Safe and Secure Networked Control Systems Under Denial-of-Service Attacks

Saurabh Amin[1], Alvaro A. Cárdenas[2], and S. Shankar Sastry[2]

[1] Systems engineering, University of California, at Berkeley - Berkeley, CA, USA
{amins}@berkeley.edu
[2] EECS Department, University of California, at Berkeley - Berkeley, CA, USA
{cardenas,sastry}@eecs.berkeley.edu

Abstract. We consider the problem of security constrained optimal control for discrete-time, linear dynamical systems in which control and measurement packets are transmitted over a communication network. The packets may be jammed or compromised by a malicious adversary. For a class of denial-of-service (DoS) attack models, the goal is to find an (optimal) causal feedback controller that minimizes a given objective function subject to safety and power constraints. We present a semi-definite programming based solution for solving this problem. Our analysis also presents insights on the effect of attack models on solution of the optimal control problem.

1 Introduction

Attacks to computer networks have become prevalent over the last decade. While most control networks have been safe in the past, they are currently more vulnerable to malicious attacks [7, 18]. The consequences of a successful attack on control networks can be more damaging than attacks on other networks because control systems are at the core of many critical infrastructures. Therefore, analyzing the security of control systems is a growing concern [4, 7, 12, 13, 15, 18].

In the control and verification community there is a significant body of work on networked control [16], stochastic system verification [6, 1], robust control [2, 11, 3, 10], and fault-tolerant control [21]. We argue that several major security concerns for control systems are not addressed by the current literature. For example, fault analysis of control systems usually assumes independent modes of failure, while during an attack, the modes of failure will be highly correlated. On the other hand, most networked control work assumes that the failure modes follow a given class of probability distributions; however, a real attacker has no incentives to follow this assumed distribution, and may attack in a non-deterministic manner. Finally, the work in stochastic system verification has addressed safety and reachability problems for fairly general systems; however, the potential applicability of these results for securing control systems has not been studied.

In this article, we formulate and analyze the problem of secure control for discrete-time linear dynamical systems. Our work is based on two ideas: (1)

the introduction of safety-constraints as one of the top security requirements of a control system, and (2) the introduction of new adversary models—we generalize traditional uncertainty classes for control systems to incorporate more realistic attacks. The goal in our model is to minimize a performance function such that a safety specification is satisfied with high probability and power limitations are obeyed in expectation when the sensor and control packets can be dropped by a random or a resource-constrained attacker. Our analysis uses tools from optimal control theory such as dynamic and convex programming.

1.1 Attacks on control systems

Malicious cyber attacks to control systems can be classified as either *deception* attacks or *denial-of-service* DoS attacks.

In the context of control systems, integrity refers to the trustworthiness of sensor and control data packets. A lack of integrity results in deception: when a component receives false data and believes it to be true. In Figure 1, A1 and A3 represent deception attacks, where the adversary sends false information $\tilde{y} \neq y$ or $\tilde{u} \neq u$ from (one or more) sensors or controllers. The false information can include: an incorrect measurement, the incorrect time stamp, or the incorrect sender identity. The adversary can launch these attacks by compromising some sensors (A1) or controllers (A3).

On the other hand, availability of a control system refers to the ability of all components of being accessible. Lack of availability results in a DoS of sensor and control data. A2 and A4 represent *DoS attacks* in Figure 1, where the adversary prevents two entities from communicating. To launch a DoS the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood with network traffic some devices, etc.

Lastly, A5 represents a direct attack against the actuators or the plant. Solutions to these attacks, fall in the realm of detecting such attacks and improving the physical security of the system.

As shown by the analysis of a database that tracked cyber-incidents affecting industrial control systems from 1982 to 2003 [4], DoS is the most likely threat to control systems; therefore in this article we focus on DoS attacks, leaving deception attacks for future work.

2 Problem Setting

2.1 System Model

We consider a linear time invariant stochastic system over a time horizon $k = 0, \ldots, N-1$ with measurement and control packets subject to DoS attacks (γ_k, ν_k):

$$x_{k+1} = Ax_k + Bu_k^a + w_k \qquad k = 0, \ldots, N-1, \qquad (1)$$

$$u_k^a = \nu_k u_k \qquad \nu_k \in \{0, 1\}, \qquad (2)$$

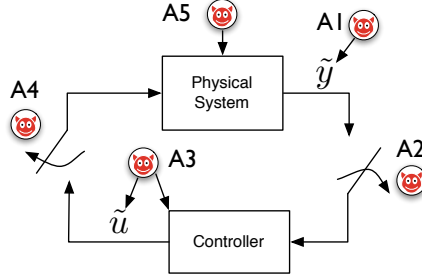$$x_k^a = \gamma_k x_k \qquad \gamma_k \in \{0, 1\}, \qquad (3)$$

Fig. 1. Attacks on a control system: $A1$ and $A3$ indicate integrity attacks, $A2$ and $A4$ indicate DoS attacks, and $A5$ indicate direct physical attacks to the process.

where $x_k \in \mathbb{R}^n$ and $u_k \in \mathbb{R}^m$ denote the state and the control input respectively, $w_k \in \mathbb{R}^n$ is independent, Gaussian distributed noise with mean 0 and covariance W (denoted as $w_k \sim \mathcal{N}(0, W)$), $x_0 \sim \mathcal{N}(\bar{x}, P_0)$ is the initial state, and $\{\gamma_k\}$ (resp. $\{\nu_k\}$) is the sensor (resp. actuator) attack sequence. Also, x_0 and w_k are uncorrelated. The available state (resp. available control input) is denoted by x_k^a (resp. u_k^a) after a DoS attack on the measurement (resp. control) packet. Following [16], for an acknowledgment based communication protocol such as TCP, the information set available at time k is $\mathcal{I}_k = \{x_0^a, \ldots, x_k^a, \gamma_0^k, \nu_0^{k-1}\}$ where $\gamma_i^j = (\gamma_i, \ldots, \gamma_j)$ and $\nu_i^j = (\nu_i, \ldots, \nu_j)$. Define $u_0^{N-1} = (u_0, \ldots, u_{N-1})$.

We note that due to (3), the controller receives perfect state information x_k when $\gamma_k = 1$ and 0 when $\gamma_k = 0$. However, our analysis presented can also be extended for the case of measurement equation $y_k^a = \gamma_k C_s x_k + v_k$.

2.2 Goals and Requirements

At this stage, we have not specified any restrictions on the DoS attack actions except that $(\gamma_k, \nu_k) \in \{0, 1\}^2$ for $k = 0, \ldots, N-1$. We will impose constraints on the attacker actions in Section 3.1. Given such constraints, our goal is to synthesize a causal feedback control law $u_k = \mu_k(\mathcal{I}_k)$ such that for the system (1), (2), and (3), the following finite-horizon objective function is minimized

$$J_N(\bar{x}, P_0, u_0^{N-1}) = \mathbf{E}\left[x_N^\top Q^{xx} x_N + \sum_{k=0}^{N-1} \begin{pmatrix} x_k \\ u_k \end{pmatrix}^\top \begin{pmatrix} I_n & 0 \\ 0 & \nu_k I_m \end{pmatrix} Q \begin{pmatrix} x_k \\ u_k \end{pmatrix} \bigg| u_0^{N-1}, \bar{x}, P_0\right] \tag{4}$$

where $Q^{xx} \succ 0$, and $Q \succeq 0$ is partitioned as

$$Q = \begin{pmatrix} Q^{xx} & 0 \\ 0 & Q^{uu} \end{pmatrix} \in \mathbb{R}^{(n+m)\times(n+m)},$$

and constraints on *both* the state and the input in an expected sense

$$\mathbf{E}\left[\begin{pmatrix} x_k \\ u_k \end{pmatrix}^{\top} \begin{pmatrix} I_n & 0 \\ 0 & \nu_k I_m \end{pmatrix} H_i \begin{pmatrix} x_k \\ u_k \end{pmatrix}\right] \leq \beta_i \quad \text{for } i = 1, \ldots, L, \text{ and } k = 0, \ldots, N-1 \quad (5)$$

with $H_i \succeq 0$ and scalar constraints on the state and the input in a probabilistic sense

$$\mathbf{P}\left[t_i^{\top} \begin{pmatrix} I_n & 0 \\ 0 & \nu_k I_m \end{pmatrix} \begin{pmatrix} x_k \\ u_k \end{pmatrix} \leq \alpha_i\right] \geq (1 - \varepsilon) \quad \text{for } i = 1, \ldots, T, \text{ and } k = 0, \ldots, N-1 \quad (6)$$

with $t_i \in \mathbb{R}^{n+m}$ are satisfied. The constraints (5) can be viewed as *power constraints* that limit the energy of state and control inputs at each time step. The constraint (6) can be interpreted as a *safety specification* stipulating that the state and the input remain within the hyperplanes specified by t_i and α_i with a sufficiently high probability, $(1 - \varepsilon)$, for $k = 0, \ldots, N-1$. Equations (5) and (6) are to be interpreted as conditioned on the initial state, i.e., $\mathbf{E}[\cdot] := \mathbf{E}[\cdot|x_0]$ and $\mathbf{P}[\cdot] := \mathbf{P}[\cdot|x_0]$.

3 Optimal control with constraints and random attacks

3.1 A random DoS attack model

Networked control formulations have previously considered the loss of sensor or control packets and their impact on the system. While previous results model packet drops caused by random events (and not by an attacker) we believe these packet drop models can be used as a first-step towards understanding the impact of DoS attacks to our objective and constraints.

One of these models is the Bernoulli packet drop model, in which at each time, the attacker randomly jams a measurement (resp. control) packet according to independent Bernoulli trials with success probability $\bar{\gamma}$ (resp. $\bar{\nu}$). This attack model, referred as the $\text{Ber}(\bar{\gamma}, \bar{\nu})$ adversary, has the following admissible attack actions

$$\mathcal{A}_{\text{Ber}(\bar{\gamma}, \bar{\nu})} = \{(\gamma_0^{N-1}, \nu_0^{N-1}) | \mathbf{P}(\gamma_k = 1) = \bar{\gamma}, \mathbf{P}(\nu_k = 1) = \bar{\nu}, \ k = 0, \ldots, N-1\}. \quad (7)$$

For the $\mathcal{A}_{\text{Ber}(\bar{\gamma}, \bar{\nu})}$ model, we can write the Kalman filter equations for the state estimate $\hat{x}_{k|k} := \mathbf{E}[x_k|\mathcal{I}_k]$ and the state estimation error $e_{k|k} := (x_k - \hat{x}_{k|k})$. For the update step we have

$$\hat{x}_{k+1|k} = A\hat{x}_{k|k} + \nu_k B u_k \text{ and, } e_{k+1|k} = Ae_{k|k} + w_k$$

and for the correction step

$$\hat{x}_{k+1|k+1} = \gamma_{k+1} x_{k+1} + (1 - \gamma_{k+1})\hat{x}_{k+1|k} \text{ and, } e_{k+1|k+1} = (1 - \gamma_{k+1})e_{k+1|k},$$

starting with $\hat{x}_{0|-1} = \bar{x}$ and $e_{0|-1} \sim \mathcal{N}(0, P_0)$. It follows that the error covariance matrices $\Sigma_{k+1|k} := \mathbf{E}[e_{k+1|k}e_{k+1|k}^{\top}|\mathcal{I}_k]$ and $\Sigma_{k|k} := \mathbf{E}[e_{k|k}e_{k|k}^{\top}|\mathcal{I}_k]$ do not

depend on the control input u_k. Thus, the separation principle holds for TCP-like communication [16]. Furthermore, it is easy to see that

$$\mathbf{E}[e_{k|k}x_{k|k}^\top] = 0. \tag{8}$$

Taking expectations w.r.t. $\{\gamma_k\}$, the expected error covariances follow

$$\mathbf{E}_\gamma[\Sigma_{k+1|k}] = A\mathbf{E}_\gamma[\Sigma_{k|k}]A^\top + W \text{ and, } \mathbf{E}_\gamma[\Sigma_{k+1|k+1}] = (1-\bar{\gamma})\mathbf{E}_\gamma[\Sigma_{k+1|k}],$$

for $k = 0, \ldots, N-1$ starting with the initial condition $\Sigma_{0|-1} = P_0$. For the ease of notation, we denote $\hat{x}_{k+1} := \hat{x}_{k+1|k}$, $e_{k+1} := e_{k+1|k}$, and $\Sigma_{k+1} := \Sigma_{k+1|k}$. Using the Kalman filter equations we obtain for $k = 0, \ldots, N-1$

$$\hat{x}_{k+1} = A\hat{x}_k + \nu_k B u_k + \gamma_k A e_k \tag{9}$$

$$e_{k+1} = (1 - \gamma_k)A e_k + w_k \tag{10}$$

$$\mathbf{E}_\gamma[\Sigma_{k+1}] = (1 - \bar{\gamma})A\mathbf{E}_\gamma[\Sigma_k]A^\top + W. \tag{11}$$

Definition 1. *For Bernoulli attacks, $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \mathcal{A}_{Ber(\bar{\gamma},\bar{\nu})}$ over systems controlled over TCP-like communication protocols, the safety-constrained robust optimal control problem is equivalent to minimizing* (4) *subject to* (9), (11), (5) *and* (6).

3.2 Controller parameterization

In this section, we deal with the safety-constrained optimal control problem as defined in Definition 1. Naive implementation of the control law $u_k^* = -L_k\hat{x}_{k|k}$ may not guarantee constraint satisfaction for any initial state. Recent research has shown that for the optimal control problems involving state and input constraints, more general causal feedback controllers can guarantee a larger set of initial states for which the constrained optimal control problem admits a feasible solution [3, 10, 17, 14, 19]. Specifically, these approaches consider the problem of designing causal controllers that are affine in all previous measurements such that a convex objective function is minimized subject to constraints imposed by the system dynamics, and the state and inputs constraints are satisfied.

When considering a system under DoS attacks, (1), (2), and (3), the class of causal feedback controllers can be defined as an affine function of the available measurements, i.e.,

$$u_k = \bar{u}_k + \sum_{j=0}^{k} \gamma_j M_{k,j} x_j, \qquad k = 0, \ldots, N-1 \tag{12}$$

where $\bar{u}_k \in \mathbb{R}^m$ is the open-loop part of the control, and $M_{k,j} \in \mathbb{R}^{m \times n}$ is the feedback gain or the recourse at time k from sensor measurement x_j. For a lost measurement packet, say $x_{j'}$ for $\gamma_{j'} = 0$, the corresponding feedback gain $M_{k,j'}$ has no contribution toward the control policy. We note that the

above parameterization can be re-expressed as an affine function of innovations $v_{k|k-1} := \gamma_k(x_k - \hat{x}_{k|k-1}) = \gamma_k e_k$ as

$$u_k = u_k^\circ + \sum_{j=0}^{k} \gamma_j M_{k,j} e_j, \qquad k = 0, \ldots, N-1 \qquad (13)$$

where $u_k^\circ := \bar{u}_k + \sum_{j=0}^{k} \gamma_j M_{i,j} \hat{x}_{j|j-1}$.

Remark 1. When only the current available measurement is used for computing the feedback policy, the mapping μ_k can be expressed as

$$u_k = \bar{u}_k + \gamma_k M_{k,k} x_k = u_k^\circ + \gamma_k M_k e_k, \qquad k = 0, \ldots, N-1, \qquad (14)$$

where $M_k := M_{k,k}$ for ease of notation and $u_k^\circ := \bar{u}_k + \gamma_k M_k \hat{x}_{k|k-1}$. □

3.3 Convex characterization

In this section, we will show that unlike (12), the use of control parameterization (13) yields an affine representation of state and control trajectories in terms of the control parameters $\bar{u}_k$ (or u_k°) and $M_{k,j}$. We use $\mathbf{x}$, $\hat{\mathbf{x}}$, $\mathbf{u}$, $\mathbf{e}$ and $\mathbf{w}$ to denote the respective trajectories over the time horizon $0, \ldots, N$. That is, $\mathbf{x} = (x_0^\top, \ldots, x_N^\top)^\top \in \mathbb{R}^{n(N+1)}$ and similarly for $\hat{\mathbf{x}} \in \mathbb{R}^{n(N+1)}$ and $\mathbf{e} \in \mathbb{R}^{n(N+1)}$; $\mathbf{u} = (u_0^\top, \ldots, u_{N-1}^\top)^\top \in \mathbb{R}^{mN}$ and similarly for $\mathbf{w} \in \mathbb{R}^{nN}$. Using this representation, the system (1) and the control parameterization (12) can be written as

$$\mathbf{x} = \mathbf{A}\mathbf{w} + \mathbf{B}\mathbf{N}\mathbf{u} + \mathbf{x_0}, \qquad (15)$$

$$\mathbf{u} = \bar{\mathbf{u}} + \mathbf{M}\boldsymbol{\Gamma}\mathbf{x}, \qquad (16)$$

where $\mathbf{x_0}$, $\mathbf{A}$, $\mathbf{B}$, $\boldsymbol{\Gamma}$, $\mathbf{N}$ are given in the Appendix and

$$\mathbf{M} = \begin{pmatrix} M_{0,0} & 0 & \ldots & 0 \\ M_{1,0} & M_{1,1} & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ M_{N-1,0} & \ldots & M_{N-1,N-1} & 0 \end{pmatrix} \in \mathbb{R}^{mN \times n(N+1)}, \quad \bar{\mathbf{u}} = \begin{pmatrix} \bar{u}_0 \\ \vdots \\ \bar{u}_{N-1} \end{pmatrix} \in \mathbb{R}^{mN} \qquad (17)$$

Using (15) and (16), we can show that the closed-loop system response can be written as

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{u} \end{pmatrix} = \begin{pmatrix} \tilde{\mathbf{G}}_{\mathbf{xw}} \\ \tilde{\mathbf{G}}_{\mathbf{uw}} \end{pmatrix} \mathbf{w} + \begin{pmatrix} \tilde{\mathbf{x}} \\ \tilde{\mathbf{u}} \end{pmatrix} \qquad (18)$$

where

$$\tilde{\mathbf{G}}_{\mathbf{xw}} = \left(\mathbf{A} + \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma}(I - \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma})^{-1}\mathbf{A} \right)$$

$$\tilde{\mathbf{G}}_{\mathbf{uw}} = \left(\mathbf{M}\boldsymbol{\Gamma}(I - \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma})^{-1}\mathbf{A} \right)$$

$$\tilde{\mathbf{x}} = \mathbf{x_0} + \mathbf{B}\mathbf{N}\bar{\mathbf{u}} + \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma}(I - \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma})^{-1}(\mathbf{x_0} + \mathbf{B}\mathbf{N}\bar{\mathbf{u}})$$

$$\tilde{\mathbf{u}} = \mathbf{M}\boldsymbol{\Gamma}(I - \mathbf{B}\mathbf{N}\mathbf{M}\boldsymbol{\Gamma})^{-1}(\mathbf{x_0} + \mathbf{B}\mathbf{N}\bar{\mathbf{u}}) + \bar{\mathbf{u}}$$

Equation (18) is nonlinear in the control parameters $(\bar{\mathbf{u}}, \mathbf{M})$ and hence, parameterization (12) cannot be directly used for solving constrained stochastic optimal control problems. On the other hand, using (10), the error trajectory can be written as

$$\mathbf{e} = \mathbf{e}_0 + \mathbf{H}\mathbf{w} \tag{19}$$

where $\mathbf{e_0}$ and $\mathbf{H}$ are also given in the Appendix. Using (19), (15) and the control parameterization (13) we can re-express the closed-loop system response as

$$\begin{pmatrix} \mathbf{x} \\ \mathbf{u} \end{pmatrix} = \begin{pmatrix} \hat{\mathbf{G}}_{\mathbf{xw}} \\ \hat{\mathbf{G}}_{\mathbf{uw}} \end{pmatrix} \mathbf{w} + \begin{pmatrix} \hat{\mathbf{x}} \\ \hat{\mathbf{u}} \end{pmatrix} \tag{20}$$

where

$$\hat{\mathbf{G}}_{\mathbf{xw}} = (\mathbf{A} + \mathbf{BNM\Gamma H}), \qquad\qquad \hat{\mathbf{G}}_{\mathbf{uw}} = \mathbf{M\Gamma H}$$
$$\hat{\mathbf{x}} = \mathbf{BNM\Gamma e_0} + \mathbf{x_0} + \mathbf{BNu}^\circ, \qquad\qquad \hat{\mathbf{u}} = \mathbf{M\Gamma e_0} + \mathbf{u}^\circ$$

Thus, we arrive at the following result

Theorem 1. *Under the error feedback parameterization* (13), *the closed loop system response* (20) *is affine in the control parameters* $(\mathbf{u}^\circ, \mathbf{M})$. $\qquad\square$

We will now use the error feedback parameterization (13) for our analysis. Alternatively, we also note the following result:

Remark 2. Using the transformation

$$\mathbf{Q} := \mathbf{M\Gamma}(I - \mathbf{BNM\Gamma})^{-1}, \qquad\qquad \mathbf{r} := (I + \mathbf{QBN})\bar{\mathbf{u}} \tag{21}$$

where $\mathbf{Q} \in \mathbb{R}^{mN \times n(N+1)}$ and $\mathbf{r} \in \mathbb{R}^{mn}$, the terms in equation (18) can be written as: $\mathbf{G}_{\mathbf{xw}} = (I + \mathbf{BNQ})\,\mathbf{A}$, $\mathbf{G}_{\mathbf{uw}} = \mathbf{QA}$, $\tilde{\mathbf{x}} = (I + \mathbf{BNQ})\,\bar{\mathbf{x}} + \mathbf{BNr}$, and $\tilde{\mathbf{u}} = \mathbf{Q}\bar{\mathbf{x}} + \mathbf{r}$. Using simple matrix operations, the relations in (21) can be inverted as $\mathbf{M\Gamma} = (I + \mathbf{QBN})^{-1}\mathbf{Q}$ and $\bar{\mathbf{u}} = (I - \mathbf{M\Gamma HN})\mathbf{r}$. Thus, under parameterization (21), the closed-loop system response also becomes affine in the control parameters $(\mathbf{r}, \mathbf{Q})$.
$$\square$$

3.4   Safety-constrained optimal control for Bernoulli attacks

For the control parameterization (12), and for the Bernoulli attack model, $\mathcal{A}_{\mathrm{Ber}(\bar{\gamma}, \bar{\nu})}$ we will now solve the safety-constrained optimal control problem as stated in Lemma 1, i.e., minimize (4) subject to (9), (11), (5), and (6). We state the following useful lemma

Lemma 1 (Schur Complements). *For all* $X \in \mathbb{S}^n$, $Y \in \mathbb{R}^{m \times n}$, $Z \in \mathbb{S}^m$, *the following statements are equivalent:*

$$\text{a)}\, Z \succ 0, X - Y^\top Z^{-1} Y \succeq 0,$$
$$\text{b)}\, Z \succ 0, \begin{pmatrix} X & Y^\top \\ Y & Z \end{pmatrix} \succeq 0$$

For the sake of simplicity we will consider the parameterization (14). However, our results can be re-derived for the parameterization (12). First, we will derive the expression for

$$V_k = \mathbf{E}\left[\begin{pmatrix} \hat{x}_k \\ u_k^\circ \end{pmatrix} \begin{pmatrix} \hat{x}_k \\ u_k^\circ \end{pmatrix}^\top \right]$$

Using (14), the update equation for the state estimate (9) becomes

$$\hat{x}_{k+1} = A\hat{x}_k + \nu_k Bu_k^\circ + \gamma_k(A + \nu_k BM_k)e_k, \tag{22}$$

and further defining $F = [I_n, 0] \in \mathbb{R}^{n \times (n+m)}$ we have,

$$FV_{k+1}F^\top = V_{k+1}^{\hat{x}\hat{x}} = \mathbf{E}\left[\hat{x}_{k+1}\hat{x}_{k+1}^\top \right]$$

$$= \mathbf{E}\left[(A\hat{x}_k + \nu_k Bu_k^\circ + \gamma_k(A + \nu_k BM_k)e_k)(A\hat{x}_k + \nu_k Bu_k^\circ + \gamma_k(A + \nu_k BM_k)e_k)^\top \right]$$

$$= [A \mid \sqrt{\bar{\nu}}B] \mathbf{E}\left[\begin{pmatrix} \hat{x}_k \\ u_k^\circ \end{pmatrix} \begin{pmatrix} \hat{x}_k \\ u_k^\circ \end{pmatrix}^\top \right] [A \mid \sqrt{\bar{\nu}}B]^\top$$

$$+ \sqrt{\bar{\gamma}}(A + \sqrt{\bar{\nu}}BM_k)\mathbf{E}_\gamma[\Sigma_k](A + \sqrt{\bar{\nu}}BM_k)^\top \sqrt{\bar{\gamma}}$$

$$= [AV_k \mid \sqrt{\bar{\nu}}BV_k] (V_k)^{-1} [AV_k \mid \sqrt{\bar{\nu}}BV_k]^\top$$

$$+ \sqrt{\bar{\gamma}}(A\mathbf{E}_\gamma[\Sigma_k] + \sqrt{\bar{\nu}}BU_k)(\mathbf{E}_\gamma[\Sigma_k])^{-1}(A\mathbf{E}_\gamma[\Sigma_k] + \sqrt{\bar{\nu}}BU_k)^\top \sqrt{\bar{\gamma}}$$

where we have used $U_k = M_k\mathbf{E}_\gamma[\Sigma_k]$. An upper bound on V can be obtained in the form of the following LMI by replacing the equality by $\succeq$ and using Schur complements for $k = 0, \ldots, N-1$:

$$\begin{bmatrix} (FV_{k+1}F^\top) & * & * & * \\ [AV_k \ \sqrt{\bar{\nu}}BV_k]^\top & 0 \ V_k & * \\ \sqrt{\bar{\gamma}}(A\mathbf{E}_\gamma[\Sigma_k] + \sqrt{\bar{\nu}}BU_k)^\top & 0 \ 0 \ \mathbf{E}_\gamma[\Sigma_k] \end{bmatrix} \succeq 0 \tag{23}$$

The objective function (4) can be expressed as

$$\mathbf{E}\left[\mathbf{Tr}\left\{ Q^{xx}x_N x_N^\top \right\} \right] + \sum_{k=0}^{N-1} \mathbf{E}\left[\mathbf{Tr}\left\{ \begin{pmatrix} Q^{xx} & 0 \\ 0 & \nu_k Q^{uu} \end{pmatrix} \begin{pmatrix} x_k \\ u_k \end{pmatrix} \begin{pmatrix} x_k \\ u_k \end{pmatrix}^\top \right\} \right]$$

$$= \mathbf{Tr}\left\{ Q^{xx}\mathbf{E}\left[x_N x_N^\top \right] \right\} + \sum_{k=0}^{N-1} \mathbf{Tr}\left\{ \begin{pmatrix} Q^{xx} & 0 \\ 0 & \mathbf{E}[\nu_k]Q^{uu} \end{pmatrix} \mathbf{E}\left[\begin{pmatrix} x_k \\ u_k \end{pmatrix} \begin{pmatrix} x_k \\ u_k \end{pmatrix}^\top \right] \right\}$$

$$= \mathbf{Tr}\left\{ Q^{xx}\mathbf{E}\left[\hat{x}_N \hat{x}_N^\top \right] \right\} + \sum_{k=0}^{N-1} \mathbf{Tr}\left\{ \begin{pmatrix} Q^{xx} & 0 \\ 0 & \bar{\nu}Q^{uu} \end{pmatrix} \mathbf{E}\left[\begin{pmatrix} \hat{x}_k \\ u_k \end{pmatrix} \begin{pmatrix} \hat{x}_k \\ u_k \end{pmatrix}^\top \right] \right\}$$

$$+ \sum_{k=0}^{N} \mathbf{Tr}\left\{ Q^{xx}\mathbf{E}_\gamma[\Sigma_k] \right\}$$

Since Σ_k does not depend on the control input (refer to eq. (11)), $\sum_{k=0}^{N} \mathbf{Tr}\left\{ Q^{xx}\mathbf{E}_\gamma[\Sigma_k] \right\}$ is a constant and minimizing $J_N(\bar{x}, P_0, u_0^{N-1})$ is the same as minimizing

$$\mathbf{Tr}\left\{ Q^{xx}V_N^{\hat{x}\hat{x}} \right\} + \sum_{k=0}^{N-1} \mathbf{Tr}\left\{ \begin{pmatrix} Q^{xx} & 0 \\ 0 & \bar{\nu}Q^{uu} \end{pmatrix} P_k \right\} \tag{24}$$

where $V_N^{\hat{x}\hat{x}}$ is equal to $\mathbf{E}\left[\hat{x}_N \hat{x}_N^\top\right]$ and the upper bound P_k is defined as

$$
P_k \succeq \mathbf{E}\left[\begin{pmatrix}\hat{x}_k \\ u_k\end{pmatrix}\begin{pmatrix}\hat{x}_k \\ u_k\end{pmatrix}^\top\right] = \mathbf{E}\left[\begin{pmatrix}\hat{x}_k \\ u_k^\circ + \gamma_k M_k e_k\end{pmatrix}\begin{pmatrix}\hat{x}_k \\ u_k^\circ + \gamma_k M_k e_k\end{pmatrix}^\top\right]
$$

$$
= \mathbf{E}\left[\begin{pmatrix}\hat{x}_k \\ u_k^\circ\end{pmatrix}\begin{pmatrix}\hat{x}_k \\ u_k^\circ\end{pmatrix}^\top\right] + \begin{bmatrix}0 & 0 \\ 0 & \bar{\gamma} U_k (\mathbf{E}_\gamma[\Sigma_k])^{-1} U_k^\top\end{bmatrix}
$$

Again using Schur complement, we obtain for $k = 0, \ldots, N-1$

$$
\begin{bmatrix} P_k & * & * \\ V_k & V_k & * \\ \begin{bmatrix}0 \\ \sqrt{\bar{\gamma}}U_k\end{bmatrix}^\top & 0 & \mathbf{E}_\gamma[\Sigma_k]\end{bmatrix} \succeq 0 \tag{25}
$$

The power constraints (5) can be written as

$$
\mathbf{Tr}\left\{H_i\begin{bmatrix}I_n & 0 \\ 0 & \mathbf{E}[\nu_k]I_m\end{bmatrix}\mathbf{E}\left[\begin{pmatrix}x_k \\ u_k\end{pmatrix}\begin{pmatrix}x_k \\ u_k\end{pmatrix}^\top\right]\right\}
$$

$$
= \mathbf{Tr}\left\{H_i\begin{bmatrix}I_n & 0 \\ 0 & \bar{\nu}I_m\end{bmatrix}\mathbf{E}\left[\begin{pmatrix}\hat{x}_k \\ u_k\end{pmatrix}\begin{pmatrix}\hat{x}_k \\ u_k\end{pmatrix}^\top\right]\right\} + \mathbf{Tr}\left\{H_i^{xx}\mathbf{E}_\gamma[\Sigma_k]\right\}
$$

Therefore the power constraints (5) become for $i = 1, \ldots, L, k = 0, \ldots, N-1$

$$
\mathbf{Tr}\left\{H_i\begin{bmatrix}I_n & 0 \\ 0 & \bar{\nu}I_m\end{bmatrix}P_k\right\} \leq \beta_i - \mathbf{Tr}\left\{H_i^{xx}\mathbf{E}_\gamma[\Sigma_k]\right\}. \tag{26}
$$

Thus, we can now state the following theorem

Theorem 2. *For the* $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \mathcal{A}_{Ber(\bar{\gamma}, \bar{\nu})}$ *attack model the optimal causal controller of the form* (14) *for the system* (1), (2), (3) *that minimizes the objective function* (4) *subject to power constraints* (5) *is equivalent to solving the following semidefinite program (SDP):*

$$
\mathcal{P}(\bar{x}, P_0, N) : \begin{cases}\min_{V_i, P_i, U_i}(24) \\ subject~to~(23), (25), (26).\end{cases} \tag{27}
$$

$\square$

In order to handle the safety specification (6), we refer to Theorem 3.1 in [5] which says that for any $\epsilon \in (0, 1)$, the chance constraint of the form

$$
\inf_{d \sim \mathcal{D}} \mathbf{P}\left[d^\top \tilde{x} \leq 0\right] \geq 1 - \epsilon
$$

is equivalent to the second order cone constraint (SOCP)

$$
\sqrt{\frac{1-\epsilon}{\epsilon}}\tilde{x}^\top \Gamma \tilde{x} + \hat{d}^\top \tilde{x} \leq 0
$$

where $\mathcal{D}$ is the set of all probability distributions with mean $\hat{d}$ and covariance Γ, d is the uncertain data with distributions in the set of distributions $\mathcal{D}$, and $\tilde{x}$ is the decision variable. We claim without proof that safety specifications of type (6) can be converted to SOCP constraints following [5],[19].

4 Modeling general DoS attacks

From the security viewpoint, it might be difficult to justify the incentive for the attacker to follow a $\mathcal{A}_{\mathrm{Ber}(\bar{\gamma}, \bar{\nu})}$ model. Therefore, in this section we introduce more general attack models that impose constraints on the DoS attack actions (γ_k, ν_k).

First, note that if we know in advance the strategy of the attacker—for any arbitrary sequence $(\gamma_0^{N-1}, \nu_0^{N-1})$—we can use the results from the previous theorem.

Corollary 1. *The results of Theorem 2 be specialized to any given attack signature $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \{0, 1\}^{2N}$.* $\square$

However, in practice we do not know the strategy of the attacker, thus we need to prepare for all possible attacks. Our model constrains the attacker action in time by restricting the DoS attacks on the measurement (resp. control) packet for *at most* $p < N$ (resp. $q < N$) time steps anywhere in the time interval $i = 0, \dots, N-1$. This attack model is motivated by limitations on the resources of the adversary—such as its battery power, or the response time of the defenders—which in turn limits the number of times it can block a transmission. We refer this attack model as the (p, q) adversary and it has the following admissible attack actions

$$\mathcal{A}_{pq} = \{(\gamma_0^{N-1}, \nu_0^{N-1}) \in \{0, 1\}^{2N} \big| \parallel \gamma_0^{N-1} \parallel_1 \geq N - p, \parallel \nu_0^{N-1} \parallel_1 \geq N - q\}, \qquad (28)$$

where $\parallel \cdot \parallel_1$ denotes the $1-$norm. The size of $\mathcal{A}_{pq}$ is $\sum_{i=0}^{p} \binom{N}{N-i} \cdot \sum_{j=0}^{q} \binom{N}{N-j}$.

An interesting sub-class of $\mathcal{A}_{pq}$ attack actions is the class of block attack strategies

$$\mathcal{A}_{pq}^{\tau_x \tau_u} = \{(\gamma_0^{N-1}, \nu_0^{N-1}) \in \{0, 1\}^{2N} | \gamma_{\tau_x}^{\tau_x + p - 1} = 0, \nu_{\tau_u}^{\tau_u + q - 1} = 0\} \qquad (29)$$

where $\tau_x \in \{0, \dots, N-p\}$ and $\tau_u \in \{0, \dots, N-q\}$ are the times at which the attacker starts jamming the measurement and control packets respectively. The size of $\mathcal{A}_{pq}^{\tau_x \tau_u}$ is $(N - p + 1) \cdot (N - q + 1)$. The intuition behind this attack sub-class is that an attacker will consume all of its resources continuously in order to maximize the damage done to the system. In this attack sub-class, p and q can represent the response time of defensive mechanisms. For example, a packet-flooding attack may be useful until network administrators implement filters or replicate the node under attack; similarly a jamming attack may be useful only until the control operators find the jamming source and neutralize it.

We note that $\mathcal{A}_{pq}$ and $\mathcal{A}_{pq}^{\tau_x \tau_u}$ are *non-deterministic attack models* in that the attacker can choose its action non-deterministically as long as the constraints defined by the attack model are satisfied.

4.1 DoS attacks against the safety constraint

One possible objective of the attacker can be to violate safety constraints:

Definition 2. *[Most unsafe attack] For a given attack model $\mathcal{A}$ and control strategy $\mu_k(\mathcal{I}_k)$, the best attack plan to violate safety specification that a output vector $z_k := (Cx_k + \nu_k Du_k)$ remains within safe set $\mathcal{S}$ is*

$$\max_{\mathcal{A}} \mathbf{P}[(Cx_k + \nu_k D\mu(I_k)) \in \mathcal{S}^c] \text{ for } k = 0, \ldots, N-1 \tag{30}$$

where $\mathcal{S}^c$ denotes the unsafe set.

We will now show that for control parameterization (12), the block pq attacks, $\mathcal{A}_{pq}^{\tau_x \tau_u}$ can be viewed as the best attack plan for violating the safety constraint (refer to Definition 2). We can write the system equation (1) as

$$x_{k+1} = Ax_k + \nu_k B\bar{u}_k + \nu_k \sum_{j=0}^{k} \gamma_j M_{k,j} x_j + w_k$$

and for the attack strategy $\mathcal{A}_{pq}^{\tau_x \tau_u}$:

$$x_{k+1} = \begin{cases} Ax_k + w_k \text{ for } k = \tau_u, \ldots, \tau_u + q - 1 \\ Ax_k + B\bar{u}_k + B\sum_{j=0}^{\min(\tau_x - 1, k)} M_{k,j} x_j \\ +\mathbf{1}(k \geq \tau_x + p)B\sum_{j=0}^{k} M_{k,j} x_j + w_k \text{ for } k = \begin{cases} 0, \ldots, \tau_u - 1 \\ \tau_u + q, \ldots, N-1. \end{cases} \end{cases} \tag{31}$$

Now, if we ignore $\bar{u}_k$ and substitute $\tau_x = 0$, $\tau_u = p$ in (31) we obtain

$$x_{k+1} = \begin{cases} Ax_k + w_k \text{ for } k = 0, \ldots, p+q-1 \\ Ax_k + B\sum_{j=p}^{k} M_{k,j} x_j \text{ for } k = p+q, \ldots, N-1 \end{cases} \tag{32}$$

Thus, using the attack strategy $\mathcal{A}_{pq}^{0p}$, the first $p+q-1$ time steps evolve as open-loop and beyond time step $p+q$, the system evolves as closed using available measurements since time p. With this strategy output vector z_k is expected to violate the safety constraint in the shortest time.

5 Formulation of new challenges

From the controller's viewpoint, it is of interest to design control laws that are robust against all attacker actions, i.e.:

Definition 3. *[Minimax (robust) control] For a given attack model $\mathcal{A}$, the security constrained robust optimal control problem is to synthesize a control law that minimizes the maximum cost over all $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \mathcal{A}$, subject to the power and safety constraints. This can be written as the minimax problem*

$$\min_{\mu_k(\mathcal{I}_k)} \max_{\mathcal{A}} [(4) \text{ subject to } (1), (2), (3), (5) \text{ and}, (6)]. \tag{33}$$

In general, we note that the problem (33) may not always be feasible. When $\mathcal{A}$ is probabilistic, Definition 3 can be treated in sense of expectation or almost-surely.

On the other hand, from the attacker's viewpoint, it is of interest to determine the optimal *attack plan* that degrades performance, i.e.,

Definition 4. *[Maximin (worst-case) attack] For a given attack model $\mathcal{A}$, the optimal attack plan is the attacker action that maximizes the minimum operating costs. This can be written as the maximin problem*

$$\max_{\mathcal{A}} \min_{\mu_k(\mathcal{I}_k)} \left[(4) \ subject \ to \ (1),(2),\ (3) \right]. \tag{34}$$

As a first effort to analyze these goals we first consider the classical linear quadratic control problem, and analyze the cost function for the case of (1) no attacks, (2) $\mathcal{A}_{\mathrm{Ber}(\bar{\gamma},\bar{\nu})}$attacks, and (3) $\mathcal{A}_{pq}$ attacks.

The problem is to find the optimal control policy $u_k = \mu_k(\mathcal{I}_k)$ that minimizes the objective (4) for the system (1), (2), and (3). The solution of this problem can be obtained in closed form using dynamic programming (DP) recursions [9, 16].

We recall that for the case of no-attack, i.e., $(\gamma_k, \nu_k) = (1,1)$ for all k, the optimal control law is given by $u_k^* = -L_k x_k$ where $L_k := (B^\top S_{k+1} B + Q^{uu})^{-1} B^\top S_{k+1} A$ and the matrices S_k are chosen such that $S_N = Q^{xx}$ and for $k = N-1, \ldots, 0$,

$$S_k = A^\top S_{k+1} + Q^{xx} - R_k$$

with $R_k = L_k^\top (B^\top S_{k+1} B + Q^{uu}) L_k$. The optimal cost is given by

$$J_N^* = \bar{x}^\top S_0 \bar{x} + \mathbf{Tr}\{S_0 P_0\} + \sum_{k=0}^{N-1} \mathbf{Tr}\{S_{k+1} W\}. \tag{35}$$

Following [16], the optimal control law for the case of $\mathcal{A}_{\mathrm{Ber}(\bar{\gamma},\bar{\nu})}$ attack model is given by $u_k^* = -L_k \hat{x}_{k|k}$ where $\hat{x}_{k|k}$ is given by the Kalman filter equations; the expressions for L_k, R_k, S_N are same as those for the no-attack case, and for $k = N-1, \ldots, 0$,

$$S_k = A^\top S_{k+1} A + Q^{xx} - \bar{\nu} R_k.$$

The optimal cost in this case is given by

$$J_{N,\mathcal{A}_{\mathrm{Ber}(\bar{\gamma},\bar{\nu})}}^* = \bar{x}^\top S_0 \bar{x} + \mathbf{Tr}\{S_0 P_0\} + \sum_{k=0}^{N-1} \mathbf{Tr}\{S_{k+1} W\} + \sum_{k=0}^{N-1} \mathbf{Tr}\{\bar{\nu} R_k \mathbf{E}_\gamma[\Sigma_{k|k}]\} \tag{36}$$

Lemma 2. $J_{N,\mathcal{A}_{Ber(\bar{\gamma},\bar{\nu})}}^* \geq J_N^*$ for all $(\bar{\gamma}, \bar{\nu}) \in [0,1]$. $\square$

We now consider the case of $\mathcal{A}_{pq}$ attacks. We can solve the problem of optimal attack plan for the $\mathcal{A}_{pq}$ attack class (refer to Definition 4):
For any *given* attack signature, $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \{0,1\}^{2N}$, the update equations

of error covariance are $\Sigma_{k+1|k} = A\Sigma_{k|k}A^\top + W$ and $\Sigma_{k+1|k+1} = (1-\gamma_{k+1})\Sigma_{k+1|k}$ and the optimal cost is given by

$$J_{N,\mathcal{A}_{pq}} = \bar{x}^\top S_0 \bar{x} + \mathbf{Tr}\{S_0 P_0\}$$
$$+ \sum_{k=0}^{N-1} \mathbf{Tr}\{S_{k+1}Q\} + \sum_{k=0}^{N-1} \mathbf{Tr}\{(A^\top S_{k+1}A + Q^{xx} - S_k)\Sigma_{k|k}\} \qquad (37)$$

where $S_N = Q^{xx}$ and for $k = N-1,\dots,0$,

$$S_k = A^\top S_{k+1}A + Q^{xx} - \nu_k A^\top S_{k+1}B(B^\top S_{k+1}B + Q^{uu})^{-1}B^\top S_{k+1}A. \qquad (38)$$

and for $k = 1,\dots,N-1$,

$$\Sigma_{k|k} = \prod_{j=1}^{k}(1-\gamma_j)A^k P_0 A^{k^\top} + \sum_{i=0}^{k-1}\prod_{j=(k-i)}^{k}(1-\gamma_j)A^i W A^{i^\top}. \qquad (39)$$

Proposition 1 *An optimal attack plan for $\mathcal{A}_{pq}$ attack model is a solution of the following optimization problem:*

$$\max_{\mathcal{A}_{pq}}(37) \ \text{subject to} \ \ (38),\ (39),$$
$$\| \gamma_0^{N-1} \|_1 \geq (N-p), \ \text{and} \ \| \nu_0^{N-1} \|_1 \geq (N-q).$$

We note that while $\Sigma_{k|k}$ is affected by the *past* measurement attack sequence $\{\gamma_0^k\}$, S_k is affected by the *future* control attack sequence $\{\nu_k^{N-1}\}$.

Remark 3. We can use dynamic programming or convex duality theory to solve the problem without the ℓ_1 constraints on γ_0^{N-1} and ν_0^{N-1}, see [9]. In this case, it is well-known that the optimal control policy is given by the linear feedback law that depends only on the current state. To solve the constrained problem as posed in Proposition 1, we propose to use suitable convex relaxations for the ℓ_1 constraints and solve the relaxed problem using semidefinite programming. $\square$

In future work we intend to address these problems and extend our results to deception attacks.

References

1. Amin, S., Abate, A., Prandini, M., Lygeros, J., Sastry, S.: *Reachability Analysis for Controlled Discrete Time Stochastic Hybrid Systems.* Hybrid Systems: Computation and Control, pp. 49–63(2006).
2. Amin, S., Bayen, A. M., El Ghaoui, L., Sastry, S. S.: *Robust feasibility for control of water flow in a reservoir canal system.* Proceedings of the 46th IEEE Conference on Decision and Control, pp. 1571-1577 (2007).

3. Ben-Tal, A., Boyd, S., Nemirovski, A.: *Control of uncertainty-affected discrete time linear systems via convex programming.* Technical Report, Minerva Optimization Center, Technion, Haifa, Israel (2005).
4. Byres, E., Lowe, J.: *The myths and facts behind cyber security risks for industrial control systems.* In Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies (2004).
5. Calafiore, G.C., El Ghaoui, L.: *Linear programming with probability constraints.* In Proceedings of the 2007 American Control Conference, New York, USA (2007).
6. Chatterjee, K., de Alfaro, L., Henzinger, T. A.: *Termination criteria for solving concurrent Safety and reachability games.* CORR: http://arxiv.org/abs/0809.4017 (2008).
7. Cárdenas, A. A., Amin, S., Sastry, S.: *Research Challenges for the Security of Control Systems.* 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium, San Jose, CA, (2008).
8. Downs, J. J., Vogel, E. F.: *A plant-wide industrial process control problem.* Computers & Chemical Engineering, vol. 17, no.3, pp. 245–255 (1993).
9. Gattami, A.: *Optimal decision with limited information.* PhD thesis, Department of Automatic Control, Lund University (2007).
10. Goulart, P. J., Kerrigan, E. C., Maciejowski, J. M.: *Optimization over state feedback policies for robust control with constraints.* Automatica, vol. 42, no. 4, pp. 523–533 (2006).
11. Mayne, D. Q., Rawlings, J. B., Rao, C. V., Scokaert, P. O. M.: *Constrained model predictive control: stability and optimality.* Automatica, vol. 36, no. 6, pp. 789–814 (2000).
12. Nguyen, K. C., Alpcan, T., Basar, T.: *A decentralized Bayesian attack detection algorithm for network security.* Proc. of 23rd Intl. Information Security Conf, Milan, pp. 413–428 (2008).
13. Pinar, A., Meza, J., Donde, V., Lesieutre, B.: *Optimization strategies for the vulnerability analysis of the power grid.* Submitted to SIAM Journal on Optimization (2008).
14. Primbs, J., Sung, C.: *Stochastic receding horizon control of constrained linear systems with state and control multiplicative noise.* Submitted to IEEE Transactions on Automatic Control (2007).
15. Salmeron, J., Wood, K., Baldick, B.: *Analysis of electric grid security under terrorist threat.* IEEE Transactions on power systems, vol. 19, pp. 905–912 (2004).
16. Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., Sastry, S.: *Foundations of control and estimation over lossy networks.* Proceedings of the IEEE, Special issue on networked control systems, vol. 95, no. 1, pp. 163–187 (2007).
17. Skaf, J., Boyd, S.: *Design of affine controllers via convex optimization.* Submitted to the IEEE Transactions on Automatic Control, (2008).
18. Turk, R. J.: *Cyber Incidents Involving Control Systems.* Technical Report, Idaho National Laboratory, (2005).
19. van Hessem, D., Bosgra, O.: *A full solution to the constrained stochastic closed-loop MPC problem via state and innovations feedback and its receding horizon implementation.* In Proceedings of the 2003 Conference on Decision and Control, Maui, Hawaii, USA (2003).
20. Wang, Y., Boyd, S.: *Fast model predictive control using online optimization.* Submitted to IEEE Transactions on Control Systems Technology, (2008).
21. Yu, Z. H., Li, W., Lee, J. H., Morari, M.: *State estimation based model predictive control applied to shell control problem: a case study.* Chemical engineering science, vol. 49, no. 3, pp. 285–301 (1994).

6 Appendix

$$\mathbf{x_0} := \begin{pmatrix} I_n \\ A \\ A^2 \\ \vdots \\ A^N \end{pmatrix} x_0 \in \mathbb{R}^{n(N+1)}, \quad \mathbf{A} := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ I_n & 0 & 0 & \dots & 0 \\ A & I_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ A^{N-1} & A^{N-2} & A^{N-3} & \dots & I_n \end{pmatrix} \in \mathbb{R}^{n(N+1)\times nN},$$

$$\mathbf{B} := \mathbf{A}(I_N \otimes B) = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ B & 0 & 0 & \dots & 0 \\ AB & B & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ A^{N-1}B & A^{N-2}B & A^{N-3}B & \dots & B \end{pmatrix} \in \mathbb{R}^{n(N+1)\times mN},$$

$$\mathbf{\Gamma} = \operatorname{diag}(\gamma_0^{N-1}) \otimes I_n = \begin{pmatrix} \gamma_0 I_n & & \\ & \ddots & \\ & & \gamma_{N-1}I_n \end{pmatrix} \in \mathbb{R}^{nN \times nN},$$

$$\mathbf{N} = \operatorname{diag}(\nu_0^{N-1}) \otimes I_m = \begin{pmatrix} \nu_0 I_m & & \\ & \ddots & \\ & & \nu_{N-1}I_m \end{pmatrix} \in \mathbb{R}^{mN \times mN},$$

and

$$\mathbf{e_0} = \begin{pmatrix} I_n \\ (1-\gamma_0)A \\ (1-\gamma_0)(1-\gamma_1)A^2 \\ \vdots \\ \prod_{j=0}^{N-1}(1-\gamma_j)A^N \end{pmatrix} e_0 \in \mathbb{R}^{n(N+1)}$$

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ I_n & 0 & \dots & 0 \\ (1-\gamma_1)A & I_n & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \prod_{j=1}^{N-1}(1-\gamma_j)A^{N-1} & \prod_{j=2}^{N-1}(1-\gamma_j)A^{N-2} & \dots & I_n \end{pmatrix} \in \mathbb{R}^{n(N+1)\times nN}$$