A Model Predictive Controller with Constrained Estimation for Systems under Denial-of-Service Attacks ⋆

First A. Author * **Second B. Author, Jr.** **

* *National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).*
** *Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar. colostate.edu)*

Abstract: Abstract of not more than 250 words. These instructions give you guidelines for preparing papers for IFAC technical meetings. Please use this document as a template to prepare your manuscript. For submission guidelines, follow instructions on paper submission system as well as the event website.

Keywords: Model Predictive Control, Denial of Service, packet dropouts, networked control systems.

1. INTRODUCTION

Cyber-security on Networked Control Systems (NCS) from the viewpoint of automatic control keeps growing in interest and research due the potential threads that arise around shared communication between actuators, sensors, and controllers, see Lucia et al. (2016); Cheng et al. (2016); Ali et al. (2018); Pang et al. (2019); Lun et al. (2019). A type of DoS attack over NCS can interrupt the actuator and sensor communication channels by random packet flooding that can consume resources, such as network bandwidth, and CPU cycles. As a result, the increased packet-dropout reduces the control and estimation performance, and could potentially lead the system to instability. Although control theory developed many fault tolerant and disturbance rejection algorithms, they are commonly constrained by the system dynamics and do not have malicious intentions like a DoS attack does. Moreover, this type of cyberattack can be coordinated, remain undetected, and is not constrained by the system dynamics, see Teixeira et al. (2015). Consequently, the design of robust control and estimation process needs to be more flexible to consider this type of thread.

A basic model that describes the intermittent communication problems is the through identical, independent, and distributed (i.i.d.) discrete Bernoulli packet-dropout, see Imer et al. (2006); Schenato et al. (2007); Tabbara and Nesic (2008); Shi et al. (2010); Li and Shi (2014); te Yu and Fu (2015); Li et al. (2018). Correlated channels Quevedo et al. (2013). Markov channelQuevedo and Nešić (2012); Wu et al. (2015)

- MPC justification - MPC frameworks that have been used.

From the MPC viewpoint, Lucia et al. (2016) reviews MPC approaches against cyber-attacks. The authors divide them by category: lossy communication, transmission delays, and resource awareness. The authors review the advantages of implementing MPC to tackle cyber-attacks by showing examples of event-triggered MPC control with efficient implementations in embedded systems. However, the event-triggered MPC method is proposed as a robust control design that requires the solution of three optimization problems at each time instant which can be computationally inefficient.

DoS attack can be dangerous due to the packet loss in the communication channel, and it does not need knowledge about the system dynamics. In Sinopoli et al. (2004), a modified time-varying Kalman filter is proposed to handle the packet loss in the measurement channel. The authors develop a method of Kalman filtering heavy intermittent packet losses in a TCP channel, and shows the existence of critical conditions of the packet delivery to guarantee the stability of the estimation process. However, the method only considers a Bernoulli packet dropout model and not a generalized lossy communication model. Consequently, it serves as the basis for the following LQG controller. In Sinopoli et al. (2005) and Schenato et al. (2007); Imer et al. (2006), the authors define an optimal LQG controller merged with the modified Kalman filter in Sinopoli et al. (2004) that is able to handle packet losses not only in TCP but also in UDP channel. The authors establish stability conditions for the existence of an optimal solution based on the packet delivery rate of the communication channel.

From the MPC perspective, Quevedo et al. (2015) proposes a stochastic MPC approach that considers a stochastic cost function, and it is compared with a deterministic cost function in Quevedo and Nešić (2012). The authors propose a type of smart actuator which contains a buffer and selection logic to protect the actuator against packet loss. Working in parallel-in serial-out with the MPC controller,

⋆ Sponsor and financial support acknowledgment goes here. Paper titles should be written in uppercase and lowercase letters, not all uppercase.

the smart actuator acknowledges the controller when there is a packet loss and the MPC solves a tentative constrained plant until the smart actuator detects no packet losses.

In summary, much research has been developing around cyber-security and MPC, and there is still a lot of work to be done. From the deterministic to the stochastic domain, from the attacker and defence viewpoint. For the sake of this document, there are some assumptions to meet for FDI and DoS attacks over the MPC scheme. Other types of vulnerabilities are out of the scope of this project.

Notation: A set $\mathcal{X} \subseteq \mathbb{R}^n$ is invariant for $x_{k+1} = f(x,u)$ under control $u = \kappa(x)$ if and only if $\forall x \in \mathcal{X}$ it holds $x_{k+1} = f(x,\kappa(x)) \in \mathcal{X}$. The notation $x_{k+j|k}$ is the prediction of x for j steps ahead given the discrete sampling time k. The probability of an event Ω is $\mathbf{Pr}[\Omega]$, the conditional expectation of x given y is $\mathbb{E}[x|y]$, and the unconditional expectation is $\mathbb{E}[x] = \hat{x}$. $A \succeq 0$ is positive semi-definite matrix, and $A \succ 0$ is positive definite matrix, $\mathbf{I}_n$ stands for the identity matrix $n \times n$. The quadratic form is written as $\|x\|_Q^2 = x^\intercal Q x$. A vector is expressed in normal face, and a sequence of vectors is represented in bold face.

2. PROBLEM STATEMENT

Consider the following discrete-time LTI system subject to DoS attacks and additive disturbances,

$$\begin{aligned} x_{k+1} &= Ax_k + \nu_k B u_k + w_k \\ y_k &= \gamma_k C x_k + z_k \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, and $y \in \mathbb{R}^p$, are the states, input, and output vectors respectively. $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}, C \in \mathbb{R}^{p\times n}$, are the state, input, and output matrices respectively, and x_k is available at each sampling time k. The control objective is to regulate $x \to 0$ as $k \to \infty$ despite the effect of the DoS attacks and disturbances, while satisfying any state constraints $x \in \mathcal{X} \subseteq \mathbb{R}^n$, and input constraints $u \in \mathcal{U} \subseteq \mathbb{R}^m$.

Assumption 1. The pair (A,B) is stabilizable, and (C,A) is observable. A, B and C are known.

Assumption 2. The sets $\mathcal{X}$ and $\mathcal{U}$ are PC-sets.

Assumption 3. The process noise $w_k \sim \mathcal{N}(0, Q_w)$ with covariance Q_w, and the measurement noise $z_k \sim \mathcal{N}(0, R_z)$ with covariance R_z are known at each k.

Assumption 4. The attack over the actuator channel ν_k, and the attack over the sensor channel γ_k are known at each k, and are uncorrelated.

Definition 5. The DoS attack is defined as a multiplicative identical, independent, and distributed (i.i.d) discrete Bernoulli packet dropout model,

$$\nu \sim \mathcal{B}(\bar{\nu}) \begin{cases} \mathbf{Pr}[\nu = 1] = \bar{\nu} \\ \mathbf{Pr}[\nu = 0] = 1 - \bar{\nu} \end{cases} \tag{2}$$

$$\gamma \sim \mathcal{B}(\bar{\gamma}) \begin{cases} \mathbf{Pr}[\nu = 1] = \bar{\gamma} \\ \mathbf{Pr}[\nu = 0] = 1 - \bar{\gamma} \end{cases} \tag{3}$$

where $\bar{\nu}$ and $\bar{\gamma}$ are the probabilities of the packet success delivery.

3. PRELIMINARES

3.1 LQG-TCP

The optimal LQG solution proposed in Schenato et al. (2007) for the TCP-like communication channel considers an Acknowledgement (ACK) of the packet loss due to ν_k and γ_k. This ACK is defined within an information set $\mathcal{I}_k = \{y^k, \nu^{k-1}, \gamma^k\}$ that acknowledges the controller and estimator about the packet delivery, and it is sent within the same time step, where $y^k = (y_k, y_{k-1}, \ldots, y_1)$, $\nu^k = (\nu_k, \nu_{k-1}, \ldots, \nu_1)$, $\gamma^k = (\gamma_k, \gamma_{k-1}, \ldots, \gamma_1)$. Since the attack ν_k is uncorrelated with the control input u_k, it is not necessary to penalize the input when the packet does not make through the channel. The problem is to minimize the expectation of the following cost function,

$$J_N(\hat{x}_k, u_k) = \mathbb{E}\left[\sum_{k=0}^{N-1} \left(\|x_k\|_Q^2 + v_k \|u_k\|_R^2\right) + \|x_N\|_Q^2 \;\middle|\; \mathcal{I}_k\right] \tag{4}$$

such that, the optimal solution is,

$$\begin{cases} u_k^* = -(B^\intercal S_k B + R)^{-1} B^\intercal S_k A \; \hat{x}_k \\ S_{k+1} = A^\intercal S_k A + Q + (\nu_k A^\intercal S_k B) \; u_k^* \\ S_0 = Q \end{cases} \tag{5}$$

where S_k is the optimal cost and $\hat{x}_k$ is the estimated state. Notice that u_k^* does not depend on the attack ν_k. To complete the approach, a modified time-varying KF for a TCP channel (KF-TCP) is used as described in Sinopoli et al. (2005). Although LQG-TCP can stabilize the system, it can not handle constraints as MPC technique does.

3.2 Conventional MPC under DoS attack

Given Assumption 3, a steady-state Kalman Filter (KF) with gain L_{KF} can be implemented to handle the disturbance. Therefore, the problem is to minimize,

$$\mathbb{P}_N(\hat{x}_k) : \min_{\mathbf{u}_k} \sum_{j=0}^{N-1} \left(\left\|\hat{x}_{k+j|k}\right\|_Q^2 + \left\|u_{k+j|k}\right\|_R^2\right) + \left\|\hat{x}_{k+N|k}\right\|_P^2 \tag{6}$$

$$\begin{aligned} \text{s.t.} \quad \hat{x}_{k|k} &= \hat{x}_k \\ \hat{x}_{k+1+j|k} &= A\hat{x}_{k+j|k} + \nu_{k|k} B u_{k+j|k} + w_{k|k} \\ \hat{x}_{k+j|k} &\in \mathcal{X} \subseteq \mathbb{R}^n \\ u_{k+j|k} &\in \mathcal{U} \subseteq \mathbb{R}^m \\ \hat{x}_{k+N|k} &\in \mathcal{X}_f \subseteq \mathbb{R}^n \end{aligned}$$

where $Q \in \mathbb{R}^{n\times n}$ and $R \in \mathbb{R}^{m\times m}$ are the state, and input penalty matrices. $P \in \mathbb{R}^{n\times n}$ is the terminal cost matrix, $N \in \mathbb{N}$ is the horizon length, and $\mathcal{X}_f$ is the terminal set. The optimal solution is $\mathbf{u}_k^* = \left\{u_{k|k}^*, u_{k+1|k}^*, \ldots, u_{k+N-1|k}^*\right\}$, and with the application of the Receding Horizon (RH) principle, the implicit nonlinear time-variant control law is $u_{k|k}^* = \kappa_N(x_k)$, which is defined for $x_k \in \mathcal{X}_N$. Where $\mathcal{X}_N = \{x_k : \mathcal{U}_N(x_k) \neq 0\}$ is the feasible region, and $\mathcal{U}_N(x_k)$ is the set of feasible solutions that steer $x \to 0$. Fig. 1 shows the attack scheme.

The stability can be guaranteed if (A,B) is stabilizable, $(Q^{1/2}, A)$ is observable, $Q \succeq 0$, $R \succ 0$, P satisfies the Lyapunov equation for some stabilizing K,

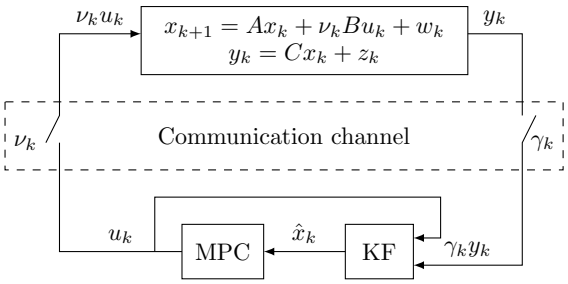


Fig. 1. Conventional MPC under DoS attack.

$$(A+BK)^\intercal P(A+BK) - P = -(Q + K^\intercal RK) \tag{7}$$

and $\mathcal{X}_f$ is an admissible invariant set for mode-2 dynamics $x_{k+1} = (A+BK)x_k$ with respect to $\mathcal{X}$ and $\mathcal{U}$.

4. MPC-TCP APPROACH

Given the fact that LQG-TCP shares properties with MPC, this section extends that approach to the constrained case for a TCP channel (MPC-TCP). The objective is to minimize the expectation of the cost function considering the attack ν. Fig. 2 shows the scheme. Notice

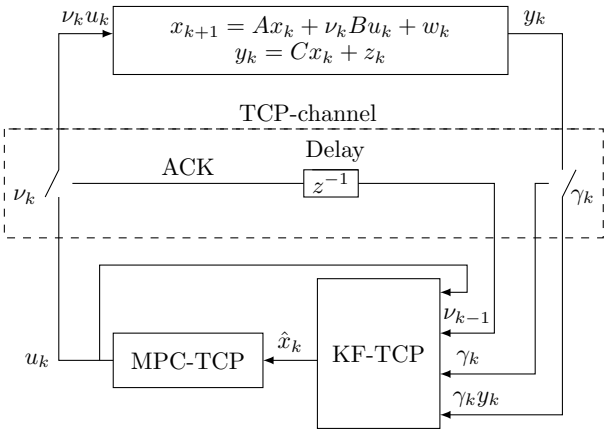


Fig. 2. Attack scheme with MPC-TCP approach.

that the delay in the TCP-channel is not a transportation delay, which means that ν_{k-1} is available immediately to the KF-TCP block.

4.1 Problem formulation

Let us define the predicted compact form of the cost function by introducing the attack ν_k in the MPC formulation and penalizing the input when the packet is lost. The cost function is,

$$J_N(x_k, \mathbf{u}_k) = \sum_{j=0}^{N-1} \left(\left\|x_{k+j|k}\right\|_Q^2 + \left\|\nu_{k+j|k} u_{k+j|k}\right\|_R^2 \right) + \left\|x_{k+N|k}\right\|_P^2 \tag{8}$$

applying the attack vector $\nu_k = \nu_{k|k}$ into the model (1) recursively, and stacking without w_k,

$$\underbrace{\begin{bmatrix} x_{k+1|k} \\ x_{k+2|k} \\ \vdots \\ x_{k+N|k} \end{bmatrix}}_{\mathbf{x}_k} = \underbrace{\begin{bmatrix} A \\ A^2 \\ \vdots \\ A^N \end{bmatrix}}_{F} + \underbrace{\begin{bmatrix} B & 0 & \dots & 0 \\ AB & B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A^{N-1}B & A^{N-2}B & \dots & B \end{bmatrix}}_{G} \times \underbrace{\begin{bmatrix} \nu_{k|k}\ u_{k|k} \\ \nu_{k+1|k}\ u_{k+1|k} \\ \vdots \\ \nu_{k+N-1|k}\ u_{k+N-1|k} \end{bmatrix}}_{\mathbf{u}_{\mathbf{a}k}} \tag{9}$$

the prediction equality constraint results in,

$$\mathbf{x}_k = Fx_k + G\mathbf{u}_{\mathbf{a}k} \tag{10}$$

where $\mathbf{x}_k$, and $\mathbf{u}_{\mathbf{a}k}$ are the state, and attacked input predictions over all the steps $j = 0, 1, 2, \dots, N$.

Now, rewriting the cost function (8) and stacking as,

$$x_{k|k}^\intercal Q x_{k|k} + \begin{bmatrix} x_{k+1|k} \\ x_{k+2|k} \\ \vdots \\ x_{k+N|k} \end{bmatrix}^\intercal \underbrace{\begin{bmatrix} Q & 0 & \dots & 0 \\ 0 & Q & \ddots & \vdots \\ \vdots & \ddots & Q & 0 \\ 0 & \dots & 0 & P \end{bmatrix}}_{\tilde{Q}} \begin{bmatrix} x_{k+1|k} \\ x_{k+2|k} \\ \vdots \\ x_{k+N|k} \end{bmatrix}$$

$$+ \begin{bmatrix} \nu_{k|k}u_{k|k} \\ \nu_{k+1|k}u_{k+1|k} \\ \vdots \\ \nu_{k+N-1|k}u_{k+N-1|k} \end{bmatrix}^\intercal \underbrace{\begin{bmatrix} R & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & R \end{bmatrix}}_{\tilde{R}} \begin{bmatrix} \nu_{k|k}u_{k|k} \\ \nu_{k+1|k}u_{k+1|k} \\ \vdots \\ \nu_{k+N-1|k}u_{k+N-1|k} \end{bmatrix}$$

and with $x_{k|k} = x_k$ the general problem is,

$$\mathbb{P}_N(x_k) : \min_{\mathbf{u}_k} \ x_k^\intercal Q x_k + \mathbf{x}_k^\intercal \tilde{Q} \mathbf{x}_k + \mathbf{u}_{\mathbf{a}k}^\intercal \tilde{R} \mathbf{u}_{\mathbf{a}k} \tag{11}$$

$$\begin{aligned} \text{s.t.} \quad & \mathbf{x}_k = Fx_k + G\mathbf{u}_{\mathbf{a}k} \\ & x_{k+j|k} \in \mathcal{X} \\ & u_{k+j|k} \in \mathcal{U} \\ & x_{k+N|k} \in \mathcal{X}_f \end{aligned}$$

Let us define the expectation of the problem as,

$$\mathbb{P}_N(x_k) : \min_{\mathbf{u}_k} \ \mathbb{E}\left[x_k^\intercal Q x_k + \mathbf{x}_k^\intercal \tilde{Q} \mathbf{x}_k + \mathbf{u}_{\mathbf{a}k}^\intercal \tilde{R} \mathbf{u}_{\mathbf{a}k} \ \middle| \mathcal{I}_k \right] \tag{12}$$

$$\text{s.t.} \quad \mathbb{E}\left[\mathbf{x}_k\right] = \mathbb{E}\left[Fx_k + G\mathbf{u}_{\mathbf{a}k}\right] \tag{13}$$

If $\mathbb{E}[x_k|\mathcal{I}_k] = \hat{x}_k$, $\mathbb{E}[\nu_k|\mathcal{I}_k] = \bar{\nu}$, $\mathbb{E}[\mathbf{u}_k] = \hat{\mathbf{u}}_k$. $\mathbb{E} = [\nu_k u_k] = \mathbb{E}[\nu_k]\mathbb{E}[u_k]$,

$$\mathbb{E}[\mathbf{u}_{\mathbf{a}k}] = \mathbb{E}\begin{bmatrix} \nu_{k|k}\ u_{k|k} \\ \nu_{k+1|k}\ u_{k+1|k} \\ \vdots \\ \nu_{k+N-1|k}\ u_{k+N-1|k} \end{bmatrix} = \begin{bmatrix} \bar{\nu}\ \mathbb{E}[u_{k|k}] \\ \bar{\nu}\ \mathbb{E}[u_{k+1|k}] \\ \vdots \\ \bar{\nu}\ \mathbb{E}[u_{k+N-1|k}] \end{bmatrix}$$

$$\mathbb{E}[\mathbf{u}_{\mathbf{a}k}] = \bar{\nu}\ \hat{\mathbf{u}}_{\mathbf{k}} \tag{14}$$

hence,

$$\hat{\mathbf{x}}_k = F\hat{x}_k + G\bar{\nu}\hat{\mathbf{u}}_k \tag{15}$$

Applying the expectation to (12) using the fact $\mathbb{E}[x_k^\intercal Q x_k] = \hat{x}_k^\intercal Q \hat{x}_k + trace(QP_k)$,

$$J_N(\hat{x}_k, \hat{\mathbf{u}}_k) = \hat{x}_k^\intercal Q \hat{x}_k + \hat{\mathbf{x}}_k^\intercal \tilde{Q} \hat{\mathbf{x}}_k + \bar{\nu}^2 \hat{\mathbf{u}}_k^\intercal \tilde{R} \hat{\mathbf{u}}_k + trace\left[QP_k + \tilde{Q}P_k + \tilde{R}\ cov(\mathbf{u}_{\mathbf{a}k})\right] \tag{16}$$

where P_k is the state covariance matrix. Because there is no need to predict P_k, it is sufficient to use the covariance matrix $P_{k+1|k}$ of the innovation step in (33), which is bounded according to *Lemma 3.7* in Schenato et al. (2007). Also, there is no covariance between ν_k and u_k, $cov(\mathbf{u_a}k) = 0$.

Now, substituting (15) in (16),

$$J_N(\hat{x}_k, \hat{\mathbf{u}}_k) = \hat{x}_k^\intercal Q \hat{x}_k + (F\hat{x}_k + G\bar{\nu}\hat{\mathbf{u}}_k)^\intercal \tilde{Q}(F\hat{x}_k + G\bar{\nu}\hat{\mathbf{u}}_k) + \bar{\nu}^2 \hat{\mathbf{u}}_k^\intercal \tilde{R}\hat{\mathbf{u}}_k + trace\left[(Q+\tilde{Q})P_{k+1|k}\right] \quad (17)$$

reordering in QP compact form, the expected cost function results in,

$$J_N(\hat{x}_k, \hat{\mathbf{u}}_k) = \frac{1}{2}\hat{\mathbf{u}}_k^\intercal \bar{\nu}^2 H \hat{\mathbf{u}}_k + \bar{\nu} c^\intercal \hat{\mathbf{u}}_k + \alpha_v \quad (18)$$

where,

$$\begin{cases} H = 2(G^\intercal \tilde{Q} G + \tilde{R}) \\ c = L\hat{x}_k, \quad L = 2G^\intercal \tilde{Q} F \\ \alpha_v = \hat{x}_k^\intercal M \hat{x}_k + \beta \\ M = Q + F^\intercal \tilde{Q} F, \quad \beta = trace\left[(Q+\tilde{Q})P_{k+1|k}\right] \end{cases} \quad (19)$$

Considering that ν_k can be a strong attack, let us introduce a slack variable ϵ_k to soft the state constraints x_k and to recover feasibility,

$$J_N(\hat{x}_k, \hat{\mathbf{u}}_k, \epsilon_k) = \frac{1}{2}\hat{\mathbf{u}}_k^\intercal \bar{\nu}^2 H \hat{\mathbf{u}}_k + \bar{\nu} c^\intercal \hat{\mathbf{u}}_k + \alpha_v + \frac{1}{2}\epsilon_k^\intercal \sigma \epsilon_k + \rho^\intercal \epsilon_k \quad (20)$$

where σ and ρ are the norm-2 and norm-1 weights of the slack variable respectively.

Let us define the inequality constraints,

$$\underbrace{\begin{bmatrix} +\mathbf{I} \\ -\mathbf{I} \end{bmatrix}}_{P_x} x_{k+j|k} \leq \underbrace{\begin{bmatrix} +x_{max} \\ -x_{min} \end{bmatrix}}_{q_x}, \quad \underbrace{\begin{bmatrix} +\mathbf{I} \\ -\mathbf{I} \end{bmatrix}}_{P_u} u_{k+j|k} \leq \underbrace{\begin{bmatrix} +u_{max} \\ -u_{min} \end{bmatrix}}_{q_x} \quad (21)$$

stacking the input constraints $\mathcal{U} = \{u_k : P_u u_{k+j|k} \leq q_u\}$,

$$\underbrace{\begin{bmatrix} P_u & 0 & \dots & 0 \\ 0 & P_u & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & P_u \end{bmatrix}}_{\tilde{P}_u} \underbrace{\begin{bmatrix} u_{k|k} \\ u_{k+1|k} \\ \vdots \\ u_{k+N-1|k} \end{bmatrix}}_{\mathbf{u}_k} \leq \underbrace{\begin{bmatrix} q_u \\ q_u \\ \vdots \\ q_u \end{bmatrix}}_{\tilde{q}_u}$$

$$\tilde{P}_u \mathbf{u}_k \leq \tilde{q}_u \quad (22)$$

stacking the state constraints $\mathcal{X} = \{x_k : P_x x_{k+j|k} \leq q_x\}$,

$$\underbrace{\begin{bmatrix} P_x \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}}_{\tilde{P}_{x_0}} x_{k|k} + \underbrace{\begin{bmatrix} 0 & 0 & \dots & 0 \\ P_x & 0 & \dots & 0 \\ 0 & P_x & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & P_{x_N} \end{bmatrix}}_{\tilde{P}_x} \underbrace{\begin{bmatrix} x_{k+1|k} \\ x_{k+2|k} \\ \vdots \\ x_{k+N|k} \end{bmatrix}}_{\mathbf{x}_k} \leq \underbrace{\begin{bmatrix} q_x \\ q_x \\ q_x \\ \vdots \\ q_{x_N} \end{bmatrix}}_{\tilde{q}_x}$$

$$\tilde{P}_x \mathbf{x}_k \leq \tilde{q}_x - \tilde{P}_{x_0} x_k \quad (23)$$

substituting (15) in (23) to eliminate $\hat{\mathbf{x}}_k$, adding the slack variable ϵ_k, applying the expectation,

$$\begin{cases} \tilde{P}_x G \bar{\nu} \hat{\mathbf{u}}_\mathbf{k} & \leq \tilde{q}_x - (\tilde{P}_{x_0}\hat{x}_k - \tilde{P}_x F)\hat{x}_k + \epsilon_k \\ \epsilon_k & \geq 0 \end{cases}$$

and stacking with the expectation of (22),

$$\underbrace{\begin{bmatrix} \tilde{P}_u & 0 \\ \tilde{P}_x G\bar{\nu} & -I \\ 0 & -I \end{bmatrix}}_{P_{c_\epsilon}} \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix} \leq \underbrace{\begin{bmatrix} \tilde{q_u} \\ \tilde{q_x} \\ 0 \end{bmatrix}}_{q_{c_\epsilon}} + \underbrace{\begin{bmatrix} 0 \\ -\tilde{P}_{x_0} - \tilde{P}_x F \\ 0 \end{bmatrix}}_{S_{c_\epsilon}} \hat{x}_k$$

the feasible set $\mathcal{U}_N$ is,

$$\mathcal{U}_N(\hat{x}_k) = \left\{ \hat{\mathbf{u}}_k : P_{c_\epsilon} \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix} \leq q_{c_\epsilon} + S_{c_\epsilon}\ \hat{x}_k \right\} \quad (24)$$

Therefore, the constrained MPC-TCP problem is to minimize,

$$\mathbb{P}_N(\hat{x}) : \min_{\hat{\mathbf{u}}_\mathbf{k}} \frac{1}{2} \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix}^\intercal \begin{bmatrix} \bar{\nu}^2 H & 0 \\ 0 & \sigma \end{bmatrix} \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix} + [\bar{\nu}c^\intercal \ \ \rho^\intercal] \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix} + \alpha_v \quad (25)$$

$$\text{s.t.} \qquad P_{c_\epsilon} \begin{bmatrix} \hat{\mathbf{u}}_k \\ \epsilon_k \end{bmatrix} \leq q_{c_\epsilon} + S_{c_\epsilon} \hat{x}_k \quad (26)$$

with the optimal sequence,

$$\hat{\mathbf{u}}_k^* = \left\{ \hat{u}_{k|k}^*, \hat{u}_{k+1|k}^*, \dots, \hat{u}_{k+N-1|k}^* \right\} \quad (27)$$

and the estimated implicit RH nonlinear time-variant control law as,

$$\hat{u}_{k|k}^* = \kappa_N(\hat{x}_k) \quad (28)$$

Remark 6. (Unconstrained MPC-TCP) Let us define the attacked vector $\mathbf{u_a}_k$ as,

$$\mathbf{u_a}_k = \underbrace{\begin{bmatrix} \nu_{k|k} & 0 & \dots & 0 \\ 0 & \nu_{k+1|k} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \nu_{k+N-1|k} \end{bmatrix}}_{V} \underbrace{\begin{bmatrix} u_{k|k} \\ u_{k+1|k} \\ \vdots \\ u_{k+N-1|k} \end{bmatrix}}_{\mathbf{u}_k}$$

$$\mathbf{u_a}_k = V\mathbf{u}_k \quad (29)$$

replacing (29) in (11) and (10), the problem is,

$$\begin{aligned} \mathbb{P}_N(x_k) : \min_{\mathbf{u}_k} \ & x_k^\intercal Q x_k + \mathbf{x}_k^\intercal \tilde{Q} \mathbf{x}_k + (V\mathbf{u}_k)^\intercal \tilde{R}(V\mathbf{u}_k) \\ \text{s.t.} \quad & \mathbf{x}_k = Fx_k + GV\mathbf{u}_k \end{aligned} \quad (30)$$

now substituting the modified predicted equality constraint into the problem $\mathbb{P}_N(x_k)$, the QP compact form can be written as,

$$J_N(x_k, \mathbf{u}_k) = \frac{1}{2}\mathbf{u}_k^\intercal VHV\mathbf{u}_k + c^\intercal V\mathbf{u}_k + \alpha \quad (31)$$

where, $\alpha = x_k^\intercal M x_k$. The solution can be obtained if $\nabla_{\mathbf{u}_k} J_N(x_k, \mathbf{u}_k) = 0$, considering that $V^\intercal = V$, $V^2 = V$, and because x_k is estimated by the unconstrained KF-TCP as $\hat{x}_k$, we obtain $\mathbf{u}_k^* = -H^{-1}L\hat{x}_k$, with the RH control input as $u_k^* = K_N\hat{x}_k$. Such that, u_k^* is an explicit solution and it is similar to (5).

4.2 Constrained KF-TCP

Let us define the unconstrained KF-TCP as proposed Sinopoli et al. (2005). If,

$$\begin{cases} \hat{x}_{k|k} = \mathbb{E}[x_k|\mathcal{I}_k] \\ e_{k|k} = x_k - \hat{x}_{k|k} \\ P_{k|k} = \mathbb{E}[e_{k|k}e_{k|k}^\intercal|\mathcal{I}_k] \end{cases} \quad (32)$$

the **innovation** step is,

$$\begin{cases} \hat{x}_{k+1|k} = A\hat{x}_{k|k} + \nu_k B u_k \\ e_{k+1|k} = Ae_{k|k} + w_k \\ P_{k+1|k} = AP_{k|k}A^\intercal + Q_w \end{cases} \tag{33}$$

because $y_k,\ \gamma_k,\ w_k$ and $\mathcal{I}_k$ are independent, the **correction** step is,

$$\begin{cases} \hat{x}_{k+1|k+1} = \hat{x}_{k+1|k} + \gamma_{k+1}K_{k+1}\left(y_{k+1} - C\hat{x}_{k+1|k}\right) \\ e_{k+1|k+1} = \left(I - \gamma_{k+1}K_{k+1}C\right)e_{k+1|k} - \gamma_{k+1}K_{k+1}\nu_{k+1} \\ P_{k+1|k+1} = P_{k+1|k} - \gamma_{k+1}K_{k+1}C\ P_{k+1|k} \\ K_{k+1} = P_{k+1|k}C^\intercal(CP_{k+1|k}C^\intercal + R_z)^{-1} \end{cases} \tag{34}$$

Considering the state constraints $\mathcal{X}$, the approach is to project the unconstrained estimation onto the constrained surface in order to improve the estimation process, see Simon (2010). Hence, the **constrained innovation** step is,

$$\begin{aligned} \tilde{x}_{k+1|k} &= \arg\min_x \left\|x - \hat{x}_{k+1|k}\right\|^2_{(P_{k+1|k})^{-1}} \\ \text{s.t.} \quad & P_x x \le q_x \end{aligned} \tag{35}$$

and the **constrained correction** step is,

$$\begin{aligned} \tilde{x}_{k+1|k+1} &= \arg\min_x \left\|x - \hat{x}_{k+1|k+1}\right\|^2_{(P_{k+1|k+1})^{-1}} \\ \text{s.t.} \quad & P_x x \le q_x \end{aligned} \tag{36}$$

The stability of the estimation process can be guaranteed if,

$$\begin{aligned} & \bar{\gamma} > \gamma_c,\ \bar{\nu} > \nu_c \\ \text{s.t.}\ \ & 1 - \frac{1}{max_i\ |\lambda_i^u(A)|^2} \le \gamma_c,\ \nu_c \le 1 - \frac{1}{\prod_i\ |\lambda_i^u(A)|^2} \end{aligned} \tag{37}$$

where $\lambda_i^u(A)$ are the unstable eigenvalues of state matrix A of the system. ν_c, γ_c are the critical probabilities which are defined in Sinopoli et al. (2005).

4.3 Stability and Feasibility

To guarantee stability, the aim is to construct a terminal constraint set $\mathcal{X}_f$ such that the feasibility of the problem (25) for x_k implies constraints satisfaction for mode-2. An approach is to extend mode-1 constraints by n steps,

$$\begin{aligned} P_x x_{k+j|k} &\le q_x,\ j = 0, \dots, N-1, N, \dots, N+n-1 \\ P_u u_{k+j|k} &\le q_u,\ j = 0, \dots, N-1, N, \dots, N+n-1 \end{aligned} \tag{38}$$

use deadbeat mode-2 constraints as terminal constraints for $j = N, \dots, N+n-1$, and apply the expectation to handle the introduction of the attack ν in mode-2,

$$\begin{cases} \mathbb{E}[x_{k+j|k}] = \mathbb{E}[(A+BK)^j x_{k+N|k}] \\ \mathbb{E}[\nu_{k+j|k}u_{k+j|k}] = \mathbb{E}[\nu_{k+j|k}K(A+BK)^j x_{k+N|k}] \end{cases}$$

$$\begin{cases} \hat{x}_{k+j|k} = (A+BK)^j \hat{x}_{k+N|k} \\ \bar{\nu}\hat{u}_{k+j|k} = \bar{\nu}K(A+BK)^j \hat{x}_{k+N|k} \end{cases}$$

subtituing in (38),

$$\begin{aligned} P_x(A+BK)^j \hat{x}_{k+N|k} &\le q_x \\ P_u\bar{\nu}K(A+BK)^j \hat{x}_{k+N|k} &\le q_u \end{aligned}$$

stacking,

$$\underbrace{\begin{bmatrix} Px & 0 & \dots & 0 \\ P_u\bar{\nu}K & 0 & \dots & 0 \\ 0 & P_x & \dots & 0 \\ 0 & P_u\bar{\nu}K & \dots & 0 \\ \dots & \dots & \dots & \dots \end{bmatrix}}_{\mathcal{M}} \underbrace{\begin{bmatrix} (A+BK)^0 \\ (A+BK)^1 \\ \vdots \\ (A+BK)^{n-1} \end{bmatrix}}_{P_{x_N}} \hat{x}_{k+N|k} \le \underbrace{\begin{bmatrix} q_x \\ q_u \\ q_x \\ q_u \\ \vdots \end{bmatrix}}_{q_{x_N}}$$

where, $\mathcal{M} = \mathbf{I}_{n\times n} \otimes \begin{bmatrix} P_x \\ P_u\bar{\nu}K \end{bmatrix}$, $q_{x_N} = \mathbf{1}_{n\times 1} \otimes \begin{bmatrix} q_x \\ q_u \end{bmatrix}$

Therefore, for any $\hat{x}_{k+N|k} \in \mathcal{X}_f$,

$$\mathcal{X}_f = \{\hat{x}_{k+N|k} : P_{x_N}\hat{x}_{k+N|k} \le q_{x_N}\} \tag{39}$$

$\mathcal{X}_f$ is an admissible invariant set for mode-2 dynamics, and constraints $\mathcal{X}$ and $\mathcal{U}$, that is,

$$\begin{aligned} \hat{x}_{k+N|k} \in \mathcal{X}_f &\Rightarrow \hat{x}_{k+N|k} \in \mathcal{X} \\ \hat{u}_{k+N|k} = K(\hat{x}_{k+N|k}) &\in \mathcal{U} \end{aligned}$$

5. ALGORITHM

Given the attack scheme and conditions presented in the previous sections, the algorithm for the constrained MPC-TPC is as follows,

Algorithm 1. (Constrained MPC-TCP).

1: Set the probabilities $\bar{\nu}$ and $\bar{\gamma}$.
2: Test the bounds of $\bar{\nu}$ and $\bar{\gamma}$ using (37).
3: Compute the feasible set $\mathcal{X}_N$ defined in (24).
4: Initialize $x(0) \leftarrow x_0$.
5: **for** $k = 0 : \infty$ **do**
6: Measure the current attacked noisy output y_k.
7: Apply the constrained KF-TCP to obtain $\hat{x}_k$.
8: For the current $\hat{x}_k$, solve the QP problem (25).
9: Apply the first control input $\hat{u}^*_{k|k} = \kappa_N(\hat{x}_k)$.
10: Wait one time step.
11: Increment k.
12: **end for**

6. NUMERICAL EXAMPLE

This section presents examples of DoS attack over an unstable non-minimum phase system controlled by unconstrained and constrained MPC, and controlled by LQG-TCP, unconstrained and constrained MPC-TCP.

The unstable non-minimum phase system in discrete LTI state-space model sampled for $T_s = 0.1[s]$ is,

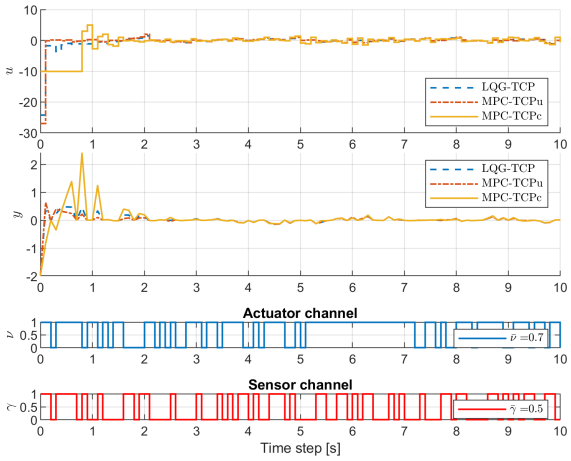
$$A = \begin{bmatrix} 1.12 & 0.20 \\ 0.11 & 1.01 \end{bmatrix}, \quad B = \begin{bmatrix} 0.11 \\ 0.06 \end{bmatrix}, \quad C = [-1\ \ 1]$$

with $w(k) \sim \mathcal{N}(0, Q_w)$, $z(k) \sim \mathcal{N}(0, R_z)$, $Q_w = 1\times10^{-4}\mathbf{I}_2$, $R_z = 1\times10^{-4}$. For the QP optimization problem, $Q = 1\times10^6\mathbf{I}_2$, $R = 1$, and $N = 10$. The constraints and initial value x_0 are, $|x| \le 2$, $|u| \le 10$, $x_0 = [0 \quad 1.5]^\intercal$, and the stabilizing mode-2 gain $K = [-11.03 \quad 11.02]$. The attack is $\nu \sim \mathcal{B}(0.8)$ and $\gamma \sim \mathcal{B}(0.5)$.

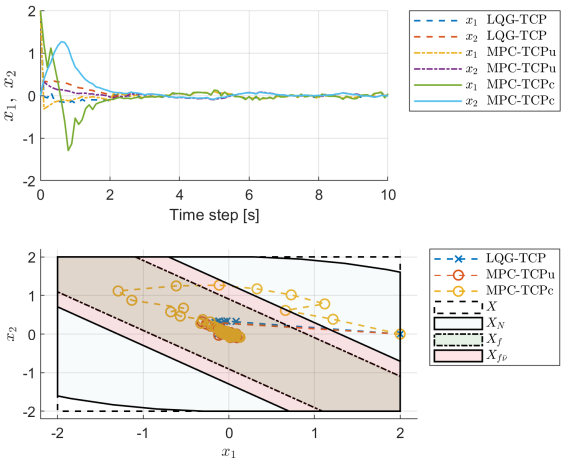
7. CONCLUSIONS

ACKNOWLEDGEMENTS

Place acknowledgments here.



(a) Input u_k and output y_k



(b) States behaviour and phase-plot

Fig. 3. LQG-TCP and MPC-TCP with DoS attack.

REFERENCES

Ali, S., Balushi, T.A., Nadir, Z., and Hussain, O.K. (2018). *Cyber Security for Cyber Physical Systems*. Springer International Publishing. doi:10.1007/978-3-319-75880-0.

Cheng, P., Zhang, H., and Chen, J. (2016). *Cyber Security for Industrial Control Systems: from the viewpoint of close-loop*. Taylor & Francis Ltd.

Imer, O.C., Yüksel, S., and Başar, T. (2006). Optimal control of LTI systems over unreliable communication links. *Automatica*, 42(9), 1429–1439. doi:10.1016/j.automatica.2006.03.011.

Löfberg, J. (2012). Oops! i cannot do it again: Testing for recursive feasibility in MPC. *Automatica*, 48(3), 550–555. doi:10.1016/j.automatica.2011.12.003.

Li, H. and Shi, Y. (2014). Network-based predictive control for constrained nonlinear systems with two-channel packet dropouts. *IEEE Transactions on Industrial Electronics*, 61(3), 1574–1582. doi:10.1109/tie.2013.2261039.

Li, P., Kang, Y., Zhao, Y.B., and Yuan, Z. (2018). Packet-based model predictive control for networked control systems with random packet losses. In *2018 IEEE Conference on Decision and Control (CDC)*. IEEE. doi:10.1109/cdc.2018.8619194.

Lucia, S., Kögel, M., Zometa, P., Quevedo, D.E., and Findeisen, R. (2016). Predictive control, embedded cyberphysical systems and systems of systems – a perspective. *Annual Reviews in Control*, 41, 193–207. doi:10.1016/j.arcontrol.2016.04.002.

Lun, Y.Z., D'Innocenzo, A., Smarra, F., Malavolta, I., and Benedetto, M.D.D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software*, 149, 174–216. doi:10.1016/j.jss.2018.12.006.

Pang, Z.H., Liu, G.P., Zhou, D., and Sun, D. (2019). *Networked Predictive Control of Systems with Communication Constraints and Cyber Attacks*. Springer Singapore. doi:10.1007/978-981-13-0520-7.

Quevedo, D.E., Ahlen, A., and Johansson, K.H. (2013). State estimation over sensor networks with correlated wireless fading channels. *IEEE Transactions on Automatic Control*, 58(3), 581–593. doi:10.1109/tac.2012.2212515.

Quevedo, D.E., Mishra, P.K., Findeisen, R., and Chatterjee, D. (2015). A stochastic model predictive controller for systems with unreliable communications. *IFAC-PapersOnLine*, 48(23), 57–64. doi:10.1016/j.ifacol.2015.11.262.

Quevedo, D.E. and Nešić, D. (2012). Robust stability of packetized predictive control of nonlinear systems with disturbances and markovian packet losses. *Automatica*, 48(8), 1803–1811. doi:10.1016/j.automatica.2012.05.046.

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., and Sastry, S.S. (2007). Foundations of control and estimation over lossy networks. *Proceedings of the IEEE*, 95(1), 163–187. doi:10.1109/jproc.2006.887306.

Shi, L., Epstein, M., and Murray, R.M. (2010). Kalman filtering over a packet-dropping network: A probabilistic perspective. *IEEE Transactions on Automatic Control*, 55(3), 594–604. doi:10.1109/tac.2009.2039236.

Simon, D. (2010). Kalman filtering with state constraints: a survey of linear and nonlinear algorithms. *IET Control Theory & Applications*, 4(8), 1303–1318. doi:10.1049/iet-cta.2009.0032.

Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M., and Sastry, S. (2004). Kalman filtering with intermittent observations. *IEEE Transactions on Automatic Control*, 49(9), 1453–1464. doi:10.1109/tac.2004.834121.

Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., and Sastry, S. (2005). Optimal control with unreliable communication: the TCP case. In *Proceedings of the 2005, American Control Conference, 2005.* IEEE. doi:10.1109/acc.2005.1470488.

Tabbara, M. and Nesic, D. (2008). Input–output stability of networked control systems with stochastic protocols and channels. *IEEE Transactions on Automatic Control*, 53(5), 1160–1175. doi:10.1109/tac.2008.923691.

te Yu, J. and Fu, L.C. (2015). An optimal compensation framework for linear quadratic gaussian control over lossy networks. *IEEE Transactions on Automatic Control*, 60(10), 2692–2697. doi:10.1109/tac.2015.2406977.

Teixeira, A., Sou, K.C., Sandberg, H., and Johansson, K.H. (2015). Secure control systems: A quantitative risk management approach. *IEEE Control Systems*, 35(1),

24–45. doi:10.1109/mcs.2014.2364709.
Wu, J., Shi, L., Xie, L., and Johansson, K.H. (2015). An improved stability condition for kalman filtering with bounded markovian packet losses. *Automatica*, 62, 32–38. doi:10.1016/j.automatica.2015.09.005.

Appendix A. NOTES

(1) If Xf is bigger, does it improve the stability?. My first thought was yes, that is why I introduced the attack ν in mode-2, and named it as $\mathcal{X}_{f_\nu}$.
(2) Should I put the derivation of the equations in Appendix?.
(3) One of the drawbacks of the constrained MPC-TCP algorithm was the unfeasibility when I started the simulation in an extreme of $\mathcal{X}_N$ (e.g $x(0) = [2; 1.5]$), that is why I introduced a constrained Kalman Filter to the predicted states. It really improved the results, but because of the soft constraint sometimes the states violate the constraints, specially in the transient zone. I'm sure that with a proper MHE-TCP this problem can be solved.
(4) I wanted to obtain the critical probabilities ν_c and γ_c solving the following LMI in Matlab (for γ is similar),
$$\nu_c = \arg\min_{\nu} \Phi_\nu(Y, Z) > 0,\ 0 \leq Y \leq I$$
$$\Phi = \begin{bmatrix} Y & \sqrt{\nu}(YA^\intercal + ZB^\intercal) & \sqrt{1-\nu}YA^\intercal \\ \sqrt{\nu}(AY + BZ^\intercal) & Y & 0 \\ \sqrt{1-\nu}AY & 0 & Y \end{bmatrix}$$
where $Z = X^{-1}K, Y = X^{-1}, X = P_k = P, K = -AXC^\intercal(CXC^\intercal + R_z)^{-1}$. Which are formulated in Sinopoli et al. (2005) p.5, but I could not obtain a satisfactory result. I think the problem is the formulation in Matlab. I attached the script in the root of the paper folder as `LMI.m` in case you want to take a look. Do you think is worth trying to solve those values?, considering that those conditions are for the unconstrained case.
(5) I made several simulations for different $x(0)$ and $\bar{\nu}, \bar{\gamma}$. I uploaded them in the folder '`figure`' with different subfolders code-named as follows:
`x0(1.5, 0.5) 100k nu0.8,gamma0.5`
`x(0)` $= [$`1.5 0.5`$]^\intercal$, 100k=100 steps, $\bar{\nu} = 0.8, \bar{\gamma} = 0.5$. Please take a look of them and let me know which ones would be good examples.
(6) There is a special case `x0(1.5, 0.5) 100k nu0.3,gamma0.3` where the stability bounds of the LQG-TCP are not fulfilled but the constrained MPC-TCP still can managed with a lot of effort.
(7) Also, I made a simulation with 1000 realizations and plot the mean values in a folder called '`Mean-1000r`' in case it can be mentioned.
(8) I wrote down the monotonic descent for the closed-loop system in the conventional MPC, and I used the same approach for the MPC-TCP, is it ok?. Should I write down for the tail of the solution $\mathbf{u}_k^*$ as you did in your lecture notes?. On the other hand, I found a paper where the recursive feasibility can be tested using Farka's lemma, Löfberg (2012), do you think is a good way to test recursive feasibility?.
(9) introduce zero-input strategy Schenato et al. (2007); te Yu and Fu (2015)
(10) know attack, unknown attack strategyLi et al. (2018)