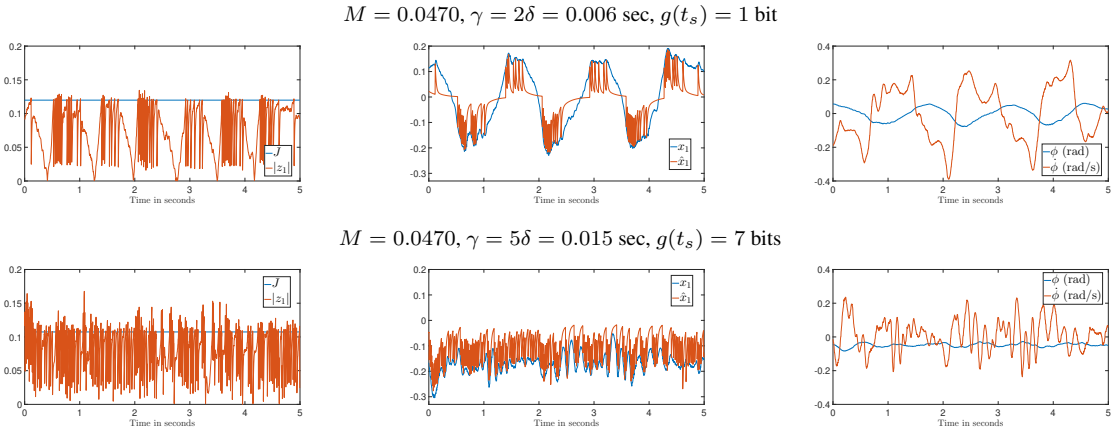


Figure 3.11: Experimental results for stabilizing the inverted pendulum over a digital channel with random delay upper bounded by two sampling times (first row) and five sampling times (second row). When $\gamma = 2\delta$, the packet size is 1 bit and when $\gamma = 5\delta$, the packet size becomes 7 bits.

scheme, we encode the information in timing via event-triggering control in a state-dependent fashion to achieve input-to-state practical stability (ISpS) in the presence of unknown but bounded delay. We also discuss the different approaches to eliminate the ISS assumption.

We consider sensor, communication channel, controller system depicted in Figure 2.1, and a continuous nonlinear plant

$$\dot{x} = f(x(t), u(t), w(t)), \tag{3.55}$$

where x, u, and w are real numbers representing the plant state, control input, and plant distur-

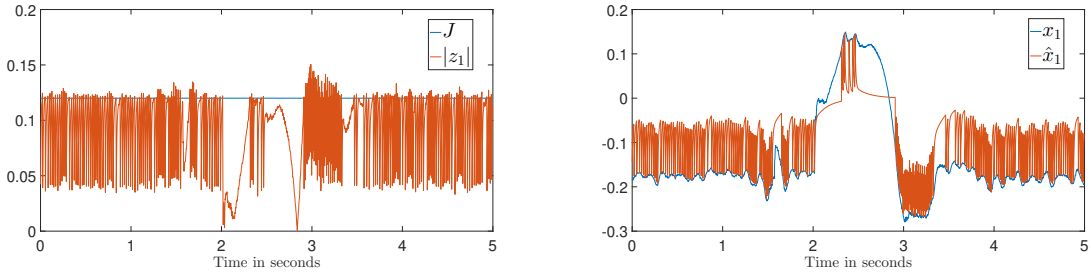


Figure 3.12: Robustness of the event-triggered control strategy against additional disturbances.

bance. Furthermore, we assume that for all time $t \geq 0$

$$|w(t)| \leq M. \tag{3.56}$$

As in (3.4), the controller constructs the state estimation $\hat{x}$, which evolves during the inter-reception times as

$$\dot{\hat{x}} = f(\hat{x}(t), u(t), 0) \quad t \in (t_c^k, t_c^{k+1}), \tag{3.57}$$

starting at $\hat{x}(t_c^{k+})$ that is constructed by the controller using information received up to time t_c^{k+}. The explicit way to construct $\hat{x}(t_c^{k+})$ will be explained later in this section (see (3.74)). As discussed in Section 3.4.1, we assume the sensor can also calculate the controller's state estimate $\hat{x}(t)$.

The state estimation error is defined as (3.5), thus for $t \in (t_c^k, t_c^{k+1})$ we have

$$\dot{z} = f(x(t), u(t), w(t)) - f(\hat{x}(t), u(t), 0). \tag{3.58}$$

A triggering occurs at time

$$t_s^k = k(\alpha + \gamma) \tag{3.59}$$

and the sensor transmits a packet $p(t_s)$ of length $g(t_s)$ to the controller if

$$|z_1(t_s^k)| \geq J, \tag{3.60}$$

where J and α are non-negative real numbers, γ is the upper bound on the channel delay, $k \in \mathbb{N}$,

and $t_s^0 = 0$. We choose $g(t_s)$ such that after decoding we have

$$|z(t_c^{k+})| \leq J. \tag{3.61}$$

Clearly, the periodic event-triggering scheme (3.59) and (3.60) does not exhibit Zeno behavior, meaning that there cannot be infinitely many triggering events in a finite time interval. In fact, we have

$$\Delta_k' = t_s^{k+1} - t_s^k \geq \alpha + \gamma. \tag{3.62}$$

Remark 18. Unlike the linear case, a closed form solution of (3.58) is not known in general. Consequently, to simplify the encoding process, we use the periodic event-triggering scheme (3.59) and (3.60) (cf. [69]), which is different from the continues time event-triggering scheme (3.6) where a triggering could occur at any time $t_s^k \geq 0$. •

Assumption 3 *The dynamic* (3.55) *satisfies the Lipschitz property*

$$|f(x,u,w) - f(\hat{x},u,0)| \leq L_x|x-\hat{x}| + L_w|w|, \tag{3.63}$$

where $L_x > 0$, $L_w > 0$, *and*

$$|z(t)| = |x(t) - \hat{x}(t)| \leq \Upsilon(\gamma). \tag{3.64}$$

Here for all $0 \leq \vartheta \leq \gamma$, $\Upsilon(\vartheta)$ *is defined as follows*

$$\Upsilon(\vartheta) := Je^{L_x(\alpha+\gamma+\vartheta)} + \frac{L_w M}{L_x}\left(e^{L_x(\alpha+\gamma+\vartheta)} - 1\right). \tag{3.65}$$

The reason for choosing the specific value for $\Upsilon(\gamma)$ in (3.64) will become clear by looking at the

following Lemma. If a triggering occurs at time t_s^k, we define

$$\underline{t}^k = \inf\left\{t \in (t_s^{k-1}, t_s^k] \; ; \; |z(t)| = J\right\}. \tag{3.66}$$

By continuity of z during the inter-reception time, and using (3.58) and (3.61), we see that $\underline{t}^k$ is well defined. This definition is used in the next Lemma.

Lemma 13. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.55) *satisfying Lipschitz property* (3.63), *estimator dynamics* (3.57), *triggering strategy* (3.59), *and* (3.60). *Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$ *and* (3.61) *occurs at all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$. *Then for all time* $t \in [\underline{t}^k, t_c^k)$, *where* $\vartheta = t - t_s^k$, *we have*

$$\begin{aligned} &|z(t)| \leq \\ &\Upsilon_w(\vartheta) := Je^{L_x(\alpha+\gamma+\vartheta)} + \frac{L_w|w|_t}{L_x}\left(e^{L_x(\alpha+\gamma+\vartheta)} - 1\right). \end{aligned} \tag{3.67}$$

Proof. For all time $t \in [\underline{t}^k, t_c^k)$ the state estimation error evolves according to (3.58) with the initial condition $z(\underline{t}^k) = J$, where $\underline{t}^k$ is defined as (3.66). Thus, for all $t \in [\underline{t}^k, t_c^k)$

$$\begin{aligned} |z(t)| &\leq Je^{L_x(t-\underline{t}^k)} + L_w\int_{\underline{t}^k}^t |w(t)e^{L_x(t-\underline{t}^k)}|dt && \text{(3.68a)} \\ &\leq Je^{L_x(t-\underline{t}^k)} + \frac{L_w|w|_t}{L_x}\left(e^{L_x(t-\underline{t}^k)} - 1\right) \\ &= Je^{L_x(t-t_s+t_s-\underline{t}^k)} + \frac{L_w|w|_t}{L_x}\left(e^{L_x(t-t_s+t_s-\underline{t}^k)} - 1\right) \\ &\leq Je^{L_x(\vartheta+\alpha+\gamma)} + \frac{L_w|w|_t}{L_x}\left(e^{L_x(\vartheta+\alpha+\gamma)} - 1\right), && \text{(3.68b)} \end{aligned}$$

where (3.68a) follows from the Lipschitz property (3.63) and Gronwall-Bellman inequality, as $\underline{t}^k \in (t_s^{k-1}, t_s^k]$ we have $t_s^k - \underline{t}^k \leq \alpha + \gamma$ and (3.68b) follows. ∎

Lemma 13 has two important implications. First, if a triggering event does not occur at t_s^k

for all $t \in (t_s^{k-1}, t_s^k]$ we have $|z(t)| \leq J$, hence using (3.61), under the assumptions of Lemma 13 for all time $t \geq 0$ we have

$$|z(t)| \leq \Upsilon_w(\vartheta) \overset{(a)}{\leq} \Upsilon_w(\gamma) \overset{(b)}{\leq} \Upsilon(\gamma), \tag{3.69}$$

where (a) follows from $\vartheta \leq \gamma$, and (b) follows from (3.56) and (3.65). Also, this last inequality explains why we defined the Lipschitz property as (3.64). The second important implication of Lemma 13 is that for all $k \in \mathbb{N}$ we have

$$z(t_s^k) \in [-\Upsilon(0), \Upsilon(0)].$$

To construct the packet $p(t_s)$ of length $g(t_s)$, we uniformly quantize the interval $[-\Upsilon(0), \Upsilon(0)]$ into $2^{g(t_s)}$ equal intervals of size $2\gamma(0)/2^{g(t_s)}$. Once the controller receives the packet, it determines the correct sub-interval and selects its center point as the estimate of $z(t_s^k)$, which is represented by $\bar{z}(t_s)$. In this case, we have

$$|z(t_s) - \bar{z}(t_s)| \leq \Upsilon(0)/2^{g(t_s)}. \tag{3.70}$$

By (3.5) we have $x(t_s) = z(t_s) + \hat{x}(t_s)$, thus using $\bar{z}(t_s)$ the controller can construct an estimate of $x(t_s)$ which we denote by $\bar{x}(t_s)$ as follows

$$\bar{x}(t_s) = \bar{z}(t_s) + \hat{x}(t_s). \tag{3.71}$$

By (3.70) we deduce that

$$|\bar{x}(t_s) - x(t_s)| \leq \Upsilon(0)/2^{g(t_s)}. \tag{3.72}$$

For all $t \in [t_s, t_c]$ consider the differential equation

$$\dot{\bar{x}} = f(\bar{x}(t), u(t), 0) \tag{3.73}$$

with initial condition $\bar{x}(t_s)$ given in (3.71), and let its solution at time t_c be equal to $\hat{x}(t_c^+)$, namely

$$\hat{x}(t_c^+) = \bar{x}(t_s) + \int_{t_s}^{t_c} f(\bar{x}(t), u(t), 0). \tag{3.74}$$

We use the above quantization policy to find a sufficient packet size in the next Theorem.

Theorem 14. *Consider the plant-sensor-channel-controller model with plant dynamics* (3.55) *with Lipschitz property* (3.63)*, estimator dynamics* (3.57)*, triggering strategy* (3.59)*, and* (3.60)*. Assume* $|z(0)| = |x(0) - \hat{x}(0)| < J$*, then there exists a quantization policy that achieves* (3.61) *for all reception times* $\{t_c^k\}_{k\in\mathbb{N}}$ *with any packet size*

$$g(t_s) \geq \max\left\{0, \log\left(\frac{\Upsilon(0)e^{L_x\gamma}}{J - \frac{L_w M}{L_x}\left(e^{L_x\gamma} - 1\right)}\right)\right\}, \tag{3.75}$$

provided

$$J \geq \frac{L_w M}{L_x}\left(e^{L_x\gamma} - 1\right). \tag{3.76}$$

Proof. For all $t \in [t_s, t_c]$ we have

$$|x(t) - \bar{x}(t)| = |x(t_s) - \bar{x}(t_s)| + \left| \int_{t_s}^{t} f(x, u, w)dt - \int_{t_s}^{t} f(\bar{x}, u, 0)dt \right| \leq \tag{3.77a}$$

$$|x(t_s) - \bar{x}(t_s)| + \int_{t_s}^{t} \left(L_x|x - \bar{x}| + L_w|w| \right) dt \leq \tag{3.77b}$$

$$|x(t_s) - \bar{x}(t_s)|e^{L_x(t-t_s)} + L_w \int_{t_s}^{t} |w(t)e^{L_x(t-t_s)}|dt \leq \tag{3.77c}$$

$$|x(t_s) - \bar{x}(t_s)|e^{L_x(t-t_s)} + \frac{L_w M}{L_x} \left(e^{L_x(t-t_s)} - 1 \right) \tag{3.77d}$$

where we used (3.55) and (3.73) along the triangle inequality to arrive at (3.77a), (3.77b) follows from Lipschitz property (3.63), and (3.77c) follows from solving the linear differential equation $\dot{x}(t) - \dot{\bar{x}}(t) = L_x(x - \bar{x}) + L_w w$ with initial condition $x(t_s) - \bar{x}(t_s)$ (see Gronwall-Bellman inequality), and (3.77d) follows from (3.56).

Using (3.3), (3.72), (3.74) and (3.77) we deduce

$$|z(t_c^+)| = |x(t_c) - \hat{x}(t_c^+)| \leq \frac{\Upsilon(0)}{2^{g(t_s)}} e^{L_x\gamma} + \frac{L_w M}{L_x} \left(e^{L_x\gamma} - 1 \right).$$

Consequently,

$$\frac{\Upsilon(0)}{2^{g(t_s)}} e^{L_x\gamma} + \frac{L_w M}{L_x} \left(e^{L_x\gamma} - 1 \right) \leq J \tag{3.78}$$

suffices to ensure (3.61) at all reception time. Using (3.76), (3.78) is equivalent to

$$2^{g(t_s)} \geq \frac{\Upsilon(0) e^{L_x\gamma}}{J - \frac{L_w M}{L_x} \left(e^{L_x\gamma} - 1 \right)}.$$

The result now follows by noticing the packet size should be no-negative. ∎

In the next assumption we restrict the class of nonlinear systems.

Assumption 4 *There exists a control policy $u(t) = \mathfrak{U}(\hat{x}) = \mathfrak{U}(x - z)$ which renders the dynamics* (3.55) *($\dot{x} = f(x, \mathfrak{U}(x-z), w)$) ISS with respect to $z(t)$ and $w(t)$, that is, there exists $\beta' \in \mathcal{KL}$, $\Pi' \in \mathcal{K}_\infty(0)$, and $\psi' \in \mathcal{K}_\infty(0)$ such that for all $t \geq 0$*

$$|x(t)| \leq \beta'\left(|x(0)|, t\right) + \Pi'\left(|z|_t\right) + \psi'\left(|w|_t\right).$$

Remark 19. Although Assumption 4 is restrictive, it is widely used in control of nonlinear systems under communication constraint [37, 115, 174]. An exception is the work [37] which eliminated this assumption for systems without disturbances. An alternative ISS assumption which centers around state estimation $\hat{x}$ is proposed in [115] where the evolution of state estimation $\hat{x}$ is described by an *impulsive system* [71]. As in our event-triggering design the behavior of the state estimation $\hat{x}$ is described with an impulsive system (3.57) and (3.74), the study of this alternative ISS assumption for our setup with a digital communication channel with bounded but unknown delay is an interesting research venue. •

The proof of the following Corollary is in the Appendix.

Corollary 2. *Under the assumptions of Theorem 14 and Assumption 4 for any packet size lower bounded as* (3.75) *there exists a control policy which renders the dynamics* (3.55) *ISpS.*

Using (3.62) the triggering rate, the frequency at which triggering occurs, is trivially upper bounded by $(\alpha + \gamma)^{-1}$. As a result, under assumptions of Corollary 2 we deduce that for any information transmission rate (2.9)

$$R_s \geq \frac{1}{\alpha + \gamma} \max\left\{0, \log\left(\frac{\Upsilon(0) e^{L_x \gamma}}{J - \frac{L_w M}{L_x}\left(e^{L_x \gamma} - 1\right)}\right)\right\}, \tag{3.79}$$

there exists a control law that renders the dynamic (3.55) ISpS. *Proof.* Theorem 14 states that with any packet size lower bounded as (3.75) there exists a quantization policy that achieves (3.61) for all reception times $\{t_c^k\}_{k\in\mathbb{N}}$. Thus using Lemma 13 and (3.69) we deduce for all time $t \geq 0$ we have

$$|z(t)| \leq \Upsilon_w(\gamma),$$

where $\Upsilon_w(\gamma)$ is defined as (3.67). Consequently, for all time $t \geq 0$, $|z(t)|$ is upper bounded by summation of a $\mathcal{K}_\infty(d)$ function of γ with $d = Je^{L_x\alpha}$ and a $\mathcal{K}_\infty^2(0, d')$ function of $|w|_t$ and γ with $d' = (e^{L_x\alpha} - 1)L_w M/L_x$. Therefore, using Assumption 4 the result follows. ∎

Remark 20. The lower bound given on the packet size in (3.75) might not be a natural number in general. This lower bound is used to properly bound the information transmission rate (2.9) in (3.79). In addition, the lower bound (3.75) might be zero. When $g(t_s) = 0$ there is no need to put any data payload in the packet and the plant can be stabilized using only timing information. However, in this case the sensor still needs to inform the controller about the occurrence of a triggering event. Consequently, when $g(t_s) = 0$ is sufficient, the sensor can stabilize the system by transmitting a fixed symbol from a unitary alphabet to the controller (see chapter 4). In practice, the packet size should be a natural number or zero, so if we do not want to use the fixed symbol from a unitary alphabet, the packet size

$$g(t_s) = \max\left\{1, \left\lceil \log\left(\frac{\Upsilon(0)e^{L_x\gamma}}{J - \frac{L_w M}{L_x}\left(e^{L_x\gamma} - 1\right)}\right)\right\rceil\right\}, \tag{3.80}$$

is sufficient for stabilization (the latter is the one used in our simulations of Section 3.9). •

Remark 21. As we used the trivial upper bound on the triggering rate $(\alpha + \gamma)^{-1}$ to deduce the bound (3.79), this upper bound on R_s might be too conservative in general. •

Remark 22. When $\gamma = M = 0$, the data-rate theorem states that the rate at which the controller

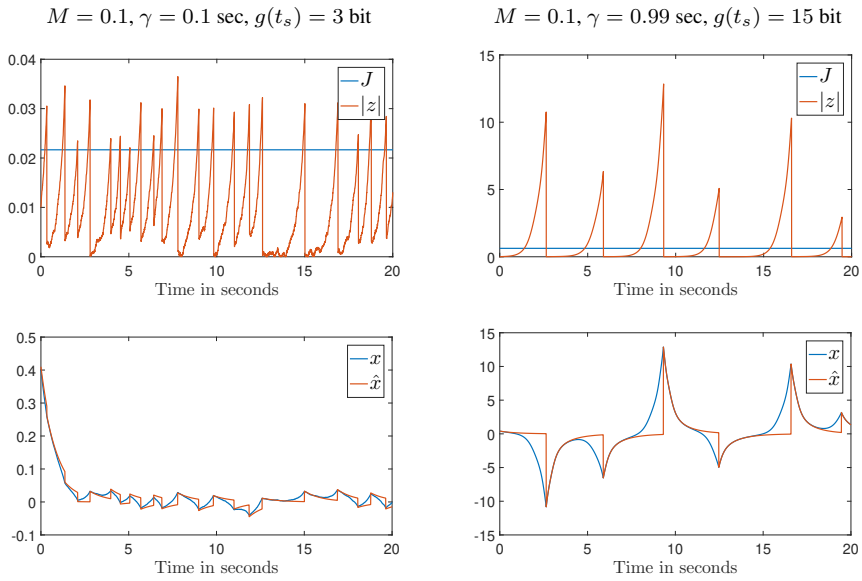


Figure 3.13: Simulation results for stabilization of the plant (3.81). We used the following parameters for the simulation: sampling time $\delta = 0.005$, simulation time $T = 20$, $u(t) = -4\hat{x}(t)$, $\alpha = 0.01$, packet size (3.80), and triggering threshhold $J = (e^{3\gamma} - 1)M/3 + 0.01$.

receives information should be at least as large as the intrinsic entropy rate of the plant defined in [142]. In our design, we can supply this information only using the implicit timing information in the triggering events. In fact, when $\alpha \to 0$ the periodic event-triggering control schemes (3.59) and (3.60) become equivalent to the continuous time event-triggering policy (3.6). In this case, in a triggering time t_s the controller can discover the exact value of $x(t_s)$ using equation $x(t_s) = \hat{x}(t_s) \pm J$ by receiving a single bit corresponding to the sign of $z(t_s)$. As there is no system disturbance, the controller then can track $x(t)$ using (3.57) after a single triggering time, and R_s (2.9) will be arbitrarily small. •

3.9 Simulations for nonlinear systems

This section presents simulation results validating the proposed nonlinear scheme. While our analysis is for continuous-time plants, we perform the simulations in discrete time with a

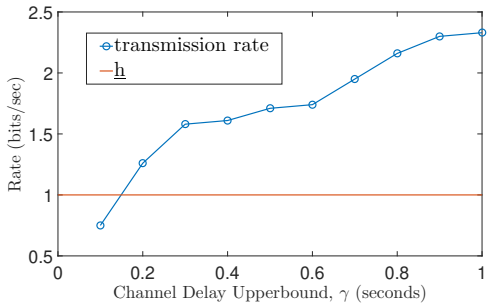


Figure 3.14: Information transmission rate in simulations compared to (3.82). We used the following parameters for the simulation: sampling time $\delta = 0.01$ seconds, simulation time $T = 100$ seconds, $u(t) = -2\hat{x}(t)$, $z(0) = 0.01$, $M = 0.05$, $\alpha = 0.01$, packet size (3.80), and triggering threshhold $J = (e^{3\gamma} - 1)M/3 + 0.05$. Note that the rate calculated from simulations can not start at $\gamma = 0$ because the minimum channel delay upper bound is equal to two sampling time.

small sampling time δ. In this case, as discussed in Section 3.7.2, the minimum upper bound for the channel delay is equal to two sampling times. We illustrate the execution of our design for the system

$$\dot{x} = f(x(t), u(t), w(t)) = 2x(t) + \sin(x(t)) + u(t) + w(t). \tag{3.81}$$

During inter-reception time, state estimation is defined according to (3.57). Thus, using (3.58), for $t \in (t_c^k, t_c^{k+1})$ we deduce

$$\dot{z}(t) = 2z(t) + \sin x - \sin \hat{x} + w(t).$$

Since $|\sin x - \sin \hat{x}| \leq |x - \hat{x}|$, the dynamics (3.81) satisfies the Lipschitz property (3.63) with $L_x = 3$, $L_w = 1$ for all $|z(t)| \in \mathbb{R}_{\geq 0}$.

A set of two simulations are carried out for different values of γ and M. Each column in Figure 3.13 presents one set of simulation. The first row shows the triggering threshold J and the absolute value of the state estimation error $|z(t)|$. If the absolute value of this error is equal to J during the period $\alpha + \gamma$, the sensor transmits a packet at the end of this period, and the jumping

strategy (3.74) adjusts $\hat{x}$ at the reception time to ensure the plant is ISpS.

Note that the amount this error exceeds the triggering function depends on the random channel delay, upper bounded by γ. The second row of Figure 3.13 presents the evolution of the state (3.81) and its estimation (3.57). As expected, when γ increases, while the plant remains ISpS the controller performance deteriorate significantly.

As discussed in Section 3.7.3, according to the data-rate theorem, to stabilize the plant, the information rate communicated over the channel in data payload and timing should be larger than the entropy rate of the plant (see Section 3.2 and [88]). Using [142] the entropy rate of the plant (3.81) at point x^* is equal to $h(x^*) = \partial f/\partial x|_{x=x^*} = 2 + \cos(x^*(t))$. Thus, for any value of the state, the information accessible to the controller about the plant or the information rate communicated over the channel in data payload and timing, should be larger than

$$h(x) \geq \underline{h} = 1. \tag{3.82}$$

Figure 3.14 presents the simulation of information transmission rate versus the delay upper bound γ in the communication channel to render (3.55) ISpS. It can be seen that for small values of γ, the plant is ISpS with an information transmission rate smaller than the one prescribed by the data-rate theorem. Furthermore, as γ increases, more information has to be sent via data payload for stabilization since larger delay corresponds to more uncertainties about the value of the states at the controller and less timing information.

3.10 Conclusion

We have presented an event-triggered control scheme for the stabilization of noisy, scalar real and complex, continuous, linear time-invariant systems over a communication channel subject to random bounded delay. We have developed an algorithm for encoding-decoding the quantized version of the estimated state, leading to the characterization of a sufficient transmission rate for

stabilizing these systems. We also identified a necessary condition on the transmission rate for real systems. Future work will study the identification of necessary conditions on the transmission rate in complex systems, develop event-triggered designs for vector systems with real and complex eigenvalues, and perform experiments with the proposed controllers in practical scenarios.

On the theoretical side, future work will explore the theory and implementation of multivariate nonlinear system with uncertainty in its parameters. On the practical validation side, we also plan to test the proposed nonlinear scheme on our inverted pendulum prototype.

Chapter 3, in part, is a reprint of the material as it appears in M. J. Khojasteh, M. Hedayatpour, J. Cortés, M. Franceschetti, "Event-triggered stabilization over digital channels of linear systems with disturbances," arXiv:1805.01969, 2018, submitted for publication in *Automatica*, and M. J. Khojasteh, M. Hedayatpour, M. Franceschetti, "Theory and implementation of event-triggered stabilization over digital channels," In *Proc. IEEE 58th Annual Conference on Decision and Control (CDC)*, 2019. The dissertation author was the primary investigator and author of these papers.

Chapter 4

Stabilizing a linear system using phone calls

4.1 Introduction

A networked control system with a feedback loop over a communication channel provides a first-order approximation of a cyber-physical system (CPS), where the interplay between the communication and control aspects of the system leads to new and unexpected analysis and design challenges [72, 97, 200]. In this setting, data-rate theorems quantify the impact of the communication channel on the ability to stabilize the system. Roughly speaking, these theorems state that stabilization requires a communication rate in the feedback loop at least as large as the intrinsic entropy rate of the system, expressed by the sum of the logarithms of its unstable eigenvalues [12, 40, 60, 121, 123, 139, 206, 212]

We consider a specific communication channel in the loop — a *timing channel*. Here, information is communicated through the timestamps of the symbols transmitted over the channel; the time is carrying the message. This formulation is motivated by recent works in event-triggering control, showing that the timing of the triggering events carries information that can be used for

stabilization [88, 91, 92, 95, 99, 119]. However, while in these works the timing information was not explicitly quantified and the analysis was limited to specific event-triggering strategies, our goal is to determine what is the value of a timestamp from an information-theoretic perspective, when this is used for control.

To illustrate the proof of concept that timing carries information useful for control, we consider the simple case of stabilization of a scalar, undisturbed, continuous-time, unstable, linear system over a timing channel and rely on the information-theoretic notion of *timing capacity* of the channel, namely the amount of information that can be encoded using time stamps [2, 4, 6, 14, 30, 64, 66, 120, 151, 160, 161, 172, 185, 193, 201]. In this setting, the sensor can communicate with the controller by choosing the timestamps at which symbols from a unitary alphabet are transmitted. The controller receives each transmitted symbol after a random delay is added to the timestamp. We show the following data-rate theorem. For the state to converge to zero in probability, the timing capacity of the channel should be at least as large as the entropy rate of the system. Conversely, in the case the random delays are exponentially distributed, we show that when the strict inequality is satisfied, we can drive the state to zero in probability by using a decoder that refines its estimate of the transmitted message every time a new symbol is received [33]. We also derive analogous necessary and sufficient conditions for the problem of estimating the state of the system with an error that tends to zero in probability.

The books [54, 123, 212] and the surveys [60, 139] provide detailed discussions of data-rate theorems and related results. A portion of the literature studied stabilization over "bit-pipe channels," where a rate-limited, possibly time-varying and erasure-prone communication channel is present in the feedback loop [70, 130, 132, 141, 191]. For more general noisy channels, Tatikonda and Mitter [190] and Matveev and Savkin [124] showed that the state of undisturbed linear systems can be forced to converge to zero almost surely (a.s.) if and only if the Shannon capacity of the channel is larger than the entropy rate of the system. In the presence of disturbances, in order to keep the state bounded a.s., a more stringent condition is required, namely the zero-error

Table 4.1: Capacity notions used to derive data-rate theorems in the literature under different notions of stability, channel types, and system disturbances.

Work	Disturbance	Channel	Stability condition	Capacity
[191]	NO	Bit-pipe	$\lvert X(t)\rvert \to 0$ a.s.	Shannon
[124, 190]	NO	DMC	$\lvert X(t)\rvert \to 0$ a.s.	Shannon
[125]	bounded	DMC	$\mathbb{P}(\sup_t \lvert X(t)\rvert < \infty) = 1$	Zero-Error
[123, Ch. 8]	bounded	DMC	$\mathbb{P}(\sup_t \lvert X(t)\rvert < K_\epsilon) > 1-\epsilon$	Shannon
[164]	bounded	DMC	$\sup_t \mathbb{E}(\lvert X(t)\rvert^m) < \infty$	Anytime
[141]	unbounded	Bit-Pipe	$\sup_t \mathbb{E}(\lvert X(t)\rvert^2) < \infty$	Shannon
[130–132]	unbounded	Var. Bit-pipe	$\sup_t \mathbb{E}(\lvert X(t)\rvert^m) < \infty$	Anytime
This chapter	NO	Timing	$\lvert X(t)\rvert \xrightarrow{P} 0$	Timing

capacity of the channel must be larger than the entropy rate of the system [125]. Nair derived a similar information-theoretic result in a non-stochastic setting [138]. Sahai and Mitter [164] considered moment-stabilization over noisy channels and in the presence of system disturbances of bounded support, and provided a data-rate theorem in terms of the anytime capacity of the channel. They showed that to keep the mth moment of the state bounded, the anytime capacity of order m should be larger than the entropy rate of the system. The anytime capacity has been further investigated in [85, 131, 144, 184]. Matveev and Savkin [123, Chapter 8] have also introduced a weaker notion of stabilty in probability, requiring the state to be bounded with probability $(1-\epsilon)$ by a constant that diverges as $\epsilon \to 0$, and showed that in this case it is possible stabilize linear systems with bounded disturbances over noisy channels provided that the Shannon capacity of the channel is larger than the entropy rate of the system. The various results, along with our contribution, are summarized in Table 4.1. The main point that can be drawn from all of these results is that the relevant capacity notion for stabilization over a communication channel critically depends on the notion of stability and on the system's model. From the system's perspective, our set-up is closest to the one in [124, 190, 191], as there are no disturbances and the objective is to drive the state to zero. Our convergence in probability provides a stronger necessary condition for stabilization, but a weaker sufficient condition than the one in these works. We

also point out that our notion of stability is considerably stronger than the notion of probabilistic stability proposed in [123, Chapter 8]. Some additional works considered nonlinear plants without disturbances [36,115,142], and switched linear systems [114,209] where communication between the sensor and the controller occurs over a bit-pipe communication channel. The recent work in [166] studies estimation of nonlinear systems over noisy communication channels, and the work in [102] investigates the trade-offs between the communication channel rate and the cost of the linear quadratic regulator for linear plants.

Parallel work in control theory has investigated the possibility of stabilizing linear systems using timing information. One primary focus of the emerging paradigm of event-triggered control [3,9,13,43,45,65,68,69,77,82,93,110,118,154,173,186,196,204] has been on minimizing the number of transmissions while simultaneously ensuring the control objective [88, 147, 187]. Rather than performing periodic communication between the system and the controller, in event-triggered control communication occurs only as needed, in an opportunistic manner. In this setting, the timing of the triggering events can carry useful information about the state of the system, that can be used for stabilization [88, 91, 92, 95, 99, 119]. In this context, it has been shown that the amount of timing information is sensitive to the delay in the communication channel. While for small delay stabilization can be achieved using only timing information and transmitting data payload (i.e. physical data) at a rate arbitrarily close to zero, for large values of the delay this is not the case, and the data payload rate must be increased [91, 95]. In this chapter we extend these results from an information-theoretic perspective, as we explicitly quantify the value of the timing information, independent of any transmission strategy. To quantify the amount of timing information alone, we restrict to transmitting symbols from a unitary alphabet, i.e. at zero data payload rate.

Research directions left open for future investigation include the study of "mixed" strategies, using both timing information and physical data transmitted over a larger alphabet, as well as generalizations to vector systems and the study of systems with disturbances. In the latter

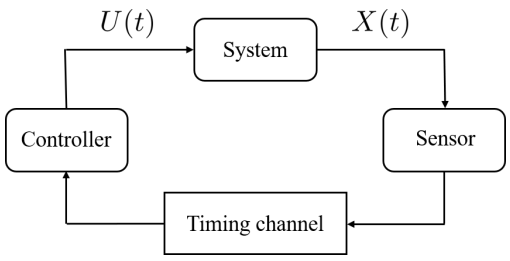


Figure 4.1: Model of a networked control system where the feedback loop is closed over a timining channel.

case, it is likely that usage of stronger notions of capacity, or weaker notions of stability, will be necessary.

In this chapter, we let $X^n = (X_1, \cdots, X_n)$ denote a vector of random variables and let $x^n = (x_1, \cdots, x_n)$ denote its realization.

4.2 System and channel model

We consider the networked control system depicted in Fig. 4.1. The system dynamics are described by a scalar, continuous-time, noiseless, linear time-invariant (LTI) system

$$\dot{X}(t) = aX(t) + bU(t), \tag{4.1}$$

where $X(t) \in \mathbb{R}$ and $U(t) \in \mathbb{R}$ are the system state and the control input respectively. The constants $a, b \in \mathbb{R}$ are such that $a > 0$ and $b \neq 0$. The initial state $X(0)$ is random and is drawn from a distribution of bounded differential entropy and bounded support, namely $h(X(0)) < \infty$ and $|X(0)| < L$, where L is known to both the sensor and the controller. Conditioned on the realization of $X(0)$, the system evolves deterministically. Both controller and sensor have knowledge of the system dynamics in (4.1). We assume the sensor can measure the state of the system with infinite precision, and the controller can apply the control input to the system with infinite precision and with zero delay.

The sensor is connected to the controller through a *timing channel* (the telephone signaling channel defined in [2]). The operation of this channel is analogous to that of a telephone system where a transmitter signals a phone call to the receiver through a "ring" and, after a random time required to establish the connection, is aware of the "ring" being received. Communication between transmitter and receiver can then occur without any vocal exchange, but encoding messages in the "waiting times" between consecutive calls.

4.2.1 The channel

We model the channel as carrying symbols ♠ from a unitary alphabet, and each transmission is received after a random delay. Every time a symbol is received, the sender is notified of the reception by an instantaneous acknowledgement. The channel is initialized with a ♠ received at time $t = 0$. After receiving the acknowledgement for the ith ♠, the sender waits for W_{i+1} seconds and then transmits the next ♠. Transmitted symbols are subject to i.i.d. random delays $\{S_i\}$. Letting D_i be the inter-reception time between two consecutive symbols, we have

$$D_i = W_i + S_i. \tag{4.2}$$

It follows that the reception time of the nth symbol is

$$\mathcal{T}_n = \sum_{i=1}^{n} D_i. \tag{4.3}$$

Fig. 4.2 provides an example of the timing channel in action.

4.2.2 Source-channel encoder

The sensor in Fig. 4.1 can act as a source and channel encoder. Based on the knowledge of the initial condition $X(0)$, system dynamics (4.1), and L, it can select the waiting times $\{W_i\}$

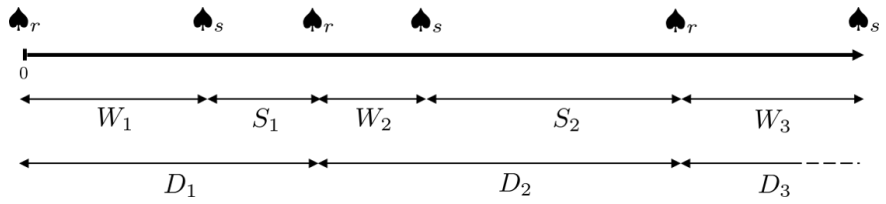


Figure 4.2: The timing channel. Subscripts s and r are used to denote sent and received symbols, respectively.

between the reception and the transmission of consecutive symbols. As in [2, 185] we assume that the causal acknowledgements received by the sensor every time a ♠ is delivered to the controller are not used to choose the waiting times, but only to avoid queuing, ensuring that every symbol is sent after the previous one has been received. In practice, the causal acknowledgment can be obtained without assuming an additional communication channel in the feedback loop. The controller can signal the acknowledgement to the sensor by applying a control input to the system that excites a specific frequency of the state each time a symbol has been received. This strategy is known in the literature as "acknowledgement through the control input" [91, 123, 164, 190].

4.2.3 Anytime decoder

At any time $t \geq 0$, the controller in Fig. 4.1 can use the inter-reception times of all the symbols received up to time t, along with the knowledge of L and of the system dynamics (4.1) to compute the control input $U(t)$ and apply it to the system. The control input can be refined over time, as the estimate of the source can be decoded with increasing accuracy when more and more symbols are received. The objective is to design an encoding and decoding strategy to stabilize the system by driving the state to zero in probability, i.e. we want $|X(t)| \xrightarrow{P} 0$ as $t \to \infty$.

Although the computational complexity of different encoding-decoding schemes is a key practical issue, in this chapter we are concerned with the existence of schemes satisfying our objective, rather than with their practical implementation.

4.2.4 Capacity of the channel

In the channel coding process, we assume the use of random codebooks, namely the waiting times $\{W_i\}$ used to encode any given message are generated at random in an i.i.d. fashion, and are also independent of the random delays $\{S_i\}$. This assumption is made for analytical convenience, and it does not change the capacity of the timing channel. The following definitions are derived from [2], incorporating our random coding assumption.

Definition 2 *A (n, M, T, δ)-i.i.d.-timing code for the telephone signaling channel consists of a codebook of M codewords $\{(w_{i,m}, i = 1, \ldots, n),\ m = 1 \ldots M\}$, where the symbols in each codeword are picked i.i.d. from a common distribution as well as a decoder, which upon observation of $(D_1, \ldots, D_n)$ selects the correct transmitted codeword with probability at least $1 - \delta$. Moreover, the codebook is such that the expected random arrival time of the nth symbol is at most T, namely*

$$\mathbb{E}\left(\mathcal{T}_n\right) \leq T.$$

Definition 3 *The rate of an (n, M, T, δ)-i.i.d.-timing code is*

$$R = (\log M)/T.$$

Definition 4 *The timing capacity C of the telephone signaling channel is the supremum of the achievable rates, namely the largest R such that for every $\gamma > 0$ there exists a sequence of $(n, M_n, T_n, \delta_{T_n})$-iid-timing codes that satisfy*

$$\frac{\log M_n}{T_n} > R - \gamma,$$

and $\delta_{T_n} \to 0$ as $n \to \infty$.

The following result [2, Theorem 8] applies to our random coding set-up, since the capacity in [2] is achieved by random codes.

Theorem 15. *[Anantharam and Verdú] The timing capacity of the telephone signaling channel is given by*

$$C = \sup_{\chi>0} \sup_{\substack{W\geq 0 \\ \mathbb{E}(W)\leq\chi}} \frac{I(W; W+S)}{\mathbb{E}(S)+\chi}, \tag{4.4}$$

and if S is exponentially distributed then

$$C = \frac{1}{e\mathbb{E}(S)} \quad \text{[nats/sec]}. \tag{4.5}$$

4.3 Main results

4.3.1 Necessary condition

To derive a necessary condition for the stabilization of the feedback loop system depicted in Fig. 4.1, we first consider the problem of estimating the state in open-loop over the timing channel. We show that for the estimation error to tend to zero in probability, the timing capacity must be greater than the entropy rate of the system. This result holds for any source and channel coding strategy adopted by the sensor, and for any strategy adopted by the controller to generate the control input. Our proof employs a rate-distortion argument to compute a lower bound on the minimum number of bits required to represent the state up to any given accuracy, and this leads to a corresponding lower bound on the required timing capacity of the channel. We then show that the same bound holds for stabilization, since in order to have $|X(t)| \xrightarrow{P} 0$ as $t \to \infty$ in closed-loop, the estimation error in open-loop must tend to zero in probability.

4.3.2 Sufficient condition

To derive a sufficient condition for stabilization, we first consider the problem of estimating the state in open-loop over the timing channel. We provide an explicit source-channel coding scheme which guarantees that if the timing capacity is larger than the entropy rate of the system, then the estimation error tends to zero in probability. We then show that this condition is also sufficient to construct a control scheme such that $|X(t)| \xrightarrow{P} 0$ as $t \to \infty$. The main idea behind our strategy is based on the realization that in the absence of disturbances all is needed to drive the state to zero is communicate the initial condition $X(0)$ to the controller with accuracy that increases exponentially over time. Once this is achieved, the controller can estimate the state $X(t)$ with increasing accuracy over time, and continuously apply an input that drives the state to zero. This idea has been exploited before in the literature [190, 191], and the problem is related to the anytime reliable transmission of a real-valued variable over a digital channel [33]. Here, we cast this problem in the framework of the timing channel. A main difficulty in our case is to ensure that we can drive the system's state to zero in probability despite the unbounded random delays occurring in the timing channel.

In the source coding process, we quantize the interval $[-L, L]$ uniformly using a tree-structured quantizer [63]. We then map the obtained source code into a channel code suitable for transmission over the timing channel, using the capacity-achieving random codebook of [2]. Given $X(0)$, the encoder picks a codeword from an arbitrarily large codebook and starts transmitting the real numbers of the codeword one by one, where each real number corresponds to a holding time, and proceeds in this way forever. Every time a sufficiently large number of symbols are received, we use a maximum likelihood decoder to successively refine the controller's estimate of $X(0)$. Namely, the controller re-estimates $X(0)$ based on the new inter-reception times and all previous inter-reception times, and uses it to compute the new state estimate of $X(t)$ and control input $U(t)$. We show that when the sensor quantizes $X(0)$ at sufficiently high resolution, and when the timing capacity is larger than the entropy rate of the system, the controller can construct

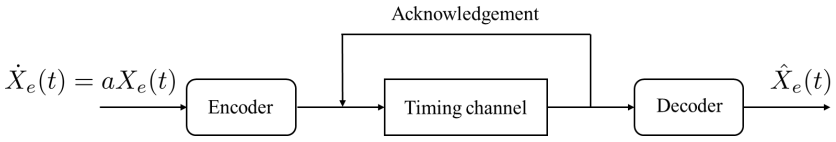


Figure 4.3: The estimation problem.

a sufficiently accurate estimate of $X(t)$ and compute $U(t)$ such that $|X(t)| \xrightarrow{P} 0$.

4.4 The estimation problem

We start considering the estimation problem depicted in Fig. 4.3. By letting $b = 0$ in (4.1) we obtain the open-loop equation

$$\dot{X}_e(t) = aX_e(t). \tag{4.6}$$

Our first objective is to obtain an estimate of the state $\hat{X}_e(t_n)$, given the reception of n symbols over the telephone signaling channel, such that $|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0$ as $n \to \infty$, at any sequence of estimation times t_n such that

$$1 < \lim_{n\to\infty} \frac{t_n}{\mathbb{E}(\mathcal{T}_n)} \leq \Gamma. \tag{4.7}$$

In practice, the condition (4.7) ensures that as $n \to \infty$ the estimation error is evaluated after n symbols have been received, see Fig. 4.4. As before, we assume that the encoder has causal knowledge of the reception times via acknowledgements through the system as depicted in Fig. 4.3.

4.4.1 Necessary condition

The next theorem provides a necessary rate for the state estimation error to tend to zero in probability.

Theorem 16. *Consider the estimation problem depicted in Fig. 4.3 with system dynamics* (4.6)*. Consider transmitting n symbols over the telephone signaling channel* (4.2)*, and a sequence of estimation times satisfying* (4.7)*. If $|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0$, then*

$$I(W; W+S) \geq a\,\Gamma\,\mathbb{E}(W+S) \quad [\text{nats}], \tag{4.8}$$

and consequently

$$C \geq \Gamma a \ \ [\text{nats/sec}]. \tag{4.9}$$

The proof of Theorem 16 is given in Appendix 4.9.

Remark 23. *The entropy-rate of our system is a nats/time [31, 32, 117, 142, 163]. This represents the amount of uncertainty per unit time generated by the sytem in open loop. Letting $\Gamma \to 1$,* (4.8) *recovers a typical scenario in data-rate theorems: to drive the error to zero the mutual information between an encoding symbol W and its received noisy version $W+S$ should be larger than the average "information growth" of the state during the inter-reception interval D, which is given by*

$$\mathbb{E}(aD) = a\,\mathbb{E}(W+S).$$

On the other hand, for any fixed $\Gamma > 1$ our result shows that we must pay a penalty of a factor of Γ in the case there is a time lag between the reception time $\mathcal{T}_n$ of the last symbol and the estimation time t_n, see Fig. 4.4. Finally, the case $\Gamma \to \infty$ requires transmission of a codeword carrying an infinite amount of information over a channel of infinite capacity, thus revealing the initial state of the system with infinite precision. This case is equivalent to transmitting a single real number over a channel without error, or a single symbol from a unitary alphabet with zero delay. •

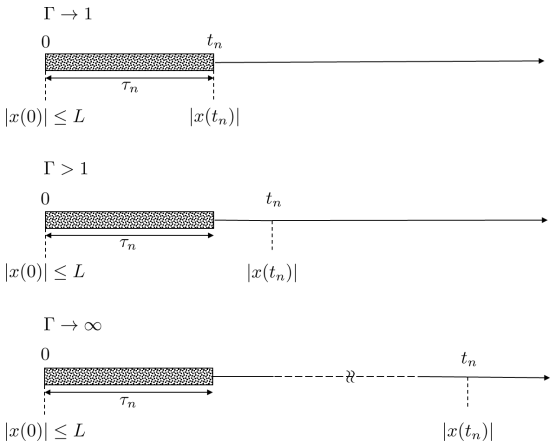


Figure 4.4: Codeword transmission and state estimation for different estimation time sequences $\{t_n\}$.

4.4.2 Sufficient condition

The next theorem provides a sufficient condition for convergence of the state estimation error to zero in probability along any sequence of estimation times t_n satisfying (4.7), in the case of exponentially distributed delays.

Theorem 17. *Consider the estimation problem depicted in Fig. 4.3 with system dynamics* (4.6)*. Consider transmitting n symbols over the telephone signaling channel* (4.2)*. Assume $\{S_i\}$ are drawn i.i.d. from exponential distribution with mean $\mathbb{E}(S)$. If the capacity of the timing channel is at least*

$$C > a\Gamma \quad [\text{nats/sec}],$$

then for any sequence of times $\{t_n\}$ that satisfies (4.7)*, we can compute an estimate $\hat{X}_e(t_n)$ such that as $n \to \infty$, we have*

$$|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0.$$

The proof of Theorem 17 is given in Appendix 4.9. The result is strengthened in the

next section (see Remark 24), showing that $C > a$ is sufficient to drive the state estimation error converges to zero in probability for all $t \to \infty$.

4.5 The stabilization problem

4.5.1 Necessary condition

We now turn to consider the stabilization problem. Our first lemma states that if in closed-loop we are able to drive the state to zero in probability, then in open-loop we are also able to estimate the state with vanishing error in probability.

Lemma 14. *Consider stabilization of the closed-loop system* (4.1) *and estimation of the open-loop system* (4.6) *over the timing channel* (4.2)*. If there exists a controller such that* $|X(t)| \xrightarrow{P} 0$ *as* $t \to \infty$*, in closed-loop, then there exists an estimator such that* $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ *as* $t \to \infty$*, in open-loop.*

Proof. From (4.1), we have in closed loop

$$X(t) = e^{at}X(0) + \zeta(t),$$
$$\zeta(t) = e^{at}\int_0^t e^{-a\varrho}bU(\varrho)d\varrho.$$

It follows that if

$$\lim_{t\to\infty} \mathbb{P}\left(|X(t)| \leq \epsilon\right) = 1,$$

then we also have

$$\lim_{t\to\infty} \mathbb{P}\left(\left|e^{at}X(0) + \zeta(t)\right| \leq \epsilon\right) = 1. \tag{4.10}$$

On the other hand, from (4.6) we have in open loop

$$X_e(t) = e^{at}X(0),$$

and we can choose $\hat{X}_e(t) = -\zeta(t)$ so that

$$|X_e(t) - \hat{X}_e(t)| = |e^{at}X(0) + \zeta(t)| \xrightarrow{P} 0,$$

where the last step follows from (4.10). ∎

The next theorem provides a necessary rate for the stabilization problem.

Theorem 18. *Consider the stabilization of the closed-loop system* (4.1)*. If* $|X(t)| \xrightarrow{P} 0$ *as* $t \to \infty$*, then*

$$I(W; W + S) \geq a\, \mathbb{E}(W + S) \quad [\text{nats}],$$

and consequently

$$C \geq a \ \ [\text{nats/sec}].$$

Proof. By Lemma 14 we have that if $|X(t)| \xrightarrow{P} 0$, then $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ for all $t \to \infty$, and in particular along a sequence $\{t_n\}$ satisfying (4.7). The result now follows from Theorem 16 letting $\Gamma \to 1$. ∎

4.5.2 Sufficient condition

Our next lemma strengthens our estimation results, stating that it is enough for the state estimation error to converge to zero in probability as $n \to \infty$ along any sequence of estimation times $\{t_n\}$ satisfying (4.7), to ensure it converges to zero for all $t \to \infty$.

Lemma 15. *Consider estimation of the system* (4.6) *over the timing channel* (4.2). *If there exists* $\Gamma_0 > 1$ *such that along the sequence of estimation times* $t_n = \Gamma_0 \mathbb{E}(\mathcal{T}_n)$ *we have* $|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0$ *as* $n \to \infty$, *then for all* $t \to \infty$ *we also have* $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$.

Proof. We have that for $t_n = \Gamma_0 \mathbb{E}(\mathcal{T}_n)$ and for all $\epsilon' > 0$, and $\phi > 0$, there exist n_ϕ such that for all $n \geq n_\phi$

$$\mathbb{P}\left(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon'\right) \leq \phi. \tag{4.11}$$

Let $t_{n_\phi} = \Gamma_0 \mathbb{E}(\mathcal{T}_{n_\phi})$ be the time at which we estimate the state for the n_ϕth time. We want to show that for all $t \in [t_{n_\phi}, t_{n_\phi+1}]$ and $\epsilon > 0$, we also have

$$\mathbb{P}\left(|X_e(t) - \hat{X}_e(t)| > \epsilon\right) \leq \phi.$$

Consider the random time $\mathcal{T}_{n_\phi}$ at which ♠ is received for the n_ϕth time. We have

$$\begin{aligned} t_{n_\phi+1} - t_{n_\phi} &= \Gamma_0 \, \mathbb{E}(\mathcal{T}_{n_\phi+1}) - \Gamma_0 \, \mathbb{E}(\mathcal{T}_{n_\phi}) \\ &= (n_\phi + 1)\Gamma_0 \, \mathbb{E}(D) - n_\phi \Gamma_0 \, \mathbb{E}(D) \\ &= \Gamma_0 \, \mathbb{E}(D). \end{aligned} \tag{4.12}$$

For all $t \in [t_{n_\phi}, t_{n_\phi+1}]$, from the open-loop equation (4.6) we have

$$X_e(t) = e^{a(t-t_{n_\phi})} X_e(t_{n_\phi}). \tag{4.13}$$

We then let

$$\hat{X}_e(t) = e^{a(t-t_{n_\phi})} \hat{X}_e(t_{n_\phi}). \tag{4.14}$$

Combining (4.13) and (4.14) and using (4.12), we obtain that for all $t \in [t_{n_\phi}, t_{n_\phi+1}]$

$$|X_e(t) - \hat{X}_e(t)| \leq e^{a\Gamma_0 \mathbb{E}(D)} |X_e(t_{n_\phi}) - \hat{X}_e(t_{n_\phi})|.$$

From which it follows that

$$\begin{aligned} &\mathbb{P}\left(|X_e(t) - \hat{X}_e(t)| > \epsilon' e^{a\Gamma_0 \mathbb{E}(D)}\right) \\ &\leq \mathbb{P}\left(|X_e(t_{n_\phi}) - \hat{X}_e(t_{n_\phi})| > \epsilon'\right). \end{aligned}$$

Since (4.11) holds for all $n \geq n_\phi$, we also have

$$\mathbb{P}\left(|X_e(t_{n_\phi}) - \hat{X}_e(t_{n_\phi})| \geq \epsilon'\right) \leq \phi.$$

We can now let $\epsilon' < \epsilon e^{-a\Gamma_0 \mathbb{E}(D)}$ and the result follows. ∎

Remark 24. *Lemma 15 yields an immediate extension of Theorem 17, showing that for exponentially distributed delays, if $C > a$ then we have $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ as $t \to \infty$. This follows by noticing that if $C > a$ then there exists a $\Gamma_0 > 1$ such that $C > a\Gamma_0$, and hence by Theorem 17 along the sequence of estimation times $t_n = \Gamma_0 \mathbb{E}(\mathcal{T}_n)$ we have $|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0$ as $n \to \infty$. Then, by Lemma 15 we also have $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ as $t \to \infty$.* •

The next key lemma states that if we are able to estimate the state with vanishing error in probability, then we are also able to drive the state to zero in probability.

Lemma 16. *Consider stabilization of the closed-loop system* (4.1) *and estimation of the open-loop system* (4.6) *over the timing channel* (4.2)*. If there exists an estimator such that $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ as $t \to \infty$, in open-loop, then there exists a controller such that $|X(t)| \xrightarrow{P} 0$ as $t \to \infty$, in closed-loop.*

Proof. We start by showing that if there exists an open-loop estimator such that $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$ as $t \to \infty$, then there also exists a closed-loop estimator such that $|X(t) - \hat{X}(t)| \xrightarrow{P} 0$ as $t \to \infty$. We construct the closed-loop estimator based on the open-loop estimator as follows. The sensor in closed-loop runs a copy of the open-loop system by constructing the virtual open-loop dynamic

$$X_e(t) = X(0)e^{at}. \tag{4.15}$$

Using the open-loop estimator, for all $t > 0$ the controller acquires the open-loop estimate $\hat{X}_e(t)$ such that $|X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0$. It then uses this estimate to construct the closed-loop estimate

$$\hat{X}(t) = \hat{X}_e(t) + e^{at} \int_0^t e^{-a\varrho} bU(\varrho) d\varrho. \tag{4.16}$$

Since from (4.1) the true state in closed loop is

$$X(t) = X(0)e^{at} + e^{at} \int_0^t e^{-a\varrho} bU(\varrho) d\varrho, \tag{4.17}$$

it follows by combining (4.15), (4.16) and (4.17) that

$$|X(t) - \hat{X}(t)| = |X_e(t) - \hat{X}_e(t)| \xrightarrow{P} 0. \tag{4.18}$$

What remains to be proven is that if $|X(t) - \hat{X}(t)| \xrightarrow{P} 0$, then there exists a controller such that $|X(t)| \xrightarrow{P} 0$.

Let $b > 0$ and choose k so large that $a - bk < 0$. Let $U(t) = -k\hat{X}(t)$. From (4.1), we have

$$\dot{X}(t) = (a - bk)X(t) + bk[X(t) - \hat{X}(t)]. \tag{4.19}$$

By solving (4.19) and using the triangle inequality, we get

$$|X(t)| \leq |e^{(a-bk)t}X(0)| + \left| \int_0^t e^{(t-\varrho)(a-bk)} bk(X(\varrho) - \hat{X}(\varrho))d\varrho \right|. \tag{4.20}$$

Since $|X(0)| < L$ and $a - bk < 0$, the first term in (4.20) tends to zero as $t \to \infty$. Namely, for any $\epsilon > 0$ there exist a number N_ϵ such that for all $t \geq N_\epsilon$, we have

$$|e^{(a-bk)t}X(0)| \leq \epsilon.$$

Since by (4.18) we have that $|X(t) - \hat{X}(t)| \xrightarrow{P} 0$, we also have that for any $\epsilon, \delta > 0$ there exist a number N'_ϵ such that for all $t \geq N'_\epsilon$, we have

$$\mathbb{P}\left(|X(t) - \hat{X}(t)| \leq \epsilon\right) \geq 1 - \delta.$$

It now follows from (4.20) that for all $t \geq \max\{N_\epsilon, N'_\epsilon\}$ the following inequality holds with probability at least $(1 - \delta)$

$$\begin{aligned} |X(t)| \leq \epsilon + bke^{t(a-bk)} \int_0^{N'_\epsilon} e^{-\varrho(a-bk)} |X(\varrho) - \hat{X}(\varrho)| d\varrho \\ + \epsilon bke^{t(a-bk)} \int_{N'_\epsilon}^t e^{-\varrho(a-bk)} d\varrho. \end{aligned} \tag{4.21}$$

Since both sensor and controller are aware that $|X(0)| < L$, by (4.15) we have that for all $t \geq 0$ the open-loop estimate acquired by the controller satisfies $\hat{X}_e(t) \in [-Le^{at}, Le^{at}]$. By (4.18) the closed-loop estimation error is the same as the open-loop estimation error, and we then have that for all $\varrho \in [0, N'_\epsilon]$

$$|X(\varrho) - \hat{X}(\varrho)| = |X_e(\varrho) - \hat{X}_e(\varrho)| \leq 2Le^{aN'_\epsilon}. \tag{4.22}$$

Substituting (4.22) into (4.21), we obtain that with probability at least $(1-\delta)$

$$\begin{aligned}|X(t)| \leq & \epsilon + 2Lbke^{[t(a-bk)+aN'_\epsilon]}\frac{e^{-N'_\epsilon(a-bk)}-1}{-(a-bk)} \\ & + \epsilon bke^{t(a-bk)}\ \frac{e^{-t(a-bk)}-e^{-N'_\epsilon(a-bk)}}{-(a-bk)}. \end{aligned} \tag{4.23}$$

By first letting ϵ be sufficiently close to zero, and then letting t be sufficiently large, we can make the right-hand side of (4.23) arbitrarily small, and the result follows. ∎

The next theorem combines the results above, providing a sufficient condition for convergence of the state to zero in probability in the case of exponentially distributed delays.

Theorem 19. *Consider the stabilization of the system* (4.1)*. Assume* $\{S_i\}$ *are drawn i.i.d. from an exponential distribution with mean* $\mathbb{E}(S)$*. If the capacity of the timing channel is at least*

$$C > a \quad [\text{nats/sec}],$$

then $|X(t)| \xrightarrow{P} 0$ *as* $t \to \infty$*.*

Proof. The result follows by combining Remark 24 and Lemma 16. ∎

4.6 Comparison with previous work

4.6.1 Comparison with stabilization over the erasure channel

In [190] the problem of stabilization of the discrete-time version of the system in (4.1) over an erasure channel has been considered. In this discrete model, at each time step of the system's evolution the sensor transmits I bits to the controller and these bits are successfully delivered with probability $1-\mu$, or they are dropped with probability μ, in an independent fashion. It is shown that a necessary condition for $X(k) \xrightarrow{a.s} 0$ is that the capacity of this I-bit erasure

channel is

$$(1-\mu)I \geq \log a \ \ [\text{bits/sec}]. \tag{4.24}$$

Since almost sure convergence implies convergence in probability, by Theorem 18 we have that the following necessary condition holds in our setting for $X(t) \xrightarrow{a.s.} 0$:

$$\frac{I(W;W+S)}{\mathbb{E}(W+S)} \geq a \quad [\text{nats/sec}]. \tag{4.25}$$

We now compare (4.24) and (4.25). The rate of expansion of the state space of the continuous system in open loop is a nats per unit time, while for the discrete system is $\log a$ bits per unit time. Accordingly, (4.24) and (4.25) are parallel to each other: in the case of (4.25) the controller must receive at least $a\mathbb{E}(W+S)$ nats representing the initial state during a time interval of average length $\mathbb{E}(W+S)$. In the case of (4.24) the controller must receive at least $\log a/(1-\mu)$ bits representing the initial state over a time interval whose average length corresponds to the average number of trials before the first successful reception

$$(1-\mu)\sum_{k=0}^{\infty}(k+1)\mu^k = \frac{1}{1-\mu}.$$

4.6.2 Comparison with event triggering strategies

The works [88, 91, 95, 99, 119] use event-triggering strategies that exploit timing information for stabilization over a digital communication channel. These strategies encode information over time in a specific state-dependent fashion and use a combination of timing information and data payload to convey information used for stabilization. Our framework, by considering transmission of symbols from a unitary alphabet, uses only timing information for stabilization. In Theorem 18 we provide a fundamental limit on the rate at which information can be encoded

in time, independent on any transmission strategy. Theorem 19 then shows that this limit can be achieved, in the case of exponentially distributed delays.

The work [99] shows that using event triggering it is possible to achieve stabilization with any positive transmission rate over a zero-delay digital communication channel. Indeed, for channels without delay achieving stabilization at zero rate is easy. One could for example transmit a single symbol at a time equal to any bijective mapping of $x(0)$ into a point of the non-negative reals. For example, we could transmit ♠ at time $t = \tan^{-1}(x(0))$ for $t \in [0, \pi]$. The reception of the symbol would reveal the initial state exactly, and the system could be stabilized.

The work in [95] shows that when delay is positive, but sufficiently small, a triggering policy can still achieve stabilization with any positive transmission rate. However, as the delay increases past a critical threshold, the timing information becomes so much out-of-date that the transmission rate must begin to increase. In our case, since the capacity of our timing channel depends on the distribution of the delay, we may also expect that a large value of the capacity, corresponding to a small average delay, would allow for stabilization to occur using only timing information. Indeed, when delays are distributed exponentially, from (4.5) and Theorems 18 and 19 it follows that as longs as the expected value of delay is

$$\mathbb{E}(S) < \frac{1}{ea},$$

it is possible to stabilize the system by using only timing information. On the other hand, the system is not stabilizable using only timing information if the expected value of the delay becomes larger than $(ea)^{-1}$.

4.7 Numerical example

We now present a numerical simulation of stabilization over the telephone signaling channel. While our analysis is for continuous time systems, the simulation is performed in

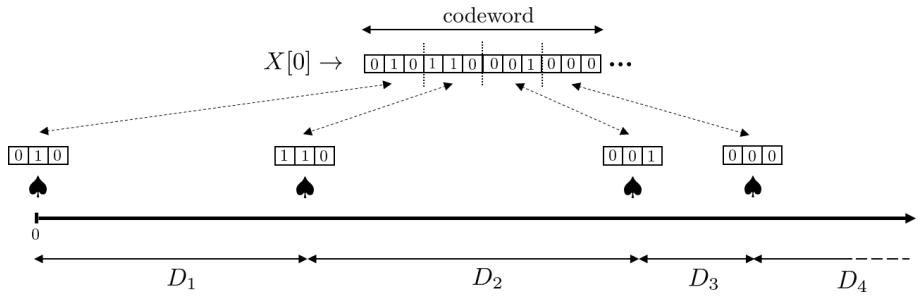


Figure 4.5: Evolution of the channel used in the simulation in an error-free case. Each time ♠ is received, a new codeword is decoded using all the symbols received up to that time. The decoded codeword represents the initial state $X[0]$ with a precision that increases by $\mathbb{E}(D)C$ bits at each symbol reception. In the figure, for illustration purposes we have assumed $\mathbb{E}(D)C = 3$ bits.

discrete time, considering the system

$$X[m] = aX[m] + U[m], \text{ for } m \in \mathbb{N},$$

where $a > 1$ so that the system is unstable.

In this case, assuming i.i.d. geometrically distributed delays $\{S_i\}$, the sufficient condition for stabilization becomes

$$C > \log a \quad [\text{nats/sec}],$$

where C is the timing capacity of the discrete telephone signaling channel [14]. The timing capacity is achieved in this case using i.i.d. waiting times $\{W_i\}$ that are distributed according to a mixture of a geometric and a delta distribution. This results in $\{D_i\}$ also being i.i.d. geometric [14, 185].

Assuming that a decoding operation occurs at time m using all k_m symbols received up to this time, and following the source-channel coding scheme described in the proof of Theorem 17,

the controller decodes an estimate $\hat{X}_m[0]$ of the initial state and estimates the current state as

$$\hat{X}[m] = a^m \hat{X}_m[0] + \sum_{j=0}^{m-1} a^{m-1-j} U[j]. \tag{4.26}$$

The estimate $\hat{X}_m[0]$ corresponds to the binary representation of $X(0)$ using $\lceil k_m \mathbb{E}(D) C \rceil$ bits, provided that there is no decoding error in the tranmsission. Accordingly, in our simulation we let $\eta > 0$ and $P_e = e^{-\eta k_m}$, and we assume that at every decoding time, with probability $(1 - P_e)$ we construct a correct quantized estimate of the initial state $\hat{X}_m[0]$ using $\lceil k_m \mathbb{E}(D) C \rceil$ bits. Alternatively, with probability P_e we construct an incorrect quantized estimate. In the case of a correct estimate, we apply the asymptotically optimal control input $U[m] = -K\hat{X}[m]$, where $K > 0$ is the control gain and $\hat{X}[m]$ is obtained from (4.26). In the case of an incorrect estimate, the state estimate used to construct the control input can be arbitrary. We consider three cases: (i) we do not apply any control input and let the system evolve in open loop, (ii) we apply the control input using the previous estimate, (iii) we apply the opposite of the asymptotically optimal control input: $U[m] = K\hat{X}[m]$. In all cases, the control input remains fixed to its most recent value during time required for a new estimate to be performed.

Fig. 4.5 pictorially illustrates the evolution of our simulation in an error-free case in which the binary representation of $X[0]$ is refined by $\mathbb{E}(D)C = 3$ bits at each symbol reception.

Numerical results are depicted in Fig. 4.6. The first and second columns represent the absolute value of the state and control input, respectively, when the timing capacity is larger than the entropy rate of the system ($C > \log a$). The third column represents the absolute value of the state when the timing capacity is smaller than the entropy rate of the system ($C < \log a$). In the first row, in the presence of a decoding error we do not apply any control input and let the system evolve in open-loop; in the second row, we apply the control using the previous estimate; the third row, we apply the opposite of the optimal control. The simulation parameters were chosen as follows: $a = 1.2$, $\mathbb{E}(D) = 2$, and $P_e = e^{-\eta k_m}$, where $\eta = 0.09$. For the optimal control gain

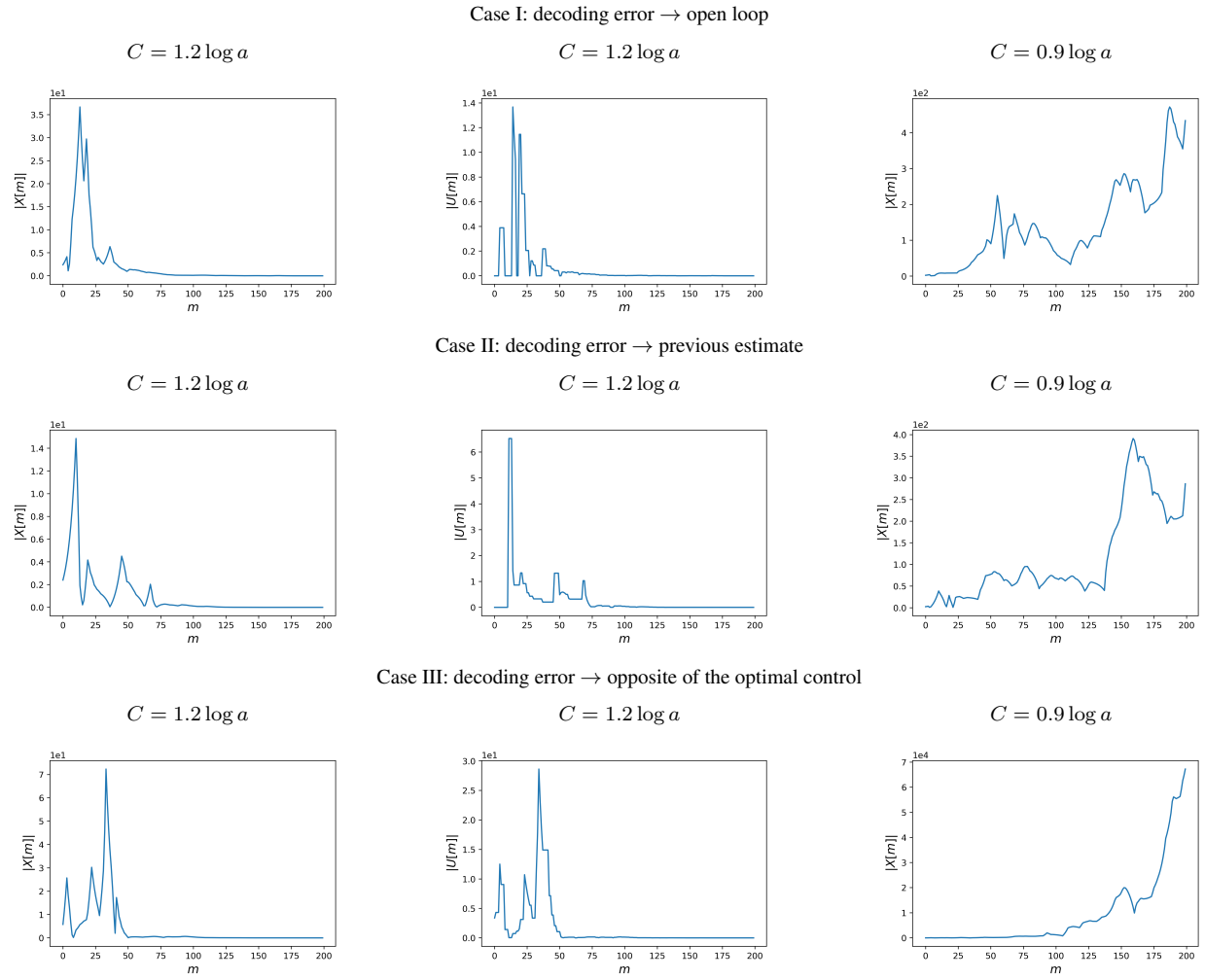


Figure 4.6: The simulation results.

we have chosen $K = 0.4$, which is optimal with respect to the (time-averaged) linear quadratic regulator (LQR) control cost $(1/200)\mathbb{E}[\sum_{m=0}^{199}(0.01X_k^2 + 0.5U_k^2) + 0.01X_{200}^2]$.

As depicted in Fig. 4.6 the state converge to zero in all cases, provided that the timing capacity is above the entropy rate of the system. In contrast, when the timing capacity is below the entropy rate, the state diverges.

Fig. 4.7 illustrates the percentage of times at which the controller successfully stabilized the plant versus the capacity of the channel in a run of 500 Monte Carlo simulations. The phase transition behavior at the critical value $C = \log a$ is clearly evident.

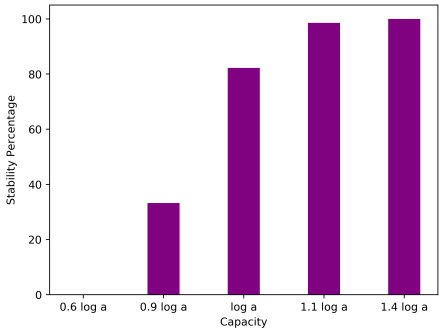


Figure 4.7: The percentage of times stabilization was achieved versus the capacity of the channel across a run of 500 simulations for each value of the capacity. Successful stabilization is defined in these simulations as $|X[250]| \leq 0.05$. In case of a decoding error, no control input is applied and we let the system evolve in open loop. The simulation parameters were chosen as follows: $a = 1.2$, $\mathbb{E}(D) = 2$, and $P_e = e^{-\eta k_m}$, where $\eta = 0.09$. For the control gain, we have chosen $K = 0.4$, which is optimal with respect to the (time-averaged) linear quadratic regulator (LQR) control cost $(1/200)\mathbb{E}[\sum_{m=0}^{199}(0.01X_k^2 + 0.5U_k^2) + 0.01X_{200}^2]$.

4.8 Conclusions

In the framework of control of dynamical systems over communication channels, it has recently been observed that event-triggering policies encoding information over time in a state-dependent fashion can exploit timing information for stabilization in addition to the information traditionally carried by data packets [88, 91, 92, 95, 99, 119]. In a more general framework, this chapter studied from an information-theoretic perspective the fundamental limitation of using *only* timing information for stabilization, independent of any transmission strategy. We showed that for stabilization of an undisturbed scalar linear system over a channel with a unitary alphabet, the timing capacity [2] should be at least as large as the entropy rate of the system. In addition, in the case of exponentially distributed delays, we provided a tight sufficient condition using a coding strategy that refines the estimate of the decoded message as more and more symbols are received. Important open problems for future research include the effect of system disturbances, understanding the combination of timing information and packets with data payload, and extensions to vector systems.

Our derivation ensures that when the timing capacity is larger than the entropy rate, the estimation error does not grow unbounded, in probability, even in the presence of the random delays occurring in the timing channel. This is made possible by communicating a real-valued variable (the initial state) at increasingly higher resolution and with vanishing probability of error. This strategy has been previously studied in [33] in the context of estimation over the binary erasure channel, rather than over the timing channel. It is also related to communication at increasing resolution over channels with feedback via posterior matching [137, 175]. The classic Horstein [75] and Schalkwijk-Kailath [171] schemes are special cases of posterior matching for the binary symmetric channel and the additive Gaussian channel respectively. The main idea in our setting is to employ a tree-structured quantizer in conjunction to a capacity-achieving timing channel codebook that grows exponentially with the tree depth, and re-compute the estimate of the real-valued variable as more and more channel symbols are received. The estimate is re-computed for a number of received symbols that depends on the channel rate and on the average delay. In contrast to posterior matching, we are not concerned with the complexity of the encoding-decoding strategy, but only with its existence. We also do not assume a specific distribution for the real value we need to communicate, and we do not use the feedback signal to perform encoding, but only to avoid queuing [2, 185]. We point out that our control strategy does not work in the presence of disturbances: in this case one needs to track a state that depends not only on the initial condition, but also on the evolution of the disturbance. This requires to update the entire history of the system's states at each symbol reception [164], leading to a different, i.e. non-classical, coding model. Alternatively, remaining in a classical setting one could aim for less, and attempt to obtain results using weaker probabilistic notions of stability, such as the one in [123, Chapter 8].

Finally, by showing that in the case of no disturbances and exponentially distributed delay it is possible to achieve stabilization at zero data-rate only for sufficiently small average delay $\mathbb{E}(S) < (ea)^{-1}$, we confirmed from an information-theoretic perspective the observation made in

[95] regarding the existence of a critical delay value for stabilization at zero data-rate.

Chapter 4, in full, is a reprint of the material in M. J. Khojasteh, M. Franceschetti, G. Ranade, "Stabilizing a linear system using phone calls: when time is information" arXiv:1804.00351, 2018, being prepared for publication. The dissertation author was the primary investigator and author of this paper.

4.9 Appendix: proofs of the estimation results

4.9.1 Proof of Theorem 16

We start by introducing a few definitions and proving some useful lemmas.

Definition 5 *For any $\epsilon > 0$ and $\phi > 0$, we define the rate-distortion function of the source $\dot{X}_e = aX_e(t)$ at times $\{t_n\}$ as*

$$R^{\epsilon}_{t_n}(\phi) = \inf_{\mathbb{P}\left(\hat{X}_e(t_n)|X_e(t_n)\right)} \Bigg\{ I\left(X_e(t_n); \hat{X}_e(t_n)\right) : \mathbb{P}\left(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon\right) \leq \phi \Bigg\}. \tag{4.27}$$

The proof of the following lemma adapts an argument of [190] to our continuous-time setting.

Lemma 17. *We have*

$$R^{\epsilon}_{t_n}(\phi) \geq (1-\phi)\left[at_n + h(X(0))\right] - \ln 2\epsilon - \frac{\ln 2}{2} \quad \text{[nats]}. \tag{4.28}$$

Proof. Let

$$\xi = \begin{cases} 0 & \text{if } |X_e(t_n) - \hat{X}_e(t_n)| \leq \epsilon \\ 1 & \text{if } |X_e(t_n) - \hat{X}_e(t_n)| > \epsilon. \end{cases} \tag{4.29}$$

Using the chain rule, we have

$$\begin{aligned} & I(X_e(t_n); \hat{X}_e(t_n)) \\ & = I(X_e(t_n); \xi, \hat{X}_e(t_n)) - I(X_e(t_n); \xi | \hat{X}_e(t_n)) \\ & = I(X_e(t_n); \xi, \hat{X}_e(t_n)) - H(\xi | \hat{X}_e(t_n)) \\ & \quad + H(\xi | X_e(t_n), \hat{X}_e(t_n)). \end{aligned}$$

Given $X(t_n)$ and $\hat{X}(t_n)$, there is no uncertainty in ξ, hence we deduce

$$\begin{aligned} & I(X_e(t_n); \hat{X}_e(t_n)) \\ & = I(X_e(t_n); \xi, \hat{X}_e(t_n)) - H(\xi | \hat{X}_e(t_n)) \\ & = h(X_e(t_n)) - h(X_e(t_n) | \xi, \hat{X}_e(t_n)) - H(\xi | \hat{X}_e(t_n)) \\ & = h(X_e(t_n)) - h(X_e(t_n) | \xi = 0, \hat{X}_e(t_n)) \mathbb{P}(\xi = 0) \\ & \quad - h(X_e(t_n) | \xi = 1, \hat{X}_e(t_n)) \mathbb{P}(\xi = 1) - H(\xi | \hat{X}_e(t_n)). \end{aligned}$$

Since $H(\xi | \hat{X}_e(t_n)) \leq H(\xi) \leq \ln 2/2$ [nats], $\mathbb{P}(\xi = 0) \leq 1$, and $\mathbb{P}(\xi = 1) \leq \phi$, it then follows that

$$\begin{aligned} & I(X_e(t_n); \hat{X}_e(t_n)) \geq \\ & h\left(X_e(t_n)\right) - h\left(X_e(t_n) - \hat{X}_e(t_n) | \xi = 0, \hat{X}_e(t_n)\right) \\ & \quad - h\left(X_e(t_n) | \xi = 1, \hat{X}_e(t_n)\right) \phi - \frac{\ln 2}{2}. \end{aligned}$$

Since conditioning reduces the entropy, we have

$$\begin{aligned} &I(X_e(t_n); \hat{X}_e(t_n)) \geq h(X_e(t_n)) \\ &- h(X_e(t_n) - \hat{X}_e(t_n)|\xi = 0) - h(X_e(t_n))\phi - \frac{\ln 2}{2} \\ &= (1-\phi)h(X_e(t_n)) - h(X_e(t_n) - \hat{X}_e(t_n)|\xi = 0) - \frac{\ln 2}{2}. \end{aligned}$$

By (4.29) and since the uniform distribution maximizes the differential entropy among all distributions with bounded support, we have

$$I(X_e(t_n); \hat{X}_e(t_n)) \geq (1-\phi)h(X_e(t_n)) - \ln 2\epsilon - \frac{\ln 2}{2}. \tag{4.30}$$

Since $X_e(t_n) = X(0)\, e^{at_n}$, we have

$$h(X_e(t_n)) = \ln e^{at_n} + h(X(0)) = at_n + h(X(0)). \tag{4.31}$$

Combining (4.30), and (4.31) we obtain

$$I(X_e(t_n); \hat{X}_e(t_n)) \geq (1-\phi)\left(at_n + h(X(0))\right) - \ln 2\epsilon - \frac{\ln 2}{2}.$$

Finally, noting that this inequality is independent of $\mathbb{P}(\hat{X}_e(t_n)|X_e(t_n))$ the result follows. ∎

Remark 25. *By letting $\phi = \epsilon$ in* (4.28)*, we have*

$$R^{\epsilon}_{t_n}(\epsilon) \geq (1-\epsilon)at_n + \epsilon',$$

where

$$\epsilon' = (1-\epsilon)h\left(X(0)\right) - \ln 2\epsilon - \frac{\ln 2}{2}.$$

For sufficiently small ϵ we have that $\epsilon' \geq 0$, and hence

$$\frac{R^{\epsilon}_{t_n}(\epsilon)}{t_n} \geq (1-\epsilon)a.$$

It follows that for sufficiently small ϵ the rate distortion per unit time of the source must be at least as large as the entropy rate of the system. Since the rate distortion represents the number of bits required to represent the state of the process up to a given fidelity, this provides an operational characterization of the entropy rate of the system. •

The proof of the following lemma follows a converse argument of [2] with some modifications due to our different setting.

Lemma 18. *Under the same assumptions as in Theorem 16, we have*

$$I\left(X_e(t_n); \hat{X}_e(t_n)\right) \leq nI(W; W+S).$$

Proof. We denote the transmitted message by $V \in \{1, \ldots, M\}$ and the decoded message by $U \in \{1, \ldots, M\}$. Then

$$X_e(t_n) \to V \to (D_1, \ldots, D_n) \to U \to \hat{X}_e(t_n),$$

is a Markov chain. Therefore, using the data-processing inequality [35], we have

$$I\left(X_e(t_n); \hat{X}_e(t_n)\right) \leq I(V; U) \leq I(V; D_1, \ldots, D_n). \tag{4.32}$$

By the chain rule for the mutual information, we have

$$I(V; D_1, \ldots, D_n) = \sum_{i=1}^{n} I(V; D_i | D^{i-1}). \tag{4.33}$$

Since W_i is uniquely determined by the encoder from V, using the chain rule we deduce

$$\sum_{i=1}^{n} I(V; D_i|D^{i-1}) = \sum_{i=1}^{n} I(V, W_i; D_i|D^{i-1}). \tag{4.34}$$

In addition, again using the chain rule, we have

$$\begin{aligned}\sum_{i=1}^{n} I(V, W_i; D_i|D^{i-1}) = &\sum_{i=1}^{n} I(W_i; D_i|D^{i-1}) \\ &+ \sum_{i=1}^{n} I(V; D_i|D^{i-1}, W_i).\end{aligned} \tag{4.35}$$

D_i is conditionally independent of V when given W_i. Thus:

$$\sum_{i=1}^{n} I(V; D_i|D^{i-1}, W_i) = 0. \tag{4.36}$$

Combining (4.34), (4.35), and (4.36) it follows that

$$\sum_{i=1}^{n} I(V; D_i|D^{i-1}) = \sum_{i=1}^{n} I(W_i; D_i|D^{i-1}). \tag{4.37}$$

Since the sequences $\{S_i\}$ and $\{W_i\}$ are i.i.d. and independent of each other, it follows that the sequence $\{D_i\}$ is also i.i.d., and we have

$$\sum_{i=1}^{n} I(W_i; D_i|D^{i-1}) = nI(W; D). \tag{4.38}$$

By combining (4.32), (4.33), (4.37) and (4.38) the result follows. ∎

We are now ready to finish the proof of Theorem 16.

Proof. By the assumption of the theorem, for any $\epsilon > 0$ we have

$$\lim_{n\to\infty} \mathbb{P}\left(|X_e(t_n) - \hat{X}_e(t_n)| \leq \epsilon\right) = 1.$$

Hence, for any $\epsilon > 0$ and any $\phi > 0$ there exist n_ϕ such that for $n \geq n_\phi$

$$\mathbb{P}\left(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon\right) \leq \phi. \tag{4.39}$$

Using (4.39), (4.27), and Lemma 17 it follows that for $n \geq n_\phi$

$$R^\epsilon_{t_n}(\phi) \geq (1-\phi)\left[at_n + h(X(0))\right] - \ln 2\epsilon - \frac{\ln 2}{2}. \tag{4.40}$$

By (4.27), we have

$$I(X_e(t_n); \hat{X}_e(t_n)) \geq R^\epsilon_{t_n}(\phi), \tag{4.41}$$

and using Lemma (18) it follows that

$$nI(W; W+S) \geq I\left(X_e(t_n); \hat{X}_e(t_n)\right). \tag{4.42}$$

Combining (4.40), (4.41), and (4.42) we obtain that for $n \geq n_\phi$

$$I(W; W+S) \geq \\ \frac{(1-\phi)at_n}{n} + \frac{(1-\phi)h(X(0)) - \ln 2\epsilon - \frac{\ln 2}{2}}{n}.$$

We now let $\phi \to 0$, so that $n \to \infty$, and we have

$$I(W; W+S) \geq a \lim_{n\to\infty} \frac{t_n}{n}. \tag{4.43}$$

Since, $\mathbb{E}(\mathcal{T}_n) = n\mathbb{E}(D_n)$ from (4.7) it follows that

$$\mathbb{E}(D) \leq \lim_{n\to\infty} \frac{t_n}{n} \leq \Gamma\mathbb{E}(D). \tag{4.44}$$

Since $|X_e(t_n) - \hat{X}_e(t_n)| \xrightarrow{P} 0$ for all the measurement times t_n satisfying (4.44), we let $\lim_{n\to\infty} t_n/n = \Gamma\mathbb{E}(D)$ in (4.43) and (4.8) follows. Finally, using (4.4) and noticing

$$\sup_{\substack{W\geq 0\\ \mathbb{E}(W)\leq\chi}} \frac{I(W;W+S)}{\mathbb{E}(S)+\chi} \geq \sup_{\substack{W\geq 0\\ \mathbb{E}(W)=\chi}} \frac{I(W;W+S)}{\mathbb{E}(S)+\chi},$$

we deduce that if (4.8) holds then (4.9) holds as well. ∎

4.9.2 Proof of Theorem 17

Proof. If $\mathbb{E}(S) = 0$ the timing capacity is infinite, and the result is trivial. Hence, for the rest of the proof we assume that

$$\mathbb{E}(S+W) \geq \mathbb{E}(S) > 0,$$

which by (4.3) implies that $\mathbb{E}(\mathcal{T}_n) \to \infty$ as $n \to \infty$. As a consequence, by (4.7) we also have that $t_n \to \infty$ as $n \to \infty$.

The objective is to design an encoding and decoding strategy, such that for all $\epsilon, \delta > 0$ and sufficiently large n, we have

$$\mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon) < \delta. \tag{4.45}$$

We start by bounding the probability of the event that the nth symbol does not arrive by the estimation deadline t_n. Since $\lim_{n\to\infty} t_n/\mathbb{E}(\mathcal{T}_n) > 1$, it follows that there exists $\nu > 0$ such that for large enough n we have

$$t_n > (1+\nu)\mathbb{E}(\mathcal{T}_n).$$

Hence, for large enough n, we have that the probability of missing the deadline is

$$\mathbb{P}(\mathcal{T}_n > t_n) \leq \mathbb{P}[\mathcal{T}_n > (1+\nu)\mathbb{E}(\mathcal{T}_n)]. \tag{4.46}$$

Since the waiting times $\{W_i\}$ and the random delays $\{S_i\}$ are i.i.d. sequences and independent of each other, it follows by the strong law of large numbers that (4.46) tends to zero as $n \to \infty$. We now have

$$\begin{aligned}
&\mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon) = \\
&\mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon \mid t_n \geq \mathcal{T}_n)\mathbb{P}(t_n \geq \mathcal{T}_n) \\
&+ \mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon \mid t_n < \mathcal{T}_n)\mathbb{P}(t_n < \mathcal{T}_n) \\
&\leq \mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon \mid t_n \geq \mathcal{T}_n) + \mathbb{P}(t_n < \mathcal{T}_n),
\end{aligned} \tag{4.47}$$

where the second term in the sum (4.47), tends to zero as $n \to \infty$. It follows that to ensure (4.45) it suffices to design an encoding and decoding scheme, such that for all $\epsilon, \delta > 0$ and sufficiently large n, we have that the conditional probability

$$\mathbb{P}(|X_e(t_n) - \hat{X}_e(t_n)| > \epsilon \mid t_n \geq \mathcal{T}_n) < \delta. \tag{4.48}$$

From the open-loop equation (4.6), we have

$$X_e(t_n) = e^{at_n} X(0), \tag{4.49}$$

from which it follows that the decoder can construct the estimate

$$\hat{X}_e(t_n) = e^{at_n} \hat{X}_{t_n}(0), \tag{4.50}$$

where $\hat{X}_{t_n}(0)$ is an estimate of $X(0)$ constructed at time t_n using all the symbols received by this time.

By (4.49) and (4.50), we now have that (4.48) is equivalent to

$$\mathbb{P}(|X(0) - \hat{X}_{t_n}(0)| > \epsilon e^{-at_n} \mid t_n \geq \mathcal{T}_n) < \delta, \tag{4.51}$$

namely it suffices to design an encoding and decoding scheme to communicate the initial condition with exponentially increasing reliability in probability. Our coding procedure that achieves this objective is described next.

Source coding

We let the source coding map

$$\mathcal{Q} : [-L, L] \to \{0, 1\}^{\mathbb{N}} \tag{4.52}$$

be an infinite tree-structured quantizer [63]. This map constructs the infinite binary sequence $\mathcal{Q}(X(0)) = \{Q_1, Q_2, \ldots\}$ as follows. $Q_1 = 0$ if $X(0)$ falls into the left-half of the interval $[-L, L]$, otherwise $Q_1 = 1$. The sub-interval where $X(0)$ falls is then divided into half and we let $Q_2 = 0$ if $X(0)$ falls into the left-half of this sub-interval, otherwise $Q_2 = 1$. The process then continues in the natural way, and Q_i is determined accordingly for all $i \geq 3$.

Using the definition of truncation operator from Section 1.4, for any $n' \geq 1$ we can define

$$\mathcal{Q}_{n'} = \pi_{n'} \circ \mathcal{Q}.$$

It follows that $\mathcal{Q}_{n'}(X(0))$ is a binary sequence of length n' that identifies an interval of length

$L/2^{n'-1}$ that contains $X(0)$. We also let

$$\mathcal{Q}_{n'}^{-1} : \{0,1\}^{n'} \to [-L, L]$$

be the right-inverse map of $\mathcal{Q}_{n'}$, which assigns the middle point of the last interval identified by the sequence that contains $X(0)$. It follows that for any $n' \geq 1$, this procedure achieves a quantization error

$$|X(0) - \mathcal{Q}_{n'}^{-1} \circ \mathcal{Q}_{n'}(X(0))| \leq \frac{L}{2^{n'}}. \tag{4.53}$$

•

Channel coding

In order to communicate the quantized initial condition over the timing channel, the truncated binary sequence $Q_{n'}(X(0))$ needs to be mapped into a channel codeword of length n.

We consider a channel codebook of n columns and M_n rows. The codeword symbols $\{w_{i,m}, i = 1, \cdots, n;\ m = 1 \cdots M_n\}$ are drawn i.i.d. from a distribution which is mixture of a delta function and an exponential and such that $\mathbb{P}(W_i = 0) = e^{-1}$, and $\mathbb{P}(W_i > w \mid W_i > 0) = \exp\{\frac{-w}{e\mathbb{E}(S)}\}$. By Theorem 3 of [2], if the delays $\{S_i\}$ are exponentially distributed, using a maximum likelihood decoder this construction achieves the timing capacity. Namely, letting

$$T_n = \mathbb{E}(\mathcal{T}_n) = n\mathbb{E}(D), \tag{4.54}$$

using this codebook we can achieve any rate

$$R = \lim_{n\to\infty} \frac{\log M_n}{T_n} < C$$

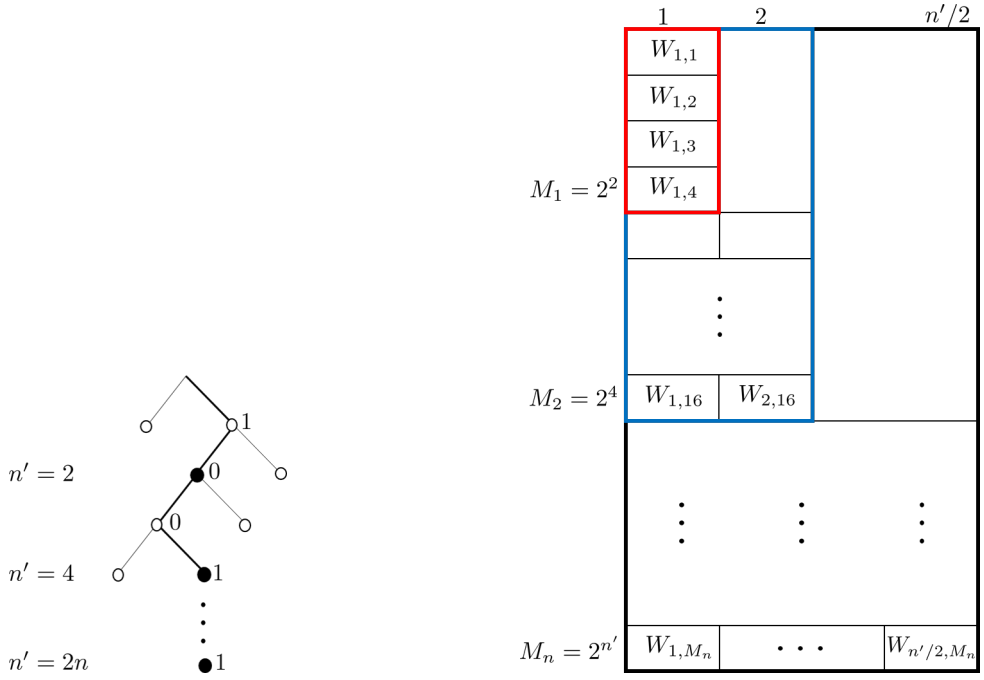


Figure 4.8: Tree-structured quantizer and the corresponding codebook for $R\mathbb{E}(D) = 2$. In this case, every received channel symbol refines the source coding representation by two bits.

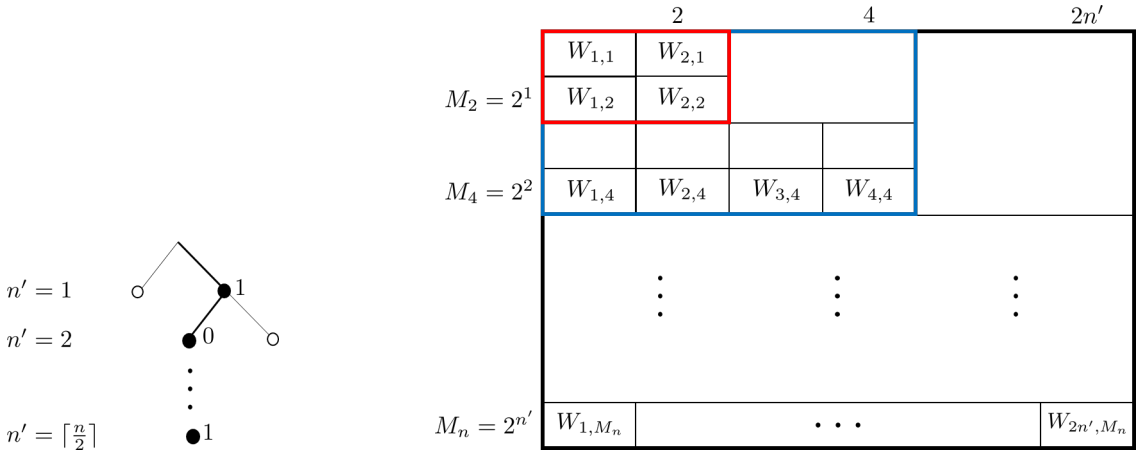


Figure 4.9: Tree-structured quantizer and the corresponding codebook for $R\mathbb{E}(D) = 0.5$. In this case, every two received channel symbols refine the source coding representation by one bit.

over the timig channel.

Next, we describe the mapping between the source coding and the channel coding con-

structions. •

Source-channel mapping

We first consider the direct mapping. For all $i \geq 1$, we let $n' = \lceil iR\mathbb{E}(D) \rceil$ and consider the $2^{n'}$ possible outcomes of the source coding map $\mathcal{Q}_{n'}(X(0))$. We associate them, in a one-to-one fashion, to the rows of a codebook $\Psi_{n'}$ of size $2^{n'} \times \lceil n'/R\mathbb{E}(D) \rceil$. This mapping is defined as

$$\mathcal{E}_{n'} : \{0,1\}^{n'} \to \Psi_{n'}.$$

By letting $i \to \infty$, the codebook becomes a double-infinite matrix Ψ_∞, and the map becomes

$$\mathcal{E} : \{0,1\}^{\mathbb{N}} \to \Psi_\infty. \tag{4.55}$$

Thus, as $i \to \infty$, $X(0)$ is encoded as

$$X(0) \xrightarrow{\mathcal{Q}} \{0,1\}^{\mathbb{N}} \xrightarrow{\mathcal{E}} \Psi_\infty.$$

We now consider the inverse mapping. Since the elements of $\Psi_{n'}$ are drawn independently from a continuous distribution, with probability one no two rows of the codebook are equal to each other, so for any $i \geq 1$ and number of received symbols $n = \lceil i/R\mathbb{E}(D) \rceil$ we define

$$\mathcal{E}_{n'}^{-1} : \Psi_{n'} \to \{0,1\}^{n'},$$

where $n' = \lceil nR\mathbb{E}(D) \rceil$. This map associates to every row in the codebook a corresponding node in the quantization tree at level n'.

Figures 4.8 and 4.9 show the constructions described above for the cases $R\mathbb{E}(D) = 2$

and $R\mathbb{E}(D) = 0.5$, respectively. In Fig. 4.8, the nodes in the quantization tree at level $n' = \lceil iR\mathbb{E}(D) \rceil = 2, 4, 6, \ldots$, are mapped into the rows of a table of $M_n = 2^2, 2^4, 2^6, \ldots$ rows and $n = 1, 2, 3 \ldots$ columns. Conversely, the rows in each table are mapped into the corresponding nodes in the tree. In Fig. 4.9, the nodes in the quantization tree at level $n' = \lceil iR\mathbb{E}(D) \rceil = 1, 2, 3, \ldots$, are mapped into the rows of a table of $M_n = 2, 2^2, 2^3, \ldots$ rows and $n = 2, 4, 6, \ldots$ columns. Conversely, the rows in each table are mapped into the corresponding nodes in the tree.

Next, we describe how the encoding and decoding operations are performed using these maps and how transmission occurs over the channel. •

One-time encoding

The encoding of the initial state $X(0)$ occurs at the sensor in one-shot and then the corresponding symbols are transmitted over the channel, one by one. Given $X(0)$, the source encoder computes $Q(X(0))$ according to the source coding map (4.52) and the channel encoder picks the corresponding codeword $\mathcal{E}(Q(X(0)))$ from the doubly-infinite codebook according to the map (4.55). This codeword is an infinite sequence of real numbers, which also corresponds to a leaf at infinite depth in the quantization tree. Then, the encoder starts transmitting the real numbers of the codeword one by one, where each real number corresponds to a holding time, and proceeds in this way forever. According to the source-channel mapping described above, transmitting $n = \lceil n'/R\mathbb{E}(D) \rceil$ symbols using this scheme corresponds to transmitting, for all $i \geq 1$, $n' = \lceil iR\mathbb{E}(D) \rceil$ source bits, encoded into a codeword $\mathcal{E}_{n'}(Q_{n'}(X(0)))$, picked from a truncated codebook of $2^{n'}$ rows and n columns. •

Anytime Decoding

The decoding of the initial state $X(0)$ occurs at the controller in an anytime fashion, refining the estimate of $X(0)$ as more and more symbols are received.

For all $i \geq 1$ the decoder updates its guess for the value of $X(0)$ any time the number

of symbols received equals $n = \lceil i/R\mathbb{E}(D) \rceil$. Assuming a decoding operation occurs after n symbols have been received, the decoder picks the maximum likelihood codeword from a truncated codebook of size $M_n \times n$ and by inverse mapping it finds the corresponding node in the tree. It follows that at the nth random reception time $\mathcal{T}_n$, the decoder utilizes the inter-reception times of all n symbols received up to this time to construct the estimate $\hat{X}_{\mathcal{T}_n}(0)$. First, a maximum likelihood decoder $\mathcal{D}_n$ is employed to map the inter-reception times $(D_1, \ldots, D_n)$ to an element of $\Psi_{n'}$. This element is then mapped to a binary sequence of length n' using $\mathcal{E}_{n'}^{-1}$. Finally, $\mathcal{Q}_{n'}^{-1}$ is used to construct $\hat{X}_{\mathcal{T}_n}(0)$. It follows that at the nth reception time where decoding occurs, we have

$$(D_1, \ldots, D_n) \xrightarrow{\mathcal{D}_n} \Psi_{n'} \xrightarrow{\mathcal{E}_{n'}^{-1}} \{0,1\}^{n'} \xrightarrow{\mathcal{Q}_{n'}^{-1}} [-L, L],$$

and we let

$$\hat{X}_{\mathcal{T}_n}(0) = \mathcal{Q}_{n'}^{-1}\left(\mathcal{E}_{n'}^{-1}\left(\mathcal{D}_n(D_1, \ldots, D_n)\right)\right).$$

Thus, as $n \to \infty$ the final decoding process becomes

$$(D_1, D_n, \ldots) \xrightarrow{\mathcal{D}} \Psi_\infty \xrightarrow{\mathcal{E}^{-1}} \{0,1\}^{\mathbb{N}} \xrightarrow{\mathcal{Q}^{-1}} [-L, L].$$

•

To conclude the proof, we now show that if $C > \Gamma a$, then it is possible to perform the above encoding and decoding operations with arbitrarily small probability of error while using a codebook so large that it can accommodate a quantization error at most $L/2^{n'} < \epsilon e^{-at_n}$.

Since the channel coding scheme achieves the timing capacity, we have that for any $R < C$, as $n \to \infty$ the maximum likelihood decoder selects the correct transmitted codeword with arbitrarily high probability. It follows that for any $\delta > 0$ and n sufficiently large, we have

with probability at least $(1-\delta)$ that

$$\mathcal{Q}_{n'}(X(0)) = \mathcal{E}_{n'}^{-1}\left(\mathcal{D}_n(D_1,\ldots,D_n)\right),$$

and then by (4.53) we have

$$|X(0) - \hat{X}_{\mathcal{T}_n}(0)| \leq \frac{L}{2^{n'}}. \tag{4.56}$$

We now consider a sequence of estimation times $\{t_n\}$ satisfying (4.7) and let the estimate at time $t_n \geq \mathcal{T}_n$ in (4.51) be $\hat{X}_{t_n}(0) = \hat{X}_{\mathcal{T}_n}(0)$. By (4.56) we have that the sufficient condition for estimation reduces to

$$\frac{L}{2^{n'}} \leq \epsilon e^{-at_n},$$

which means having the size of the codebook M_n be such that

$$\frac{L}{M_n} \leq \epsilon e^{-at_n},$$

or equivalently

$$\frac{\log M_n - \log L + \log \epsilon}{t_n} \geq a. \tag{4.57}$$

Using (4.54), we have

$$\begin{aligned}\frac{\log M_n - \log L + \log \epsilon}{t_n} &= \frac{\log M_n - \log L + \log \epsilon}{T_n} \cdot \frac{T_n}{t_n} \\ &= \frac{\log M_n - \log L + \log \epsilon}{T_n} \\ &\quad \cdot \frac{\mathbb{E}(\mathcal{T}_n)}{t_n}.\end{aligned}$$

Taking the limit for $n \to \infty$, we have

$$\lim_{n\to\infty} \frac{\log M_n - \log L + \log \epsilon}{T_n} \cdot \frac{\mathbb{E}(\mathcal{T}_n)}{t_n} \geq R \cdot \frac{1}{\Gamma}.$$

It follows that as $n \to \infty$ the sufficient condition (4.57) can be expressed in terms of rate as

$$R \geq \Gamma a.$$

It follows that the rate must satisfy

$$C > R \geq \Gamma a$$

and since $C > \Gamma a$, the proof is complete. ∎

Chapter 5

Learning-based attacks in cyber-physical systems

Recent technological advances in wireless communications and computation, and their integration into networked control and cyber-physical systems (CPS), open the door to a myriad of exciting opportunities in cloud robotics [81].

However, the distributed nature of CPS is often a source of vulnerability. Security breaches in CPS can have catastrophic consequences ranging from hampering the economy by obtaining financial gain, through hijacking autonomous vehicles and drones, and all the way to terrorism by manipulating life-critical infrastructures [199]. Real-world instances of security breaches in CPS, that were discovered and made available to the public, include the revenge sewage attack in Maroochy Shire, Australia; the Ukraine power grid cyber-attack; the German steel mill cyber-attack; the Davis-Besse nuclear power plant attack in Ohio, USA; and the Iranian uranium-enrichment facility attack via the Stuxnet malware [165]. Consequently, studying and preventing such security breaches via control-theoretic methods have received a great deal of attention in recent years [11, 23, 27, 44, 47, 94, 143, 176, 178, 194, 198, 207, 215].

An important and widely used class of attacks in CPS is based on the "man-in-the-middle"

(MITM) attack technique [182]: an attacker takes over the control and sensor signals of the physical plant. The attacker overrides the control signals with malicious inputs to push the plant toward a catastrophic trajectory. Consequently, many CPS constantly monitor the plant outputs to detect possible attacks. The attacker, on the other hand, aims to override the sensor readings in a manner that would be indistinguishable from the legitimate ones.

The MITM attack has been extensively studied in two special cases [127,135,169,182,216]. The first case is the *replay attack*, in which the attacker observes and records the legitimate system behavior for a given time window and then replays this recording periodically at the controller's input [127, 135, 216]. The second case is the *statistical-duplicate attack*, which assumes that the attacker has acquired complete knowledge of the dynamics and parameters of the system, and can construct arbitrarily long fictitious sensor readings that are statistically identical to the actual signals [169, 182]. The replay attack assumes no knowledge of the system parameters—and as a consequence, it is relatively easy to detect it. An effective way to counter the replay attack consists of superimposing a random watermark signal, unknown to the attacker, on top of the control signal [53, 56, 73, 76]. The statistical-duplicate attack assumes full knowledge of the system dynamics—and as a consequence, it requires a more sophisticated detection procedure, as well as additional assumptions on the attacker or controller behavior to ensure it can be detected. To combat the attacker's full knowledge, the controller may adopt *moving target* [80, 205] or *baiting* [58, 74] techniques. Alternatively, the controller may introduce private randomness in the control input using *watermarking* [169]. In this scenario, a vital assumption is made: although the attacker observes the true sensor readings, it is barred from observing the control actions, as otherwise it would be omniscient and undetectable.

Our contribution is fourfold. First, we observe that in many practical situations, the attacker does not have full knowledge of the system and cannot simulate a statistically indistinguishable copy of the system. On the other hand, the attacker can carry out more sophisticated attacks simply replaying previous sensor readings, by attempting to "learn" the system dynamics

from the observations. For this reason, we study *learning-based attacks* and show that they can outperform replay attacks by analyzing the performance using a specific learning algorithm. Second, we derive asymptotic bounds on the detection and deception probabilities for *any* (measurable) control policy when the attacker uses *any arbitrary* learning algorithm to estimate the dynamics of the plant. Third, for any learning algorithm utilized by the attacker to estimate the dynamics of the plant, we show that adding a proper *privacy-enhancing signal* to the "nominal control policy" provides enhanced guarantees on the detection probability. Forth, we study the trade-off between the performance of the learning algorithm, and the performance of arbitrary detection and control strategies adopted by the controller, providing a tight bound on the scaling of the expected time required to detect the attack, as the probability of detection tends to one.

Throughout this chapter, we assume that the attacker has *full access to both sensor and control signals*. The controller, on the other hand, has perfect knowledge of the system dynamics and tries to discover the attack from the injected observations. The assumed information-pattern imbalance between the controller and the attacker is justified since the controller is tuned in much longer than the attacker and thus has knowledge of the system dynamics to a far greater precision than the attacker. Since the success or failure of the attacker are dictated by the its learning capabilities, our work complements the recent progress in learning-based control [15, 38, 39, 61, 158, 159, 162, 167, 197].

In this chapter, we denote by $x_i^j = (x_i, \cdots, x_j)$ the realization of the tuple of random variables $X_i^j = (X_i, \cdots, X_j)$ for $i, j \in \mathbb{N}, i \leq j$. Random matrices and vectors are represented by boldface capital letters (e.g. $\mathbf{A}$) and their realizations are represented by typewriter letters (e.g. $\mathtt{A}$).

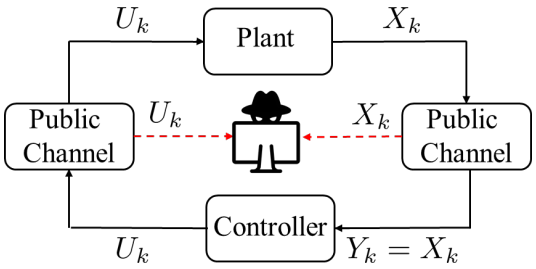


Figure 5.1: Learning (exploration): During this phase, the attacker eavesdrops and learns the system, without altering the input signal to the controller ($Y_k = X_k$).

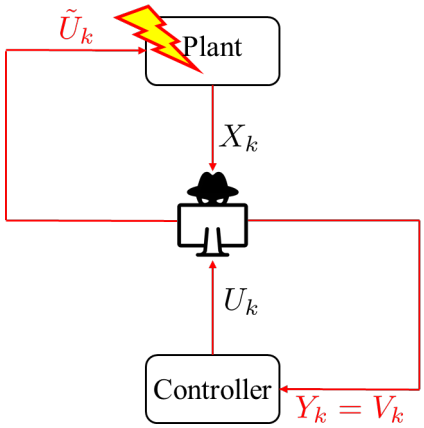


Figure 5.2: Hijacking (exploitation): During this phase, the attacker hijacks the system and intervenes as a MITM in two places: acting as a fake plant for the controller ($Y_k = V_k$) by impersonating the legitimate sensor, and as a malicious controller ($\tilde{U}_k$) for the plant aiming to destroy the plant.

Figure 5.3: System model during learning-based attack phases.

5.1 Problem Setup

We consider the networked control system depicted in Figure 5.3, where the plant dynamics are described by a scalar, discrete-time, linear time-invariant (LTI) system

$$X_{k+1} = aX_k + U_k + W_k, \tag{5.1}$$

where X_k, a, U_k, W_k are real numbers representing the plant state, open-loop gain of the plant, control input, and plant disturbance, respectively, at time $k \in \mathbb{N}$. The controller, at time k,

observes Y_k and generates a control signal U_k as a function of Y_1^k. If the attacker does not tamper sensor reading , at any time $k \in \mathbb{N}$, we have $Y_k = X_k$. We assume that the initial condition X_0 has a known (to all parties) distribution and is independent of the disturbance sequence $\{W_k\}$. For analytical purposes, we assume $\{W_k\}$ is an i.i.d. Gaussian process $\mathcal{N}(0, \sigma^2)$ known to all parties. We assume that $U_0 = W_0 = 0$. Moreover, to simplify the notation, let $Z_k := (X_k, U_k)$ denote the state-and-control input at time k and its trajectory up to time k—by

$$Z_1^k := (X_1^k, U_1^k).$$

The controller is equipped with a detector that tests for anomalies in the observed history Y_1^k. When the controller detects an attack, it shuts the system down and prevents the attacker from causing further "damage" to the plant. The controller/detector is aware of the plant dynamics (5.1) and knows the open-loop gain a of the plant. On the other hand, the attacker knows the plant dynamics (5.1) as well as the plant state X_k, and control input U_k (or equivalently, Z_k) at time k (see Figure 5.3). However, it does not know the open-loop gain a of the plant.

In what follows, it will be convenient to treat the open-loop gain of the plant as a random variable A that is *fixed in time*, whose PDF f_A is known to the attacker, and whose realization a is known to the controller. We assume all random variables to exist on a common probability space with probability measure $\mathbb{P}$, and U_k to be a *measurable function* of Y_1^k for all time $k \in \mathbb{N}$. We also denote the probability measure conditioned on $A = a$ by $\mathbb{P}_a$. Namely, for any measurable event C, we define

$$\mathbb{P}_a(C) = \mathbb{P}(C|A = a).$$

A is further assumed to be independent of X_0 and $\{W_k|k \in \mathbb{N}\}$.

5.1.1 Learning-based attacks

We define *Learning-based attacks* that consist of two disjoint, consecutive, passive and active phases, as follows.

Phase 1: Learning (exploration). During this phase, the attacker passively observes the control input and the plant state to learn the open-loop gain of the plant. As illustrated in Figure 5.1, for all $k \in [0, L]$, the attacker observes the control input U_k and the plant state X_k, and tries to learn the open-loop gain a, where L is the duration of the learning phase. We denote by $\hat{A}$ the attacker's estimate of the open-loop gain a. •

Phase 2: Hijacking (exploitation). In this phase, the attacker aims to destroy the plant using $\tilde{U}_k$ while remaining undetected. As illustrated in Figure 5.2, from time $L + 1$ and onwards the attacker hijacks the system and feeds a malicious control signal to the plant $\tilde{U}_k$ and a fictitious sensor reading $Y_k = V_k$ to the controller. •

We assume that the attacker can use *any arbitrary* learning algorithm to estimate the open-loop gain a during the learning phase, and upon estimation is completed, we assume that during the hijacking phase the fictitious sensor reading is constructed in the following way

$$V_{k+1} = \hat{A}V_k + U_k + \tilde{W}_k\,, \qquad\qquad k = L, \ldots, T-1, \tag{5.2}$$

where $\tilde{W}_k$ for $k = L, \ldots, T-1$ are i.i.d. Gaussian $\mathcal{N}(0, \sigma^2)$; U_k is the control signal generated by the controller, which is fed with the fictitious virtual signal V_k by the attacker; $V_L = X_L$; and $\hat{A}$ is the estimate of the open-loop gain of the plant at the conclusion of Phase 1.

5.1.2 Detection

The controller/detector, being aware of the dynamic (5.1) and the open-loop gain a, attempts to detect possible attacks by testing for statistical deviations from the typical behavior of the system (5.1).

Definition 6 The decision time T is the time at which the controller makes a decision regarding the presence or absence of the attacker.

Under legitimate system operation (corresponding to the *null hypothesis*), the controller observation Y_k behaves according to

$$Y_{k+1} - aY_k - U_k(Y_1^k) \sim \text{ i.i.d. } \mathcal{N}(0, \sigma^2). \tag{5.3}$$

In case of an attack, during Phase 2 ($k > L$), (5.3) can be rewritten as

$$\begin{aligned} &V_{k+1} - aV_k - U_k(Y_1^k) \\ &\quad = V_{k+1} - aV_k + \hat{A}V_k - \hat{A}V_k - U_k(Y_1^k) && \text{(5.4a)} \\ &\quad = \tilde{W}_k + \left(\hat{A} - a\right) V_k, && \text{(5.4b)} \end{aligned}$$

where (5.4b) follows from (5.2). Hence, the estimation error $(\hat{A} - a)$ dictates the ease with which an attack can be detected.

Since the Gaussian PDF with zero mean is fully characterized by its variance, we shall test for anomalies in the latter, i.e., test whether the empirical variance of (5.3) is equal to the second moment of the plant disturbance $\mathbb{E}[W^2]$. To that end, we shall use a test that sets a confidence interval of length $2\delta > 0$ around the expected variance, i.e., it checks whether

$$\frac{1}{T} \sum_{k=1}^{T} \left[Y_{k+1} - aY_k - U_k(Y_1^k)\right]^2 \in (\text{Var}[W] - \delta, \text{Var}[W] + \delta), \tag{5.5}$$

where T is the decision time. That is, as is implied by (5.4), the attacker manages to deceive the controller and remain undetected if

$$\frac{1}{T} \left(\sum_{k=1}^{L} W_k^2 + \sum_{k=L+1}^{T} (\tilde{W}_k + (\hat{A} - a)V_k)^2 \right) \in (\text{Var}[W] - \delta, \text{Var}[W] + \delta). \tag{5.6}$$

5.1.3 Performance Measures

Definition 7 *The hijack indicator at decision time T is defined as*

$$\Theta_T := \begin{cases} 0, & \forall j \leq T : \ Y_j = X_j \, ; \\ 1, & \textit{otherwise}. \end{cases}$$

At the decision time T, the controller uses Y_1^T to construct an estimate $\hat{\Theta}_T$ of Θ_T. More precisely, $\hat{\Theta}_T = 0$ if (5.5) occurs, otherwise $\hat{\Theta}_T = 1$. •

Definition 8 *The probability of deception is the probability of the attacker deceiving the controller and remain undetected at the time instance T*

$$P_{\text{Dec}}^{a,T} := \mathbb{P}_a \left(\hat{\Theta}_T = 0 \middle| \Theta_T = 1 \right). \tag{5.7}$$

In addition, the detection probability at decision time T is defined as

$$P_{\text{Det}}^{a,T} := 1 - P_{\text{Dec}}^{a,T}.$$

Likewise, the probability of false alarm is the probability of detecting the attacker when it is not present, namely

$$P_{\text{FA}}^{a,T} := \mathbb{P}_a \left(\hat{\Theta}_T = 1 \middle| \Theta_T = 0 \right). \qquad \bullet$$

In this case, using Chebyshev's inequality, (5.5), since the system disturbances are i.i.d. Gaussian $\mathcal{N}(0, \sigma^2)$, we have

$$P_{\text{FA}}^{T} \leq \frac{\text{Var}[W^2]}{\delta^2 T} = \frac{3\sigma^4}{\delta^2 T}.$$

We further define the deception, detection, and false alarm probabilities w.r.t. the probability measure $\mathbb{P}$, without conditioning on A, and denote them by P_{Dec}^T, P_{Det}^T, and P_{FA}^T, respectively. For instance, P_{Det}^T is defined, w.r.t. a PDF f_A of A, as

$$P_{\text{Det}}^T := \mathbb{P}\left(\hat{\Theta}_T = 1 \middle| \Theta_T = 1\right) = \int_{-\infty}^{\infty} P_{\text{Det}}^{a,T} \, f_A(a) da \tag{5.8}$$

5.2 Statement of the results

In this section, we describe the main results of this work. We want to provide lower and upper bounds on the deception probability (5.7) of the learning-based attack (5.2) where $\hat{A}$ in (5.2) is constructed using *any arbitrary* learning algorithm. In addition, our results are valid for *any measurable* control policy U_k. We find a lower bound on the deception probability by characterizing what attacker can at least achieve using a least-squares (LS) algorithm, and we derive an information theoretic upper bound using Fano's inequality [149]. While our analysis is restricted to the asymptotic case, $T \to \infty$, it is straightforward to extend this treatment to the non-asymptotic case.

For analytical purposes, we assume that the power of the fictitious sensor reading is equal to $\beta^{-1} < \infty$, namely

$$\lim_{T\to\infty} \frac{1}{T} \sum_{k=L+1}^{T} V_k^2 = 1/\beta \qquad \text{a.s. w.r.t. } \mathbb{P}_a. \tag{5.9}$$

Remark 26. Assuming the control policy is memoryless, namely U_k is only dependent on Y_k, the process V_k is Markov for $k \geq L+1$. By further assuming that $L = o(T)$ and using the generalization of the law of large numbers for Markov processes [51], we deduce

$$\lim_{T\to\infty} \frac{1}{T} \sum_{k=L+1}^{T} V_k^2 \geq \text{Var}\left[W\right] \qquad \text{a.s. w.r.t. } \mathbb{P}_a.$$

Consequently, in this case we have $\beta \leq 1/\mathrm{Var}\,[W]$. In addition, when the control policy is linear and stabilizes (5.2), that is $U_k = -\Omega Y_k$ and $|\hat{A} - \Omega| < 1$, it is easy to verify that (5.9) holds true for $\beta = (1 - (\hat{A} - \Omega)^2)/\mathrm{Var}\,[W]$. •

5.2.1 Lower Bound on the Deception Probability

To provide a lower bound on the deception probability $P_{\mathrm{Dec}}^{a,T}$, we consider a specific estimate of $\hat{A}$ at the conclusion of the first phase by the attacker. To this end, we use LS estimation due to its efficiency and amenability to recursive update over observed incremental data [122, 158, 167, 168, 197]. The LS algorithm approximates the overdetermined system of equations

$$\begin{pmatrix} X_2 \\ X_3 \\ \vdots \\ X_L \end{pmatrix} = A \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_{L-1} \end{pmatrix} + \begin{pmatrix} U_1 \\ U_2 \\ \vdots \\ U_{L-1} \end{pmatrix},$$

by minimizing the Euclidean distance $\hat{A} = \mathrm{argmin}_A \, \|X_{k+1} - AX_k - U_k\|$ to estimate (or "identify") the plant, the solution to which is

$$\hat{A} = \frac{\sum_{k=1}^{L-1}(X_{k+1} - U_k)X_k}{\sum_{k=1}^{L-1} X_k^2} \qquad \text{a.s. w.r.t. } \mathbb{P}_a. \tag{5.10}$$

Remark 27. Since we assumed $W_k \sim \mathcal{N}(0, \sigma^2)$ for all $k \in \mathbb{N}$, $\mathbb{P}_a(X_k = 0) = 0$. Thus, (5.10) is well-defined. •

Using LS estimation (5.10), our linear learning-based attack (5.2) achieves *at least* the asymptotic deception probability stated in the following theorem, for *any measurable* control policy.

Theorem 20. *Consider any linear learning-based attack* (5.2) *with fictitious sensor reading power*

that satisfies (5.9) *and an arbitrary measurable control policy* $\{U_k\}$*. Then, the asymptotic deception probability, when using the variance test* (5.5)*, is bounded from below as*

$$\lim_{T\to\infty} P_{\text{Dec}}^{a,T} = \mathbb{P}_a\left(|\hat{A}-a| < \sqrt{\delta\beta}\right) \tag{5.11a}$$

$$\geq \mathbb{P}_a\left(\frac{\left|\sum_{k=1}^{L-1} W_k X_k\right|}{\sum_{k=1}^{L-1} X_k^2} < \sqrt{\delta\beta}\right) \tag{5.11b}$$

$$\geq 1 - \frac{2}{(1+\delta\beta)^{L/2}}. \tag{5.11c}$$

Proof. We break the proof of Theorem 20 into several lemmas that are stated and proved next.

In the case of any learning-based attack (5.2), in the limit of $T \to \infty$, the empirical variance, which is used in the variance test (5.5), can be expressed in terms of the estimation error of the open-loop gain as follows.

Lemma 19. *Consider any learning-based attack* (5.2) *with fictitious sensor reading power that satisfies* (5.9) *and some measurable control policy* $\{U_k\}$*. Then, the variance test* (5.5) *reduces to*

$$\lim_{T\to\infty} \frac{1}{T}\sum_{k=1}^{T}(Y_{k+1} - aY_k - U_k(Y_1^k))^2 = \text{Var}\,[W] + \frac{(\hat{A}-a)^2}{\beta} \quad \textit{a.s. w.r.t. } \mathbb{P}_a.$$

Proof of Lemma 19: Since the hijacking phase of a learning-based attack (5.2) starts at time

$k = L + 1$, using (5.1) and (5.4) we have

$$\begin{aligned}
&\frac{1}{T}\sum_{k=1}^{T}(Y_{k+1} - aY_k - U_k(Y_1^k))^2 \\
&= \frac{1}{T}\left(\sum_{k=1}^{L} W_k^2 + \sum_{k=L+1}^{T}(\tilde{W}_k + (\hat{A} - a)V_k)^2\right) \qquad (5.12a) \\
&= \frac{1}{T}\left(\sum_{k=1}^{L} W_k^2 + \sum_{k=L+1}^{T}\tilde{W}_k^2\right) \\
&\quad + \frac{(\hat{A} - a)^2}{T}\sum_{k=L+1}^{T} V_k^2 + \frac{2(\hat{A} - a)}{T}\sum_{k=L+1}^{T}\tilde{W}_k V_k\,. \qquad (5.12b)
\end{aligned}$$

Let $\mathcal{F}_k$ be the $\sigma-$filed generated by $(V_k, \hat{A}, W_k, U_k)$, for $k = L, \ldots, T-1$. Then clearly, V_{k+1} is $\mathcal{F}_k$ measurable, also $(W_{k+1}, \mathcal{F}_k)$ is a Martingale difference sequence. Thus, using [103, Lemma 2, part iii] the last term in (5.12b) reduces to

$$\sum_{k=L+1}^{T}\tilde{W}_k V_k = o\left(\sum_{k=L+1}^{T} V_k^2\right) + O(1) \quad \text{a.s.} \qquad (5.13)$$

in the limit $T \to \infty$.

Note further that

$$\lim_{T\to\infty}\frac{1}{T}\left(\sum_{k=1}^{L} W_k^2 + \sum_{k=L+1}^{T}\tilde{W}_k^2\right) = \mathrm{Var}\,[W] \quad \text{a.s.} \qquad (5.14)$$

by the strong law of large numbers [51].

Substituting (5.9) in (5.12), (5.14) in (5.12), using (5.13), and taking T to infinity concludes the proof of the lemma. •

In the following lemma, we prove (5.11a) for any learning-based attack (5.2), and any measurable control policy.

Lemma 20. *Consider any learning-based attack* (5.2) *with fictitious sensor reading power that*

satisfies (5.9) *and a measurable control policy* $\{U_k\}$*. Then, the asymptotic deception probability, under the variance test* (5.5)*, is equal to*

$$\lim_{T\to\infty} P_{\text{Dec}}^{a,T} = \mathbb{P}_a\left(|\hat{A}-a| < \sqrt{\delta\beta}\right).$$

Proof of Lemma 20: Under the variance test,

$$\lim_{T\to\infty} P_{\text{Dec}}^{a,T} = \lim_{T\to\infty} \mathbb{E}_{\mathbb{P}_a}\left[\mathbb{1}_T\right],$$

where $\mathbb{1}_T$ is one if (5.5) occurs and zero otherwise. Using the dominated convergence theorem [51] and Lemma 19, we deduce

$$\lim_{T\to\infty} P_{\text{Dec}}^{a,T} = \mathbb{E}_{\mathbb{P}_a}\left[\mathbb{1}'_T\right],$$

where $\mathbb{1}'_T$ is one if

$$\text{Var}\left[W\right] + \frac{(\hat{A}-a)^2}{\beta} \in \left(\text{Var}\left[W\right]-\delta, \text{Var}\left[W\right]+\delta\right)$$

and zero otherwise. Consequently,

$$\lim_{T\to\infty} P_{\text{Dec}}^{a,T} = \mathbb{P}_a\left((\hat{A}-a)^2 \in (-\delta\beta, \delta\beta)\right),$$

and the result follows. •

Clearly, the estimation error of the LS algorithm (5.10) is [158]

$$\hat{A}-a = \frac{\sum_{k=1}^{L-1} W_k X_k}{\sum_{k=1}^{L-1} X_k^2} \qquad \text{a.s. w.r.t. } \mathbb{P}_a$$

Consequently, by (5.11a), learning-based attack (5.2) can at least achieve the asymptotic deception

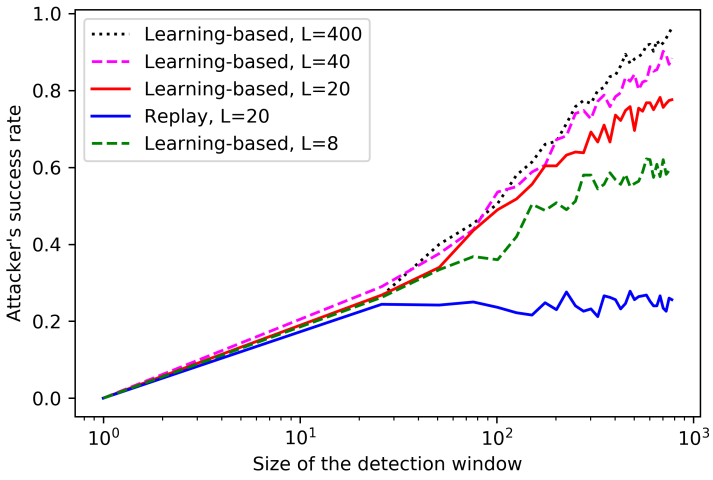


Figure 5.4: The attacker's success rate $P_{\text{Dec}}^{a,T}$ versus the size of the detection window T.

probability (5.11b). Finally, since, for $k \in \{1, \dots, L\}$, U_k is a measurable function of $Y_1^k = X_1^k$, (5.11c) follows using Theorem 4 of [158]. ∎

Example 1 In this example, we compare the empirical performance of the variance-test with our developed bound in Theorem 20. At every time T, the controller tests the empirical variance for abnormalities over a detection window $[1, T]$, using a confidence interval $2\delta > 0$ around the expected variance (5.5). Here, $a = 1$, $\delta = 0.1$, $U_k = -0.88aY_k$ for all $1 \leq k \leq T = 800$, and $\{W_k\}$ are i.i.d. Gaussian $\mathcal{N}(0, 1)$, and 500 Monte Carlo simulations were performed.

The learning-based attacker (5.2) uses the LS algorithm (5.10) to estimate a, and as illustrated in Figure 5.4, the attacker's success rate increases as the duration of learning phase L increases. This is in agreement with (5.11c) since the attacker can improve its estimate of a and the estimation error $|\hat{A} - a|$ reduces as L increases. As discussed in Section 5.1.3, the false alarm rate decays to zero as the size of the detection window T tends to infinity. Hence, for a sufficiently large detection window size, the attacker's success rate could potentially tend to one. Indeed, such behavior is observed in Figure 5.4 for a learning-based attacker (5.2) with $L = 400$.

Also, Figure 5.4 illustrates that our learning-based attack outperforms the replay attack. A

replay attack with a recording length of $L = 20$ and a learning-based attack with a learning phase of length $L = 20$ are compared, and the success rate of the replay attack saturates at a lower value. Moreover, a learning-based attack with a learning phase of length $L = 8$ has a higher success rate than a replay attack with a larger recording length of $L = 20$. •

5.2.2 Upper Bound on the Deception Probability

We now derive an upper bound on the deception probability (5.7) of any learning-based attack (5.2) where $\hat{A}$ in (5.2) is constructed using *any arbitrary* learning algorithm, for *any measurable* control policy, when A is distributed over a symmetric interval $[-R, R]$. Similar results can be obtained for other interval choices. Since the uniform distribution has the highest entropy among all distributions with finite support [149], we further assume A is distributed uniformly over the interval $[-R, R]$. We assume the attacker knows the distribution of A (including the value of R), whereas the controller knows the true value of A (as before).

Theorem 21. *Let A be distributed uniformly over $[-R, R]$ for some $R > 0$, and consider any measurable control policy $\{U_k\}$ and any learning-based attack* (5.2) *with fictitious sensor reading power* (5.9) *that satisfies $\sqrt{\delta\beta} \leq R$. Then, the asymptotic deception probability, when using the variance test* (5.5)*, is bounded from above as*

$$\lim_{T\to\infty} P_{\text{Dec}}^T = \mathbb{P}(|A - \hat{A}| < \sqrt{\delta\beta}) \tag{5.15a}$$

$$\leq \Lambda := \frac{I(A; Z_1^L) + 1}{\log(R/\sqrt{\delta\beta})}\,. \tag{5.15b}$$

In addition, if for all $k \in \{1, \dots, L\}$, $A \to (X_k, Z_1^{k-1}) \to U_k$ is a Markov chain, then for any sequence of probability measures $\{\mathbb{Q}_{X_k|Z_1^{k-1}}\}$, such that for all $k \in \{1, \dots, L\}$ $\mathbb{P}_{X_k|Z_1^{k-1}} \ll$

$\mathbb{Q}_{X_k|Z_1^{k-1}}$, *we have*

$$\Lambda \leq \frac{\sum_{k=1}^{L} D\left(\mathbb{P}_{X_k|Z_1^{k-1},A}\middle\|\mathbb{Q}_{X_k|Z_1^{k-1}}\middle|\mathbb{P}_{Z_1^{k-1},A}\right)+1}{\log\left(R/\sqrt{\delta\beta}\right)}. \tag{5.16}$$

Proof. We start by proving (5.15a). Using Lemma 20 and (5.8) we deduce

$$\begin{aligned}\lim_{T\to\infty} P_{\text{Dec}}^T &= \frac{1}{2R}\int_{-R}^{R} \mathbb{P}_a\left(|\hat{A}-a|<\sqrt{\delta\beta}\right) da \\ &= \frac{1}{2R}\int_{-R}^{R} \mathbb{E}_{\mathbb{P}_a}\left[\mathbb{1}_c\right] da,\end{aligned}$$

where $\mathbb{1}_c$ is one if $|\hat{A}-a|<\sqrt{\delta\beta}$ and zero otherwise. Consequently, using Tonelli's theorem [51] it follows that

$$\lim_{T\to\infty} P_{\text{Dec}}^T = \mathbb{P}(|A-\hat{A}|<\sqrt{\delta\beta}). \tag{5.17}$$

We now continue by proving (5.15b). Since the attacker observed the plant state and control input during the learning phase which lasts L time steps, and since $A\to(X_1^L,U_1^L)\to\hat{A}$ constitutes a Markov chain, using the continuous domain version of Fano's inequality [49, Prop. 2], we have

$$\inf_{\hat{A}} \mathbb{P}\left(\left|A-\hat{A}\right|\geq\sqrt{\delta\beta}\right) \geq 1-\frac{I(A;Z_1^L)+1}{\log(R/\sqrt{\delta\beta})}, \tag{5.18}$$

whenever $\sqrt{\delta\beta}\leq R$. Finally, using (5.17), (5.18), (5.15b) follows.

To prove (5.16), we further bound $I(A;Z_1^L)$ from above via KL divergence manipulations. The proof of the following lemma follows the arguments of [155], and is detailed here for completeness.

Lemma 21. *Assume that $A\to(X_k,Z_1^{k-1})\to U_k$ is a Markov chain for all $k\in\{1,\dots,L\}$. Let $\left\{\mathbb{Q}_{X_k|Z_1^{k-1}}\right\}$ be a sequence of probability measures satisfying $\mathbb{P}_{X_k|Z_1^{k-1}}\ll\mathbb{Q}_{X_k|Z_1^{k-1}}$ for all k.*

Then, for all k, we have

$$I(A; Z_1^k) = \sum_{k=1}^{L} I(A; X_k | Z_1^{k-1}) \\ \leq \sum_{k=1}^{L} D\left(\mathbb{P}_{X_k|Z_1^{k-1},A} \middle\| \mathbb{Q}_{X_k|Z_1^{k-1}} \middle| \mathbb{P}_{Z_1^{k-1},A}\right).$$

Proof of Lemma 21: We start by applying the chain rule for mutual information to $I\left(A; Z_1^L\right)$ as follows.

$$I(A; Z_1^L) = \sum_{k=1}^{L} I\left(A; Z_k \middle| Z_1^{k-1}\right). \tag{5.19}$$

We next bound $I\left(A; Z_k \middle| Z_1^{k-1}\right)$ from above.

$$I\left(A; Z_k \middle| Z_1^{k-1}\right) = I\left(A; X_k, U_k \middle| Z_1^{k-1}\right) \tag{5.20a}$$

$$= I\left(A; X_k \middle| Z_1^{k-1}\right) \tag{5.20b}$$

$$= D\left(\mathbb{P}_{X_k|Z_1^{k-1},A} \middle\| \mathbb{P}_{X_k|Z_1^{k-1}} \middle| \mathbb{P}_{Z_1^{k-1},A}\right) \tag{5.20c}$$

$$= \mathbb{E}_{\mathbb{P}}\left[\log \frac{d\mathbb{P}_{X_k|Z_1^{k-1},A}}{d\mathbb{P}_{X_k|Z_1^{k-1}}}\right] \tag{5.20d}$$

$$= \mathbb{E}_{\mathbb{P}}\left[\log \frac{d\mathbb{P}_{X_k|Z_1^{k-1},A}}{d\mathbb{Q}_{X_k|Z_1^{k-1}}}\right] - \mathbb{E}_{\mathbb{P}}\left[\log \frac{d\mathbb{P}_{X_k|Z_1^{k-1}}}{d\mathbb{Q}_{X_k|Z_1^{k-1}}}\right] \tag{5.20e}$$

$$\leq D(\mathbb{P}_{X_k|Z_1^{k-1},A} \| \mathbb{Q}_{X_k|Z_1^{k-1}} | \mathbb{P}_{Z_1^{k-1},A}), \tag{5.20f}$$

where we substitute the definition of $Z_k := (X_k, U_k)$ to arrive at (5.20a), (5.20b) follows from the chain rule for mutual information and the Markovity assumption $A \to (X_k, Z_1^{k-1}) \to U_k$, we use the definition of the conditional mutual information in terms of the conditional KL divergence (recall the notation section) to attain (5.20c) and (5.20d), the manipulation in (5.20e) is valid due to the condition $\mathbb{P}_{X_k|Z_1^{k-1}} \ll \mathbb{Q}_{X_k|Z_1^{k-1}}$ in the setup of the lemma, and (5.20f) follows from the

non-negativity property of the KL divergence.

Substituting (5.20) in (5.19) concludes the proof. •

Applying the bound of Lemma 21 to the first bound of the theorem (5.15b) proves the second bound of the theorem (5.16). ∎

Remark 28. *By looking at the numerator in* (5.15b)*, it follows that the bound on the deception probability becomes looser as the amount of information revealed about the open-loop gain A by the observation Z_1^L increases. On the other hand, by looking at the denominator, the bound becomes tighter as R increases. This is consistent with the observation of Zames [155, 213] that system identification becomes harder as the uncertainty about the open-loop gain of the plant increases. In our case, a larger uncertainty interval R corresponds to a poorer estimation of A by the attacker, which leads, in turn, to a decrease in the achievable deception probability. The denominator can also, be interpreted as the intrinsic uncertainty of A when it is observed at resolution $\sqrt{\delta\beta}$, as it corresponds to the entropy of the random variable A when it is quantized at such resolution.* •

In conclusion, Theorem 21 provides two upper bounds on the deception probability. The first bound (5.15b) clearly shows that increasing the privacy of the open-loop gain A—manifested in the mutual information between A and the state-and-control trajectory Z_1^L during the exploration phase—reduces the deception probability. The second bound (5.16) allows freedom in choosing the auxiliary probability measure $\mathbb{Q}_{X_k|Z_1^{k-1}}$, making it a rather useful bound. For instance, by choosing $\mathbb{Q}_{X_k|Z_1^{k-1}} \sim \mathcal{N}(0, \sigma^2)$, for all $k \in \mathbb{N}$, we can rewrite the upper bound (5.16) in term of $\mathbb{E}_{\mathbb{P}}\left[(AX_{k-1} + U_{k-1})^2\right]$ as follows.

Corollary 3 *Under the assumptions of Theorem 21, if for all $k \in \{1, \dots, L\}$, $A \to (X_k, Z_1^{k-1}) \to$*

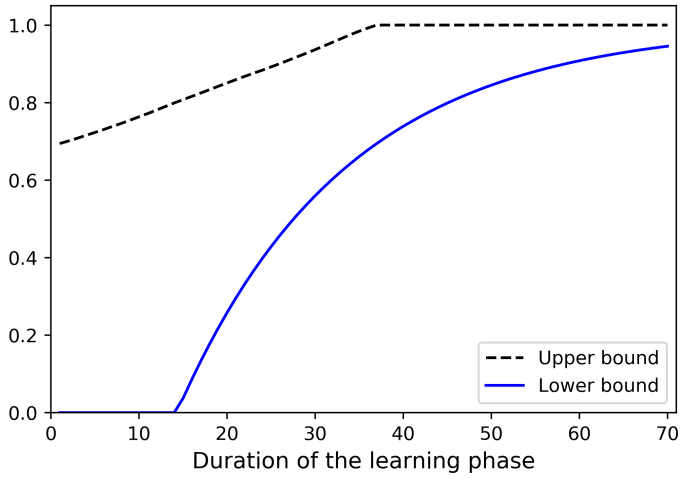


Figure 5.5: Comparison of the lower and upper bounds on the deception probability, of Theorem 20 and Corollary 3, respectively.

U_k is a Markov chain, then asymptotic deception probability is bounded from above by

$$\lim_{T\to\infty} P_{\text{Dec}}^T \leq G(Z_1^L), \tag{5.21a}$$

$$G(Z_1^L) := \frac{\frac{\log e}{2\sigma^2}\sum_{k=1}^{L}\mathbb{E}_{\mathbb{P}}\left[(AX_{k-1}+U_{k-1})^2\right]+1}{\log\left(R/\sqrt{\delta\beta}\right)}. \tag{5.21b}$$

Proof. Set $\mathbb{Q}_{X_k|Z_1^{k-1}} \sim \mathcal{N}(0,\sigma^2)$. Then, $\mathbb{P}_{X_k|Z_1^{k-1},A} = \mathcal{N}(AX_{k-1}+U_{k-1},\sigma^2)$, and consequently the measure-domination condition $\mathbb{P}_{X_k|Z_1^{k-1}} \ll \mathbb{Q}_{X_k|Z_1^{k-1}}$ holds.

$$\begin{aligned} &D(\mathbb{P}_{X_k|Z_1^{k-1},A}\|\mathbb{Q}_{X_k|Z_1^{k-1}}|\mathbb{P}_{Z_1^{k-1},A}) \\ &= \mathbb{E}_{\mathbb{P}}\left[D\left(\mathcal{N}(AX_{k-1}+U_{k-1},\sigma^2)\middle\|\mathcal{N}(0,\sigma^2)\right)\right] \\ &= \frac{\log e}{2\sigma^2}\mathbb{E}_{\mathbb{P}}\left[(AX_{k-1}+U_{k-1})^2\right]. \end{aligned} \tag{5.22}$$

The result follows by combining (5.16) and (5.22). ∎

Example 2 Theorem 20 provides a lower bound on the deception probability given $A = a$. Hence, by applying the law of total probability w.r.t. the PDF f_A of A as in (5.8), we can apply

the result of Theorem 20 to provide a lower bound also on the average deception probability for a random open-loop gain A. In this context, Figure 5.5 compares the lower and upper bounds on the deception probability provided by Theorem 20, $\max\{0, 1 - (2/(1+\delta\beta)^{L/2})\}$, and Corollary 3, $\min\{1, G(Z_1^L)\}$, respectively, where A is distributed uniformly over $[-0.9, 0.9]$. (5.21a) is valid when the control input is not a function of random variable A; hence, we assumed $U_k = -0.045Y_k$ for all time $k \in \mathbb{N}$. Here $\delta = 0.1$, $\{W_k\}$ are i.i.d. Gaussian with zero mean and variance of 0.16, and for simplicity, we let $\beta = 1.1$. Although, in general, the attacker's estimation of the random open-loop gain A and consequently the power of fictitious senor reading (5.9) vary based on the learning algorithm and the realization of A, the comparison of the lower and upper bounds in Figure 5.5 is restricted to a fixed β. 2000 Monte Carlo simulations were performed.

5.2.3 Privacy-enhancing signal

For a given duration of learning phase L, to increase the security of the system, at any time k the controller can add a privacy-enhancing signal Γ_k to an unauthenticated control policy $\{\bar{U}_k | k \in \mathbb{N}\}$:

$$U_k = \bar{U}_k + \Gamma_k\,, \qquad\qquad k \in \mathbb{N}. \tag{5.23}$$

We refer to such a control policy U_k as the *authenticated* control policy $\bar{U}_k$. We denote the states of the system that would be generated if only the unauthenticated control signal $\bar{U}_1^k$ were applied by $\bar{X}_1^k$, and the resulting trajectory—by $\bar{Z}_1^k := (\bar{X}_1^k, \bar{U}_1^k)$.

The following numerical example illustrates the effect of the privacy-enhancing signal on the deception probability.

Example 3 Here, the attacker uses the LS algorithm (5.10), the detector uses the variance test (5.5), $a = 1$, $T = 600$, $\delta = 0.1$, and $\{W_k\}$ are i.i.d. Gaussian $\mathcal{N}(0, 1)$. Figure 5.6 compares the attacker's success rate, the empirical $P_{\text{Dec}}^{a,T}$, as a function of the duration L of the learning

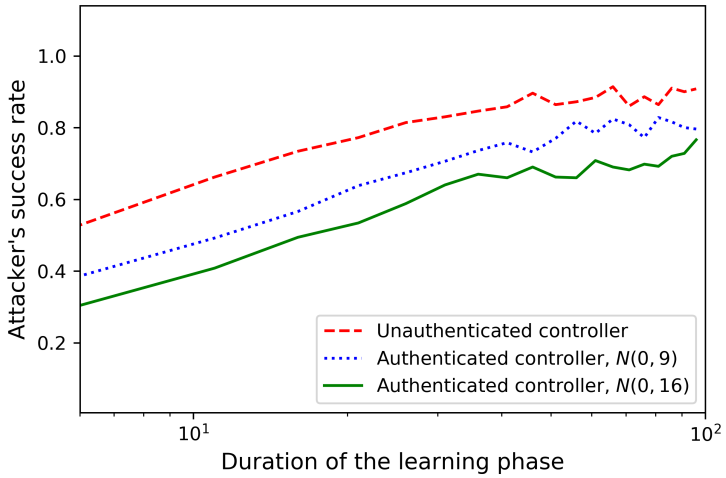


Figure 5.6: The attacker's success rate $P_{\text{Dec}}^{a,T}$ versus the duration of the exploration phase L.

phase for three different control policies: I) unauthenticated control signal $\bar{U}_1^k = -aY_k$ for all k, II) authenticated control signal (5.23), where Γ_k are i.i.d. Gaussian $\mathcal{N}(0, 9)$, III) authenticated control signal (5.23), where Γ_k are i.i.d. Gaussian $\mathcal{N}(0, 16)$. As illustrated in Figure 5.6, for the authenticated and unauthenticated control signals, the attacker's success rate increases as the duration of the learning phase increases. This is in agreement with (5.11c) since the attacker can improve its estimate of a as L increases. Also, for a fix L the attacker performance deteriorates as the power of privacy-enhancing signal Γ_k increases. Namely, Γ_k hampers the learning process of the attacker and the estimation error $|\hat{A} - a|$ increases as the power of privacy-enhancing signal increases. 500 Monte Carlo simulations were performed. •

Remark 29. A "good" privacy-enhancing signal entails little increase in the control cost [16, 17] compared to its unauthenticated version while providing enhanced detection probability (5.7) and/or false alarm probability. Finding the optimal privacy-enhancing signal is an interesting research venue. •

One may envisage that superimposing any noisy signal Γ_k on top of the control policy $\{\bar{U}_k | k \in$

$\mathbb{N}\}$ would necessarily enhance the detectability of *any* learning-based attack (5.2) since the observations of the attacker are in this case noisier. However, it turns out that injecting a strong noise for some learning algorithm may speed up the learning process as it improves the power of the signal magnified by the open-loop gains with respect to the observed noise [10]. Any signal Γ_k that satisfies the condition proposed in the following corollary will provide enhanced guarantees on the detection probability when the attacker uses *any arbitrary* learning algorithm to estimate the uniformly distributed A over the symmetric interval $[-R, R]$.

Corollary 4 *For any control policy $\{\bar{U}_k | k \in \mathbb{N}\}$ with trajectory $\bar{Z}_1^k = (\bar{X}_1^k, \bar{U}_1^k)$ and its corresponding authenticated control policy U_1^k (5.23) with trajectory $Z_1^k = (X_1^k, U_1^k)$, under the assumptions of Corollary 3, if for all $k \in \{2, \dots, L\}$*

$$\mathbb{E}_{\mathbb{P}}\left[\Psi_{k-1}^2 + 2\Psi_{k-1}(A\bar{X}_{k-1} + \bar{U}_{k-1})\right] < 0, \tag{5.24}$$

where $\Psi_{k-1} := \sum_{j=1}^{k-1} A^{k-1-j}\Gamma_j$, for any $L \geq 2$, the following majorization of G (5.21b) holds:

$$G(Z_1^L) < G(\bar{Z}_1^L). \tag{5.25}$$

Proof. Using (5.1) and (5.23), we can rewrite $\bar{X}_k$ and X_k explicitly as follows

$$\begin{aligned}
\bar{X}_k &= A^k X_0 + \sum_{j=1}^{k-1} A^{k-1-j}(\bar{U}_j + W_j), \\
X_k &= A^k X_0 + \sum_{j=1}^{k-1} A^{k-1-j}(U_j + W_j) \\
&= A^k X_0 + \sum_{j=1}^{k-1} A^{k-1-j}(\bar{U}_j + \Gamma_j + W_j) \\
&= \bar{X}_k + \Psi_{k-1}\,.
\end{aligned}$$

Thus, by (5.1), the following relation holds

$$AX_{k-1} + U_{k-1} = A\bar{X}_{k-1} + \bar{U}_{k-1} + \Psi_{k-1}\,. \tag{5.26}$$

By comparing

$$G(\bar{Z}_1^L) := \frac{\frac{\log e}{2\sigma^2}\sum_{k=1}^{L}\mathbb{E}_{\mathbb{P}}\left[(A\bar{X}_{k-1} + \bar{U}_{k-1})^2\right] + 1}{\log\left(R/\sqrt{\delta\beta}\right)},$$

with

$$G(Z_1^L) = \frac{\frac{\log e}{2\sigma^2}\sum_{k=1}^{L}\mathbb{E}_{\mathbb{P}}\left[(A\bar{X}_{k-1} + \bar{U}_{k-1} + \Psi_{k-1})^2\right] + 1}{\log\left(R/\sqrt{\delta\beta}\right)},$$

in which we have utilized (5.26), and provided (5.24), we arrive at $G(\bar{Z}_1^L) > G(Z_1^L)$. ∎

Example4 In this example, we describe a class of privacy-enhancing signal that yield better guarantees on the deception probability. For all $k \in \{2, \ldots, L\}$, clearly $\Psi_{k-1} = -(AX_{k-1} + U_{k-1})/\eta$ satisfies the condition in (5.24) for any $\eta \in \{2, \ldots, L\}$. Thus, by choosing the privacy-enhancing signals $\Gamma_1 = -(AX_1 + U_1)/\eta$, and $\Gamma_k = -(AX_k + U_k)/\eta - \sum_{j=1}^{k-2} A^{k-1-j}\Gamma_j$ for all $k \in \{3, \ldots, L\}$, (5.25) holds. •

5.3 Extension to vector systems

We generalize here the results of Section 5.2 to vector systems. Consider the networked control system depicted in Figure 5.3, and let the plant dynamics be described by a discrete-time, linear time-invariant (LTI) system

$$\mathbf{X}_{k+1} = \mathtt{A}\mathbf{X}_k + \mathbf{U}_k + \mathbf{W}_k, \tag{5.27}$$

where $\mathbf{X}_k \in \mathbb{R}^{n\times 1}$, $\mathbf{U}_k \in \mathbb{R}^{n\times 1}$, $\mathtt{A} \in \mathbb{R}^{n\times n}$, $\mathbf{W}_k \in \mathbb{R}^{n\times 1}$ represent the plant state, control input, open-loop gain of the plant, and plant disturbance, respectively, at time $k \in \mathbb{N}$. The controller, at time k, observes $\mathbf{Y}_k$ and generates a control signal $\mathbf{U}_k$ as a function of $\mathbf{Y}_1^k$, and $\mathbf{Y}_k = \mathbf{X}_k$ at times $k \in \mathbb{N}$ at which the attacker does not tamper the sensor reading. We assume that the initial condition $\mathbf{X}_0$ has a known (to all parties) distribution and is independent of the disturbance sequence $\{\mathbf{W}_k\}$. For analytical purposes, we further assume $\{\mathbf{W}_k\}$ is a process with i.i.d. multivariate Gaussian saples of zero mean and a covariance matrix $\mathbf{\Sigma}$ that is known to all parties. Without loss of generality, we assume that $\mathbf{W}_0 = 0$, $\mathbb{E}[X_0] = 0$, and take $U_0 = 0$.

We assume the attacker uses the vector analogue of learning based attacks described in Section 5.1.1 where the attacker can use *any* learning algorithm to estimate the open-loop gain matrix $\mathtt{A}$ during the learning phase. The estimation $\hat{\mathbf{A}}$ constructed by the attacker at the conclusion of the learning phase is utilized to construct the fictitious sensor readings $\{\mathbf{V}_k\}$ according to vector analogue of (5.2), where $\{\tilde{\mathbf{W}}_k | k = L, \ldots, T-1\}$ are i.i.d. multivariate Gaussian with zero and covariance $\mathbf{\Sigma}$.

Similarly to the scalar case, for analytical purposes, we assume that the power of the fictitious sensor reading is equal to $1/\beta < \infty$, namely

$$\lim_{T\to\infty} \frac{1}{T} \sum_{k=L+1}^{T} \|\mathbf{V}_k\|^2 = \frac{1}{\beta} \qquad \text{a.s. w.r.t. } \mathbb{P}_{\mathtt{A}}\,. \tag{5.28}$$

Since the multivariate Gaussian distribution with zero mean is completely characterized by its covariance matrix, as in [169], we shall test for anomalies in the latter. To that end, define the error matrix

$$\mathbf{\Delta} := \mathbf{\Sigma} - \frac{1}{T} \sum_{k=1}^{T} \left[\mathbf{Y}_{k+1} - \mathtt{A}\mathbf{Y}_k - \mathbf{U}_k(\mathbf{Y}_1^k)\right] \left[\mathbf{Y}_{k+1} - \mathtt{A}\mathbf{Y}_k - \mathbf{U}_k(\mathbf{Y}_1^k)\right]^{\dagger}.$$

As in (5.5), we shall use a test that sets a confidence interval, with respect to norm, around

the expected covariance matrix, i.e., it checks whether

$$\|\mathbf{\Delta}\|_{op} \leq \gamma, \tag{5.29}$$

for the decision time T. To simplify our analysis, we chose operator norm in (5.29) which has sub-multiplicativity property.

The following lemma provides a necessary and sufficient condition for any vector analogue of learning-based attack (5.2) to deceive the controller and remain undetected, for the case of a multivariate plant (5.27) under a covariance test (5.29), in limit of $T \to \infty$.

Lemma 22. *Consider the multivariate plant* (5.27)*, with some vector analogue of learning-based attack* (5.2) *with fictitious sensor reading power that satisfies* (5.28)*, and some measurable control policy* $\{\boldsymbol{U}_k\}$*. Then, the attacker manages to deceive the controller and remain undetected, under the covaraince test* (5.29)*, a.s. in the limit* $T \to \infty$*, if and only if*

$$\lim_{T\to\infty} \frac{1}{T} \| \sum_{k=L+1}^{T} (\hat{\mathbf{A}} - \mathtt{A}) \mathbf{V}_k \mathbf{V}_k^{\dagger} (\hat{\mathbf{A}} - \mathtt{A})^{\dagger} \|_{op} \leq \gamma. \tag{5.30}$$

Proof. Since the hijacking phase of the vector analogue of the learning-based attack of (5.2)

starts at time $k = L + 1$, using (5.27) and (5.4), we have

$$\frac{1}{T}\sum_{k=1}^{T}\left[\mathbf{Y}_{k+1} - \mathtt{A}\mathbf{Y}_k - \mathbf{U}_k(Y_1^k)\right]\left[\mathbf{Y}_{k+1} - \mathtt{A}\mathbf{Y}_k - \mathbf{U}_k\right]^\dagger \tag{5.31a}$$

$$\begin{aligned}
&= \frac{1}{T}\sum_{k=1}^{L}\mathbf{W}_k\mathbf{W}_k^\dagger \\
&\quad + \frac{1}{T}\sum_{k=L+1}^{T}\left(\tilde{\mathbf{W}}_k + (\hat{\mathbf{A}} - \mathtt{A})\mathbf{V}_k\right)\left(\tilde{\mathbf{W}}_k + (\hat{\mathbf{A}} - \mathtt{A})\mathbf{V}_k\right)^\dagger \\
&= \frac{1}{T}\left(\sum_{k=1}^{L}\mathbf{W}_k\mathbf{W}_k^\dagger + \sum_{k=L+1}^{T}\tilde{\mathbf{W}}_k\tilde{\mathbf{W}}_k^\dagger\right) \\
&\quad + \frac{1}{T}\sum_{k=L+1}^{T}(\hat{\mathbf{A}} - \mathtt{A})\mathbf{V}_k\mathbf{V}_k^\dagger(\hat{\mathbf{A}} - \mathtt{A})^\dagger \\
&\quad + \frac{1}{T}\sum_{k=L+1}^{T}\left(\tilde{\mathbf{W}}_k\mathbf{V}_k^\dagger(\hat{\mathbf{A}} - \mathtt{A})^\dagger\right)^\dagger \\
&\quad + \frac{1}{T}\sum_{k=L+1}^{T}\tilde{\mathbf{W}}_k\mathbf{V}_k^\dagger(\hat{\mathbf{A}} - \mathtt{A})^\dagger\,.
\end{aligned} \tag{5.31b}$$

Let $\mathcal{F}_k$ be the σ-field generated by $\{(\mathbf{V}_k, \hat{\mathbf{A}}, \mathbf{W}_k, \mathbf{U}_k)|k = L, \ldots, T-1\}$. Then, $\mathbf{V}_{k+1}^\dagger$ is $\mathcal{F}_k$ measurable, and $(\mathbf{W}_{k+1}, \mathcal{F}_k)$ is a Martingale difference sequence, i.e., $\mathbb{E}\left[W_{k+1}|\mathcal{F}_k\right] = 0$ a.s. Consequently, using [103, Lemma 2, Part iii], we have

$$\begin{aligned}
&\sum_{k=L+1}^{T}\tilde{\mathbf{W}}_k\mathbf{V}_k^\dagger = O(1) + \\
&\begin{pmatrix}
o\left(\sum_{k=L+1}^{T}(\mathbf{V}_k^\dagger)_1^2\right) & \cdots & o\left(\sum_{k=L+1}^{T}(\mathbf{V}_k^\dagger)_n^2\right) \\
\vdots & \vdots & \vdots \\
o\left(\sum_{k=L+1}^{T}(\mathbf{V}_k^\dagger)_1^2\right) & \cdots & o\left(\sum_{k=L+1}^{T}(\mathbf{V}_k^\dagger)_n^2\right)
\end{pmatrix} \quad \text{a.s.}
\end{aligned} \tag{5.32}$$

in the limit $T \to \infty$, where $(\mathbf{V}_k^\dagger)_i^2$ denotes the square of the i-th element of $\mathbf{V}_k^\dagger$. Further, by the

strong law of large numbers:

$$\lim_{T\to\infty}\frac{1}{T}\left(\sum_{k=1}^{L}\mathbf{W}_k^{\dagger}\mathbf{W}_k+\sum_{k=L+1}^{T}\tilde{\mathbf{W}}_k^{\dagger}\tilde{\mathbf{W}}_k\right)=\mathbf{\Sigma}\ \text{ a.s.} \tag{5.33}$$

Substituting (5.32) and (5.33) in (5.31b) completes the proof. ∎

Lemma 22 has the following important implication. We notice that

$$\lim_{T\to\infty}\frac{1}{T}\|\sum_{k=L+1}^{T}(\hat{\mathbf{A}}-\mathtt{A})\mathbf{V}_k\mathbf{V}_k^{\dagger}(\hat{\mathbf{A}}-\mathtt{A})^{\dagger}\|_{op} \tag{5.34a}$$

$$\leq\lim_{T\to\infty}\frac{1}{T}\sum_{k=L+1}^{T}\|(\hat{\mathbf{A}}-\mathtt{A})\mathbf{V}_k((\hat{\mathbf{A}}-\mathtt{A})\mathbf{V}_k)^{\dagger}\|_{op} \tag{5.34b}$$

$$\leq\lim_{T\to\infty}\frac{1}{T}\sum_{k=L+1}^{T}\|(\hat{\mathbf{A}}-\mathtt{A})\mathbf{V}_k\|_{op}^2 \tag{5.34c}$$

$$\leq\frac{\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}^2}{\beta}, \tag{5.34d}$$

where the (5.34b) follows from the triangle inequality, (5.34c) and (5.34d) follow from the sub-multiplicativity of operator nroms and noticing $\|\mathbf{V}_k\|=\|\mathbf{V}_k\|_{op}$, where in the latter the power constraint (5.28) is put into forth. Thus, if $\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}^2\leq\gamma\beta$, (5.30) holds, and hence, by Lemma 22, in the limit of $T\to\infty$, the attacker is able to deceive the controller and remain undetected a.s. (5.34) implies that the norm of the estimation error, $\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}$, dictates the ease with which an attack can go undetected. This is used next to develop a lower bound on the deception probability.

5.3.1 Lower Bound on the Deception Probability

We start by observing that in the case of multivariate systems, and in contrast to their scalar counterparts, some control actions might not reveal the entire plant dynamics, and in this case the attacker might not be able to learn the plant completely. This phenomenon is captured

by the persistent excitation property of control inputs, which describes control-action signals that are sufficiently rich to excite all the system modes that will allow to learn them. While avoiding persistently exciting control inputs can be used as a way to secure the system against learning-based attacks, here, we use a probabilistic variant of this property [50, 155], and assume that the control policy satisfies it in our lower bound on the deception probability.

Definition 9 (Persistent excitation) *Given a plant* (5.27), $\zeta > 0$, *and* $\rho \in [0, 1]$, *the control policy* $\boldsymbol{U}_k$ *is* (ζ, ρ)*-persistently exciting if there exists a time* $L_0 \in \mathbb{N}$ *such that, for all* $\tau \geq L_0$,

$$\mathbb{P}_{\mathtt{A}} \left(\frac{1}{\tau} \mathbf{G}_\tau \succeq \zeta \mathtt{I}_{n \times n} \right) \geq \rho, \tag{5.35}$$

where $\mathbf{G}_\tau$ *is the summation of Gram matrix of state up to time* τ, *that is,*

$$\mathbf{G}_\tau := \sum_{k=1}^{\tau} \boldsymbol{X}_k \boldsymbol{X}_k^\dagger. \tag{5.36}$$

As in Section 5.2.1, to find a lower bound on the deception probability $P_{\text{Dec}}^{\mathtt{A},T}$, we consider a specific estimate of $\hat{\mathbf{A}}$, obtained via a specific estimation algorithm, at the conclusion of the first phase by the attacker, as follows.

LS algorithm

The vector variant of the LS algorithm (5.10), is

$$\hat{\mathbf{A}} = \begin{cases} \mathbf{0}_{n \times n}, & \det(\mathbf{G}_{L-1}) = 0; \\ \sum_{k=1}^{L-1} \left((\mathbf{X}_{k+1} - \mathbf{U}_k) \mathbf{X}_k^\dagger \right) \mathbf{G}_{L-1}^{-1}, & \text{otherwise}, \end{cases} \tag{5.37}$$

where $\mathbf{0}_{k \times \ell}$ denotes an all zero matrix of dimensions $k \times \ell$.

In the next lemma we prove an upper bound for the estimation error, $\|\hat{\mathbf{A}} - \mathtt{A}\|_{op}$, of the above LS algorithm, and use it to extend the bound (5.11b) to the vector systems using the LS

algorithm (5.37).

Lemma 23. *Consider the plant* (5.27)*. If the attacker constructs* $\hat{\mathbf{A}}$ *using LS estimation* (5.37)*, and the controller uses a policy* $\{\boldsymbol{U}_k\}$ *for which the event in* (5.35) *occurs for* $L-1$*, that is* $\mathbf{G}_{L-1}/(L-1) \succeq \zeta \mathcal{I}_{n\times n}$*. Then*

$$\|\hat{\mathbf{A}} - \mathtt{A}\|_{op} \leq \frac{1}{\zeta L} \sum_{k=1}^{L-1} \|\mathbf{W}_k \mathbf{X}_k^\dagger\|_{op} \qquad \text{a.s. w.r.t. } \mathbb{P}_{\mathtt{A}}\,. \tag{5.38}$$

Proof. Since $\mathbf{G}_{L-1}$ is a Hermitian matrix we start by noticing that since the event in (5.35) occurs for $L-1$ we have $\det(\mathbf{G}_{L-1}) \neq 0$, using [214, Theorem 7.8, part 2]. Thus, when the attacker uses the LS estimation (5.37) we deduce

$$\begin{aligned}
\hat{\mathbf{A}} - \mathtt{A} &= \left(\sum_{k=1}^{L-1} \Big((\mathbf{X}_{k+1} - \mathbf{U}_k)\mathbf{X}_k^\dagger \Big) - \mathtt{A}\mathbf{G}_{L-1} \right) \mathbf{G}_{L-1}^{-1} \\
&= \sum_{k=1}^{L-1} \Big((\mathbf{X}_{k+1} - \mathtt{A}\mathbf{X}_k - \mathbf{U}_k)\mathbf{X}_k^\dagger \Big) \mathbf{G}_{L-1}^{-1} \\
&= \sum_{k=1}^{L-1} \Big(\mathbf{W}_k \mathbf{X}_k^\dagger \Big) \mathbf{G}_{L-1}^{-1},
\end{aligned}$$

where the last two equalities follow from (5.36) and (5.27), respectively. Thus, using sub-multiplicativity of operator nroms and the triangle inequality we have

$$\|\hat{\mathbf{A}} - \mathtt{A}\|_{op} \leq \sum_{k=1}^{L-1} \|\mathbf{W}_k \mathbf{X}_k^\dagger\|_{op} \|\mathbf{G}_{L-1}^{-1}\|_{op}. \tag{5.39}$$

We now continue by upper bounding $\|\mathbf{G}_{L-1}^{-1}\|_{op}$ as follows. Since the event in (5.35) occurs for

$L-1$, using [214, Theorem 7.8, part 3] we deduce

$$\frac{1}{\zeta L}\upsilon^{\dagger}\mathtt{I}_{n\times n}\upsilon \geq \upsilon^{\dagger}\mathbf{G}_{L}^{-1}\upsilon \tag{5.40}$$

for all $\upsilon \in \mathbb{R}^{n\times 1}$. Since $\mathbf{G}_{L-1}$ is a Hermitian positive semi-definite matrix, then so is $\mathbf{G}_{L-1}^{-1}$ (see [214, Problem 1, Section 7.1]). Thus, using [214, Theorem 7.4] the Hermitian matrix $\sqrt{\mathbf{G}_{L-1}^{-1}}$ exists. We continue by noticing $\upsilon^{\dagger}\mathtt{I}_{n\times n}\upsilon = \|\upsilon\|^2$, and

$$\upsilon^{\dagger}\sqrt{\mathbf{G}_{L-1}^{-1}}^{\dagger}\sqrt{\mathbf{G}_{L-1}^{-1}}\upsilon = \left\|\sqrt{\mathbf{G}_{L-1}^{-1}}\upsilon\right\|^2.$$

Thus, using (5.40) we deduce

$$\left\|\sqrt{\mathbf{G}_{L-1}^{-1}}\right\|_{op} \leq \frac{1}{\sqrt{\zeta L}}. \tag{5.41}$$

Using (5.41), sub-multiplicativity of operator nroms, and (5.39), (5.38) follows. ∎

Theorem 22. *Consider the plant* (5.27) *with a* (ζ,ρ)*-persistently exciting control policy* $\{U_k\}$*, and any vector analogue of learning-based attack learning-based attack* (5.2) *with fictitious sensor reading power that satisfies* (5.28) *with a learning phase of duration* $L \geq L_0+1$*. Then, the asymptotic deception probability, when using the covaraince test* (5.29)*, is bounded from below as*

$$\lim_{T\to\infty} P_{\mathrm{Dec}}^{\mathtt{A},T} \geq \mathbb{P}_{\mathtt{A}}\left(\|\hat{\mathbf{A}}-\mathtt{A}\|_{op} < \sqrt{\gamma\beta}\right) \tag{5.42a}$$

$$\geq \rho\mathbb{P}_{\mathtt{A}}\left(\frac{1}{\zeta L}\sum_{k=1}^{L-1}\|\mathbf{W}_k\mathbf{X}_k^{\dagger}\|_{op} < \sqrt{\gamma\beta}\right). \tag{5.42b}$$

Proof. (5.42a) follows from Lemma 22 and (5.34). We now prove (5.42b). By the Law of total

probability,

$$\mathbb{P}_{\mathtt{A}}\left(\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}<\sqrt{\gamma\beta}\right)\geq$$
$$\mathbb{P}_{\mathtt{A}}\left(\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}<\sqrt{\gamma\beta}\middle|(1/L)\sum_{k=1}^{L}\mathbf{X}_k\mathbf{X}_k^{\dagger}\succeq\zeta\mathtt{I}_{n\times n}\right)\mathbb{P}_{\mathtt{A}}\left((1/L)\sum_{k=1}^{L}\mathbf{X}_k\mathbf{X}_k^{\dagger}\succeq\zeta\mathtt{I}_{n\times n}\right).$$

Since, the control policy is (ζ,ρ)-persistently exciting and $L-1\geq L_0$ the result now follows using Lemma 23 and (5.35). ∎

Remark 30. The bound (5.11c) for scalar system, which is *independent* of the control policy and value of state, has been developed using the concentration bounds of in [158] for the scalar LS algorithm (5.10). To best of our knowledge there are no similar concentration bounds for the vector variant of the LS algorithm (5.10) which works for *any* open-loop gain $\mathtt{A}$, and a large class of control policies. This is an interesting research venue. •

Remark 31. The implication of (5.34), which relates the deception criterion (5.30) to the estimation error $\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}$, is used to find the lower bound (5.42). Finding a lower bound in term of $\|\hat{\mathbf{A}}-\mathtt{A}\|_{op}$ for (5.34a) is the first step to extent the upper bounds provided in Theorem 21 to vector systems. This is an interesting research venue. •

Example 5 In this example, we compare the empirical performance of the covariance test against the learning-based attack which utilizes LS estimation (5.37), and the replay attack. At every time k, the controller tests the empirical covariance for abnormalities over a detection window $[1,T]$, using a confidence interval $2\gamma>0$ around the operator norm of error matrix $\mathbf{\Delta}$ (5.29). Since we are considering the Euclidean norm for vectors, the induced operator norm amounts to $\|\mathbf{\Delta}\|_{op}=\sqrt{\lambda_{max}(\mathbf{\Delta}^{\dagger}\mathbf{\Delta})}$. Here, $\gamma=0.1$, $\mathbf{U}_k=-0.9\mathtt{A}\mathbf{Y}_k$ for all $1\leq k\leq T=600$,

$$\mathtt{A}=\begin{pmatrix}1&2\\3&4\end{pmatrix},\qquad\qquad\mathbf{\Sigma}=\begin{pmatrix}1&0\\0&2\end{pmatrix}.\tag{5.43}$$

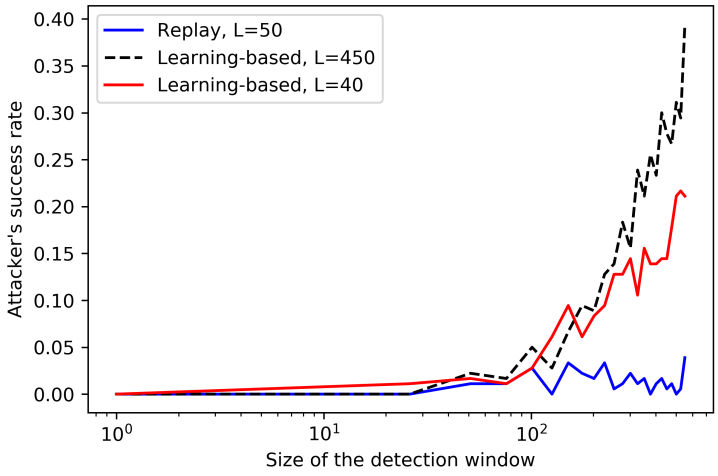


Figure 5.7: The attacker's success rate $P_{\text{Dec}}^{\mathtt{A},T}$ versus the size of the detection window T.

Figure 5.7 presents the performance averaged over 180 runs of a Monte-Carlo simulation. It illustrates that the vector variant of our learning-based attack also outperforms the replay attack. A learning-based attack with a learning phase of length $L = 40$ has a higher success rate than a replay attack with a larger recording length of $L = 50$. Similarly to the discussion for scalar systems in Section 5.1.3, the false-alarm rate decays to zero as the size of the detection window T tends to infinity. Thus, the success rate of learning-based attacks increases as the size of detection window increases. Finally, as illustrated in Figure 5.7, the attacker's success rate increases as the duration of the learning phase L increases, since the attacker improves its estimate of $\mathtt{A}$ as L increases. •

Example 6 In this example we consider the vector-plant setting with a privacy-enhancing signal (cf. Section 5.2.3) and its yielded enhanced detection probability. As in Example 5, we assume that the controller uses the empirical covariance test (5.29) and that the attacker utilizes LS estimation (5.37). Again, the false alarm rate decays to zero as the detection window size T goes to infinity. Here, $\gamma = 0.1$, $\mathtt{A}$ is as in (5.43), and $\mathbf{\Sigma} = \mathtt{I}_2$.

Figure 5.8 compares the attacker's success rate, namely, the empirical $P_{\text{Dec}}^{\mathtt{A},T}$, as a function

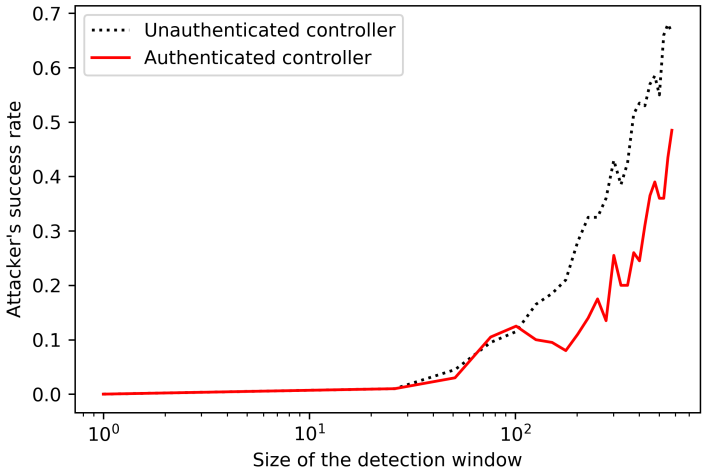


Figure 5.8: The attacker's success rate $P_{\text{Dec}}^{\mathbb{A},T}$ versus the size of the detection window T.

of size of the detection window T for two different control policies, averaged over 200 runs of a Monte-Carlo simulation: I) Unauthenticated control $\bar{\mathbf{U}}_1^k = -\mathbb{A}\mathbf{Y}_k$ for all $1 \leq k \leq T = 600$, II) The vector analogue of the authenticated control signal of (5.23), where $\mathbf{\Gamma}_k$ are i.i.d. zero-mean Gaussian with a diagonal covariance matrix with diagonal $\begin{pmatrix} 12, & 10 \end{pmatrix}$. As is evident from Figure 5.8, the privacy-enhancing signal $\mathbf{\Gamma}_k$ hampers the learning process of the attacker consequently reduces its deception probability. •

Remark 32. We concentrated on linear systems throughout this work, where, for finding a lower bound on the deception probability of the learning-based attack, the LS algorithm has been utilized. For nonlinear dynamics with high complexity, the attacker can use more sophisticated learning algorithms such as Gaussian processes [39] or Deep neural networks (DNN) [61].

We now discuss a special case for nonlinear system where our results for linear system are usefull. Consider the following scalar nonlinear system

$$X_{k+1} = f(X_k, U_k) + W_k,$$

where the plant disturbance process $\{W_k\}$ has i.i.d. Gaussian samples of zero mean and variance σ^2. As in (5.3), under legitimate system operation, the controller observation Y_k behaves according to

$$Y_{k+1} - f(Y_k, U_k) \sim \text{ i.i.d. } \mathcal{N}(0, \sigma^2). \tag{5.44}$$

Let $\hat{F}$ be the attacker estimation of the function f at the conclusion of Phase 1. We assume that during the hijacking phase the fictitious sensor reading is constructed according to the vector analogue of (5.2),

$$V_{k+1} = \hat{F}(V_k, U_k) + \tilde{W}_k\,, \qquad\qquad k = L, \ldots, T-1.$$

Then, one can replace $Y_{k+1} - aY_k - U_k$ of (5.4) with

$$Y_{k+1} - f(Y_k, U_k) = \tilde{W}_k + \hat{F}(V_k, U_k) - f(V_k, U_k),$$

in (5.5), and test whether the empirical variance of (5.44) falls within a confidence interval of 2δ around σ^2. Given the restrictive assumption that the class of learning algorithms utilized by the attacker satisfies

$$|\hat{F}(V_k, U_k) - f(V_k, U_k)| \leq \vartheta |V_k| \text{ a.s.}$$

where ϑ is a non-negative random variable, we have

$$(\tilde{W}_k + \hat{F}(V_k, U_k) - f(V_k, U_k))^2 \leq (\tilde{W}_k + \vartheta |V_k|)^2.$$

Therefore, if

$$\frac{1}{T}(\sum_{k=1}^{L} W_k^2 + \sum_{k=L+1}^{T}(\tilde{W}_k + \vartheta|V_k|)^2 \in (\mathrm{Var}\,[W] - \delta, \mathrm{Var}\,[W] + \delta), \tag{5.45}$$

the attacker will deceive the controller. Thus, by noticing the similarity of (5.6) and (5.45), and utilizing Theorem 20, we deduce

$$\lim_{T\to\infty} P_{\mathrm{Dec}}^{f,T} \geq \mathbb{P}_a\left(\vartheta < \sqrt{\delta\beta}\right). \qquad \bullet$$

5.4 Exploration vs. Exploitation

In Section 5.2, the attacker learning was only limited to the exploration phase, i.e, $\hat{A}_k = \hat{A}_L$ for all $k \geq L+1$, and the attacker only aimed to destroy the plant during the hijacking (exploration) phase. Now in this section, we assume the attacker can refine its estimate of the open-loop gain during the hijacking (exploration) phase. In other words, the learning of open-loop gain a may or may not continue during the exploitation phase. Additionally, the attacker can use different learning algorithms in the two phases, and in the hijacking (exploitation) phase, the attacker has the additional degree of freedom of being able to choose the control input to the plant.

In addition, in Section 5.2, only the variance test (5.5) was considered as a possible detection strategy. Here, we study the trade-off between the performance of the learning algorithm, and the performance of *arbitrary* detection and control strategies adopted by the controller, providing a tight bound on the scaling of the expected time required to detect the attack, as the probability of detection tends to one. We also show that this bound can be achieved by the learning-based attack and a detection strategy.

In Section 5.2 the control input U_k assumed to be any measurable function of Y_1^{k-1}, in this section, for simplicity, we assume U_k is a deterministic function of Y_1^{k-1}.

Throughout this section we use the following notation. Let $p_0(y_1^T)$ be the conditional probability of y_1^T given the attacker did not hijack the system i.e. $\Theta_1 = \ldots \Theta_L = \Theta_{L+1} = \ldots \Theta_T = 0$. Likewise, $p_1(y_1^T)$ is the conditional probability of y_1^T given the attacker intervene as MITM i.e. $\Theta_1 = \ldots = \Theta_L = 0$ and $\Theta_{L+1} = \ldots \Theta_T = 1$.

5.4.1 Main results

We start by defining the following performance measure.

Definition 10 *Given the class of learning-based attacks, the ϵ-deception time $T(\epsilon)$ is the duration required by the controller to make a decision regarding the presence or absence of an attacker with probability of correct decision at least $(1-\epsilon)$, namely $P_{\text{Dec}}^{a,T} \leq \epsilon$ where $T = L + T(\epsilon) + 1$.*

In other words, for the given class learning-based attacks, $T(\epsilon)$ is the largest time interval during which the attacker can deceive the controller and remain undetected with confidence at least ϵ. In this case, for all $L+1 \leq k \leq T(\epsilon) + L$, we have the probability of detection

$$P_{\text{Det}}^{a,T} = \mathbb{P}(\hat{\Theta}_k = 1 | \Theta_k = 1) < 1 - \epsilon.$$

We start with defining a non-divergent learning algorithm.

Definition 11 *A learning algorithm M is non-divergent if its estimation error is non-increasing in the duration of the learning i.e. for all $k_2 > k_1$*

$$|\hat{A}_{k_2} - a| \leq |\hat{A}_{k_1} - a|. \tag{5.46}$$

We then continue by proving the following proposition which characterises the KL divergence between $p_1(y_1^T)$ and $p_0(y_1^T)$ for learning-based attacks with non-divergent learning algorithm, and is useful to derive our main results.

Proposition 3 *Given the class of attacks $\mathcal{A}(L)$ with non-divergent learning algorithm M in Phase 2, for all $n > L$, the cumulative KL divergence is*

$$D(p_1(Y_1^n)||p_0(Y_1^n)) = nC(n)\frac{(\hat{A}_L - a)^2}{2\sigma^2},$$

where $C(n)$ is the time averaged deception cost of the attacker until time n, namely

$$C(n) := \frac{1}{n}\mathbb{E}\Big[\sum_{k=L+1}^{n} V_k^2\Big]. \tag{5.47}$$

Proof. As the attacker does not intervene before L, for all $n \leq L$,

$$D(p_1(Y_1^n)||p_0(Y_1^n)) = 0.$$

Thus, for all $n > L$, using the chain rule, we have

$$D(p_1(Y_1^n)||p_0(Y_1^n)) = \tag{5.48}$$
$$\sum_{k=L+1}^{n} D(p_1(Y_k|Y_1^{k-1})||p_0(Y_k|Y_1^{k-1})).$$

Since U_k is a deterministic function of Y_1^{k-1}, if $\Theta_k = 1$, for all $k > L$, we have

$$Y_k|Y_1^{k-1} \sim \mathcal{N}(\hat{A}_k Y_{k-1} + U_k, \sigma^2).$$

Similarly, if $\Theta_k = 0$, for all $k > L$, we have

$$Y_k|Y_1^{k-1} \sim \mathcal{N}(aY_{k-1} + U_k, \sigma^2).$$

Thus, for all $k > L$, we have

$$\begin{aligned} D(p_1(Y_k|Y_1^{k-1})||p_0(Y_k|Y_1^{k-1})) &= \frac{((\hat{A}_k - a)Y_{k-1})^2}{2\sigma^2}, \\ &\overset{(a)}{\leq} \frac{((\hat{A}_L - a)Y_{k-1})^2}{2\sigma^2}, \end{aligned} \tag{5.49}$$

where (a) follows from the fact that learning algorithm of the attacker in exploitation phase is non-diverging.

By (5.48) and (5.49), for all $n > L$, we have

$$D(p_1(Y_1^n)||p_0(Y_1^n)) = \mathbb{E}[\sum_{k=L+1}^{n} (Y_k)^2] \frac{(\hat{A}_L - a)^2}{2\sigma^2}.$$

The result now follows by noticing $Y_k = V_k$, for all $k > L$. ∎

To achieve its destabilizing objectives, the attacker must remain undetected. Hence, it is desirable for the attacker to maximize the deception time $T(\epsilon)$. The following theorem presents the trade-offs between the estimation error of the attacker's learning algorithm, the expected deception time $T(\epsilon)$ of any detection strategy, and the expected energy spent by to generate the ficticious signal in (5.2).

Theorem 23. *Given the class of learning-based attacks i.e. $\Theta_k = 1$ for all $k > L$, for all $0 < \epsilon < 1$, non-divergent learning algorithm M in Phase 2, decision time $T > L$, and detection strategy $\mathcal{D}$ such that*

$$P_{\text{Dec}}^{a,T} = O(|\epsilon \log \epsilon|), \tag{5.50}$$

and

$$P_{FA}^{a,T} = O(|\epsilon \log \epsilon|), \tag{5.51}$$

the deception time $T(\epsilon) = T - L - 1$ *satisfies*

$$\mathbb{E}[T(\epsilon)|L] \geq (1 + o(1))\frac{2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 C(n_0)} \quad \text{as } \epsilon \to 0,$$

where $C(n_0)$ *is defined in* (5.47)*, and*

$$n_0 := \max\left\{ n > L : \mathbb{E}\Big[\sum_{k=L+1}^{n} V_k^2 \Big] < \log(1/\epsilon)\frac{2\sigma^2}{(\hat{A}_L - a)^2} \right\}. \tag{5.52}$$

Proof. The proof of theorem consists of two parts. First, for all $0 < c < 1$ and system under learning-based attack, we show that for the probability of detection error to be small i.e. $O(|\epsilon \log \epsilon|)$, the log-likelihood ratio

$$S^T := \log\left(p_1(y_1^T)/p_0(y_1^T) \right) \tag{5.53}$$

should be greater than $-(1-c)\log\epsilon$ with high probability as $\epsilon \to 0$. Namely, the inequality

$$S^T \geq -(1-c)\log\epsilon$$

must hold with high probability, as $\epsilon \to 0$. Second, given $\hat{A}_L$, we show that there exists $0 < \bar{c} < 1$ such that for all $0 < c \leq \bar{c}$,

$$\mathbb{P}\left(T(\epsilon) \leq \frac{(1-\bar{c})2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 C(n_0)} \right) \to 0 \tag{5.54}$$

as $\epsilon \to 0$.

By (5.50) and (5.51), both type I and type II errors of the hypothesis test $\Theta_k = 1$ vs. $\Theta_k = 0$ are $O(|\epsilon \log \epsilon|)$ for $k \geq L + 1$. Thus, by [28, Lemma 4], for all $0 < c < 1$,

$$\mathbb{P}\Big(S^T \leq -(1-c)\log\epsilon \Big) = O(-\epsilon^c \log\epsilon). \tag{5.55}$$

Therefore, as $\epsilon \to 0$, the probability in (5.55) tends to 0, which concludes the first part of the proof.

For proving the second part, that is (5.54), we need the following lemma.

Lemma 24. *Given log-likelihood ratio* (5.53) *and for all* $0 < c < 1$ *we have*

$$\lim_{n' \to \infty} \mathbb{P}\left(\max_{1 \le k \le n'} S^k \ge D\left(p_1(Y_1^{n'}) || p_0(Y_1^{n'})\right) + n'c \right) = 0. \tag{5.56}$$

Proof of Lemma 24: We have

$$S^n = M_1^n + M_2^n,$$

where

$$M_1^n = \sum_{k=1}^{n} \left(\log\left(\frac{p_1(y_k|y_1^{k-1})}{p_0(y_k|y_1^{k-1})}\right) - D(p_1(Y_k|Y_1^{k-1})||p_0(Y_k|Y_1^{k-1})) \right),$$

and

$$M_2^n = \sum_{k=1}^{n} D(p_1(Y_k|Y_1^{k-1})||p_0(Y_k|Y_1^{k-1})).$$

Using the chain rule of KL-Divergence, we have

$$M_2^n = D(p_1(Y_1^n)||p_0(Y_1^n)).$$

Thus, if event in (5.56) occurs for a fixed n_1, i.e.

$$M_1^{n_1} + M_2^{n_1} \ge D(p_1(Y_1^{n_1})||p_0(Y_1^{n_1})) + n_1 c,$$

then it implies $M_1^{n_1} \ge n_1 c$. Since $Y_k|Y_1^{k-1}$ has normal distribution (see Proposition 3), there

exists a constant b such that the probability in (5.56) simplifies as

$$\begin{aligned}&\mathbb{P}\left(\max_{1\leq k\leq n'} S^k \geq (D(p_1(y_1^{n'})||p_0(y_1^{n'})) + n'c)\right)\\&\leq \mathbb{P}(\max_{1\leq k\leq n'} M_1^k \geq n'c) \overset{(a)}{\leq} b/n'c^2,\end{aligned}$$

where (a) follows from the fact that M_1^k is a martingale w.r.t filtration $\mathcal{F}_k = \sigma(Y_{1:k-1})$ with 0 mean and using the Doob-Kolmogorov extension of Chebyshev's inequality [48]. •

Given the definition of n_0 we have

$$\mathbb{E}\Big[\sum_{k=L+1}^{n_0} V_k^2\Big]\frac{(\hat{A}_L - a)^2}{2\sigma^2} < \log(1/\epsilon).$$

Therefore, using the definition of $C(n_0)$ (5.47), there exists $0 < \bar{c} < 1$ and $0 < c' < 1$ such that

$$n_0 C(n_0)\frac{(\hat{A}_L - a)^2}{2\sigma^2} + n_0 c' = (1-\bar{c})\log(1/\epsilon), \tag{5.57}$$

that is,

$$n_0 = \frac{(1-\bar{c})2\sigma^2\log(1/\epsilon)}{2\sigma^2 c' + (\hat{A}_L - a)^2 C(n_0)}. \tag{5.58}$$

Since $S^L = 0$, as discussed in [28, Theorem 2] for all $0 < c < 1$

$$\begin{aligned}\mathbb{P}(T(\epsilon) \leq n_0) \leq \mathbb{P}\Big(T(\epsilon) \leq n_0 \text{ and } S^T \geq (1-c)\log(1/\epsilon)\Big)\\ + \mathbb{P}\Big(S^T < (1-c)\log(1/\epsilon)\Big)\end{aligned}$$

Now by choosing $c = \bar{c}$ and using (5.57) we have

$$\begin{aligned}
&\mathbb{P}(T(\epsilon) \leq n_0) \leq \\
&\mathbb{P}\Big(T(\epsilon) \leq n_0 \text{ and } S^T \geq n_0 C(n_0)\frac{(\hat{A}_L - a)^2}{2\sigma^2} + n_0 c'\Big) \\
&+ \mathbb{P}\Big(S^T \leq n_0 C(n_0)\frac{(\hat{A}_L - a)^2}{2\sigma^2} + n_0 c'\Big) \\
&\leq \mathbb{P}\Big(\max_{1\leq k\leq n_0} S^k \geq n_0 C(n_0)\frac{(\hat{A}_L - a)^2}{2\sigma^2} + n_0 c'\Big) \\
&+ \mathbb{P}\Big(S^T \leq n_0 C(n_0)\frac{(\hat{A}_L - a)^2}{2\sigma^2} + n_0 c'\Big),
\end{aligned} \tag{5.59}$$

and the first and the second terms at the right-hand side of (5.59) approach zero by (5.56) and Proposition 3, and (5.55), respectively. ∎

The above theorem states that for any detection strategy $\mathcal{D}$ with probability of error $O(|\epsilon(\log(\epsilon))|)$, the expected time to reach a decision is at least $\Omega\left(\log(1/\epsilon)/((\hat{A}_L - a)^2 C(n_0))\right)$. The next theorem establishes that this bound is tight and can be achieved.

Theorem 24. *If the estimate $\hat{A}_L$ is known to the controller, for all $0 < \epsilon < 1$ and class of learning-based attacks, there exists a detection strategy $\mathcal{D}$ and a learning-based attack R^*, whose learning is only limited to the exploration phase, such that for any decision time $T > L$, we have*

$$P_{\text{Dec}}^{a,T} = O(\epsilon),$$

and

$$P_{FA}^{a,T} = O(\epsilon),$$

and the deception time $T(\epsilon) = T - L - 1$ *satisfies*

$$\mathbb{E}[T(\epsilon)|L] \leq (1 + o(1)) \frac{2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 C(n_0 + 1)}, \quad \text{as } \epsilon \to 0.$$

Proof. Let the attack be R^* where the attacker does not learn in exploitation phase, i.e. for all $k \geq L + 1$, $\hat{A}_k = \hat{A}_L$. Now, for all $k > L$ if $\Theta_k = 1$, we have

$$Y_k | Y_1^{k-1} \sim \mathcal{N}(\hat{A}_k Y_{k-1} + U_k, \sigma^2).$$

Similarly, if $\Theta_k = 0$, then

$$Y_k | Y_1^{k-1} \sim \mathcal{N}(a Y_{k-1} + U_k, \sigma^2).$$

We define sequential probability ratio test at the controller as follows. If

$$\sum_{k=1}^{n} \log \left(\frac{p_1(y_k | y_1^{k-1})}{p_0(y_k | y_1^{k-1})} \right) \geq \log(1/\epsilon),$$

then at time n, $\hat{\Theta}_n = 1$, and if

$$\sum_{k=1}^{n} \log \left(\frac{p_0(y_k | y_1^{k-1})}{p_1(y_k | y_1^{k-1})} \right) \geq \log(1/\epsilon),$$

then at time n, $\hat{\Theta}_n = 0$. For this test, the probability of error is at most ϵ, and the proof is along the same direction as [157, Theorem 1]. Given the learning-based attack, we let decision time T be

$$T = \min \left\{ n : \sum_{k=1}^{n} \log \left(\frac{p_1(y_k | y_1^{k-1})}{p_0(y_k | y_1^{k-1})} \right) \geq \log(1/\epsilon) \right\}. \tag{5.60}$$

Using [28, Lemma 2], for system under attack $\mathcal{A}(L)$ and for all $c > 0$, there exist a $b > 0$ such

that

$$P\Bigg(\sum_{k=1}^{n}\log\left(\frac{p_1(y_k|y_1^{k-1})}{p_0(y_k|y_1^{k-1})}\right) \\ < (D(p_1(Y_1^n)||p_0(Y_1^n)) - nc)\Bigg) \leq e^{-bn}. \tag{5.61}$$

Using the definition of n_0 (5.52) for all $\bar{n} > n_0$ we have

$$\log(1/\epsilon) \leq \mathbb{E}\Big[\sum_{k=L+1}^{\bar{n}} V_k^2\Big]\frac{(\hat{A}_L - a)^2}{2\sigma^2}$$
$$= D(p_1(Y_1^{\bar{n}})||p_0(Y_1^{\bar{n}})),$$

where the equality follows from Proposition 3. Thus, for any $\bar{n} > n_0$, there exist a constant $\bar{c} > 0$ such that

$$\log(1/\epsilon) \leq D(p_1(Y_1^{\bar{n}})||p_0(Y_1^{\bar{n}})) - \bar{n}c'.$$

Thus, using (5.61) we have for all $\bar{n} > n_0$ we have

$$P\Bigg(\sum_{k=1}^{\bar{n}}\log\left(\frac{p_1(y_k|y_1^{k-1})}{p_0(y_k|y_1^{k-1})}\right) < \log(1/\epsilon)\Bigg) \leq e^{-b\bar{n}}.$$

Consequently, using (5.60) and (5.58) the result follows. ∎

As $\epsilon \to 0$, $C(n_0) \to C(n_0 + 1)$, and $|\epsilon| \leq |\epsilon \log \epsilon|$. Also, an attacker whose learning is only limited to the exploration phase satisfies the condition (5.46) with equality. Thus, the bounds in Theorems 23 and 24 are tight in the limit $\epsilon \to 0$.

The attack R^* which achieves the bound on $T(\epsilon)$ is a learning-based attack whose learning is limited to the exploration phase, and the attacker focuses on destabilizing the system in the exploitation phase and does not continue to learn beyond time L. The corresponding detection strategy is a sequential probability ratio test which computes the ratio of posterior probability

of the two hypothesis i.e. attacker is present or absent, and makes a decision when this ratio crosses the threshold $\log(1/\epsilon)$ [202]. This strategy has been studied under the assumption that the samples are i.i.d. and we extend the analysis here to the dependent case of the feedback signal at the controller.

Since $|\hat{A}_k - a|$ at any time k is unknown to the attacker, the precise value of $T(\epsilon)$ cannot be determined by the attacker using the above theorems. Also, Theorem 24 assumes the knowledge of the attacker estimate $\hat{A}_L$ at the controller. Next, we derive several useful corollaries from Theorems 23 and 24 about attack and detection strategies.

In the following, for simplicity of presentation we restrict the class of learning in the exploration phase, although we expect that our results can be extended to more general settings.

Definition 12 *Let $\mathcal{L}$ be the class of all learning algorithms such that if $M \in \mathcal{L}$, then*

$$\mathbb{P}(|\hat{A}_L - a| > \eta) \leq \frac{c}{(\eta L)^\alpha},$$

where $\eta > 0$, $\alpha \geq 1$, L is duration of exploration phase, and $\hat{A}_L$ is the estimate of a after L samples.

Thus, the class $\mathcal{L}$ provides an unbiased estimate of a as the learning duration $n \to \infty$, and this estimate converges to the interval $[a - \eta, a + \eta]$ at rate $O(1/(\eta n)^\alpha)$. There are many practical learning algorithms that fall in this class. For example, in [158] it is shown that the least squares (LS) algorithm (5.10) satisfy

$$\mathbb{P}(|\hat{A}_L - a| > \eta) \leq \frac{2}{(1+\eta^2)^{L/2}}.$$

The following corollary provides a trade-off between the duration of the exploration phase L and the deception time $T(\epsilon)$ of the attacker.

Corollary 5. *For any learning algorithm $M \in \mathcal{L}$ in the exploration phase and non-divergent*

learning algorithm in the exploitation phase, and any $\delta > 0$, if

$$\frac{2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 C(n_0)} > K,$$

then expected deception time is $E[T(\epsilon)|L] \geq K$. Moreover, with probability at least $1-\delta$ the length of exploration phase L must satisfy

$$L \geq \sqrt{\frac{KC(n_0)}{2\sigma^2 \log(1/\epsilon)}} \left(\frac{c}{\delta}\right)^{1/\alpha}.$$

Proof. Using Theorem 23, if

$$\frac{2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 C(n_0)} > K,$$

then $\mathbb{E}[T(\epsilon)|L] \geq K$. Therefore,

$$|\hat{A}_L - a| \leq \sqrt{\frac{2\sigma^2 \log(1/\epsilon)}{KC(n_0)}}.$$

For $\eta = \sqrt{2\sigma^2 \log(1/\epsilon)/KC(n_0)}$ and class $\mathcal{L}$ of learning algorithms, the duration of exploration phase L is

$$L \geq \sqrt{\frac{KC(n_0)}{2\sigma^2 \log(1/\epsilon)}} \left(\frac{c}{\delta}\right)^{1/\alpha},$$

with probability at least $1-\delta$. ∎

It follows that to achieve an expected deception time of at least K, the duration L of the exploration phase should be at least $\Omega(\sqrt{K})$.

The following corollary presents the relationship between the estimation error of the learning algorithm and the deception cost of the user irrespective of the class of learning algorithm, and its proof follows from the statement of Theorem 23 by eliminating $(1 + o(1))$ factor.

Corollary 6. *(Uncertainty principle for the attacker). Given $T(\epsilon)$, class of learning-based attacks*

with non-divergent learning algorithm M in exploitation phase, and detection strategy $\mathcal{D}$ satisfying (5.50)-(5.51)*, the product of the estimation error and the average deception cost of the attacker is at least*

$$(\hat{A}_L - a)^2 C(n_0) \geq \frac{2\sigma^2 \log(1/\epsilon)}{\mathbb{E}[T(\epsilon)|L]}.$$

Thus, for a given ϵ and $\mathbb{E}[T(\epsilon)|L]$, the estimation error at the end of exploration phase and the deception cost of the attacker cannot be made arbitrarily small simultaneously. This holds irrespective of the learning algorithm.

Unlike the attacker, the controller would want to minimize the deception time $T(\epsilon)$. This can be achieved by designing appropriate detection strategies and control policies. The control policy can play a crucial role in the reduction of the deception time. However, this can be done at the expense of the energy in the control signal U_k. The following corollary provides the trade-off between the energy spent by the controller and the deception time $T(\epsilon)$.

Corollary 7. *Given the class of learning-based attacks, if $\mathbb{E}[T(\epsilon)|L] \leq K$, and for all $k \geq L+1$*

$$2\mathbb{E}[\hat{A}_k V_k U_k] \geq -\sigma^2 - \mathbb{E}[\hat{A}_k^2 V_k^2], \tag{5.62}$$

then the expected energy of the control signal

$$R(n_0) := \frac{1}{n_0}\mathbb{E}\Big[\sum_{k=L+1}^{n_0} U_k^2\Big],$$

must satisfy

$$R(n_0) \geq \frac{2\sigma^2 \log(1/\epsilon)}{(\hat{A}_L - a)^2 K}.$$

Proof. Since $\tilde{W}_k$ is independent of U_k and V_k and $\mathbb{E}[\tilde{W}_k] = 0$ we have

$$\mathbb{E}[V_{k+1}^2] - \mathbb{E}[U_k^2] = \tag{5.63}$$
$$\mathbb{E}[\hat{A}_k^2 V_k^2] + \sigma^2 + 2\mathbb{E}[\hat{A}_k V_k U_k]$$

Thus, by (5.62), we deduce

$$\mathbb{E}[V_{k+1}^2] \geq \mathbb{E}[U_k^2],$$

so we have

$$C(n_0) = \frac{1}{n_0}\mathbb{E}\left[\sum_{k=L}^{n_0} V_k^2\right] \geq \frac{1}{n_0}\mathbb{E}\left[\sum_{k=L}^{n_0} U_k^2\right].$$

The result now follows by applying Corollary 6. ∎

The above corollary shows that the expected control energy of the signal until time n_0 after the attack starting at $k = L$ will be inversely proportional to the upper bound on the deception time K. In other words, if the controller requires the deception time to be $O(K)$, then the expected control energy $R(n_0)$ should be $\Omega(1/K)$. Alternatively, the expected deception time is at least $\Omega(1/R(n_0))$. Since the L is unknown, the controller can maintain a high level of expected signal energy $\mathbb{E}[U_k^2]$ at every time instance k.

The following example shows the existence of a linear control policy that satisfies the condition (5.62).

Example 7 *For attacker R^* whose learning is only limited to the exploration phase, if $\hat{A}_L \geq 0.5$ then there exist a linear controller $U_k = -\bar{K}V_k$ that satisfies* (5.62) *while stabilizing the virtual system* (5.2).

Proof. In this example, the attack is R^*, and $\hat{A}_k = \hat{A}_L$ during the exploitation phase. In this

proof we first determine conditions on control gain $\bar{K}$ to ensure the control policy $U_k = -\bar{K}V_k$ satisfies (5.62) and stabilizes the virtual system (5.2), and then show these conditions could happen simultaneously, provided $\hat{A}_L \geq 0.5$. If $|\hat{A}_L - \bar{K}| < 1$, then the controller stabilizes the virtual plant in (5.2). Thus, we have

$$\hat{A}_L - 1 < \bar{K} < \hat{A}_L + 1. \tag{5.64}$$

As $U_k = -\bar{K}V_k$, (5.62) is equivalent to

$$\hat{A}_L(2\bar{K} - \hat{A}_L) \leq \frac{\sigma^2}{\mathbb{E}[V_k^2]}. \tag{5.65}$$

Furthermore, since $\hat{A}_L > 0$, (5.65) is equivalent to

$$\bar{K} \leq \frac{\hat{A}_L}{2} + \frac{\sigma^2}{2\hat{A}_L\mathbb{E}[V_k^2]}. \tag{5.66}$$

Thus if the control gain $\bar{K}$ satisfies the conditions (5.64) and (5.66), the controller $U_k = -\bar{K}V_k$ satisfies (5.62) while stabilizing the virtual system (5.2). Hence, it remains to prove conditions (5.64) and (5.66) occurs simultaneously, as follows.

$$\frac{\hat{A}_L}{2} + \frac{\sigma^2}{2\hat{A}_L\mathbb{E}[V_k^2]} \leq \frac{\hat{A}_L}{2} + \frac{1}{2\hat{A}_L} < \tag{5.67a}$$

$$\hat{A}_L + \frac{1}{2\hat{A}_L} \leq \hat{A}_L + 1, \tag{5.67b}$$

where (5.67a) follows by noting $\mathbb{E}[V_k^2] \geq \sigma^2$ (by rewriting (5.63) for V_k and V_{k-1}, clearly we have $\mathbb{E}[V_k^2] \geq \sigma^2$), and (5.67b) follows by the hypothesis $\hat{A}_L \geq 0.5$. ∎

5.5 Conclusions

We studied attacks on cyber-physical systems which consist of exploration and exploitation phases, where the attacker first explores the dynamic of the plant, after which it hijacks the system by playing a fictitious sensor reading to the controller/detector while and feeding a detrimental control input to the plant.

Future work will explore the extension of the established results to partially-observable vector systems where the input (actuation) matrix is not identity, revising the attacker full access to both sensor and control signals, designing optimal privacy-enhancing signals, and studying the relation between our proposed privacy-enhancing signal with the noise signal utilized to achieve differential privacy [34]. Further, since the controller does not know the exact time instant at which an attack might occur, a more realistic scenario would be that of continual testing, i.e., that in which the integrity of the system is tested at every time step and where the false alarm and deception probabilities are defined with a union across time. We leave this treatment for future research.

Chapter 5, in part, is a reprint of the material in M. J. Khojasteh, A. Khina, M. Franceschetti, T. Javidi, "Learning-based attacks in cyber-physical systems," arXiv:1809.06023, 2018, being prepared for publication. The dissertation author was the primary investigator and author of this paper. The last part of this chapter, in part, is a reprint of the material in A. Rangi, M. J. Khojasteh, M. Franceschetti, "Learning-based attacks in cyber-physical systems: exploration vs. exploitation," 2019, being prepared for publication. The dissertation author was the co-primary investigator and co-author of this paper.

Bibliography

[1] Saurabh Amin, Alvaro A Cárdenas, and S Shankar Sastry. Safe and secure networked control systems under denial-of-service attacks. In *International Workshop on Hybrid Systems: Computation and Control*, pages 31–45. Springer, 2009.

[2] Venkat Anantharam and Sergio Verdu. Bits through queues. *IEEE Transactions on Information Theory*, 42(1):4–18, 1996.

[3] D. J. Antunes and M. H. Balaghi I. Consistent event-triggered control for discrete-time linear systems with partial state information. *IEEE Control Systems Letters*, 4(1):181–186, Jan 2020.

[4] Laure Aptel and Aslan Tchamkerten. Feedback increases the capacity of queues. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 1116–1120. IEEE, 2018.

[5] Ehsan Ardestanizadeh and Massimo Franceschetti. Control-theoretic approach to communication with feedback. *IEEE Transactions on Automatic Control*, 57(10):2576–2587, 2012.

[6] Erdal Arikan. On the reliability exponent of the exponential timing channel. *IEEE Transactions on Information Theory*, 48(6):1681–1689, 2002.

[7] Rajesh Arumugam, Vikas Reddy Enti, Liu Bingbing, Wu Xiaojun, Krishnamoorthy Baskaran, Foong Foo Kong, A Senthil Kumar, Kang Dee Meng, and Goh Wai Kit. Davinci: A cloud computing framework for service robots. In *2010 IEEE international conference on robotics and automation*, pages 3084–3089. IEEE, 2010.

[8] Nadarajah Asokan, Valtteri Niemi, and Kaisa Nyberg. Man-in-the-middle in tunnelled authentication protocols. In *International Workshop on Security Protocols*, pages 28–41. Springer, 2003.

[9] Karl Johan Astrom and Bo M Bernhardsson. Comparison of riemann and lebesgue sampling for first order stochastic systems. In *IEEE Conference on Decision and Control*, volume 2, pages 2011–2016, Las Vegas, Nevada, USA, 2002.

[10] Karl Johan Åström and Peter Eykhoff. System identification-a survey. *Automatica*, 7(2):123–162, 1971.

[11] Cheng-Zong Bai, Fabio Pasqualetti, and Vijay Gupta. Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs. *Automatica*, 82:251–260, 2017.

[12] J Baillieul. Feedback designs for controlling device arrays with communication channel bandwidth constraints. In *ARO Workshop on Smart Structures, Pennsylvania State Univ*, pages 16–18, 1999.

[13] M Hadi Balaghi, Duarte J Antunes, Mohammad H Mamduhi, Sandra Hirche, et al. A decentralized consistent policy for event-triggered control over a shared contention-based network. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 1719–1724. IEEE, 2018.

[14] Anand S Bedekar and Murat Azizoglu. The information-theoretic capacity of discrete-time queues. *IEEE Transactions on Information Theory*, 44(2):446–461, 1998.

[15] Felix Berkenkamp, Matteo Turchetta, Angela Schoellig, and Andreas Krause. Safe model-based reinforcement learning with stability guarantees. In *Advances in neural information processing systems*, pages 908–918, 2017.

[16] Dimitri P Bertsekas. *Dynamic programming and optimal control*, volume 1. Athena scientific Belmont, MA, 1995.

[17] Dimitri P Bertsekas. Reinforcement learning and optimal control. *Athena Scientific*, 2019.

[18] Nicola Bezzo, James Weimer, Miroslav Pajic, Oleg Sokolsky, George J Pappas, and Insup Lee. Attack resilient state estimation for autonomous robotic systems. In *Intelligent Robots and Systems (IROS 2014), 2014 IEEE/RSJ International Conference on*, pages 3692–3698. IEEE, 2014.

[19] Alan S Brown. SCADA vs. the hackers. *Mechanical Engineering*, 124(12):37, 2002.

[20] Alvaro Cardenas, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, Shankar Sastry, et al. Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security*, volume 5, 2009.

[21] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security*, pages 355–366. ACM, 2011.

[22] Alvaro A Cardenas, Saurabh Amin, and Shankar Sastry. Secure control: Towards survivable cyber-physical systems. *System*, 1(a2):a3, 2008.

[23] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 62(5):2434–2449, 2016.

[24] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 62(5):2434–2449, 2017.

[25] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, pages 77–92. San Francisco, 2011.

[26] Thomas Chen and Saeed Abu-Nimeh. Lessons from stuxnet. *Computer*, 44(4):91–93, 2011.

[27] Yuan Chen, Soummya Kar, and José MF Moura. Cyber-physical attacks with control objectives. *IEEE Transactions on Automatic Control*, 63(5):1418–1425, 2017.

[28] Herman Chernoff. Sequential design of experiments. *The Annals of Mathematical Statistics*, 30(3):755–770, 1959.

[29] Sandeep Chinchali, Apoorva Sharma, James Harrison, Amine Elhafsi, Daniel Kang, Evgenya Pergament, Eyal Cidon, Sachin Katti, and Marco Pavone. Network offloading policies for cloud robotics: a learning-based approach. *Robotics: Science and Systems*, 2019.

[30] Todd P Coleman and Maxim Raginsky. Mutual information saddle points in channels of exponential family type. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1355–1359. IEEE, 2010.

[31] Fritz Colonius. Minimal bit rates and entropy for exponential stabilization. *SIAM Journal on Control and Optimization*, 50(5):2988–3010, 2012.

[32] Fritz Colonius and Christoph Kawan. Invariance entropy for control systems. *SIAM Journal on Control and Optimization*, 48(3):1701–1721, 2009.

[33] Giacomo Como, Fabio Fagnani, and Sandro Zampieri. Anytime reliable transmission of real-valued information through digital noisy channels. *SIAM Journal on Control and Optimization*, 48(6):3903–3924, 2010.

[34] Jorge Cortés, Geir E Dullerud, Shuo Han, Jerome Le Ny, Sayan Mitra, and George J Pappas. Differential privacy in control and network systems. In *2016 IEEE 55th Conference on Decision and Control (CDC)*, pages 4252–4272. IEEE, 2016.

[35] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[36] Claudio De Persis. n-bit stabilization of n-dimensional nonlinear systems in feedforward form. *IEEE Transactions on Automatic Control*, 50(3):299–311, 2005.

[37] Claudio De Persis and Alberto Isidori. Stabilizability by state feedback implies stabilizability by encoded state feedback. *Systems & control letters*, 53(3-4):249–258, 2004.

[38] Sarah Dean, Horia Mania, Nikolai Matni, Benjamin Recht, and Stephen Tu. On the sample complexity of the linear quadratic regulator. *Foundations of Computational Mathematics*, Aug 2019.

[39] Marc Deisenroth and Carl E Rasmussen. Pilco: A model-based and data-efficient approach to policy search. In *Proceedings of the 28th International Conference on machine learning (ICML-11)*, pages 465–472, 2011.

[40] David F Delchamps. Stabilizing a linear system with quantized state feedback. *IEEE Transactions on Automatic Control*, 35(8):916–924, 1990.

[41] Burak Demirel, Vijay Gupta, and Mikael Johansson. On the trade-off between control performance and communication cost for event-triggered control over lossy networks. In *Control Conference (ECC), 2013 European*, pages 1168–1174. IEEE, 2013.

[42] Burak Demirel, Vijay Gupta, Daniel E Quevedo, and Mikael Johansson. On the trade-off between communication and control cost in event-triggered dead-beat control. *IEEE Transactions on Automatic Control*, 62(6):2973–2980, 2016.

[43] Burak Demirel, Vijay Gupta, Daniel E Quevedo, and Mikael Johansson. On the trade-off between communication and control cost in event-triggered dead-beat control. *IEEE Transactions on Automatic Control*, 62(6):2973–2980, 2016.

[44] Seyed Mehran Dibaji, Mohammad Pirani, Anuradha M Annaswamy, Karl Henrik Johansson, and Aranya Chakrabortty. Secure control of wide-area power systems: Confidentiality and integrity threats. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 7269–7274. IEEE, 2018.

[45] Dimos V Dimarogonas, Emilio Frazzoli, and Karl H Johansson. Distributed event-triggered control for multi-agent systems. *IEEE Transactions on Automatic Control*, 57(5):1291–1297, 2011.

[46] Jian Ding, Yuval Peres, Gireeja Ranade, and Alex Zhai. When multiplicative noise stymies control. *Annals of applied probability*, 2018. To appear.

[47] VS Dolk, Pietro Tesi, Claudio De Persis, and WPMH Heemels. Event-triggered control systems under denial-of-service attacks. *IEEE Transactions on Control of Network Systems*, 4(1):93–105, 2017.

[48] Joseph L Doob. *Stochastic processes*, volume 7.

[49] John C Duchi and Martin J Wainwright. Distance-based and continuum fano inequalities with applications to statistical estimation. *arXiv preprint arXiv:1311.2669*, 2013.

[50] Marie Duflo. *Random iterative models*, volume 34. Springer Science & Business Media, 2013.

[51] Rick Durrett. *Probability: theory and examples*. Cambridge university press, 2010.

[52] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29, 2011.

[53] Chongrong Fang, Yifei Qi, Peng Cheng, and Wei Xing Zheng. Cost-effective watermark based detector for replay attacks on cyber-physical systems. In *2017 11th Asian Control Conference (ASCC)*, pages 940–945. IEEE, 2017.

[54] Song Fang, Jie Chen, and I Hideaki. *Towards integrating control and information theories*. Springer, 2017.

[55] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 59(6):1454–1467, 2014.

[56] Aidin Ferdowsi and Walid Saad. Deep learning for signal authentication and security in massive internet-of-things systems. *IEEE Transactions on Communications*, 67(2):1371–1387, 2018.

[57] David P Fidler. Was stuxnet an act of war? decoding a cyberattack. *IEEE Security & Privacy*, 9(4):56–59, 2011.

[58] David B Flamholz, Anuradha M Annaswamy, and Eugene Lavretsky. Baiting for defense against stealthy attacks on cyber-physical systems. In *AIAA Scitech 2019 Forum*, page 2338, 2019.

[59] Hamed Shisheh Foroush and Sonia Martinez. On event-triggered control of linear systems under periodic denial-of-service jamming attacks. In *Decision and Control (CDC), 2012 IEEE 51st Annual Conference on*, pages 2551–2556. IEEE, 2012.

[60] Massimo Franceschetti and Paolo Minero. Elements of information theory for networked control systems. In *Information and Control in Networks*, pages 3–37. Springer, 2014.

[61] Yarin Gal, Rowan McAllister, and Carl Edward Rasmussen. Improving pilco with bayesian neural network dynamics models. In *Data-Efficient Machine Learning workshop, ICML*, volume 4, 2016.

[62] R Gardner. The Brunn-Minkowski inequality. *Bulletin of the American Mathematical Society*, 39(3):355–405, 2002.

[63] Allen Gersho and Robert M Gray. *Vector quantization and signal compression*, volume 159. Springer Science & Business Media, 2012.

[64] James Giles and Bruce Hajek. An information-theoretic and game-theoretic study of timing channels. *IEEE Transactions on Information Theory*, 48(9):2455–2477, 2002.

[65] Antoine Girard. Dynamic triggering mechanisms for event-triggered control. *IEEE Transactions on Automatic Control*, 60(7):1992–1997, 2014.

[66] Amin Gohari, Mahtab Mirmohseni, and Masoumeh Nasiri-Kenari. Information theory of molecular communication: Directions and challenges. *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2(2):120–142, 2016.

[67] Yacov Y Haimes. Risk of terrorism to cyber-physical and organizational-societal infrastructures. *Public Works Management & Policy*, 6(4):231–240, 2002.

[68] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada. An introduction to event-triggered and self-triggered control. In *IEEE Conference on Decision and Control*, pages 3270–3285, Maui, HI, 2012.

[69] WPM Heemels Heemels, MCF Donkers, and Andrew R Teel. Periodic event-triggered control for linear systems. *IEEE Transactions on Automatic Control*, 58(4):847–861, 2012.

[70] Joao Hespanha, Antonio Ortega, and Lavanya Vasudevan. Towards the control of linear systems with minimum bit-rate. In *Proc. 15th Int. Symp. on Mathematical Theory of Networks and Systems (MTNS)*, 2002.

[71] João P Hespanha, Daniel Liberzon, and Andrew R Teel. Lyapunov conditions for input-to-state stability of impulsive systems. *Automatica*, 44(11):2735–2744, 2008.

[72] Joo P Hespanha, Payam Naghshtabrizi, and Yonggang Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, 95(1):138–162, 2007.

[73] Pedro Hespanhol, Matthew Porter, Ram Vasudevan, and Anil Aswani. Statistical watermarking for networked control systems. In *2018 Annual American Control Conference (ACC)*, pages 5467–5472. IEEE, 2018.

[74] Andreas Hoehn and Ping Zhang. Detection of covert attacks and zero dynamics attacks in cyber-physical systems. In *2016 American Control Conference (ACC)*, pages 302–307. IEEE, 2016.

[75] Michael Horstein. Sequential transmission using noiseless feedback. *IEEE Transactions on Information Theory*, 9(3):136–143, 1963.

[76] Maryam Hosseini, Takashi Tanaka, and Vijay Gupta. Designing optimal watermark signal for a stealthy attacker. In *2016 European Control Conference (ECC)*, pages 2258–2262. IEEE, 2016.

[77] M. H. Balaghi I, D. J. Antunes, M. H. Mamduhi, and S. Hirche. An optimal LQG controller for stochastic event-triggered scheduling over a lossy communication network. *IFAC-PapersOnLine*, 51(23):58–63, 2018.

[78] Z-P Jiang, A. R. Teel, and L. Praly. Small-gain theorem for ISS systems and applications. *Mathematics of Control, Signals and Systems*, 7(2):95–120, 1994.

[79] Karl Henrik Johansson, Magnus Egerstedt, John Lygeros, and Shankar Sastry. On the regularization of zeno hybrid automata. *Systems & control letters*, 38(3):141–150, 1999.

[80] Aris Kanellopoulos and Kyriakos G Vamvoudakis. A moving target defense control framework for cyber-physical systems. *IEEE Transactions on Automatic Control*, 2019.

[81] Ben Kehoe, Sachin Patil, Pieter Abbeel, and Ken Goldberg. A survey of research on cloud robotics and automation. *IEEE Transactions on automation science and engineering*, 12(2):398–409, 2015.

[82] B Asadi Khashooei, Duarte J Antunes, and WPMH Heemels. A consistent threshold-based policy for event-triggered control. *IEEE Control Systems Letters*, 2(3):447–452, 2018.

[83] A. Khina, Y. Nakahira, Y. Su, and B. Hassibi. Algorithms for optimal control with fixed-rate feedback. In *IEEE Conference on Decision and Control*, pages 6015–6020, Melbourne, Australia, Dec 2017.

[84] Anatoly Khina, Elias Riedel Garding, Gustav M Pettersson, Victoria Kostina, and Babak Hassibi. Control over gaussian channels with and without source-channel separation. *IEEE Transactions on Automatic Control*, 2019.

[85] Anatoly Khina, Wael Halbawi, and Babak Hassibi. (Almost) practical tree codes. In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 2404–2408. IEEE, 2016.

[86] Anatoly Khina, Victoria Kostina, Ashish Khisti, and Babak Hassibi. Tracking and control of gauss–markov processes over packet-drop channels with acknowledgments. *IEEE Transactions on Control of Network Systems*, 6(2):549–560, 2018.

[87] M. J. Khojasteh, P. Tallapragada, J. Cortés, and M. Franceschetti. The value of timing information in event-triggered control: The scalar case. *Allerton Conference on Communication, Control, and Computing*, pages 1165–1172, September 2016.

[88] M. J. Khojasteh, P. Tallapragada, J. Cortés, and M. Franceschetti. Time-triggering versus event-triggering control over communication channels. In *IEEE Conference on Decision and Control*, pages 5432–5437, Melbourne, Australia, Dec 2017.

[89] Mohammad Javad Khojasteh, Massimo Franceschetti, and Gireeja Ranade. Estimating a linear process using phone calls. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 127–131. IEEE, 2018.

[90] Mohammad Javad Khojasteh, Massimo Franceschetti, and Gireeja Ranade. Stabilizing a linear system using phone calls. In *2019 18th European Control Conference (ECC)*, pages 2856–2861. IEEE, 2019.

[91] Mohammad Javad Khojasteh, Mojtaba Hedayatpour, Jorge Cortés, and Massimo Franceschetti. Event-triggered stabilization of disturbed linear systems over digital channels. In *2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE, 2018.

[92] Mohammad Javad Khojasteh, Mojtaba Hedayatpour, Jorge Cortés, and Massimo Franceschetti. Event-triggering stabilization of complex linear systems with disturbances over digital channels. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 152–157. IEEE, 2018.

[93] Mohammad Javad Khojasteh, Mojtaba Hedayatpour, and Massimo Franceschetti. Theory and implementation of event-triggered stabilization over digital channels. In *2019 IEEE 58th Annual Conference on Decision and Control (CDC)*. IEEE.

[94] Mohammad Javad Khojasteh, Anatoly Khina, Massimo Franceschetti, and Tara Javidi. Authentication of cyber-physical systems under learning-based attacks. *IFAC-PapersOnLine*, 2019.

[95] Mohammad Javad Khojasteh, Pavankumar Tallapragada, Jorge Cortés, and Massimo Franceschetti. The value of timing information in event-triggered control. *IEEE Transactions on Automatic Control*, 2019.

[96] Solmaz S Kia, Jorge Cortés, and Sonia Martínez. Distributed event-triggered communication for dynamic average consensus in networked systems. *Automatica*, 59:112–119, 2015.

[97] Kyoung-Dae Kim and Panganamala R Kumar. Cyber-physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100 (Special Centennial Issue):1287–1308, 2012.

[98] Daniel Klain. On the equality conditions of the Brunn-Minkowski theorem. *Proceedings of the American Mathematical Society*, 139(10):3719–3726, 2011.

[99] E. Kofman and J. H. Braslavsky. Level crossing sampling in feedback stabilization under data-rate constraints. In *IEEE Conference on Decision and Control*, pages 4423–4428, San Diego, CA, 2006.

[100] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.

[101] Victoria Kostina and Babak Hassibi. Rate-cost tradeoffs in control. In *Allerton Conference on Communication, Control, and Computing*, pages 1157–1164, Monticello, IL, 2016. IEEE.

[102] Victoria Kostina, Yuval Peres, Miklós Z. Rácz, and Gireeja Ranade. Rate-limited control of systems with uncertain gain. *Allerton Conference on Communication, Control, and Computing*, pages 1189–1196, 2016.

[103] Tze Leung Lai and Ching Zong Wei. Least squares estimates in stochastic regression models with applications to identification and control of dynamic systems. *The Annals of Statistics*, pages 154–166, 1982.

[104] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[105] Ralph Langner. To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve. 2013.

[106] Robert M Lee, Michael J Assante, and Tim Conway. German steel mill cyber attack. *Industrial Control Systems*, 30:62, 2014.

[107] Lichun Li, Xiaofeng Wang, and Michael Lemmon. Stabilizing bit-rate of disturbed event triggered control systems. *IFAC Proceedings Volumes*, 45(9):70–75, 2012.

[108] Lichun Li, Xiaofeng Wang, and Michael Lemmon. Stabilizing bit-rate of disturbed event triggered control systems. *IFAC Proceedings Volumes*, 45(9):70–75, 2012.

[109] Lichun Li, Xiaofeng Wang, and Michael Lemmon. Stabilizing bit-rates in quantized event triggered control systems. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, pages 245–254. ACM, 2012.

[110] Lichun Li, Xiaofeng Wang, and Michael Lemmon. Stabilizing bit-rates in quantized event triggered control systems. In *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control*, pages 245–254. ACM, 2012.

[111] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, 2017.

[112] Daniel Liberzon. On stabilization of linear systems with limited information. *IEEE Transactions on Automatic Control*, 48(2):304–307, 2003.

[113] Daniel Liberzon. Nonlinear control with limited information. *Communications in Information & Systems*, 9(1):41–58, 2009.

[114] Daniel Liberzon. Finite data-rate feedback stabilization of switched and hybrid linear systems. *Automatica*, 50(2):409–420, 2014.

[115] Daniel Liberzon and João P Hespanha. Stabilization of nonlinear systems with limited information feedback. *IEEE Transactions on Automatic Control*, 50(6):910–915, 2005.

[116] Daniel Liberzon and Sayan Mitra. Entropy and minimal data rates for state estimation and model detection. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*, pages 247–256. ACM, 2016.

[117] Daniel Liberzon and Sayan Mitra. Entropy and minimal bit rates for state estimation and model detection. *IEEE Transactions on Automatic Control*, 63(10):3330–3344, 2017.

[118] Lars Lindemann, Dipankar Maity, John S Baras, and Dimos V Dimarogonas. Event-triggered feedback control for signal temporal logic tasks. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 146–151. IEEE, 2018.

[119] Steffen Linsenmayer, Rainer Blind, and Frank Allgöwer. Delay-dependent data rate bounds for containability of scalar systems. *IFAC-PapersOnLine*, 50(1):7875–7880, 2017.

[120] Xin Liu and R Srikant. The timing capacity of single-server queues with multiple flows. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 2004.

[121] Nuno C Martins, Munther A Dahleh, and Nicola Elia. Feedback stabilization of uncertain systems in the presence of a direct link. *IEEE Transactions on Automatic Control*, 51(3):438–447, 2006.

[122] Nikolai Matni, Alexandre Proutiere, Anders Rantzer, and Stephen Tu. From self-tuning regulators to reinforcement learning and back again. *arXiv preprint arXiv:1906.11392*, 2019.

[123] A. S. Matveev and A. V. Savkin. *Estimation and control over communication networks*. Springer Science & Business Media, 2009.

[124] Alexey S Matveev and Andrey V Savkin. An analogue of Shannon information theory for detection and stabilization via noisy discrete communication channels. *SIAM journal on Control and Optimization*, 46(4):1323–1367, 2007.

[125] Alexey S Matveev and Andrey V Savkin. Shannon zero error capacity in the problems of state estimation and stabilization via noisy communication channels. *International Journal of Control*, 80(2):241–255, 2007.

[126] Geoff McDonald, Liam O Murchu, Stephen Doherty, and Eric Chien. Stuxnet 0.5: The missing link. *Symantec Report*, 2013.

[127] Fei Miao, Miroslav Pajic, and George J Pappas. Stochastic game approach for replay attack detection. In *Decision and control (CDC), 2013 IEEE 52nd annual conference on*, pages 1854–1859. IEEE, 2013.

[128] Richard H Middleton, Alejandro J Rojas, James S Freudenberg, and Julio H Braslavsky. Feedback stabilization over a first order moving average Gaussian noise channel. *IEEE Transactions on Automatic Control*, 54(1):163–167, 2009.

[129] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015:91, 2015.

[130] Paolo Minero, Lorenzo Coviello, and Massimo Franceschetti. Stabilization over Markov feedback channels: the general case. *IEEE Transactions on Automatic Control*, 58(2):349–362, 2013.

[131] Paolo Minero and Massimo Franceschetti. Anytime capacity of a class of Markov channels. *IEEE Transactions on Automatic Control*, 62(3):1356–1367, 2017.

[132] Paolo Minero, Massimo Franceschetti, Subhrakanti Dey, and Girish N Nair. Data rate theorem for stabilization over time-varying feedback channels. *IEEE Transactions on Automatic Control*, 54(2):243–255, 2009.

[133] Yilin Mo, Emanuele Garone, Alessandro Casavola, and Bruno Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5967–5972. IEEE, 2010.

[134] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[135] Yilin Mo, Sean Weerakkody, and Bruno Sinopoli. Physical authentication of control systems: designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, 35(1):93–109, 2015.

[136] Richard M Murray, Karl J Astrom, Stephen P Boyd, Roger W Brockett, and Gunter Stein. Future directions in control in an information-rich world. *IEEE Control Systems*, 23(2):20–33, 2003.

[137] Mohammad Naghshvar, Tara Javidi, and Michele Wigger. Extrinsic jensen–shannon divergence: Applications to variable-length coding. *IEEE Transactions on Information Theory*, 61(4):2148–2164, 2015.

[138] Girish Nair. A non-stochastic information theory for communication and state estimation. *IEEE Transactions on Automatic Control*, 58:1497–1510, 2013.

[139] Girish Nair, Fabio Fagnani, Sandro Zampieri, and Robin J Evans. Feedback control under data rate constraints: An overview. *Proceedings of the IEEE*, 95(1):108–137, 2007.

[140] Girish N Nair, Subhrakanti Dey, and Robin J Evans. Communication-limited stabilisability of jump Markov linear systems. In *15th Int. Symp. Mathematical Theory of Networks and Systems, Notre Dame, IN*, 2002.

[141] Girish N Nair and Robin J Evans. Stabilizability of stochastic linear systems with finite feedback data rates. *SIAM Journal on Control and Optimization*, 43(2):413–436, 2004.

[142] Girish N Nair, Robin J Evans, Iven MY Mareels, and William Moran. Topological feedback entropy and nonlinear stabilization. *IEEE Transactions on Automatic Control*, 49(9):1585–1597, 2004.

[143] Luyao Niu, Jie Fu, and Andrew Clark. Minimum violation control synthesis on cyber-physical systems under attacks. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 262–269. IEEE, 2018.

[144] Rafail Ostrovsky, Yuval Rabani, and Leonard J Schulman. Error-correcting codes for automatic control. *IEEE Transactions on Information Theory*, 55(7):2931–2941, 2009.

[145] Michael Ouimet, David Iglesias, Nisar Ahmed, and Sonia Martínez. Cooperative robot localization using event-triggered estimation. *Journal of Aerospace Information Systems*, 15(7):427–449, 2018.

[146] Fabio Pasqualetti, Florian Dörfler, and Francesco Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729, 2013.

[147] Justin Pearson, Joao P Hespanha, and Daniel Liberzon. Control with minimal cost-per-symbol encoding and quasi-optimality of event-based encoders. *IEEE Transactions on Automatic Control*, 62(5):2286–2301, 2017.

[148] Johan Peralez, Vincent Andrieu, Madiha Nadri, and Ulysse Serres. Event-triggered output feedback stabilization via dynamic high-gain scaling. *IEEE Transactions on Automatic Control*, 63(8):2537–2549, 2018.

[149] Yury Polyanskiy and Yihong Wu. Lecture notes on information theory. 2017.

[150] Romain Postoyan, Adolfo Anta, Dragan Nešić, and Paulo Tabuada. A unifying lyapunov-based framework for the event-triggered control of nonlinear systems. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pages 2559–2564. IEEE, 2011.

[151] Balaji Prabhakar and Robert Gallager. Entropy and the timing capacity of discrete queues. *IEEE Transactions on Information Theory*, 49(2):357–370, 2003.

[152] Viktor Vasil_evich Prasolov. *Problems and theorems in linear algebra*, volume 134. American Mathematical Soc., 1994.

[153] Charles Chapman Pugh. *Real mathematical analysis*, volume 2011. Springer, 2002.

[154] Daniel E Quevedo, Vijay Gupta, Wann-Jiun Ma, and Serdar Yüksel. Stochastic stability of event-triggered anytime control. *IEEE Transactions on Automatic Control*, 59(12):3373–3379, 2014.

[155] Maxim Raginsky. Divergence-based characterization of fundamental limitations of adaptive dynamical systems. In *Communication, Control, and Computing (Allerton), 2010 48th Annual Allerton Conference on*, pages 107–114. IEEE, 2010.

[156] Gireeja Ranade and Anant Sahai. Control capacity. In *Information Theory (ISIT), 2015 IEEE International Symposium on*, pages 2221–2225. IEEE, 2015.

[157] Anshuka Rangi, Massimo Franceschetti, and Stefano Marano. Decentralized chernoff test in sensor networks. In *2018 IEEE International Symposium on Information Theory (ISIT)*, pages 501–505. IEEE, 2018.

[158] Anders Rantzer. Concentration bounds for single parameter adaptive control. In *2018 Annual American Control Conference (ACC)*, pages 1862–1866. IEEE, 2018.

[159] Benjamin Recht. A tour of reinforcement learning: The view from continuous control. *Annual Review of Control, Robotics, and Autonomous Systems*, 2:253–279, 2019.

[160] Thomas J Riedl, Todd P Coleman, and Andrew C Singer. Finite block-length achievable rates for queuing timing channels. In *2011 IEEE Information Theory Workshop*, pages 200–204. IEEE, 2011.

[161] Christopher Rose and I Saira Mian. Inscribed matter communication: Part I. *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, 2(2):209–227, 2016.

[162] Ugo Rosolia, Xiaojing Zhang, and Francesco Borrelli. Data-driven predictive control for autonomous systems. *Annual Review of Control, Robotics, and Autonomous Systems*, 1:259–286, 2018.

[163] Matthias Rungger and Majid Zamani. On the invariance feedback entropy of linear perturbed control systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 3998–4003. IEEE, 2017.

[164] Anant Sahai and Sanjoy Mitter. The necessity and sufficiency of anytime capacity for stabilization of a linear system over a noisy communication link. Part I: Scalar systems. *IEEE Transactions on Information Theory*, 52(8):3369–3395, 2006.

[165] Henrik Sandberg, Saurabh Amin, and Karl Henrik Johansson. Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems*, 35(1):20–23, 2015.

[166] Vahideh Sanjaroon, Alireza Farhadi, Abolfazl Seyed Motahari, and Babak H Khalaj. Estimation of nonlinear dynamic systems over communication channels. *IEEE Transactions on Automatic Control*, 63(9):3024–3031, 2018.

[167] Tuhin Sarkar and Alexander Rakhlin. Near optimal finite time identification of arbitrary linear dynamical systems. In *International Conference on Machine Learning (ICML)*, pages 5610–5618, 2019.

[168] Tuhin Sarkar, Alexander Rakhlin, and Munther A Dahleh. Finite-time system identification for partially observed lti systems of unknown order. *arXiv preprint arXiv:1902.01848*, 2019.

[169] Bharadwaj Satchidanandan and Panganamala R Kumar. Dynamic watermarking: Active defense of networked cyber–physical systems. *Proceedings of the IEEE*, 105(2):219–240, 2017.

[170] Bharadwaj Satchidanandan and PR Kumar. Control systems under attack: The securable and unsecurable subspaces of a linear stochastic system. In *Emerging Applications of Control and Systems Theory*, pages 217–228. Springer, 2018.

[171] J Schalkwijk and Thomas Kailath. A coding scheme for additive noise channels with feedback–i: No bandwidth constraint. *IEEE Transactions on Information Theory*, 12(2):172–182, 1966.

[172] Sarah H Sellke, Chih-Chun Wang, Ness Shroff, and Saurabh Bagchi. Capacity bounds on timing channels with bounded service times. In *2007 IEEE International Symposium on Information Theory*, pages 981–985. IEEE, 2007.

[173] Alexandre Seuret, Christophe Prieur, Sophie Tarbouriech, and Luca Zaccarian. Lq-based event-triggered controller co-design for saturated linear systems. *Automatica*, 74:47–54, 2016.

[174] Yoav Sharon and Daniel Liberzon. Input to state stabilizing controller for systems with coarse quantization. *IEEE Transactions on Automatic Control*, 57(4):830–844, 2012.

[175] Ofer Shayevitz and Meir Feder. Optimal feedback communication via posterior matching. *IEEE Transactions on Information Theory*, 57(3):1186–1222, 2011.

[176] Dawei Shi, Ziyang Guo, Karl Henrik Johansson, and Ling Shi. Causality countermeasures for anomaly detection in cyber-physical systems. *IEEE Transactions on Automatic Control*, 63(2):386–401, 2017.

[177] H. Shingin and Y. Ohta. Disturbance rejection with information constraints: Performance limitations of a scalar system for bounded and gaussian disturbances. *Automatica*, 48(6):1111–1116, 2012.

[178] Yasser Shoukry, Michelle Chong, Masashi Wakaiki, Pierluigi Nuzzo, Alberto Sangiovanni-Vincentelli, Sanjit A Seshia, Joao P Hespanha, and Paulo Tabuada. Smt-based observer design for cyber-physical systems under sensor attacks. *ACM Transactions on Cyber-Physical Systems*, 2(1):5, 2018.

[179] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1004–1015. ACM, 2015.

[180] Roland Siegwart, Illah Reza Nourbakhsh, and Davide Scaramuzza. *Introduction to autonomous mobile robots*. MIT press, 2011.

[181] Jill Slay and Michael Miller. Lessons learned from the maroochy water breach. In *International Conference on Critical Infrastructure Protection*, pages 73–82. Springer, 2007.

[182] Roy S Smith. A decoupled feedback structure for covertly appropriating networked control systems. *IFAC Proceedings Volumes*, 44(1):90–95, 2011.

[183] Eduardo D Sontag. Input to state stability: Basic concepts and results. In *Nonlinear and optimal control theory*, pages 163–220. Springer, 2008.

[184] Ravi Teja Sukhavasi and Babak Hassibi. Linear time-invariant anytime codes for control over noisy channels. *IEEE Transactions on Automatic Control*, 61(12):3826–3841, 2016.

[185] Rajesh Sundaresan and Sergio Verdú. Robust decoding for timing channels. *IEEE Transactions on information Theory*, 46(2):405–419, 2000.

[186] Paulo Tabuada. Event-triggered real-time scheduling of stabilizing control tasks. *IEEE Transactions on Automatic Control*, 52(9):1680–1685, 2007.

[187] P. Tallapragada and J. Cortés. Event-triggered stabilization of linear systems under bounded bit rates. *IEEE Transactions on Automatic Control*, 61(6):1575–1589, 2016.

[188] Pavankumar Tallapragada and Nikhil Chopra. On event triggered tracking for nonlinear systems. *IEEE Transactions on Automatic Control*, 58(9):2343–2348, 2013.

[189] Pavankumar Tallapragada, Massimo Franceschetti, and Jorge Cortés. Event-triggered second-moment stabilization of linear systems under packet drops. *IEEE Transactions on Automatic Control*, 63(8):2374–2388, 2018.

[190] Sekhar Tatikonda and Sanjoy Mitter. Control over noisy channels. *IEEE transactions on Automatic Control*, 49(7):1196–1201, 2004.

[191] Sekhar Tatikonda and Sanjoy Mitter. Control under communication constraints. *IEEE Transactions on Automatic Control*, 49(7):1056–1068, 2004.

[192] Sekhar Tatikonda, Anant Sahai, and Sanjoy Mitter. Stochastic linear control over a communication channel. *IEEE transactions on Automatic Control*, 49(9):1549–1561, 2004.

[193] Mehrnaz Tavan, Roy D Yates, and Waheed U Bajwa. Bits through bufferless queues. In *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 755–762. IEEE, 2013.

[194] André Teixeira, Iman Shames, Henrik Sandberg, and Karl Henrik Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, 2015.

[195] Nan Tian, Matthew Matl, Jeffrey Mahler, Yu Xiang Zhou, Samantha Staszak, Christopher Correa, Steven Zheng, Qiang Li, Robert Zhang, and Ken Goldberg. A cloud robot system using the dexterity network and berkeley robotics and automation as a service (brass). In *2017 IEEE International Conference on Robotics and Automation (ICRA)*, pages 1615–1622. IEEE, 2017.

[196] Sebastian Trimpe and Raffaello D'Andrea. Event-based state estimation with variance-based triggering. *IEEE Transactions on Automatic Control*, 59(12):3266–3281, 2014.

[197] Stephen Tu and Benjamin Recht. Least-squares temporal difference learning for the linear quadratic regulator. In *International Conference on Machine Learning (ICML)*, pages 5005–5014, 2018.

[198] Rohit Tunga, Carlos Murguia, and Justin Ruths. Tuning windowed chi-squared detectors for sensor attacks. In *2018 Annual American Control Conference (ACC)*, pages 1752–1757. IEEE, 2018.

[199] David I Urbina, Jairo A Giraldo, Alvaro A Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1092–1105. ACM, 2016.

[200] Amir Valibeygi, Raymond A de Callafon, Mark Stanovich, Michael Sloderbeck Karl Schoder, James Langston Isaac Leonard, Sourindu Chatterjee, and Rick Meeker. Microgrid control using remote controller hardware-in-the-loop over the internet. In *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5. IEEE, 2018.

[201] Aaron B Wagner and Venkat Anantharam. Zero-rate reliability of the exponential-server timing channel. *IEEE Transactions on Information Theory*, 51(2):447–465, 2005.

[202] Abraham Wald, Jacob Wolfowitz, et al. Optimum character of the sequential probability ratio test. *The Annals of Mathematical Statistics*, 19(3):326–339, 1948.

[203] Wei Wang, Romain Postoyan, Dragan Nesic, and WPMH Heemels. Periodic event-triggered control for nonlinear networked control systems. *IEEE Transactions on Automatic Control*, 2019.

[204] Xiaofeng Wang and Michael D Lemmon. Event-triggering in distributed networked control systems. *IEEE Transactions on Automatic Control*, 56(3):586–601, 2011.

[205] Sean Weerakkody and Bruno Sinopoli. Detecting integrity attacks on control systems using a moving target approach. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 5820–5826. IEEE, 2015.

[206] Wing Shing Wong and Roger W Brockett. Systems with finite communication bandwidth constraints. II. stabilization with limited information feedback. *IEEE Transactions on Automatic Control*, 44(5):1049–1053, 1999.

[207] Mengran Xue, Sandip Roy, Yan Wan, and Sajal K Das. Security and vulnerability of cyber-physical. *Handbook on securing cyber-physical critical infrastructure*, page 5, 2012.

[208] Guosong Yang and Daniel Liberzon. Finite data-rate stabilization of a switched linear system with unknown disturbance. *IFAC-PapersOnLine*, 49(18):1085–1090, 2016.

[209] Guosong Yang and Daniel Liberzon. Feedback stabilization of switched linear systems with unknown disturbances under data-rate constraints. *IEEE Transactions on Automatic Control*, 63(7):2107–2122, 2017.

[210] Hikmet Yildiz, Yu Su, Anatoly Khina, and Babak Hassibi. Event-triggered stochastic control via constrained quantization. In *2019 Data Compression Conference (DCC)*, pages 612–612. IEEE, 2019.

[211] Jaehyun Yoo and Karl H Johansson. Event-triggered model predictive control with a statistical learning. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.

[212] Serdar Yüksel and Tamer Başar. *Stochastic Networked Control Systems: Stabilization and Optimization under Information Constraints*. Springer Science & Business Media, 2013.

[213] George Zames. Adaptive control: Towards a complexity-based general theory. *Automatica*, 34(10):1161–1167, 1998.

[214] Fuzhen Zhang. *Matrix theory: basic results and techniques*. Springer Science & Business Media, 2011.

[215] Minghui Zhu and Sonia Martínez. On distributed constrained formation control in operator–vehicle adversarial networks. *Automatica*, 49(12):3571–3582, 2013.

[216] Minghui Zhu and Sonia Martínez. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control*, 59(3):804–808, 2014.