The University Of Sheffield.

Study of the robustness and stability of Model Predictive Control (MPC) against cyber-attacks

by

Paulo Roberto Loma Marconi

supervised by

Dr. Paul Trodden

Submitted to the faculty of:

Automatic Control and Systems Engineering

at

The University of Sheffield

in partial fulfilment of the requirements for the degree of:

MSc in Advanced Control and Systems Engineering

September 9, 2019

EXECUTIVE SUMMARY

INTRODUCTION / BACKGROUND

The advances in computation, communication, and control systems latter the necessity to study and secure the data of the controllers, actuators and sensors in the Industrial Control Systems. Cyber-security form the viewpoint of automatic control researches the vulnerabilities of control systems against cyber-attacks.

AIMS AND OBJECTIVES

The aim is to study the robustness and stability of control systems based on Model Predictive Control (MPC) against False Data Injection (FDI) and Denial of Service (DoS) attacks from the viewpoint of control loop.

The objectives are to review the related work in the literature, establish the framework to be studied, determine the types of cyber-attacks to be used in the evaluation, analyse the robustness and stability of the case-study, evaluate the performance of the case-study by software simulation, and implement an attack rejection method against DoS attack.

ACHIEVEMENTS

The literature review helps to select the type of cyber-attacks, and overview MPC based approaches against FDI and DoS attacks. Consequently, the robustness and stability of MPC against these attacks are analysed by software simulation. A DoS rejection method for the unconstrained and constrained MPC is proposed with a modified time-varying Kalman Filter for a TCP communication channel.

CONCLUSIONS / RECOMMENDATIONS

The stability of MPC is not guaranteed against the DoS attack, because of controllability and observability losses of the system. With FDI attack, the system is guaranteed if the attack is a scalar type. A reject method against DoS attack based on MPC is proposed over the TCP channel. In the unconstrained and constrained MPC method proposed, the stability is guaranteed with dual-mode approach.

ABSTRACT

The growing of the Cyber-Physical Systems (CPS) thanks to the advances in computation, communication, and control systems latter the necessity of study and secure the data of the controllers, actuators and sensors in the Networked Control Systems (NCS).

This dissertation aims to study the robustness and stability of control systems based on Model Predictive Control (MPC) against a Denial of Service (DoS) attack over the actuation and sensor channel, and a False Data Injection (FDI) attack over the sensor channel in a TCP communication channel. The DoS attack has a Bernoulli packet drop model that forces the packet loss on both channels. The FDI attack corrupts the observation data and the state estimation process. For the FDI evaluation, a detectable attack and an undetectable attack are tested using the residual detection method.

Based on a Linear Quadratic Gaussian approach for the TCP channel (LQG-TCP), a rejection method for the unconstrained and constrained MPC case (MPC-TCP) is proposed. It was proved that the optimal solution of the unconstrained MPC-TCP is equivalent to the optimal solution in the LQG-TCP method. The robustness and stability of all the cases are evaluated via software simulation.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Paul Trodden, for his support and guidance from the beginning of the project. Thanks to his constant feedback I was able to explore possible solutions and improve the results.

Also, I would like to thank Dr. John Rossiter for taking the time to review this dissertation as my second reader.

Finally, a special thanks to my family for their support.

To my family. Gerardo, Silvia, and Pricila . . .

Contents

List of Figures

Chapter 1

Introduction

1.1 Background and Motivation

In the industry, controllers, actuators, and sensors are becoming more ubiquitous thanks to the advances in information, computation, and communication technologies. All of those devices are co-designed, connected and communicated through a networked architecture called Cyber-Physical System (CPS) [1]. Within this framework, the Networked Control System (NCS) allows the control design to be more flexible, robust, and scalable, but at the same time there is the necessity to secure the data of those components [2].

Cyber-security from the viewpoint of control theory, researches the vulnerabilities of the NCS against cyber-attacks that may reduce the performance or become potential dangers for the entire CPS, and proposes defensive strategies that mitigate or reject those attacks [2, 3].

The Stuxnet cyber-attack on an Iranian nuclear plant in 2011, is a clear example of an attack that targeted the control system loop through the Programmable Logic Controllers (PLC) installed in the system. Exploiting four zero-day[1] vulnerabilities, the Stuxnet malware that remained undetectable, was able to collect information from different measurements channels. Replacing them with false data, and inserting corrupted actuation signals, the fast-spinning centrifuges were led to unstable states that eventually damaged the equipment severely and permanently [4].

[1] A zero-day is a vulnerability that remains unknown until the interested vendor learns about it and fixes it.

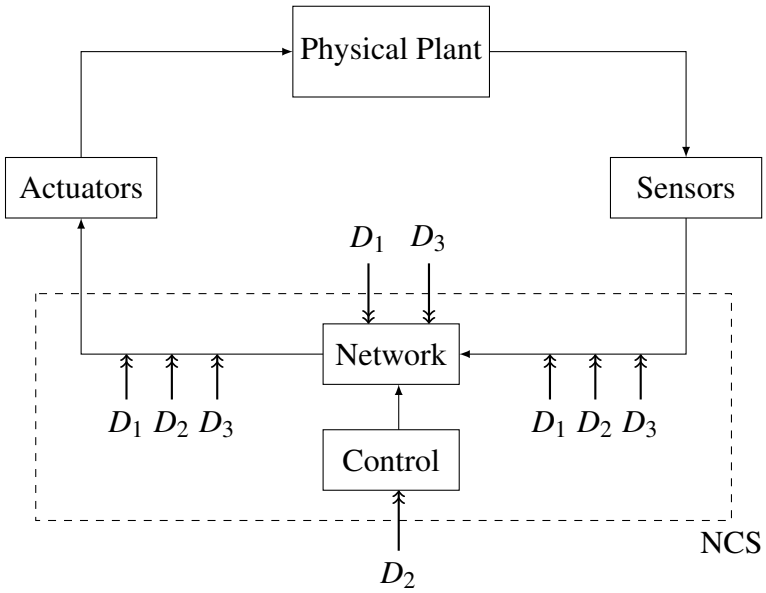
The motivation of this project is that, despite the significant amount of research that was developed around cyber-security on NCS during the last ten years [1], this area is relatively new, and there are many control algorithms to be developed, improved and studied. Model Predictive Control (MPC) provides a reason to tackle some of those challenges, due to the capacity of handling constraints, preview information, and non-linearities. Stuxnet, and other attacks, proved that the protection by software anti-virus solutions are not sufficient. In addition, CPS are getting more complex and cyber-attacks more sophisticated. Therefore, in the essence of control design, a robust protection of a system can be a cyber-secure MPC controller than can handle many types of cyber-attacks, physical faults, and disturbances.

1.2 Problem definition

Control theory developed many fault tolerant and disturbance rejection algorithms, and they can handle cyber-attacks in some way. However, a fault, and a cyber-attack are different conceptually. While a fault is commonly a physical event that is constrained by the system dynamics, it does not have a malicious intention like a cyber-attack does. Furthermore, a cyber-attacks can be coordinated, remain undetected, and is not constrained by the system dynamics [5].

Even though in CPS there are different types of cyber-attacks [1], for the NCS context that is used in this project, three distinctive groups can be listed: Disclosure, Deception, and Disruption, also called as DDD attacks [5]. Fig. 1.1 shows these can be located and implemented. Notice that they can be independent of each other, mixed, and triggered at the same time.

A Disclosure attack gains access to the communication channels and obtains useful information about the system [6, 5]. A Deception attack corrupts the signal of the sensors or actuators by introducing false data in order to force the system to an undesired state, e.g. False Data Injection (FDI) attack [7, 8, 9]. And a Disruption attack, also called Denial of Service (DoS), forces the loss of information through the communication channels that potentially derive the plant to an unstable region [10, 11].



D_1 = Disclousure (confidentiality) attack
D_2 = Deception (integrity - FDI) attack
D_3 = Disruption (availability - DoS) attack

Figure 1.1: Location of DDD attacks on NCS.

1.3 Aims and Objectives

This project aims to study the robustness and stability of control systems based on constrained Model Predictive Control (MPC) against two types of common DDD cyber-attacks over the communication channels, which are FDI and DoS attack.

In order to fulfil the aim, the following objectives were proposed:

- To review the literature of cyber-attacks on Control Systems.
- To establish the framework of study of the MPC system.
- To determine the types of cyber-attacks to be used in the evaluation.
- To formulate the MPC scheme with the selected cyber-attacks.
- To analyse the robustness and stability of the case-study.
- To evaluate the performance of the case-study by software simulation.
- To propose an attack detection/rejection method and a resilient control strategy for MPC.

1.4 Overview of the report

This project presents a study of robustness and stability of an unstable system controlled by constrained MPC which is attacked by FDI and DoS over the communication channels. Results are compared with Linear Quadratic Gaussian (LQG) controller. Also, a rejection method against DoS attack is implemented based on a modified LQG algorithm.

Chapter 2 is focused on the literature review that summarizes the state of art of CPS related with automatic control, and cyber-security from the MPC perspective. In addition, publications related to MPC, FDI and DoS attacks are mentioned.

Chapter 3 is dedicated to the background theory of MPC. The unconstrained case, and constrained case are reviewed, and the stability conditions in both cases are explained.

Chapter 4 presents the DoS attack scheme over MPC. The LQG approach to handle the DoS attack, and a detailed derivation of the proposed DoS rejection method based on MPC.

Chapter 5 presents the FDI attack scheme over MPC. The residual detection method, the detectability and undetectability conditions.

Chapter 6 summarizes the contributions of the project highlighting the completed objectives, and a brief comment about the future work.

Chapter 2

Literature review

The first part of this literature review presents a summary of the state of art of cyber-attacks on CPS, and some work related to cyber-security from the viewpoint of automatic control. The second part, and third part are focused on different cyber-attacks, some research related to the analysis of robustness and stability of control design against cyber-attacks, and finally, some detection and rejection method for FDI and DoS attacks that are used in this dissertation.

2.1 Cyber-security on CPS

A CPS can be defined as a whole architecture that integrates the computation and communication technologies with physical systems that interact with humans at different levels. Also, called system of systems, this architecture can be very complex and flexible due to the integration of hardware and software resources for control and monitoring purposes [1, 12]. NCS is a consequence of this integration due to the shared communication between the actuators, sensors, and controllers with the rest of the components [2].

In [12], cyber-security on CPS is studied as a whole architecture, and the functions of each component are described in detail, such as, Wireless Sensor Network (WSN), Embedded Systems, Real Time Systems, and NCS. The authors describe different types of attack and organize the related research work for each component. However, it covers control theory only on the surface without giving details. This book is a general reference to find related work of cyber-attacks by the CPS components.

Related to cyber-security on CPS from the viewpoint of automatic control, [1] is a state-of-art survey that classifies and analyses the publications of the last ten years, according to different categories such as, application field, type of controller, or state estimation, just to mention a few. In the interest of this project, the categories reviewed were: plant model, process and measurement noise, state estimation, detection methods, type of controllers, and DDD attacks. It was found that MPC is not categorized as a type of controller that handles cyber-attacks, but it is listed through some papers related to event-triggered and self-triggered [13]. In contrast, the attacks of interest in this project, DoS and FDI, are two of the most studied areas that have large amount of research. Within that list, two publications served as the basis of this project, which are [9] and [14].

From the MPC viewpoint, [15] 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.

2.2 DoS attacks

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 [16], 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 [17] and [14, 18], the authors define an optimal LQG controller merged with the modified Kalman filter in [16] 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, [19] proposes a stochastic MPC approach that considers a stochastic cost function, and it is compared with a deterministic cost function in [20]. 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, 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.

2.3 FDI attacks

FDI are strong attacks that can corrupt the data of the communication channel with little knowledge of the plant. One of the objectives of this type of attack is to maximize the damage while remains undetectable. In [8], the authors analyse an FDI attack in a discrete Linear Time Invariant (LTI) system with an LQG controller by assuming there is a failure packet-loss detector in the measurement channel. It is proposed sufficient conditions under which the attack destabilizes the system while bypassing the detection. The limitation is the need of a failure detector in the system but a resilience method is proposed to handle the attack.

The study of FDI attacks over the state estimation, [9] shows that the residual detection algorithm is not enough when the attacker knows about the measurement matrix of the system. Also, the authors analyse the attack impact in the measurement channel considering a static estimation process, an analysis with dynamic estimation is out of the scope. Complementary to [9], a time-invariant state estimator is proposed in [21] as a method to find insecurity conditions under which FDI attacks are undetectable proving that this method is more robust than the residual detection.

From the viewpoint of MPC, in [2] is studied the FDI attacks on NCS with delay transportation, and disturbances. In a specific chapter, the authors describe secure networked predictive control for UDP channel based on a secure UDP receiver that verifies the integrity of the information. However, this method uses an encryption algorithm as the secure UDP receiver. [22] proposes an FDI attack detection and rejection method based on MPC. The false data is injected into the control variable, if the attack is de-

tected, a generic state-feedback backup controller takes control of the system. The optimal solution of the scheme is given by the integration of the main controller and the backup controller in a single linear quadratic MPC problem. If there is no attack, the optimal solution is given only by the main controller, if there is an attack, the optimal solution is constrained by both dynamics. The downside is that the backup controller is an LQR controller with no stability guaranty. A moving-window attack-detection based on MPC is proposed in [23], it uses past samples of the corrupted states and compared them with nominal past samples in a temporal sliding window. The recorded information over such window is used to obtain a probabilistic index that guarantees the integrity of the information and make a decision about the existence of attacks. The decision is made by hypothesis testing in the window of observation. This method has some similarities with the Moving Horizon Estimation (MHE) technique.

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.

Chapter 3

Background theory

3.1 Model Predicitve Control

MPC is an optimization-based control strategy that solves a Finite-Horizon Linear Quadratic (FH-LQ) problem subject to constraints. A model of predicted states based on the system dynamics is used to minimize an objective function that satisfies constraints given the actual state. The obtained solution is a sequence of open-loop controls from which only the first one is implemented on the system, inducing feedback. The rest of the sequence is discarded and the process is repeated for the next sampling time, this method is often called Receding-Horizon (RH) principle. Advantages of MPC against other control strategies are the handling of constraints, and non-linearities [24, 25].

3.2 Unconstrained MPC

Consider the following discrete-time LTI state-space system,

$$\begin{aligned} x(k+1) &= A\,x(k) + B\,u(k) \\ y(k) &= C\,x(k), \quad k = 0,1,2,\ldots \end{aligned} \tag{3.1}$$

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, B, C, are the state, input, and output matrices. A, B, C are known, no uncertainties in the model, disturbances, and noise. $x(k)$ is available at each sampling time k.

3.2.1 Problem formulation

The objective is to regulate $x \to 0$ as $k \to \infty$ while minimizing the following cost function,

$$\begin{aligned} J_N(x(k),\mathbf{u}(k)) &= \sum_{j=0}^{N-1} \left(\|x(k+j|k)\|_Q^2 + \|u(k+j|k)\|_R^2 \right) + \|x(k+N|k)\|_P^2 \\ &= \sum_{j=0}^{N-1} (x^\intercal(k+j|k)\, Q\, x(k+j|k) + u^\intercal(k+j|k)\, R\, u(k+j|k)) \\ &\qquad + x^\intercal(k+N|k)\, P\, x(k+N|k) \end{aligned} \tag{3.2}$$

subject to,

$$\begin{aligned} x(k+1+j|k) &= A\, x(k+j|k) + B\, u(k+j|k) \\ x(k|k) &= x(k) \end{aligned} \tag{3.3}$$

for $j = 0, 1, 2, \ldots, N-1$

where $Q \in \mathbb{R}^{n\times n}$ and $R \in \mathbb{R}^{m\times m}$ are the state penalty, and input penalty matrices. $P \in \mathbb{R}^{n\times n}$ is the terminal cost matrix, $N \in \mathbb{N}$ is the horizon length, k is the sampling time, and $(k+j|k)$ can be defined as the next $(k+j)$ value given k.

With the value function defined as,

$$J_N^*(x(k),\mathbf{u}(k)) = \min_{u(k)} J_N(x(k),\mathbf{u}(k)) \tag{3.4}$$

the optimal control sequence is,

$$\begin{aligned} \mathbf{u}^*(k) &= \arg\min_{u(k)} J_N^*(x(k),\mathbf{u}(k)) \\ &= \{u^*(k|k), u^*(k+1|k), \ldots, u^*(k+N-1|k)\} \end{aligned} \tag{3.5}$$

3.2.2 QP solution

In order to solve (3.2) by optimization approach, the following predictions matrices are formulated. Setting $x(k) = x(k|k)$, and $u(k) = u(k|k)$ and applying the model (3.1)

recursively,

$$\begin{aligned}
x(k+1|k) &= A\,x(k) + B\,u(k) \\
x(k+2|k) &= A\,x(k+1|k) + B\,u(k+1|k) \\
&= A^2\,x(k) + AB\,u(k|k) + B\,u(k+1|k) \\
\vdots \quad &= \quad \vdots \\
x(k+N|k) &= A\,x(k+N-1|k) + B\,u(k+N-1|k) \\
&= A^N\,x(k) + A^{N-1}B\,u(k|k) + \cdots + B\,u(k+N-1|k)
\end{aligned}$$

stacking,

$$\underbrace{\begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix}}_{\mathbf{x}(k)} = \underbrace{\begin{bmatrix} A \\ A^2 \\ \vdots \\ A^N \end{bmatrix}}_{F} + \underbrace{\begin{bmatrix} B & 0 & \dots & 0 \\ AB & B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A^{N-1}B & A^{N-2}B & \dots & B \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} u(k|k) \\ u(k+1|k) \\ \vdots \\ u(k+N-1|k) \end{bmatrix}}_{\mathbf{u}(k)} \tag{3.6}$$

the predicted equality constraint is,

$$\mathbf{x}(k) = F\,x(k) + G\,\mathbf{u}(k) \tag{3.7}$$

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

Rewriting the cost function (3.2) as,

$$x^{\mathsf{T}}(k|k)\ Q\ x(k|k) + \begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix}^{\mathsf{T}} \underbrace{\begin{bmatrix} Q & 0 & \dots & 0 \\ 0 & Q & \ddots & \vdots \\ \vdots & \ddots & Q & 0 \\ 0 & \dots & 0 & P \end{bmatrix}}_{\tilde{Q}} \begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix}$$
$$+ \begin{bmatrix} u(k|k) \\ u(k+1|k) \\ \vdots \\ u(k+N-1|k) \end{bmatrix}^{\mathsf{T}} \underbrace{\begin{bmatrix} R & 0 & \dots & 0 \\ 0 & R & \ddots & \vdots \\ \vdots & \ddots & R & 0 \\ 0 & \dots & 0 & R \end{bmatrix}}_{\tilde{R}} \begin{bmatrix} u(k|k) \\ u(k+1|k) \\ \vdots \\ u(k+N-1|k) \end{bmatrix} \tag{3.8}$$

Therefore, with $x(k|k) = x(k)$, now the problem to minimize,

$$J_N(x(k), \mathbf{u}(k)) = x^{\mathsf{T}}(k)\ Q\ x(k) + \mathbf{x}^{\mathsf{T}}(k)\ \tilde{Q}\ \mathbf{x}(k) + \mathbf{u}^{\mathsf{T}}(k)\ \tilde{R}\ \mathbf{u}(k) \tag{3.9}$$

subject to,

$$\mathbf{x}(k) = F\ x(k) + G\ \mathbf{u}(k)$$

Substituting the predicted equality constraint (3.7) in (3.9),

$$J_N(x(k), \mathbf{u}(k)) = x^{\mathsf{T}}(k) Q x(k) + (F x(k) + G\mathbf{u}(k))^{\mathsf{T}} \tilde{Q} (F x(k) + G\mathbf{u}(k)) + \mathbf{u}^{\mathsf{T}}(k)\ \tilde{R}\mathbf{u}(k)$$

omitting (k) only for the algebraic operations,

$$
\begin{aligned}
&= x^\intercal Q x + [(Fx)^\intercal + (G\mathbf{u})^\intercal]\tilde{Q}(Fx + G\mathbf{u}) + \mathbf{u}^\intercal \tilde{R}\mathbf{u} \\
&= x^\intercal Q x + (Fx)^\intercal \tilde{Q} F x + (Fx)^\intercal \tilde{Q} G\mathbf{u} + (G\mathbf{u})^\intercal \tilde{Q} F x + (G\mathbf{u})^\intercal \tilde{Q} G\mathbf{u} + \mathbf{u}^\intercal\, \tilde{R}\mathbf{u} \\
&= \underbrace{x^\intercal Q x + x^\intercal F^\intercal \tilde{Q} F x} + \underbrace{x^\intercal F^\intercal \tilde{Q} G\mathbf{u} + \mathbf{u}^\intercal G^\intercal \tilde{Q} F x} + \underbrace{\mathbf{u}^\intercal G^\intercal \tilde{Q} G\mathbf{u} + \mathbf{u}^\intercal \tilde{R}\mathbf{u}} \\
&= x^\intercal (Q + F^\intercal \tilde{Q} F) x \quad + \quad 2\mathbf{u}^\intercal G^\intercal \tilde{Q} F x \qquad\quad + \mathbf{u}^\intercal (G^\intercal \tilde{Q} G + \tilde{R})\mathbf{u} \\
&= x^\intercal (Q + F^\intercal \tilde{Q} F) x + (2G^\intercal \tilde{Q} F x)^\intercal \mathbf{u} + \mathbf{u}^\intercal (G^\intercal \tilde{Q} G + \tilde{R})\mathbf{u} \\
&= x^\intercal \underbrace{(Q + F^\intercal \tilde{Q} F)}_{M} x + (\underbrace{2G^\intercal \tilde{Q} F}_{L} x)^\intercal \mathbf{u} + \frac{1}{2}\left[\mathbf{u}^\intercal \underbrace{2(G^\intercal \tilde{Q} G + \tilde{R})}_{H}\mathbf{u}\right] \\
&= \frac{1}{2}\mathbf{u}(k)^\intercal\, H\, \mathbf{u}(k) + \underbrace{(L\, x(k))^\intercal}_{c^\intercal}\, \mathbf{u}(k) + \underbrace{x(k)^\intercal\, M\, x(k)}_{\alpha}
\end{aligned}
$$

Finally, the cost function in QP compact form is,

$$
J_N(x(k), \mathbf{u}(k)) = \frac{1}{2}\mathbf{u}(k)^\intercal\, H\, \mathbf{u}(k) + c^\intercal\, \mathbf{u}(k) + \alpha \tag{3.10}
$$

where,

$$
\begin{aligned}
H &= 2(G^\intercal \tilde{Q} G + \tilde{R}) \\
c &= L\, x(k), \quad L = 2G^\intercal \tilde{Q} F \\
\alpha &= x^\intercal(k)\, M\, x(k), \quad M = Q + F^\intercal \tilde{Q} F
\end{aligned} \tag{3.11}
$$

Minimizing with the gradient and solving for $\mathbf{u}^*(k)$,

$$
\begin{aligned}
J_N^*(x(k), \mathbf{u}(k)) &= \min_{\mathbf{u}(k)}\ \frac{1}{2}\mathbf{u}(k)^\intercal\, H\, \mathbf{u}(k) + c^\intercal\, \mathbf{u} + \alpha \\
\nabla_{\mathbf{u}}\, J_N^*(x(k), \mathbf{u}(k)) &= 0 \\
H\, \mathbf{u}^*(k) + c &= 0 \\
\mathbf{u}^*(k) &= -H^{-1}\, c
\end{aligned}
$$

the optimal solution results in,

$$
\mathbf{u}^*(k) = -H^{-1}\, L\, x(k) \tag{3.12}
$$

where that $Q \succeq,\ P \succeq 0$ are positive semidefinite convex, and $R \succ 0$ is definite convex,

such that $H \succ 0$. The optimal solution $\mathbf{u}^*(k)$ for any $x(k)$ is unique if $H \succ 0$ is invertible.

Applying the RH principle means that only the **first** control input of the vector (3.12) is applied to the real system. That is,

$$\begin{bmatrix} u^*(k) \\ u^*(k+1) \\ \vdots \\ u^*(k+N-1) \end{bmatrix} = \begin{bmatrix} I & 0 & 0 & \dots & 0 \\ 0 & I & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & I \end{bmatrix} (-H^{-1}\, L)x(k)$$

$$u^*(k) = K_N\, x(k) \tag{3.13}$$

$$K_N = [I \quad 0 \quad 0 \quad \dots \quad 0](-H^{-1}\, L) \tag{3.14}$$

Notice that $u^*(k)$ is an explicit linear time-invariant control law because H and L do not depend on $x(k)$.

3.2.3 Stability

To guarantee the closed-loop stability of the system, the dual-mode MPC approach is used, where the terminal cost matrix P is calculated to mimic an infinite horizon, such that,

$$x^\intercal(k+N|k)\; P\, x(k+N|k) = \sum_{j=N}^{\infty} (x^\intercal(k+j|k)\; Q\, x(k+j|k) + u^\intercal(k+j|k)\; R\, u(k+j|k))$$

Using the following conditions,

- (A,B) is stabilizable
- $Q \succeq 0,\ R \succ 0$
- $(Q^{1/2},A)$ is observable

The dual-mode MPC approach establishes that, there is a unique $P \succ 0$ that satisfies the Lyapunov equation for some stabilizing gain K,

$$(A+B\,K)^\intercal\; P\; (A+B\,K) - P = -(Q + K^\intercal\; R\; K) \tag{3.15}$$

where K is the mode-2 control law that can be any value as long as $(A+B\,K)$ is stable.

Therefore, the control law (3.13) is asymptotically stabilizing. Moreover, P modifies only $\tilde{Q}$, which means that the optimal solution (3.12) remains explicit.

Mode-2 is used only for stability and performance, it is not applied to the plant. If $K = K_\infty$, where K_∞ is an infinite-horizon LQ control, the control law (3.13) is known as optimal LQ-MPC. On the other hand, if $K \neq K_\infty \rightarrow K_N \neq K_\infty$ is known as LQ-MPC suboptimal.

3.3 Constrained MPC

3.3.1 Problem Formulation

Consider the same LTI of (3.1). For the constrained case, the objective is to regulate $x \rightarrow 0$ as $k \rightarrow \infty$ while minimizing the following cost function,

$$\begin{aligned} J_N(x(k),\mathbf{u}(k)) &= \sum_{j=0}^{N-1} \left(\|x(k+j|k)\|_Q^2 + \|u(k+j|k)\|_R^2 \right) + \|x(k+N|k)\|_P^2 \\ &= \sum_{j=0}^{N-1} \left(x^\intercal(k+j|k)\, Q\, x(k+j|k) + u^\intercal(k+j|k)\, R\, u(k+j|k) \right) \\ &\qquad + x^\intercal(k+N|k)\, P\, x(k+N|k) \end{aligned} \tag{3.16}$$

subject to,

$$x(k+1+j|k) = A\, x(k+j|k) + B\, u(k+j|k)$$

$$x(k|k) = x(k)$$

$$P_x\, x(k+j|k) \leq q_x \tag{3.17}$$

$$P_u\, u(k+j|k) \leq q_u \tag{3.18}$$

$$P_{x_N}\, x(k+N|k) \leq q_{x_N} \tag{3.19}$$

for $j = 0, 1, 2, \ldots, N-1$

where the linear inequalities constraints are presented in a compact form as follows.

Defining the state constraints as,

$$\begin{cases} P_x\, x(k+j|k) & \leq q_x \\ P_{x_N}\, x(k+N|k) & \leq q_{x_N} \end{cases}$$

stacking,

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

results in,

$$\tilde{P}_x\, \mathbf{x}(k) \leq \tilde{q}_x - \tilde{P_{x_0}}\, x(k) \tag{3.20}$$

The input constraints are,

$$P_u\, u(k+j|k) \leq q_u$$

stacking,

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

results in,

$$\tilde{P}_u\, \mathbf{u}(k) \leq \tilde{q}_u \tag{3.21}$$

where $P_x,\ q_x,\ P_u$ and q_u are defined by box constraints, such that,

$$\underbrace{\begin{bmatrix} +\mathbf{I}_{n\times n} \\ -\mathbf{I}_{n\times n} \end{bmatrix}}_{P_x} x(k+j|k) \leq \underbrace{\begin{bmatrix} +x_{max} \\ -x_{min} \end{bmatrix}}_{q_x} \tag{3.22}$$

$$\underbrace{\begin{bmatrix} +\mathbf{I}_{m\times m} \\ -\mathbf{I}_{m\times m} \end{bmatrix}}_{P_u} u(k+j|k) \leq \underbrace{\begin{bmatrix} +u_{max} \\ -u_{min} \end{bmatrix}}_{q_x} \tag{3.23}$$

Note that $P_{x_N},\ q_{x_N}$ are the terminal constraints that are characterized in the stability section.

Constructing inequality constraints in a compact form,

$$\begin{cases} \tilde{P}_u\ \mathbf{u}(k) & \leq \tilde{q}_u \\ \tilde{P}_x\ \mathbf{x}(k) & \leq \tilde{q}_x - \tilde{P}_{x_0}\ x(k) \end{cases}$$

using (3.7) to eliminate $\mathbf{x}(k)$,

$$\begin{aligned} \tilde{P}_x(F\ x(k) + G\ \mathbf{u}(k)) &\leq \tilde{q}_x - \tilde{P}_{x_0}\ x(k) \\ \tilde{P}_x\ G\ \mathbf{u}(k) &\leq \tilde{q}_x + (-\tilde{P}_{x_0} - \tilde{P}_x\ F)\ x(k) \end{aligned}$$

stacking,

$$\underbrace{\begin{bmatrix} \tilde{P}_u \\ \tilde{P}_x\ G \end{bmatrix}}_{P_c} \mathbf{u}(k) \leq \underbrace{\begin{bmatrix} \tilde{q}_u \\ \tilde{q}_x \end{bmatrix}}_{q_c} + \underbrace{\begin{bmatrix} 0 \\ -\tilde{P}_{x_0} - \tilde{P}_x\ F \end{bmatrix}}_{S_c} x(k) \tag{3.24}$$

therefore,

$$P_c\ \mathbf{u}(k) \leq q_c + S_c\ x(k) \tag{3.25}$$

3.3.2 QP solution

The LQ-MPC problem in constrained compact form is to minimize,

$$J_N^*(x(k), \mathbf{u}(k)) = \min_{\mathbf{u}(k)}\ \frac{1}{2}\mathbf{u}(k)^\intercal\ H\ \mathbf{u}(k) + c^\intercal\ \mathbf{u}(k) + \alpha \tag{3.26}$$

subject to,

$$P_c\ \mathbf{u}(k) \leq q_c + S_c\ x(k)$$

where the optimal solution can be defined as,

$$\begin{aligned}\mathbf{u}^*(k) &= \arg\min_{u(k)} \left\{ \frac{1}{2}\mathbf{u}(k)^\intercal H \mathbf{u}(k) + x^\intercal(k) L^\intercal \mathbf{u}(k) + \alpha \ : P_c\mathbf{u} \leq q_c + S_c x(k) \right\} \\ &= \{u^*(k|k), u^*(k+1|k), \ldots, u^*(k+N-1|k)\}\end{aligned} \tag{3.27}$$

with the same definitions of H, L and α of the unconstrained case in (3.9).

Applying the RH principle leads to the implicit nonlinear time-variant control law,

$$u^*(k|k) = \kappa_N\left(x(k)\right) \tag{3.28}$$

and it is defined for $x(k) \in \mathcal{X}_N$, where $\mathcal{X}_N$ is the feasibility region.

The feasibility region $\mathcal{X}_N$ is the set of states for which the cost function (3.16) has a solution, and is defined as,

$$\mathcal{X}_N = \{x(k) : \mathcal{U}_N(x(k)) \neq 0\} \tag{3.29}$$

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

$$\mathcal{U}_N(x(k)) = \{\mathbf{u}(k) : P_c\ \mathbf{u}(k) \leq q_c + S_c\ x(k)\} \tag{3.30}$$

Also, the input constraint set is,

$$\mathcal{U} = \{u(k) : P_u\ u(k) \leq q_u\} \subseteq \mathbb{R}^m \tag{3.31}$$

the state constraint set is,

$$\mathcal{X} = \{x(k) : P_x\ x(k) \leq q_x\} \subseteq \mathbb{R}^n \tag{3.32}$$

and the terminal constraint set is,

$$\mathcal{X}_f = \{x(k) : P_{x_N}\, x(k) \leq q_{x_N}\} \subseteq \mathbb{R}^n \tag{3.33}$$

3.3.3 Stability

To guarantee stability, the aim is to construct a terminal constraint set $\mathcal{X}_f$ such that feasibility of the problem (3.16) for $x(k)$ satisfies constraints for mode-2,

$$\begin{aligned} x(k+N+j|k) &\in \mathcal{X},\ j = 1,2,... \\ u(k+N+j|k) &\in \mathcal{U},\ j = 1,2,... \end{aligned} \tag{3.34}$$

An approach is to use deadbeat mode-2 constraints as terminal constraints. For $j = N,\ldots,N+n-1$ in (3.34),

$$\begin{aligned} x(k+j|k) &= (A+B\,K)^j\, x(k+N|k) \\ u(k+j|k) &= K(A+B\,K)^j\, x(k+N|k) \end{aligned} \tag{3.35}$$

that is, extending the constraints for n steps beyond mode-1,

$$\underbrace{\overbrace{\begin{bmatrix} Px & 0 & \ldots & 0 \\ P_uK & 0 & \ldots & 0 \\ 0 & P_x & \ldots & 0 \\ 0 & P_uK & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \end{bmatrix}}^{\mathcal{M}} \begin{bmatrix} (A+BK)^0 \\ (A+BK)^1 \\ \vdots \\ (A+BK)^{n-1} \end{bmatrix}}_{P_{x_N}} x(k+N|k) \leq \underbrace{\begin{bmatrix} q_x \\ q_u \\ q_x \\ q_u \\ \vdots \end{bmatrix}}_{q_{x_N}} \tag{3.36}$$

where,

$$\mathcal{M} = \mathbf{I}_{n\times n} \otimes \begin{bmatrix} P_x \\ P_uK \end{bmatrix}, \qquad q_{x_N} = \mathbf{1}_{n\times 1} \otimes \begin{bmatrix} q_x \\ q_u \end{bmatrix} \tag{3.37}$$

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

$$\mathcal{X}_f = \{x(k+N|k) \in \mathbb{R}^n : P_{x_N}\, x(k+N|k) \leq q_{x_N}\} \tag{3.38}$$

This terminal constraint set has the property to be an admissible invariant set, which means that mode-2 constraints are satisfied, and mode-2 predictions stay within $\mathcal{X}_f$. This concept is called 'admissibility implies stability', in other words,

$$x(k+N|k) \in \mathcal{X}_f \Rightarrow x(k+N|k) \in \mathcal{X}$$
$$u(k+N|k) = K\ (x(k+N|k)) \in \mathcal{U}$$

In conclusion, the stability is guaranteed for the following conditions,

- (A,B) is stabilizable.
- $Q \succeq 0,\ R \succ 0$
- $(Q^{1/2},A)$ is observable.
- P satisfies the Lyapunov equation for some stabilizing K,
  $(A+B\ K)^\intercal\ P\ (A+B\ K) - P = -(Q+K^\intercal\ R\ K)$
- $\mathcal{X}_f$ is an admissible invariant set for mode-2 dynamics: $x(k+1) = (A+B\ K)\ x(k)$

then, given an $x(k) \in \mathcal{X}_N$,

- $J_N^*(x(k))$ is a Lyapunov function for mode-1 dynamics: $x(k+1) = Ax(k) + B\kappa_N(x(k))$, and recursively feasible, that is: if there is a feasible solution $J_N^*(x(k))$, then all subsequent solutions $J_N^*(x(k+1))$, $J_N^*(x(k+2)), \ldots$ exist and are feasible within $\mathcal{X}_N$.
- All constraints are satisfied.
- The origin $x = 0$ is asymptotically stable with Region of Attraction (RoA) $\mathcal{X}_N$.
- $\mathcal{X}_N$ is an admissible invariant set for mode-1 dynamics:$x(k+1) = Ax(k) + B\kappa_N(x(k))$.

Chapter 4

DoS attack

A DoS attack over a NCS consists on interrupting the communication channels of the sensor and actuation loop by packet flooding. The attacker floods the channels with a relatively large amount of random data that can consume the resources of the NCS, such as network bandwidth, and CPU cycles. As a result, the packets of data get lost at higher rate reducing the control performance that can lead the system to an unstable region.

This chapter presents the attack scheme of the system under MPC control with the description of the Bernoulli DoS attack model. A diagram shows where the attacks are located in the communication channel. There are two algorithms for the DoS attack over unconstrained and constrained MPC. The LQG-TCP approach is briefly summarized before detailed proposed MPC-TCP approach for both cases, unconstrained and constrained. And the last section presents numerical results.

4.1 Attack scheme

Consider the following discrete-time LTI state-space system,

$$\begin{aligned} x(k+1) &= A\,x(k) + \nu(k)\,B\,u(k) + w(k) \\ y(k) &= \gamma(k)\,C\,x(k) + z(k), \quad k = 0,1,2,\ldots \end{aligned} \tag{4.1}$$

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. $x(k)$ is available at each sampling time k. The process noise is $w(k) \sim \mathcal{N}(0, Q_w)$ with

covariance Q_w, the measurement noise is $z(k) \sim \mathcal{N}(0, R_z)$ with covariance R_z, both are uncorrelated, and are in the form of Additive White Gaussian Noise (AWGN).

The attack is a multiplicative Bernoulli packet drop model defined as,

$$\nu \sim \mathcal{B}(\bar{\nu}), \quad \begin{cases} \mathbb{P}[\nu = 1] = \bar{\nu}, & \\ \mathbb{P}[\nu = 0] = 1 - \bar{\nu}, & \text{Packet loss} \end{cases} \tag{4.2}$$

$$\gamma \sim \mathcal{B}(\bar{\gamma}), \quad \begin{cases} \mathbb{P}[\nu = 1] = \bar{\gamma}, & \\ \mathbb{P}[\nu = 0] = 1 - \bar{\gamma}, & \text{Packet loss} \end{cases} \tag{4.3}$$

where $\nu(k)$ is the attack over the actuation loop, and $\gamma(k)$ is the attack over the sensor loop.

To evaluate the MPC control system, Fig. 4.1 shows the attacked scheme with the following assumptions:

- The MPC block can be an unconstrained MPC or constrained MPC controller.
- There is a time-invariant steady-state Kalman Filter (KF) as optimal observer.
- The separation principle holds.
- There are no external disturbances.
- The attacks $\nu(k)$ and $\gamma(k)$ happen at random time steps.

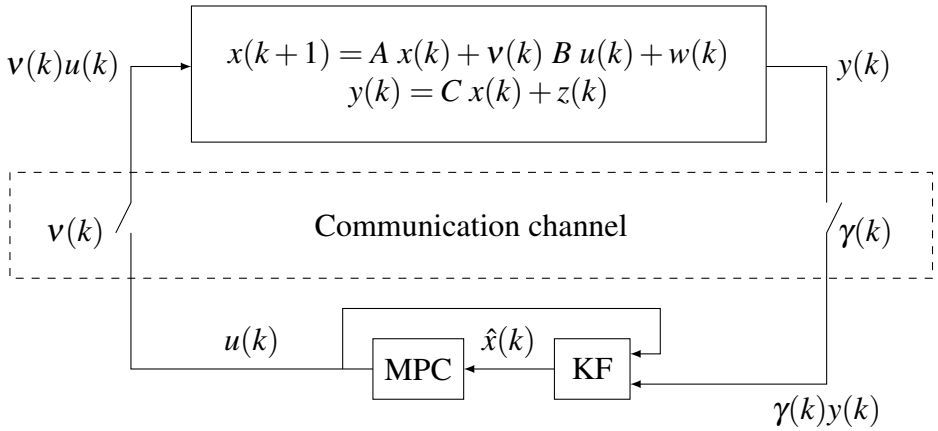


Figure 4.1: Scheme of the attack over the communication channel.

The KF gain L_{KF} is calculated as,

$$L_{KF} = A\,P_{KF}\,C^{\mathsf{T}}(C\,P_{KF}\,C^{\mathsf{T}} + R_z)^{-1} \tag{4.4}$$

$$P_{KF} = A\,P_{KF}\,A^{\mathsf{T}} - A\,P_{KF}\,C^{\mathsf{T}}(C\,P_{KF}\,C^{\mathsf{T}} + R_z)^{-1}C\,P_{KF}\,A^{\mathsf{T}} + Q_w \tag{4.5}$$

where P_{KF} is the error covariance that is the solution of the Discrete-time Ricatti Equation (DARE) of (4.5).

Finally, the closed-loop system is defined as,

$$\hat{x}(k+1) = A\,\hat{x}(k) + B\,v(k)u(k) + L_{KF}(y(k) - C\,\hat{x}(k)) \tag{4.6}$$

$$x(k+1) = \hat{x}(k+1) + w(k) \tag{4.7}$$

where $x(k+1)$ is the estimated state with the added process noise $w(k)$.

4.2 DoS attack over unconstrained MPC

Given the attack scheme and conditions presented in the previous section, Algorithm 1 presents the implementation for the unconstrained case with the attack vectors generated randomly off-line as,

$$v(k) = [v(0), \ldots, v(nk)], \quad \gamma(k) = [\gamma(0), \ldots, \gamma(nk)] \tag{4.8}$$

where nk is the final step of k.

Also, notice that the control law K_N is computed offline.

Algorithm 1: DoS attack over unconstrained MPC

Compute prediction matrices $F,\ G$ via (3.7);
Design stabilizing mode-2 gain K for $(A + B\,K)$;
Using K, compute P that satisfies Lyapunov equation (3.15);
Calculate predicted cost matrices $H,\ L,\ M$ via (3.11);
Compute the RH control law K_N using (3.14), and gain L_{KF} via (4.4);
Initialize $x(0) \leftarrow x_0$;
for $k = 0 : nk$ **do**
    Measure current attacked noisy output $y(k)$, (4.1);
    For the current state $x(k)$, apply the control law K_N and close the loop using (4.6);
    Set the noisy state $x(k+1)$ for the next iteration via (4.7);
    Wait one time step;
    Increment k;
end

4.3 DoS attack over constrained MPC

For the constrained case, remember that the control law $\kappa_N(x(k))$ is implicit. Hence, Algorithm 2 considers the online optimization for the current state $x(k)$. Again, the attack vectors are generated randomly as it was done in (4.8) for the unconstrained case.

Algorithm 2: DoS attack over constrained MPC

```
Compute prediction matrices F, G,mode-2 gain K, P, and H, L, M;
Using K, compute the deadbeat mode-2 terminal constraint X_f to guarantee
  stability via (3.38);
Compute the gain L_KF;
Compute the prediction matrices P_c, q_c, S_c using (3.25);
Initialize x(0) ← x_0;
for k = 0 : nk do
    Measure the current attacked noisy output y(k), (4.1);
    For the current x(k), solve the optimization problem given by (3.27);
    Apply the first control input u*(k) and close the loop using (4.6);
    Set the noisy state x(k+1) for the next iteration via (4.7);
    Wait one time step;
    Increment k;
end
```

4.4 Stability

For both unconstrained and constrained MPC the stability is not guaranteed because the controllability is lost because when the attack ν is zero, sets the input u to zero. In that case, if the plant is unstable, it behaves as open-loop when the attack over the actuation channel happens. The observability is lost with the γ attack because the output y is set to zero when γ is zero. When both channels are attacked, the system is uncontrollable, and unobservable.

4.5 LQG-TCP approach

The optimal LQG solution proposed in [14] for the TCP-like communication channel considers an Acknowledgement (ACK) of the packet loss due to $\nu(k)$ or $\gamma(k)$. This ACK is defined within an information set $\mathcal{I}$ that acknowledges the controller and estimator

about the packet delivery, and it is sent within the same time step. Let us define $\mathcal{I}$ as,

$$\mathcal{I}(k) = \{y^k, \gamma^k, \nu^{k-1}\} \tag{4.9}$$

where $y^k = (y(k), y(k-1), \ldots, y(1))$, $\gamma^k = (\gamma(k), \gamma(k-1), \ldots, \gamma(1))$, and $\nu^k = (\nu(k), \nu(k-1), \ldots, \nu(1))$.

Since the attack $\nu(k)$ 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. Moreover, the attack is a discrete probability distribution, so the problem now is to minimize the expectation of the following cost function,

$$J_N(x(k), \mathbf{u}(k)) = \mathbb{E}\left[\sum_{k=0}^{N-1} \left(\|x(k)\|_Q^2 + \nu(k)\|u(k)\|_R^2\right) + \|x(N)\|_Q^2\right] \tag{4.10}$$

Solving the Ricatti Difference Equation (RDE) by Dynamic Programming, the optimal solution is,

$$\begin{aligned} u^*(k) &= -(B^\intercal\, S(k)\, B + R)^{-1}\, B^\intercal\, S(k)\, A\, \hat{x}(k) && (4.11)\\ &= -L\, \hat{x}(k) \\ S(k+1) &= A^\intercal\, S(k)\, A + Q + (\nu(k)\, A^\intercal\, S(k)\, B)\; u^*(k) && (4.12)\\ S(0) &= Q && (4.13) \end{aligned}$$

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 $\nu(k)$.

The latter result indicates that the separation principle holds, which means that a modified time-varying KF for TCP channel (KF-TCP) can be designed considering the attack $\gamma(k)$ over the sensor channel. With the following variables,

$$\hat{x}(k|k) = \mathbb{E}[x(k)|\mathcal{I}(k)] \tag{4.14}$$

$$e(k|k) = x(k) - \hat{x}(k|k) \tag{4.15}$$

$$P(k|k) = \mathbb{E}[e(k|k)\; e^\intercal(k|k)|\mathcal{I}(k)] \tag{4.16}$$

and applying the previous definitions with the procedure of [16], the **innovation** step

results in,

$$\begin{aligned}\hat{x}(k+1|k) &= A\ \mathbb{E}[x(k)|\mathcal{I}] + \nu(k)\ B\ u(k) \\ &= A\ \hat{x}(k|k) + \nu(k)\ B\ u(k) \qquad (4.17)\\ e(k+1|k) &= x(k+1) - \hat{x}(k+1|k) \\ &= A\ e(k|k) + w(k) \qquad (4.18)\\ P(k+1|k) &= \mathbb{E}\left[e(k+1|k)\ e^{\mathsf{T}}(k+1|k)|\nu(k),\mathcal{I}(k)\right] \\ &= A\ P(k|k)\ A^{\mathsf{T}} + Q_w \qquad (4.19)\end{aligned}$$

because y, γ, w and $\mathcal{I}$ are independent, the **correction** step is,

$$\begin{aligned}\hat{x}(k+1|k+1) &= \hat{x}(k+1|k) + \gamma(k+1)\ K(k+1)(y(k+1) - C\ \hat{x}(k+1|k)) \qquad (4.20)\\ e(k+1|k+1) &= x(k+1) - \hat{x}(k+1|k+1) \\ &= (I - \gamma(k+1)\ K(k+1)\ C)\ e(k+1|k) \\ &\qquad - \gamma(k+1)\ K(k+1)\ \nu(k+1) \qquad (4.21)\\ P(k+1|k+1) &= P(k+1|k) - \gamma(k+1)\ K(k+1)\ C\ P(k+1|k) \qquad (4.22)\\ K(k+1) &= P(k+1|k)\ C^{\mathsf{T}}(C\ P(k+1|k)\ C^{\mathsf{T}} + R_z)^{-1} \qquad (4.23)\end{aligned}$$

From these results, it can be seen that if there is no attack over the communication channel, that is $\nu(k) = 1$ and $\gamma(k) = 1$, the modified KF-TCP behaves as a typical time-varying KF. When there is an attack $\nu(k) = 0$, the predicted state $\hat{x}(k+1|k)$ in the innovation step is defined as a state without feedback $\hat{x}(k+1|k) = A\ \hat{x}(k|k)$, the error covariance $P(k+1|k)$ gets bigger, and the Kalman gain $K(k+1)$ in the correction step gets bigger too to compensate the error estimation. If $\gamma(k) = 0$, the corrected state $\hat{x}(k+1|k+1)$ is the same as the predicted state, and corrected error covariance $P(k+1|k+1)$ is also the same as the predicted error covariance. Therefore, if the attack $\gamma(k)$ continues the error covariance will be penalized even more with $K(k+1)$ in the next time step.

4.5.1 Stability for LQG-TCP

While LQG-TCP approach can stabilize the system with a relative packet loss rate, the stability can be lost if the attack probabilities $\bar{\nu}$, and $\bar{\gamma}$ are below a certain threshold. That is,

$$\bar{\gamma} > \gamma_c, \quad \bar{\nu} > \nu_c \tag{4.24}$$

subject to,

$$1 - \frac{1}{max_i \ |\lambda_i^u(A)|^2} \leq \gamma_c, \nu_c \leq 1 - \frac{1}{\prod_i \ |\lambda_i(A)|^2} \tag{4.25}$$

where $\lambda_i^u(A)$ are the unstable eigenvalues of state matrix A of the system.

4.6 MPC-TCP approach

Given that LQG-TCP shares properties with MPC, this section extends that approach to the unconstrained and constrained MPC for a TCP channel (MPC-TCP). In the unconstrained case, the objective is to demonstrate that the optimal LQG-TCP solution is the same as the unconstrained MPC-TCP. On the other hand, in the constrained case the approach is to minimize the expectation of the cost function considering the attack. Fig. 4.2 shows the attack scheme with the MPC-TCP approach.

Notice that the delay in the TCP-channel does not consider the transportation delay which means that the $\nu(k-1)$ is available immediately for the KF-TCP block. The attack scheme is the same as the LQG-TCP approach, in fact, if the proposed unconstrained MPC-TCP is valid, the results in the simulation should look like similar.

4.6.1 Problem formulation

First, let us define the predicted form of the cost function as in (3.9) by introducing the attack $\nu(k)$ in the MPC cost function and penalizing the input when the packet is lost.

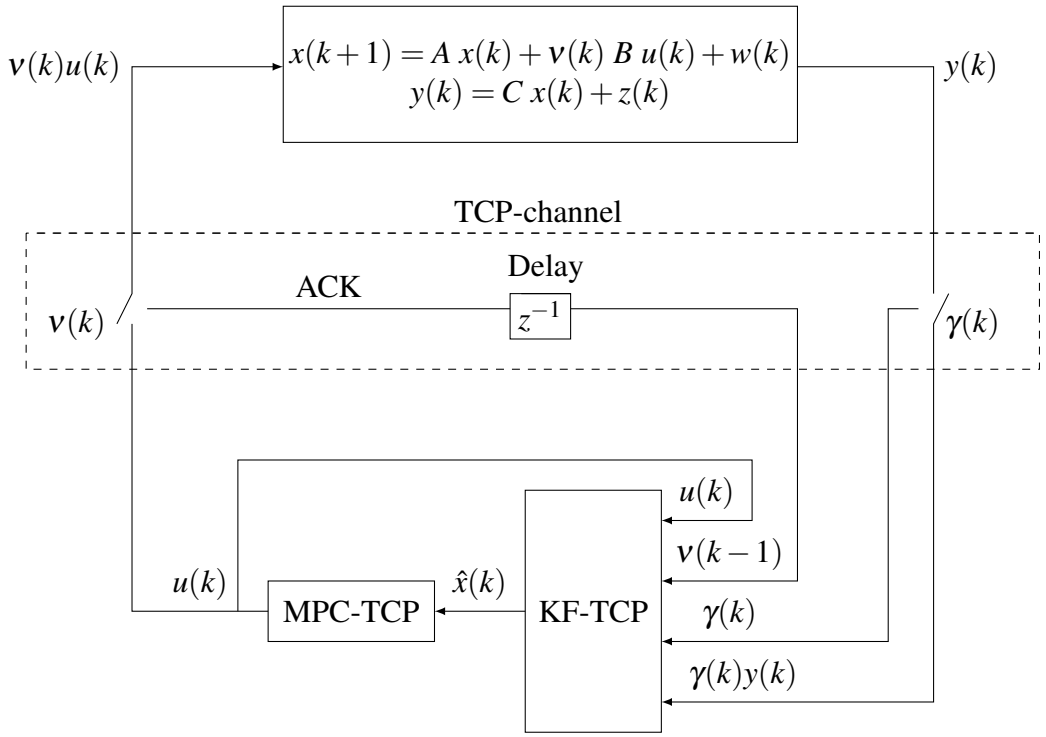


Figure 4.2: Attack scheme with MPC-TCP approach.

The problem is to minimize,

$$J_N(x(k),\mathbf{u}(k) = \sum_{j=0}^{N-1} \left(\|x(k+j|k)\|_Q^2 + \|\nu(k+j|k)\,u(k+j|k)\|_R^2\right) + \|x(k+N|k)\|_P^2 \tag{4.26}$$

Consider the attack vector $\nu(k) = \nu(k|k)$ and applying into the model (4.1) recursively without $w(k)$,

$$\begin{aligned}
x(k+1|k) &= A\,x(k) + B\,\nu(k)\,u(k) \\
x(k+2|k) &= A\,x(k+1|k) + B\,\nu(k+1|k)\,u(k+1|k) \\
&= A^2\,x(k) + AB\,\nu(k|k)\,u(k|k) + B\,\nu(k+1|k)\,u(k+1|k) \\
\vdots \quad &= \quad \vdots \\
x(k+N|k) &= A\,x(k+N-1|k) + B\,\nu(k+N-1|k)\,u(k+N-1|k) \\
&= A^N\,x(k) + A^{N-1}B\,\nu(k|k)\,u(k|k) + \cdots + B\,\nu(k+N-1|k)\,u(k+N-1|k)
\end{aligned}$$

stacking,

$$\underbrace{\begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix}}_{\mathbf{x}(k)} = \underbrace{\begin{bmatrix} A \\ A^2 \\ \vdots \\ A^N \end{bmatrix}}_{F} + \underbrace{\begin{bmatrix} B & 0 & \dots & 0 \\ AB & B & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A^{N-1}B & A^{N-2}B & \dots & B \end{bmatrix}}_{G} \underbrace{\begin{bmatrix} v(k|k)\ u(k|k) \\ v(k+1|k)\ u(k+1|k) \\ \vdots \\ v(k+N-1|k)\ u(k+N-1|k) \end{bmatrix}}_{\mathbf{u_a}(k)} \tag{4.27}$$

the prediction equality constraint is,

$$\mathbf{x}(k) = F\, x(k) + G\, \mathbf{u_a}(k) \tag{4.28}$$

where $\mathbf{x}(k)$, and $\mathbf{u_a}(k)$ are the state, and attacked input predictions over all steps $j = 0,1,2,\dots,N$.

Rewriting the cost function (4.26) as,

$$\begin{aligned} x^\intercal(k|k)\, Q\, x(k|k) + & \begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix}^\intercal \underbrace{\begin{bmatrix} Q & 0 & \dots & 0 \\ 0 & Q & \ddots & \vdots \\ \vdots & \ddots & Q & 0 \\ 0 & \dots & 0 & P \end{bmatrix}}_{\tilde{Q}} \begin{bmatrix} x(k+1|k) \\ x(k+2|k) \\ \vdots \\ x(k+N|k) \end{bmatrix} \\ & + \begin{bmatrix} v(k|k)\ u(k|k) \\ v(k+1|k)\ u(k+1|k) \\ \vdots \\ v(k+N-1|k)\ u(k+N-1|k) \end{bmatrix}^\intercal \underbrace{\begin{bmatrix} R & 0 & \dots & 0 \\ 0 & R & \ddots & \vdots \\ \vdots & \ddots & R & 0 \\ 0 & \dots & 0 & R \end{bmatrix}}_{\tilde{R}} \\ & \begin{bmatrix} v(k|k)\ u(k|k) \\ v(k+1|k)\ u(k+1|k) \\ \vdots \\ v(k+N-1|k)\ u(k+N-1|k) \end{bmatrix} \end{aligned}$$

with $x(k|k) = x(k)$, and $\mathbf{u_a}(k)$, now the problem is,

$$J_N(x(k), \mathbf{u}(k)) = x^\intercal(k)\, Q\, x(k) + \mathbf{x}^\intercal(k)\, \tilde{Q}\, \mathbf{x}(k) + \mathbf{u_a}^\intercal(k)\, \tilde{R}\, \mathbf{u_a}(k) \tag{4.29}$$

subject to,

$$\mathbf{x}(k) = F\ x(k) + G\ \mathbf{u_a}(k) \tag{4.30}$$

4.7 Unconstrained MPC-TCP

4.7.1 Problem formulation

For the unconstrained case, let us define the attacked vector $\mathbf{u_a}(k)$ as,

$$\mathbf{u_a}(k) = \begin{bmatrix} \nu(k|k)\ u(k|k) \\ \nu(k+1|k)\ u(k+1|k) \\ \vdots \\ \nu(k+N-1|k)\ u(k+N-1|k) \end{bmatrix}$$

$$= \underbrace{\begin{bmatrix} \nu(k|k) & 0 & \dots & 0 \\ 0 & \nu(k+1|k) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \nu(k+N-1|k) \end{bmatrix}}_{V} \underbrace{\begin{bmatrix} u(k|k) \\ u(k+1|k) \\ \vdots \\ u(k+N-1|k) \end{bmatrix}}_{\mathbf{u}(k)}$$

$$\mathbf{u_a}(k) = V\ \mathbf{u}(k) \tag{4.31}$$

where V is a diagonal matrix. Replacing the previous result in (4.29), and (4.30), the predicted cost function is,

$$J_N(x(k), \mathbf{u}(k)) = x^\intercal(k)\ Q\ x(k) + \mathbf{x}^\intercal(k)\ \tilde{Q}\ \mathbf{x}(k) + (V\ \mathbf{u}(k))^\intercal\ \tilde{R}\ (V\ \mathbf{u}(k)) \tag{4.32}$$

subject to,

$$\mathbf{x}(k) = F\ x(k) + G\ V\ \mathbf{u}(k) \tag{4.33}$$

now substituting the modified predicted equality constraint in the cost function (4.32),

$$J_N(x(k), \mathbf{u}(k)) = x^\intercal(k) Q x(k) + (Fx(k) + G\mathbf{u}(k))^\intercal \tilde{Q} (Fx(k) + G\mathbf{u}(k)) + (V\mathbf{u}(k))^\intercal \tilde{R} (V\mathbf{u}(k))$$

omitting (k) only for the algebraic operations,

$$
\begin{aligned}
&= x^\intercal Q x + [(Fx)^\intercal + (GV\mathbf{u})^\intercal]\tilde{Q}(Fx + GV\mathbf{u}) + (V\mathbf{u})^\intercal \tilde{R} V\mathbf{u} \\
&= x^\intercal Q x + (Fx)^\intercal \tilde{Q} Fx + (Fx)^\intercal \tilde{Q} GV\mathbf{u} + (GV\mathbf{u})^\intercal \tilde{Q} Fx + (GV\mathbf{u})^\intercal \tilde{Q} GV\mathbf{u} + (V\mathbf{u})^\intercal \tilde{R} V\mathbf{u} \\
&= \underbrace{x^\intercal Q x + x^\intercal F^\intercal \tilde{Q} F x} + \underbrace{x^\intercal F^\intercal \tilde{Q} GV\mathbf{u} + \mathbf{u}^\intercal (GV)^\intercal \tilde{Q} Fx} + \underbrace{\mathbf{u}^\intercal (GV)^\intercal \tilde{Q} GV\mathbf{u} + \mathbf{u}^\intercal V^\intercal \tilde{R} V\mathbf{u}} \\
&= x^\intercal (Q + F^\intercal \tilde{Q} F)x + 2\mathbf{u}^\intercal (GV)^\intercal \tilde{Q} Fx + \mathbf{u}^\intercal ((GV)^\intercal \tilde{Q} GV + V^\intercal \tilde{R} V)\mathbf{u} \\
&= x^\intercal (Q + F^\intercal \tilde{Q} F)x + 2\mathbf{u}^\intercal V^\intercal G^\intercal \tilde{Q} Fx + \mathbf{u}^\intercal (V^\intercal G^\intercal \tilde{Q} GV + V^\intercal \tilde{R} V)\mathbf{u}
\end{aligned}
$$

because $V^\intercal = V$,

$$
\begin{aligned}
&= x^\intercal (Q + F^\intercal \tilde{Q} F)x + 2\mathbf{u}^\intercal V G^\intercal \tilde{Q} Fx + \mathbf{u}^\intercal (V G^\intercal \tilde{Q} GV + V\tilde{R} V)\mathbf{u} \\
&= x^\intercal (Q + F^\intercal \tilde{Q} F)x + (2V G^\intercal \tilde{Q} Fx)^\intercal \mathbf{u} + \mathbf{u}^\intercal (V G^\intercal \tilde{Q} GV + V\tilde{R} V)\mathbf{u} \\
&= x^\intercal \underbrace{(Q + F^\intercal \tilde{Q} F)}_{M} x + (\underbrace{2V G^\intercal \tilde{Q} F}_{L_v} x)^\intercal \mathbf{u} + \frac{1}{2}\left[\mathbf{u}^\intercal \underbrace{2(V G^\intercal \tilde{Q} GV + V\tilde{R} V)}_{H_v}\mathbf{u}\right] \\
&= \frac{1}{2}\mathbf{u}(k)^\intercal \, H_v \, \mathbf{u}(k) + \underbrace{(L_v \, x(k))^\intercal}_{c_v^\intercal} \, \mathbf{u}(k) + \underbrace{x(k)^\intercal \, M \, x(k)}_{\alpha}
\end{aligned}
$$

but,

$$
\begin{aligned}
H_v &= 2(V G^\intercal \tilde{Q} GV + V\tilde{R} V) = V \, \underbrace{2(G^\intercal \tilde{Q} G + \tilde{R})}_{H} \, V = VHV \\
L_v &= 2V G^\intercal \tilde{Q} F = V \, \underbrace{2G^\intercal \tilde{Q} F}_{L} = VL \\
c_v^\intercal &= (V \underbrace{L \, x(k)})^\intercal = (L \, x(k))^\intercal V^\intercal = (L \, x(k))^\intercal V = c^\intercal \, V
\end{aligned}
$$

therefore, the cost function in QP compact form can be written as,

$$
J_N(x(k), \mathbf{u}) = \frac{1}{2}\mathbf{u}(k)^\intercal \, V \, H \, V \, \mathbf{u}(k) + c^\intercal \, V \, \mathbf{u}(k) + \alpha \tag{4.34}
$$

where,

$$
\begin{aligned}
H &= 2(G^\intercal \tilde{Q} G + \tilde{R}) \\
c &= L\, x(k), \quad L = 2G^\intercal \tilde{Q} F \\
\alpha &= x^\intercal(k)\, M\, x(k), \quad M = Q + F^\intercal \tilde{Q} F
\end{aligned}
\tag{4.35}
$$

4.7.2 QP solution

Minimizing for $\mathbf{u}^*(k)$,

$$
\begin{aligned}
J_N^*(x(k), \mathbf{u}(k)) &= \min_{\mathbf{u}(k)} \frac{1}{2} \mathbf{u}(k)^\intercal\, V\, H\, V\, \mathbf{u}(k) + c^\intercal\, V\, \mathbf{u} + \alpha \\
\nabla_{\mathbf{u}}\, J_N^*(x(k), \mathbf{u}(k)) &= 0 \\
\mathbf{u}^\intercal\, V\, H\, V + c^\intercal\, V &= 0 \\
\mathbf{u}^\intercal\, H^\intercal\, V^2 + c^\intercal\, V &= 0
\end{aligned}
$$

as $V^2 = V$,

$$
\begin{aligned}
\mathbf{u}^\intercal\, H^\intercal\, \not{V} + c^\intercal\, \not{V} &= 0 \\
\mathbf{u}^\intercal\, H^\intercal + c^\intercal &= 0 \quad \text{as row vector} \\
(\mathbf{u}^\intercal\, H^\intercal)^\intercal + (c^\intercal)^\intercal &= 0 \quad \text{as column vector} \\
H\, \mathbf{u}^* &= -c \\
\mathbf{u}^* &= -H^{-1}\, c
\end{aligned}
$$

because $x(k)$ is estimated by the KF-TCP, the optimal solution results in,

$$
\mathbf{u}^*(k) = -H^{-1}\, L\, \hat{x}(k) \tag{4.36}
$$

with the RH control input,

$$
u^*(k) = K_N\, \hat{x}(k) \tag{4.37}
$$

$$
K_N = [I \quad 0 \quad 0 \quad \dots \quad 0](-H^{-1}\, L) \tag{4.38}
$$

such that, $u^*(k)$ is an explicit solution and is the same as LQG-TCP (4.11), proving that the separation principle holds.

4.8 Constrained MPC-TCP

4.8.1 Problem formulation

For the constrained case, let us define the expected cost function in QP compact form as,

$$J_N(x(k),\mathbf{u}(k)) = \mathbb{E}\ \left[x^\intercal(k)\ Q\ x(k) + \mathbf{x}^\intercal(k)\ \tilde{Q}\ \mathbf{x}(k) + \mathbf{u_a}^\intercal(k)\ \tilde{R}\ \mathbf{u_a}(k)\right] \tag{4.39}$$

subject to,

$$\mathbb{E}\ [\mathbf{x}(k)] = \mathbb{E}\ [F\ x(k) + G\ \mathbf{u_a}(k)] \tag{4.40}$$

As $\mathbb{E}[x(k)] = \hat{x}(k)$, and because $\nu(k),\ u(k)$ are uncorrelated,

$$\begin{aligned}\mathbb{E}[\mathbf{u_a}(k)] &= \mathbb{E}\begin{bmatrix}\nu(k)\ u(k)\\ \nu(k+1)\ u(k+1)\\ \vdots\\ \nu(N-1)\ u(N-1)\end{bmatrix} = \begin{bmatrix}\mathbb{E}[\nu(k)]\ \mathbb{E}[u(k)]\\ \mathbb{E}[\nu(k+1)]\ \mathbb{E}[u(k+1)]\\ \vdots\\ \mathbb{E}[\nu(N-1)]\ \mathbb{E}[u(N-1)]\end{bmatrix} = \begin{bmatrix}\bar{\nu}\ \mathbb{E}[u(k)]\\ \bar{\nu}\ \mathbb{E}[u(k+1)]\\ \vdots\\ \bar{\nu}\ \mathbb{E}[u(N-1)]\end{bmatrix}\\ &= \bar{\nu}\ \mathbb{E}[\mathbf{u}(k)]\\ &= \bar{\nu}\ \hat{\mathbf{u}}(k)\end{aligned}$$

hence,

$$\hat{\mathbf{x}}(k) = F\ \hat{x}(k) + G\ \bar{\nu}\ \hat{\mathbf{u}}(k) \tag{4.41}$$

Applying the expectation to (4.39),

$$\begin{aligned}J_N(\hat{x}(k),\hat{\mathbf{u}}(k) = \hat{x}^\intercal(k)\ Q\ \hat{x}(k) + \hat{\mathbf{x}}^\intercal(k)\ \tilde{Q}\ \hat{\mathbf{x}}(k) + \bar{\nu}^2\ \hat{\mathbf{u}}^\intercal(k)\ \tilde{R}\ \hat{\mathbf{u}}(k)\\ + trace\left[Q\ P(k) + \tilde{Q}\ P(k) + \tilde{R}\ cov(\nu u)\right]\end{aligned}$$

where $P(k)$ is the state covariance matrix. Because there is no need to predict $P(k)$, it is sufficient to multiply as a constant with matrix $\tilde{Q}$. Moreover, there is no covariance between ν and u, $cov(\nu u) = 0$. Now, substituting (4.40) and expanding the terms,

$$J_N(\hat{x}(k), \hat{\mathbf{u}}(k)) = \hat{x}^\intercal(k) Q \hat{x}(k) + [(Fx(k))^\intercal + (G\bar{\nu}\hat{\mathbf{u}})^\intercal] \tilde{Q}(Fx(k) + G\bar{\nu}\hat{\mathbf{u}}) + \bar{\nu}^2 \hat{\mathbf{u}}^\intercal \tilde{R} \hat{\mathbf{u}} + trace\left[Q\, P(k) + \tilde{Q}\, P(k)\right]$$

if $\beta = trace(Q\, P(k) + \tilde{Q}\, P(k))$,

$$\begin{aligned}
&= \hat{x}^\intercal Q \hat{x} + (F\hat{x})^\intercal \tilde{Q}(F\hat{x}) + (G\bar{\nu}\hat{\mathbf{u}})^\intercal \tilde{Q}(G\bar{\nu}\hat{\mathbf{u}}) + \underbrace{(F\hat{x})^\intercal \tilde{Q}(G\bar{\nu}\hat{\mathbf{u}})} + (G\bar{\nu}\hat{\mathbf{u}})^\intercal \tilde{Q}(F\hat{x}) + \bar{\nu}^2 \hat{\mathbf{u}}^\intercal \tilde{R} \hat{\mathbf{u}} + \beta \\
&= \underbrace{\hat{x}^\intercal Q \hat{x} + \hat{x}^\intercal (F^\intercal \tilde{Q} F)\hat{x}} + \hat{\mathbf{u}}^\intercal (\bar{\nu} G^\intercal \tilde{Q} G \bar{\nu})\hat{\mathbf{u}} + \underbrace{(G\bar{\nu}\hat{\mathbf{u}})^\intercal \tilde{Q}(F\hat{x}) + (G\bar{\nu}\hat{\mathbf{u}})^\intercal \tilde{Q}(F\hat{x}) + \bar{\nu}^2 \hat{\mathbf{u}}^\intercal \tilde{R} \hat{\mathbf{u}}} + \beta \\
&= \hat{x}^\intercal (Q + F^\intercal \tilde{Q} F)\hat{x} + 2\bar{\nu}(G\hat{\mathbf{u}})^\intercal \tilde{Q}(F\hat{x}) + \underbrace{\hat{\mathbf{u}}^\intercal (\bar{\nu} G^\intercal \tilde{Q} G \bar{\nu})\hat{\mathbf{u}} + \bar{\nu}^2 \hat{\mathbf{u}}^\intercal \tilde{R} \hat{\mathbf{u}}} + \beta \\
&= \hat{x}^\intercal (Q + F^\intercal \tilde{Q} F)\hat{x} + 2\bar{\nu}(G\hat{\mathbf{u}})^\intercal \tilde{Q}(F\hat{x}) + \bar{\nu}^2 \hat{\mathbf{u}}^\intercal (\tilde{R} + G^\intercal \tilde{Q} G)\hat{\mathbf{u}} + \beta \\
&= \hat{x}^\intercal \underbrace{(Q + F^\intercal \tilde{Q} F)}_{M} \hat{x} + \bar{\nu}(\underbrace{2G^\intercal \tilde{Q} F}_{L} \hat{x})^\intercal \hat{\mathbf{u}} + \frac{1}{2}\left[\hat{\mathbf{u}}^\intercal \bar{\nu}^2 \underbrace{2(G^\intercal \tilde{Q} G + \tilde{R})}_{H} \hat{\mathbf{u}}\right] + \beta \\
&= \frac{1}{2}\hat{\mathbf{u}}(k)^\intercal\ \bar{\nu}^2\, H\, \hat{\mathbf{u}}(k) + \bar{\nu}\ \underbrace{(L\,\hat{x}(k))^\intercal}_{c^\intercal}\ \hat{\mathbf{u}}(k) + \underbrace{\hat{x}(k)^\intercal\, M\, \hat{x}(k) + \beta}_{\alpha_v}
\end{aligned}$$

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

$$J_N(\hat{x}(k), \hat{\mathbf{u}}(k)) = \frac{1}{2}\hat{\mathbf{u}}(k)^\intercal\ \bar{\nu}^2\, H\, \hat{\mathbf{u}}(k) + \bar{\nu}\, c^\intercal\, \hat{\mathbf{u}}(k) + \alpha_v \tag{4.42}$$

where,

$$\begin{aligned}
H &= 2(G^\intercal \tilde{Q} G + \tilde{R}) \\
c &= L\, x(k), \quad L = 2G^\intercal \tilde{Q} F \\
\alpha_v &= x^\intercal(k)\, M\, x(k) + \beta \\
M &= Q + F^\intercal \tilde{Q} F, \quad \beta = trace(Q\, P(k) + \tilde{Q}\, P(k))
\end{aligned} \tag{4.43}$$

4.8.2 QP solution

Considering that ν can be a strong attack e.g. $\bar{\nu} = 0.5$, let us introduce a slack variable ε to soft constraint the state x when the optimization might reach an unfeasible region,

that is,

$$\begin{aligned} J_N(\hat{x}(k),\hat{\mathbf{u}}(k),\varepsilon(k)) &= \frac{1}{2}\hat{\mathbf{u}}(k)^\intercal\ \bar{\nu}^2\ H\ \hat{\mathbf{u}}(k) + \bar{\nu}\ c^\intercal\ \hat{\mathbf{u}}(k) + \left(\frac{1}{2}\varepsilon^\intercal(k)\ \sigma\ \varepsilon(k) + \rho^\intercal\ \varepsilon(k)\right) + \alpha_v \\ &= \frac{1}{2}\left(\hat{\mathbf{u}}^\intercal\ \bar{\nu}^2\ H\ \hat{\mathbf{u}} + \varepsilon^\intercal\ \sigma\ \varepsilon\right) + \bar{\nu}\ c^\intercal\ \hat{\mathbf{u}} + \rho\ \varepsilon + \alpha_v \\ &= \frac{1}{2}\begin{bmatrix}\hat{\mathbf{u}}^\intercal & \varepsilon^\intercal\end{bmatrix}\begin{bmatrix}\bar{\nu}^2\ H & 0\\ 0 & \sigma\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}\\ \varepsilon\end{bmatrix} + \begin{bmatrix}\bar{\nu}\ c^\intercal & \rho^\intercal\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}\\ \varepsilon\end{bmatrix} + \alpha_v \end{aligned}$$

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

$$J_N(\hat{x}(k),\hat{\mathbf{u}}(k),\varepsilon(k)) = \frac{1}{2}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix}^\intercal\begin{bmatrix}\bar{\nu}^2\ H & 0\\ 0 & \sigma\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} + \begin{bmatrix}\bar{\nu}\ c^\intercal & \rho^\intercal\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} + \alpha_v$$

Applying the slack variable to the state constraints of (3.20),

$$\begin{cases} \tilde{P}_x\ \hat{\mathbf{x}}(k) & \leq \tilde{q}_x - \tilde{P_{x_0}}\ x(k) + \varepsilon(k) \\ \varepsilon(k) & \geq 0 \end{cases}$$

using (4.41),

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

reordering,

$$\underbrace{\begin{bmatrix}\tilde{P}_u & 0\\ \tilde{P}_x\ G\ \bar{\nu} & -I\\ 0 & -I\end{bmatrix}}_{P_{c\varepsilon}}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} \leq \underbrace{\begin{bmatrix}\tilde{q_u}\\ \tilde{q_x}\\ 0\end{bmatrix}}_{q_{c\varepsilon}} + \underbrace{\begin{bmatrix}0\\ -\tilde{P_{x_0}} - \tilde{P}_x\ F\\ 0\end{bmatrix}}_{S_{c\varepsilon}}\hat{x}(k)$$

Therefore, the expected QP problem in compact form is to minimize,

$$J_N(\hat{x}(k),\hat{\mathbf{u}}(k),\varepsilon(k)) = \frac{1}{2}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix}^{\mathsf{T}}\begin{bmatrix}\bar{v}^2\,H & 0\\ 0 & \sigma\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} + \begin{bmatrix}\bar{v}\;c^{\mathsf{T}} & \rho^{\mathsf{T}}\end{bmatrix}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} + \alpha_v \tag{4.44}$$

subject to,

$$P_{c_\varepsilon}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} \leq q_{c_\varepsilon} + S_{c_\varepsilon}\,\hat{x}(k) \tag{4.45}$$

with the optimal solution defined as,

$$\begin{aligned}\hat{\mathbf{u}}^*(k) &= \arg\min_{\hat{u}(k)}\left\{J_N(\hat{x}(k),\hat{\mathbf{u}}(k),\varepsilon(k))\;:P_{c_\varepsilon}\begin{bmatrix}\hat{\mathbf{u}}(k)\\ \varepsilon(k)\end{bmatrix} \leq q_{c_\varepsilon} + S_{c_\varepsilon}\,\hat{x}(k)\right\}\\ &= \{\hat{u}^*(k|k),\hat{u}^*(k+1|k),\ldots,\hat{u}^*(k+N-1|k)\}\end{aligned} \tag{4.46}$$

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

$$\hat{\mathbf{u}}^*(k|k) = \kappa_N(\hat{x}(k)) \tag{4.47}$$

4.9 Numerical example

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

4.9.1 MPC without attacks

Given the following unstable non-minimum phase system in continuous time,

$$Gp = \frac{-s+1}{(s-2)(s+1)} \tag{4.48}$$

with a zero $s = 1$, and a pole $s = 2$, both located in the Right-Half Plane (RHP) of the s plane. In discrete time with sampled at $T_s = 0.1[s]$ the system is,

$$Gp = \frac{-0.10z + 0.11}{(z - 1.22)(z - 0.90)} \tag{4.49}$$

where there is a pole $z = 1.22$ outside the unit circle, and non-minimum phase behaviour given by the zero at $z = -1.10$.

The system in discrete LTI state-space model (3.1) sampled at $T_s = 0.1[s]$ is,

$$\begin{aligned} x(k+1) &= \begin{bmatrix} 1.12 & 0.20 \\ 0.11 & 1.01 \end{bmatrix} x(k) + \begin{bmatrix} 0.11 \\ 0.06 \end{bmatrix} u(k) + w(k) \\ y(k) &= \begin{bmatrix} -1 & 1 \end{bmatrix} x(k) + z(k) \end{aligned} \tag{4.50}$$

with the given values,

$$\begin{aligned} x(0) &= \begin{bmatrix} 0 \\ 1.5 \end{bmatrix} \\ w(k) &\sim \mathcal{N}(0, Q_w), \quad z(k) \sim \mathcal{N}(0, Rz) \\ Q_w &= \begin{bmatrix} 0.01 & 0 \\ 0 & 0.01 \end{bmatrix}, \quad R_z = 0.01 \end{aligned} \tag{4.51}$$

where $x \in \mathbb{R}^2,\ y \in \mathbb{R}^1,\ u \in \mathbb{R}^1$, process noise $w \in \mathbb{R}^{2\times 1}$ with covariance $Q_w \in \mathbb{R}^{2\times 2}$, and measurement noise $z \in \mathbb{R}^1$ and covariance R_z.

With the following values for the unconstrained QP optimization problem in (3.2),

$$\begin{aligned} Q &= \begin{bmatrix} 1e^6 & 0 \\ 0 & 1e^6 \end{bmatrix}, \quad R = 1 \\ N &= 10, \quad nk = 100 \quad k = 0, 1, ..., nk \end{aligned} \tag{4.52}$$

where N is the finite horizon, k is the time step, nk is the final time step value, $Q \in \mathbb{R}^{2\times 2},\ R \in \mathbb{R}^{1\times 1}$ are the state and input penalty matrices respectively. And the constrained conditions for the QP problem in (3.16),

$$|x| \leq 2, \quad |u| \leq 10 \tag{4.53}$$

Fig. 4.3 shows the result of the controlled unstable system without attacks. Notice that both actuation and sensor channel have probability of packet delivery of 1, that is $\bar{\nu} = 1$ and $\bar{\gamma} = 1$. MPCu stands for unconstrained MPC, and MPCc for constrained MPC. In the constrained case, the input respects the constraints $|u| \leq 10$ Fig. 4.3a, and the states are stable in the feasible region $\mathcal{X}_N$, Fig. 4.3b.

Fig. 4.4a shows the 25 regions of operation where there is a feasible control law $\kappa_N(x(k))$ for every region. Fig. 4.4b shows the Piece Wise Affine (PWA) function of the implicit non-linear control law $\kappa_N(x(k))$.

4.9.2 MPC with DoS attack

The DoS attack is introduced as, $\nu(k) \sim \mathcal{B}(0.8),\ \gamma \sim \mathcal{B}(0.5)$, where $\bar{\nu} = 0.8$ and $\bar{\gamma} = 0.5$. Both attack vectors are randomly generated using (4.8). The result of the attack can be seen in Fig. 4.5.

The result in Fig. 4.5a shows that the system goes quickly to instability due to the packet loss in the actuation channel followed by the packet loss in the sensor channel. For both cases, unconstrained and constrained MPC, the stability is not guaranteed because the controllability is lost when the attack $\nu = 0$ sets the input to $u = 0$.

During the time the packet is lost, the system behaves in unstable autonomous mode, that is $x(k+1) = A\ x(k)$, where the dominant pole $z = 1.22$ forces the dynamics to the unstable region. Moreover, phase-plot in the constrained case shows in Fig. 4.5b that the on-line optimization solution for $u^*(k)$ is unfeasible in time step 0.5 because the states are outside the feasible region $\mathcal{X}_N$, it can be observed at the top edge of $\mathcal{X}_N$.

4.9.3 LQG-TCP and MPC-TCP with DoS attack

Applying LGQ-TCP approach of Section 4.5, unconstrained MPC-TCP of Section **??**, and constrained MPC-TCP of Section 4.8, Fig. 4.6 shows that the DoS attack is rejected. The stability conditions of the LQG-TCP approach (4.25) is used to guarantee the unconstrained MPC-TCP, such that,

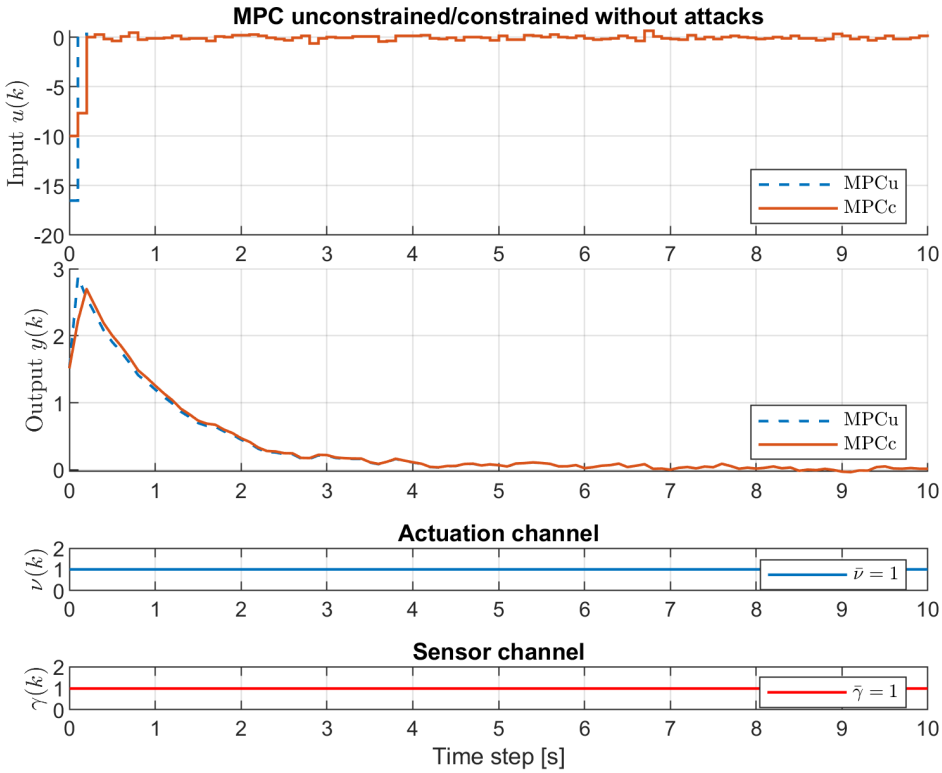
$$\bar{\gamma} > \gamma_c, \quad \bar{\nu} > \nu_c$$
$$0.5 > \gamma_c, \quad 0.8 > \nu_c$$

subject to,

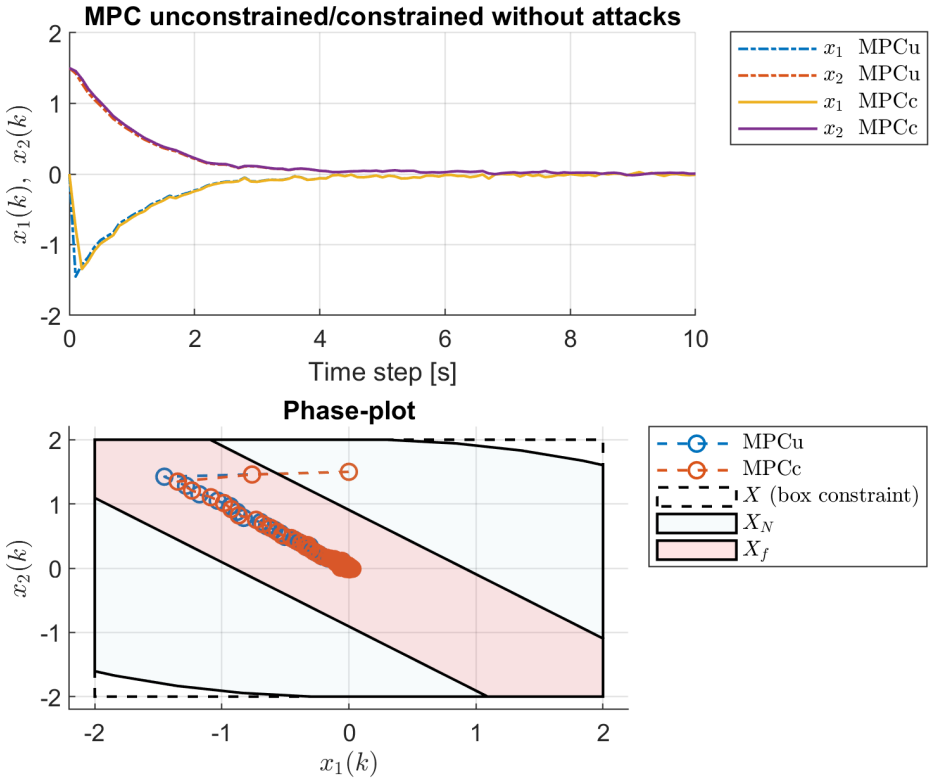
$$1 - \frac{1}{max_i \, |\lambda_i^u(A)|^2} \leq \gamma_c, \nu_c$$
$$1 - \frac{1}{1.22^2} \leq \gamma_c, \nu_c$$
$$0.33 \leq 0.5, 0.8$$

which means that the TCP channel is stable. It does not mean that they are the same for the constrained MPC-TCP. In fact, due to the non-linear behaviour of the implicit solution of the constrained MPC-TCP, further analysis is required to guarantee the stability by extending the concepts of the unconstrained MPC-TCP. Perhaps the path is to use the 'feasibility implies stability' property of the terminal set $\mathcal{X}_f$ studied in the constrained MPC case.

Another result of interest is the LQG-TCP input behaviour in Fig. 4.6a where the input values gets higher in the transient when the packet in the sensor channel is lost. This high values are because the terminal cost is Q for $x(N)$ in the cost function of LQG-TCP (4.10). In contrast, the unconstrained MPC-TCP cost function has a terminal cost P that guarantees the stability in mode-2. Therefore, LQG-TCP does not have a full guarantee of stability as unconstrained MPC-TCP has, which is one the advantages of MPC.

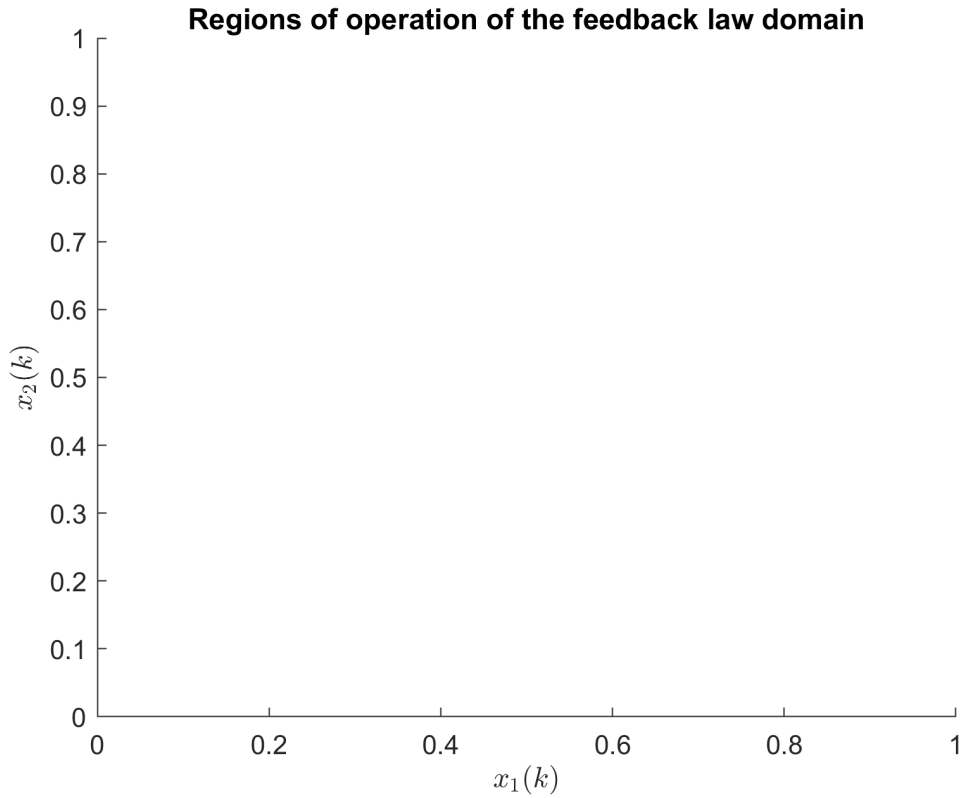


(a) Input $u(k)$ and output $y(k)$

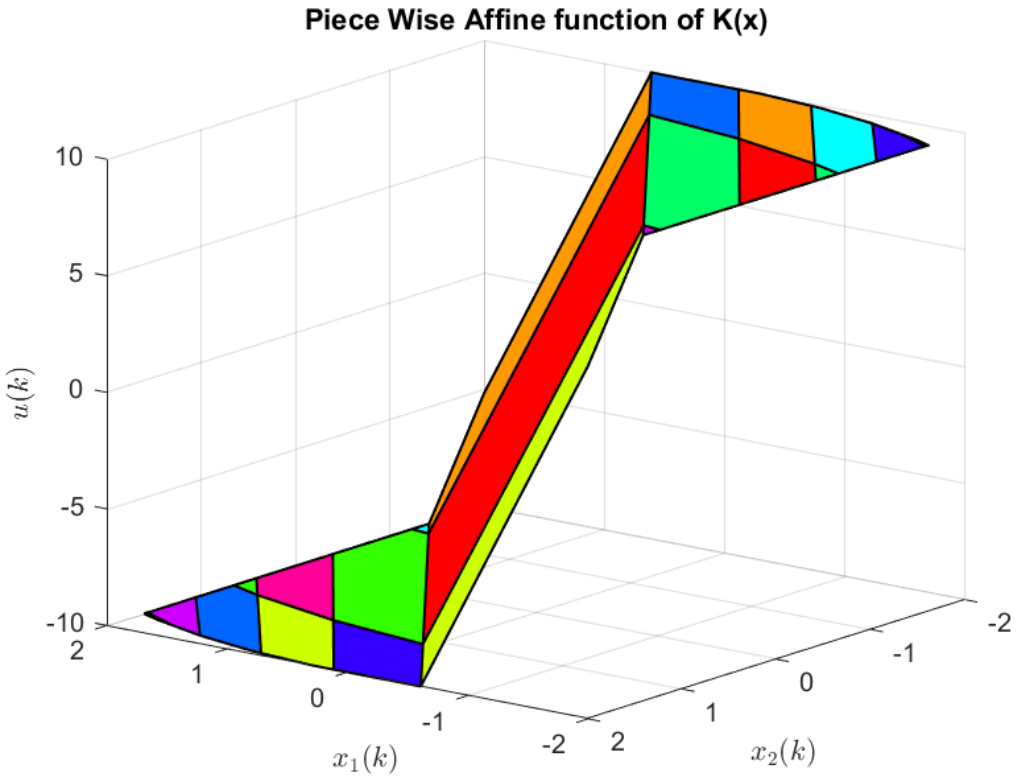


(b) States behaviour and phase-plot

Figure 4.3: System controlled by MPC without attacks.

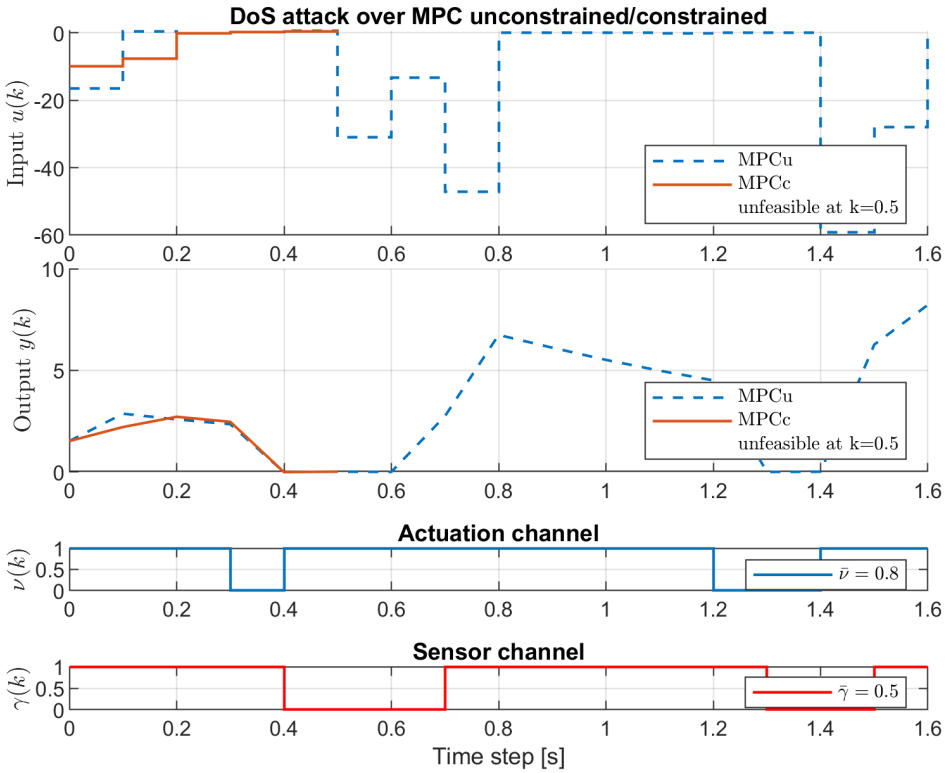


(a) Regions of Operation of the feedback control law

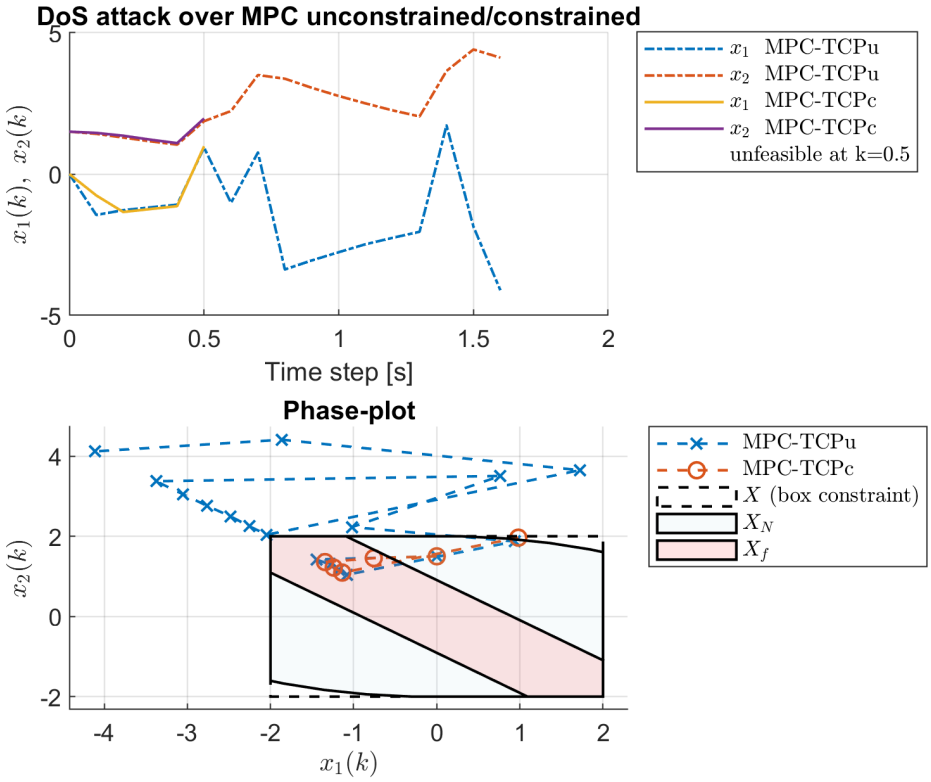


(b) PWA function of $\kappa_N(x(k))$

Figure 4.4: Regions of operations and PWA of constrained MPC without attacks.

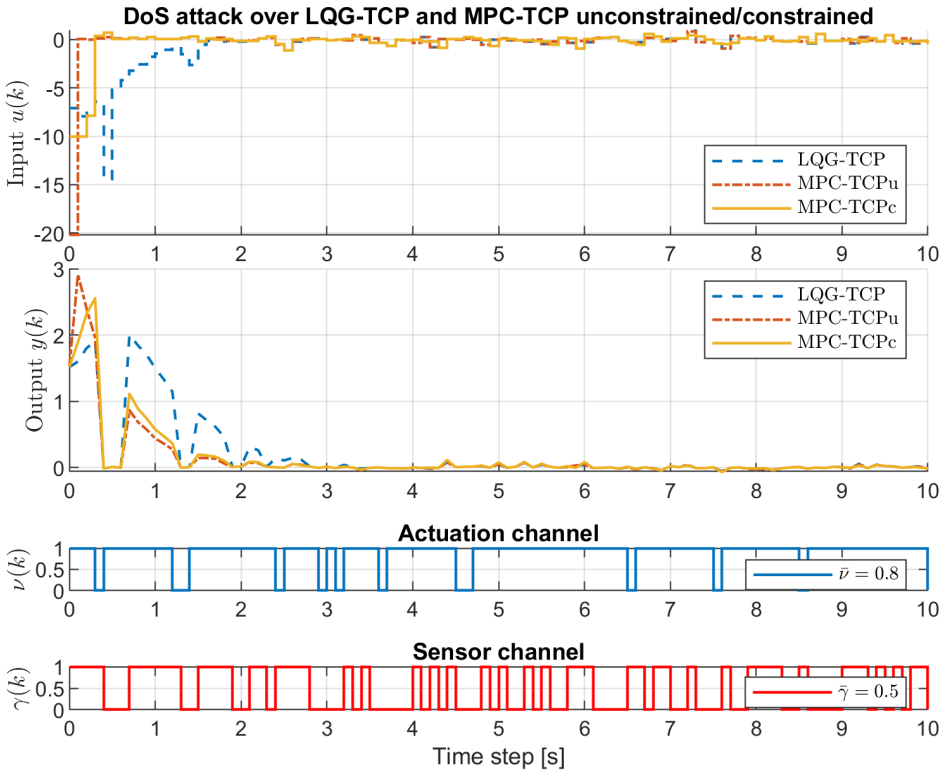


(a) Input $u(k)$ and output $y(k)$

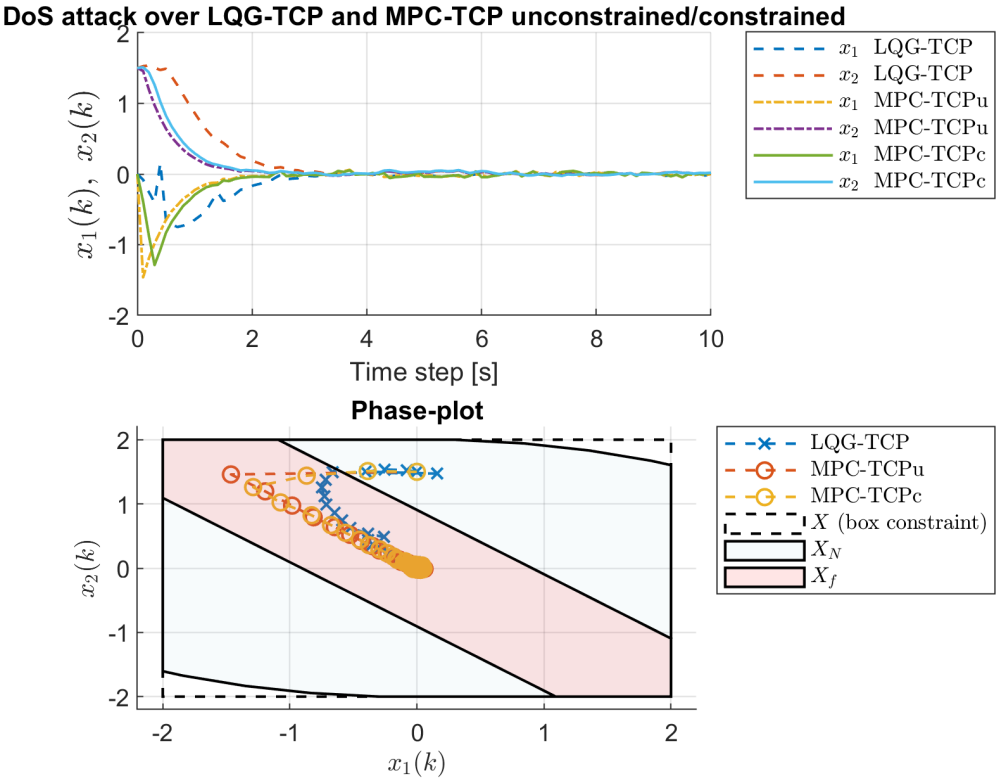


(b) States behaviour and phase-plot

Figure 4.5: MPC with DoS attack.



(a) Input $u(k)$ and output $y(k)$



(b) States behaviour and phase-plot

Figure 4.6: LQG-TCP and MPC-TCP with DoS attack.

Chapter 5

FDI attack

A FDI attack is a type of deception cyber-attack that corrupts the data over the communication channel leading the control system to work with false data that can potentially conduct the plant to an unstable region. In this chapter, an FDI attack over the sensor channel is used to analyse the system behaviour under unconstrained and constrained MPC controller. Applying a simple bad data detection criteria, the system is evaluated when the attack is detectable and undetectable. Fig. 5.1 shows the attack scheme.

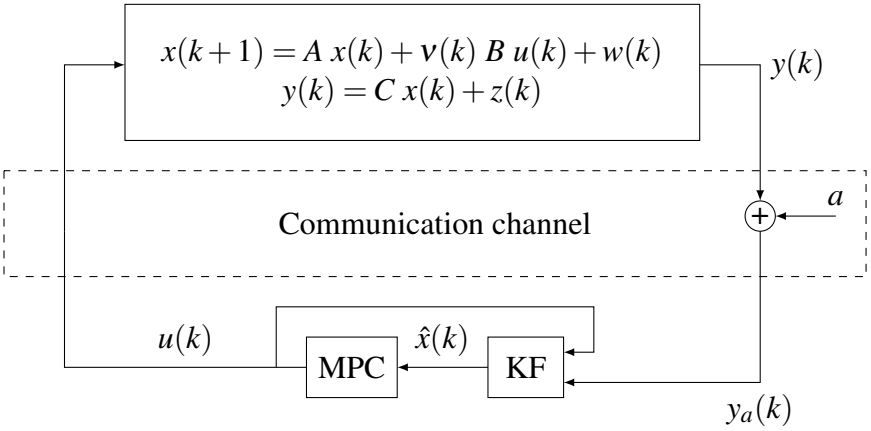


Figure 5.1: FDI attack scheme over the communication channel.

5.1 Detection method

Consider the noisy output $y(k) = C\ x(k) + z(k)$ of the discrete-time LTI state-space system in Chapter 4. Because the error over the sensor channel $z(k)$ is AWGN with $\mathcal{N}(0, R_z)$, a common method is to use a bad measurement detection using the norm-2 residual calculation to validate the integrity of the information [9]. This method es-

tablishes that the operator can decide if there is an attack or irregular behaviour in the meters of the measurement channel by performing a hypothesis testing defined as,

$$\begin{aligned} \mathcal{H}_0 &: \|y(k) - C\,\hat{x}(k)\|_2^2 < \tau \quad \text{no bad data} \\ \mathcal{H}_1 &: \|y(k) - C\,\hat{x}(k)\|_2^2 \geq \tau \quad \text{bad data present} \end{aligned} \tag{5.1}$$

where τ is the detection threshold determined by the operator.

5.1.1 Detectable attack

A detectable attack depends on the knowledge the attacker has about the system. If the attacker has access to the measurement channel and targets the output $y(k)$, such that,

$$y_a(k) = C\,x(k) + z(k) + a \tag{5.2}$$

where $a \in \mathbb{R}$ is the attack value that can be random or predefined value. The attack effect on the state estimation $\hat{x}_a$ in the closed-loop, defined in (4.6), is,

$$\begin{aligned} \hat{x}_a(k+1) &= A\,\hat{x}(k) + B\,u(k) + L_{KF}(y_a(k) - C\,\hat{x}(k)) \\ &= A\,\hat{x}(k) + B\,u(k) + L_{KF}(y(k) + a - C\,\hat{x}(k)) \\ &= A\,\hat{x}(k) + B\,u(k) + L_{KF}(y(k) - C\,\hat{x}(k)) + L_{KF}\,a \\ &= \hat{x}(k+1) + L_{KF}\,a \\ &= \hat{x}(k+1) + a_e \end{aligned}$$

where $a_e = L_{KF}\,a$ is the impact of the attack. The detection is possible applying the residual as,

$$\begin{aligned} \|y_a - C\,\hat{x}_a\|_2^2 &= \|y + a - C\,\hat{x}_a\|_2^2 \\ &= \|y + a - C(\hat{x} + a_e)\|_2^2 \\ &= \|y - C\,\hat{x} + a - C\,a_e\|_2^2 \\ &= \|y - C\,\hat{x} + a - C\,L_{KF}\,a\|_2^2 \\ &= \|y - C\,\hat{x} + a(1 - C\,L_{KF})\|_2^2 \end{aligned}$$

using the hypothesis testing,

$$\mathcal{H}_1 \ : \ \|y(k) - C\,\hat{x}(k) + a(1 - C\,L_{KF})\|_2^2 \geq \tau \tag{5.3}$$

$\mathcal{H}_1$ is satisfied and the operator determines that there is bad data in the output $y(k)$. However, the residual test only determines if there is bad data, it does not give any additional information.

5.1.2 Undetectable attack

If the attacker has knowledge about the output matrix C, and the observer gain of the estimation process, an undetectable and even more over harmful attack can be performed on the state estimation if $a = C\ L\ c$, where $c \in \mathbb{R}^n$ is the attack vector, and L is the observer gain.

Defining $a = C\,L_{KF}\ c$, the effect of the attack in (4.6) is,

$$\begin{aligned}
\hat{x}_a(k+1) &= A\,\hat{x}(k) + B\,u(k) + L_{KF}(y(k) - C(\hat{x} + c)) \\
&= A\,\hat{x}(k) + B\,u(k) + L_{KF}(y(k) - C\,\hat{x}(k)) + L_{KF}\,C\,c \\
&= \hat{x}(k+1) + L_{KF}\,C\,c \\
&= \hat{x}(k+1) + L_{KF}\,a \\
&= \hat{x}(k+1) + a_e
\end{aligned}$$

Applying the residual test, the attack is undetectable,

$$\begin{aligned}
\|y_a - C\,\hat{x}_a\|_2^2 &= \|y + a - C(\hat{x}_a)\|_2^2 \\
&= \|y + a - C(\hat{x} + a_e)\|_2^2 \\
&= \|y - C\,\hat{x} + a - C\,a_e\|_2^2 \\
&= \|y - C\,\hat{x} + C\,L_{KF}\,c - C\,L_{KF}\,c\|_2^2 \\
&= \|y - C\,\hat{x}\|_2^2
\end{aligned}$$

where the hypothesis testing results in the satisfaction of $\mathcal{H}_0$,

$$\mathcal{H}_0 \ : \ \|y(k) - C\,\hat{x}(k)\|_2^2 < \tau \tag{5.4}$$

and the operator determines that there is no bad data. Therefore, the attack on the estimation process is undetectable.

5.2 FDI attack over MPC

Because the FDI attack is over the measurement channel and the estimation process, the MPC algorithm for both scenarios, unconstrained and constrained, are the same as used in Algorithm 1 and Algorithm 2.

In addition, the stability for both cases is guaranteed if the attack $a \in \mathcal{X}_N$. On the other hand, if the attack is a function $a = f(c)$, the stability is not guaranteed. In the MPC unconstrained case, the system can easily go to the unstable region. For the MPC constrained case, if $a \notin \mathcal{X}_N$, the optimization problem is unfeasible.

5.3 Numerical example

The system for the simulation results is the same unstable non-minimum phase system of Section 4.9.1 with the addition of the FDI attack as seen in the scheme in Fig. 5.1, where the attack a is defined as,

$$\begin{aligned} \text{Detectable case:} \quad & a = 0.2 \\ \text{Undetectable case:} \quad & a = C\, L_{KF}\, c, \quad c = [0 \quad 0.2]^\intercal \end{aligned}$$

For both unconstrained and constrained MPC scenarios, the residual with attack is compared with the residual without attack to visualize the detectability and undetectability of the attack.

5.3.1 Detectable attack

Fig. 5.2 shows the behaviour of the input $u(k)$ and output $y(k)$ for the unconstrained case in the left and the constrained case in the right. Clearly the attack affects both by setting the output to track a new set point near $y = -2$. This result is because the attack can be seen as a constant disturbance in the output. Although this pseudo disturbance can be rejected with a proper MPC design, the attacker may change the constant attack

for an attack function, such that $a = f(.)$, and forces the system to the unstable region in both cases. Remember that an FDI attack is not constrained by the system dynamics and it has a malicious intention, which is different from a disturbance or a fault in the system.

Let us define a threshold detection $\tau = 0.1$, in Fig. 5.3b the residual plot for both cases shows that the attack is detectable at each step k. Therefore, the operator can determine that there is somehow of attack or disturbance of unknown nature that is affecting the system to track a setpoint instead of regulating to zero.

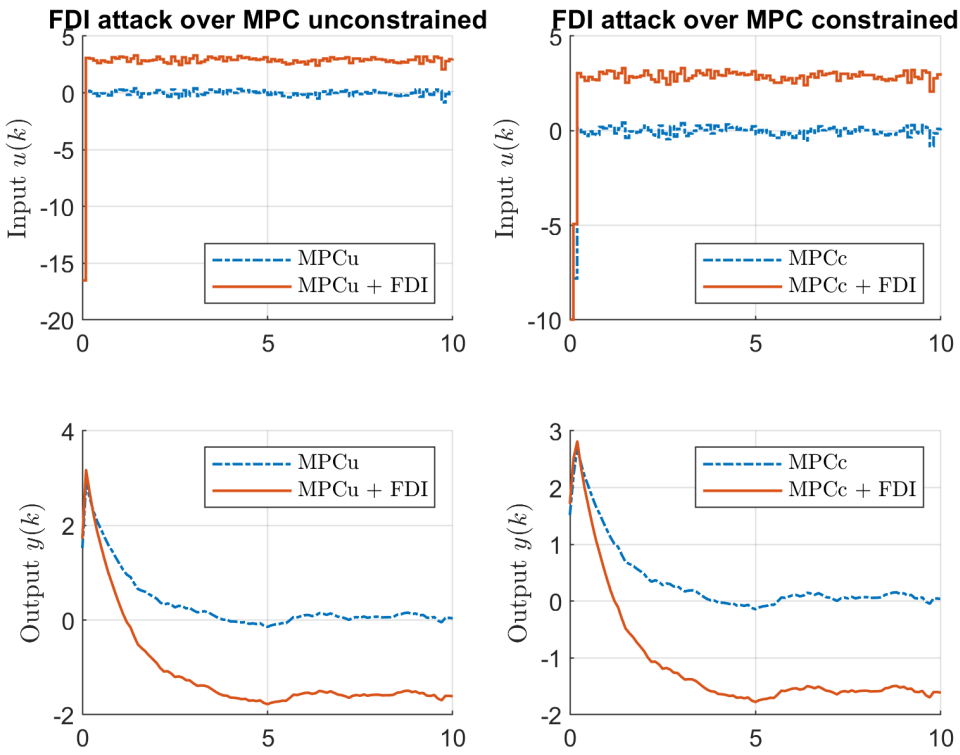
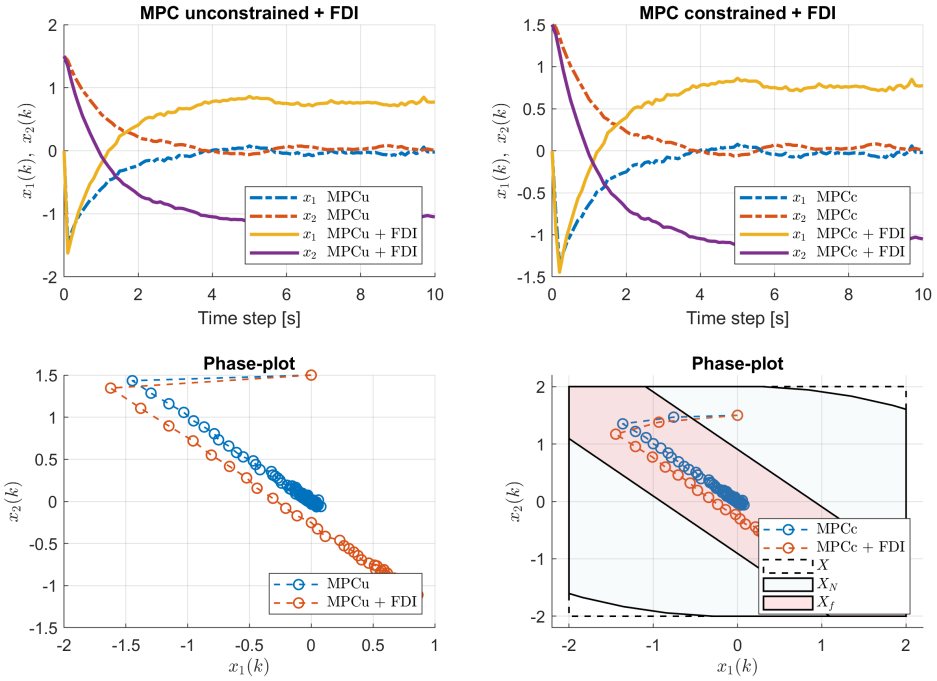


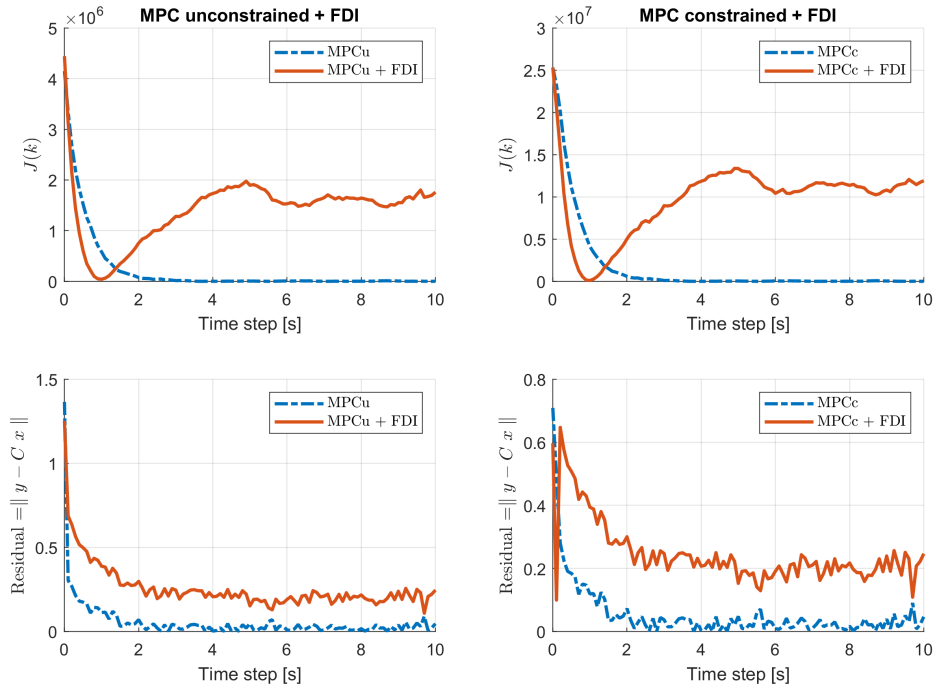
Figure 5.2: States behaviour and phase-plot for MPC with detectable FDI attack.

5.3.2 Undetectable attack

Fig. 5.4 does not show extra information than the undetectable FDI scenearion, but in Fig. 5.5b, the residual detection for both cases shows that the FDI attack can remain undetected in the steady state. During the transient response, the attack might be detected but the operator can not be sure until the system reaches the steady state. Moreover, the residual plot also shows that the with a proper attack vector c, the residual detection of



(a) States behaviour and phase-plot



(b) Cost value and residual

Figure 5.3: MPC with detectable FDI attack.

attacked MPC in the transient has lower values than the non-attacked MPC.

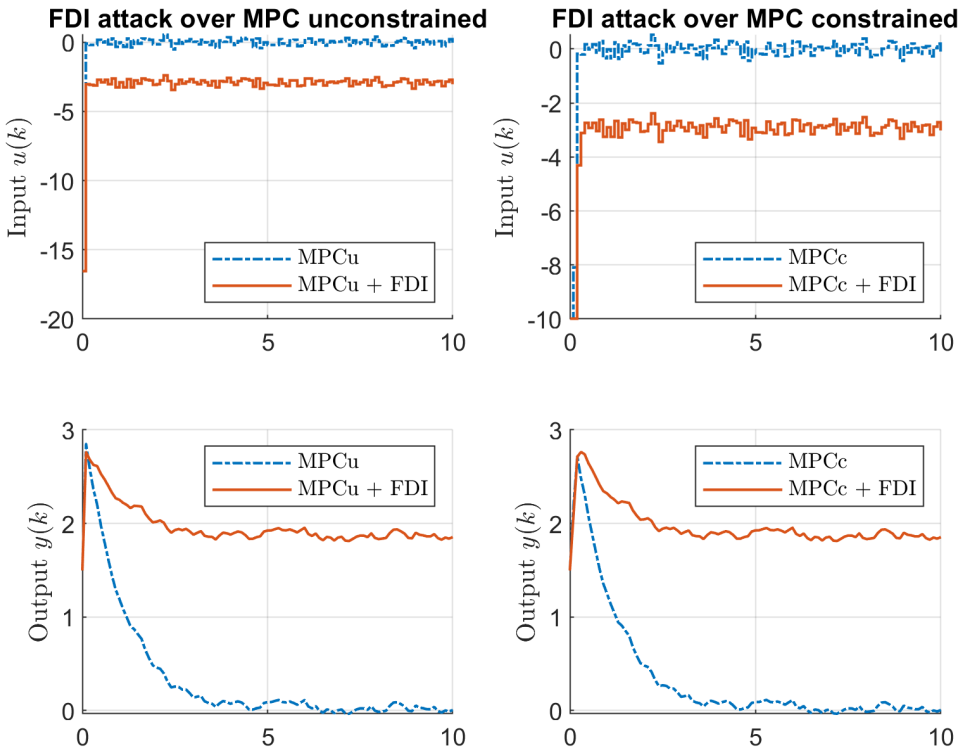
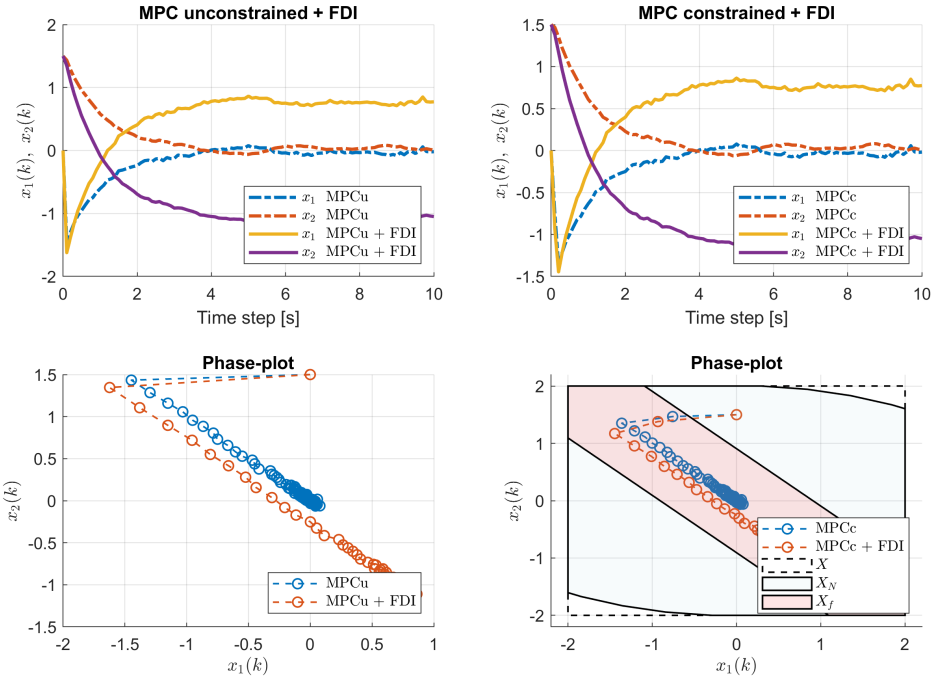
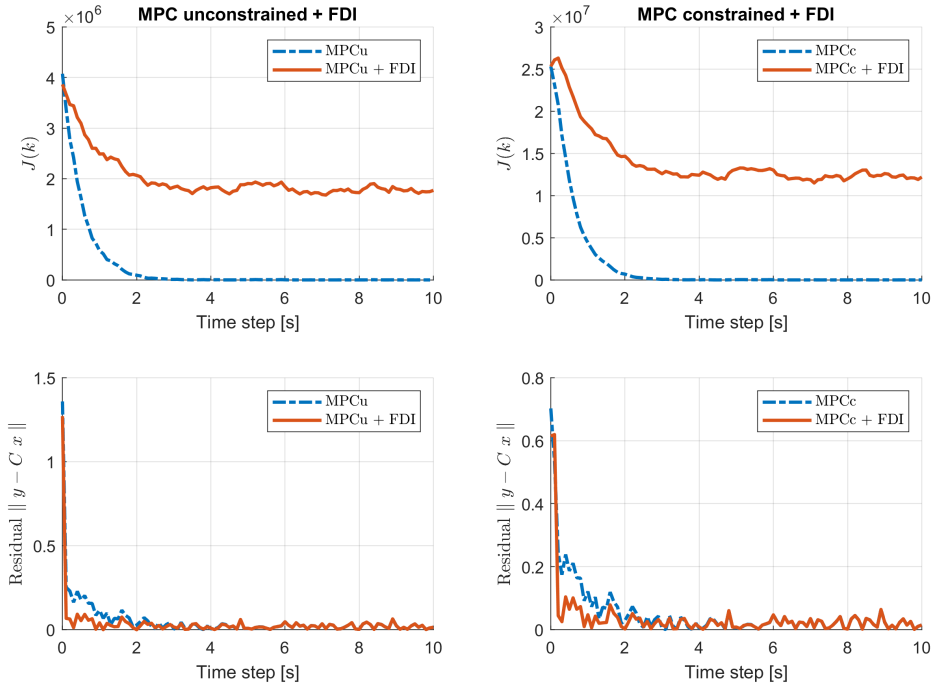


Figure 5.4: States behaviour and phase-plot for MPC with undetectable FDI attack.



(a) States behaviour and phase-plot



(b) Cost value and residual

Figure 5.5: MPC with undetectable FDI attack.

Chapter 6

Conclusions

6.1 Summary of contributions

The main contributions of this dissertation are the proposal of a constrained MPC-TCP rejection method against Bernoulli DoS attacks based on an LQG-TCP approach. Also, analytical results of the behaviour of MPC against DoS and FDI attack, and demonstration of the equivalence of the optimal solution for the unconstrained MPC-TCP and the LQG-TCP.

Literature review

In Chapter 2, it was mentioned the state of art of cyber-security on CPS from the viewpoint of control systems. Some papers and books were consulted to establish the architecture and framework of study of NCS in CPS, and two types of cyber-attacks were selected due to their potential threat level on NCS, DoS attack and FDI attack.

For the related work in DoS attacks, the LQG-TCP approach and a modified KF-TCP were selected to extend the research to the unconstrained and constrained MPC. For the FDI attack, the work that presents the basis of residual detection method was used to study the detectability of MPC against FDI attack.

MPC attacked with DoS

In Chapter 3, the background theory for MPC was summarized with the conditions for stability. In Chapter 4, the attack scheme over the communication channel, and the algorithms for the simulation in both cases, unconstrained and constrained MPC, were detailed. Also, the LQG-TCP section presented the innovation step and correction step of the KF-TCP.

MPC-TCP approach for DoS attack

In Section 4.6 of Chapter 4, it was developed the proposed MPC-TCP approach based on the LQG-TCP concept and the background theory of MPC. The formulation was presented in detail with the corresponding derivations of the solutions. For the unconstrained MPC-TCP, it was proved that the RH optimal solution $u*(k)$ is equivalent to the optimal solution of the LQG-TCP. Even though the LQG-TCP minimizes the expectation of the cost to obtain the optimal solution, the unconstrained MPC-TCP case does not use that method. It was only necessary to use a predicted diagonal matrix V as the attack v for $N-1$ steps.

For the constrained MPC-TCP, it was necessary to use the expectation of the cost function and penalize the matrix H with $\bar{v}^2$ and the matrix L with $\bar{v}$ of the QP compact form. In addition, a slack variable was added to the cost function to soft constraint the states so the on-line feasible solution can be guaranteed. This slack variable was a norm-2 proposition but a more relaxed version can be used with the norm-1. Both types were tested and validated but only the norm-2 version was implemented.

All the scenarios were tested with a numerical example that used a simple unstable non-minimum phase system in discrete LTI state-space model.

MPC attacked with FDI

Chapter 5 presented a simple FDI attack scheme over the sensor channel with the use of the residual detection method. It was presented in detail the conditions of a detectable and undetectable FDI attack, and the impact of them in the closed-loop. A detectable attack was simple to formulate and easy to detect because it had only access to the output. On the other hand, the undetectable case had knowledge about the observer gain of the estimation process, that for the MPC scheme was the gain of the Kalman Filter. For the numerical examples, the unconstrained case, and constrained case were simulated with and without attack to observe the effects.

6.2 Future work

Given the contributions in this dissertation, the following future work is mentioned as follows.

The stability conditions of the communication channel for the unconstrained MPC-

TCP method are the same as the LQG-TCP. In the constrained MPC-TPC, those conditions don not apply, and it seems they are more restrictive due the constraints of the system. It is necessary to investigate the stability conditions for the packet losses given strong DoS attacks, e.g. $\bar{\nu} \approx 0.3,\ \bar{\gamma} \approx 0.3$.

The KF-TCP works very well against DoS attack, but the Moving Horizon Estimation (MHE) needs to be investigated as an alternative of the KF-TCP because MHE is the dual of the MPC method and it can handle constraints in the estimation process. The sliding window method in [23] is a good start point to tackle this problem.

From the viewpoint of the attacker, optimized attacks can be tested over the unconstrained and constrained MPC-TCP approach to study the robustness and stability. A DoS detection method can be introduced in the MPC-TCP problem formulation. Also, constrained MPC for UDP channel needs to be investigated due the existence of LQG-UDP solution.

To explore feasibility solutions, chance constraints seems to suit in MPC-TCP given the stochastic properties of chance constraints. Finally, it is worth it to extend the research to Distributed MPC against DoS and FDI attacks to analyse the stability and robustness.

REFERENCES

[1] Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, and Maria Domenica Di Benedetto. "State of the art of cyber-physical systems security: An automatic control perspective". In: *Journal of Systems and Software* 149 (2019), pp. 174–216. DOI: 10.1016/j.jss.2018.12.006.

[2] Zhong-Hua Pang, Guo-Ping Liu, Donghua Zhou, and Dehui Sun. *Networked Predictive Control of Systems with Communication Constraints and Cyber Attacks*. Springer Singapore, 2019. DOI: 10.1007/978-981-13-0520-7.

[3] Peng Cheng, Heng Zhang, and Jiming Chen. *Cyber Security for Industrial Control Systems: from the viewpoint of close-loop*. Taylor & Francis Ltd., Mar. 23, 2016. 325 pp.

[4] T M Chen and S Abu-Nimeh. "Lessons from Stuxnet". In: *Computer* 44.4 (2011), pp. 91–93. DOI: 10.1109/mc.2011.115.

[5] André Teixeira, Kin Cheong Sou, Henrik Sandberg, and Karl Henrik Johansson. "Secure Control Systems: A Quantitative Risk Management Approach". In: *IEEE Control Systems* 35.1 (2015), pp. 24–45. DOI: 10.1109/mcs.2014.2364709.

[6] Erfan Nozari, Pavankumar Tallapragada, and Jorge Cortés. "Differentially Private Average Consensus with Optimal Noise Selection". In: *IFAC-PapersOnLine* 48.22 (2015), pp. 203–208. DOI: 10.1016/j.ifacol.2015.10.331.

[7] Fabio Pasqualetti, Florian Dorfler, and Francesco Bullo. "Attack Detection and Identification in Cyber-Physical Systems". In: *IEEE Transactions on Automatic Control* 58.11 (2013), pp. 2715–2729. DOI: 10.1109/tac.2013.2266831.

[8] Yilin Mo and Bruno Sinopoli. "False Data Injection Attacks in Control Systems". In: *Proc. 1st Workshop Secure Control Systems* (2010).

[9] Yao Liu, Peng Ning, and Michael K. Reiter. “False data injection attacks against state estimation in electric power grids”. In: *ACM Transactions on Information and System Security* 14.1 (2011), pp. 1–33. DOI: 10.1145/1952982.1952995.

[10] Claudio De Persis and Pietro Tesi. “Input-to-State Stabilizing Control Under Denial-of-Service”. In: *IEEE Transactions on Automatic Control* 60.11 (2015), pp. 2930–2944. DOI: 10.1109/tac.2015.2416924.

[11] Shan Liu, Shanbin Li, and Bugong Xu. “Event-triggered resilient control for cyber-physical system under denial-of-service attacks”. In: *International Journal of Control* (2018), pp. 1–13. DOI: 10.1080/00207179.2018.1537518.

[12] Saqib Ali, Taiseera Al Balushi, Zia Nadir, and Omar Khadeer Hussain. *Cyber Security for Cyber Physical Systems*. Springer International Publishing, 2018. DOI: 10.1007/978-3-319-75880-0.

[13] Zhiheng Xu and Quanyan Zhu. “Secure and Resilient Control Design for Cloud Enabled Networked Control Systems”. In: *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy - CPS-SPC '15*. ACM Press, 2015. DOI: 10.1145/2808705.2808708.

[14] Luca Schenato, Bruno Sinopoli, Massimo Franceschetti, Kameshwar Poolla, and S. Shankar Sastry. “Foundations of Control and Estimation Over Lossy Networks”. In: *Proceedings of the IEEE* 95.1 (2007), pp. 163–187. DOI: 10.1109/jproc.2006.887306.

[15] Sergio Lucia, Markus Kögel, Pablo Zometa, Daniel E. Quevedo, and Rolf Findeisen. “Predictive control, embedded cyberphysical systems and systems of systems – A perspective”. In: *Annual Reviews in Control* 41 (2016), pp. 193–207. DOI: 10.1016/j.arcontrol.2016.04.002.

[16] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M.I. Jordan, and S.S. Sastry. “Kalman Filtering With Intermittent Observations”. In: *IEEE Transactions on Automatic Control* 49.9 (2004), pp. 1453–1464. DOI: 10.1109/tac.2004.834121.

[17] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, and S.S. Sastry. “Optimal control with unreliable communication: the TCP case”. In: *Proceedings of the*

2005, American Control Conference, 2005. IEEE, 2005. DOI: 10.1109/acc.2005.1470488.

[18] Orhan C. Imer, Serdar Yüksel, and Tamer Başar. "Optimal control of LTI systems over unreliable communication links". In: *Automatica* 42.9 (2006), pp. 1429–1439. DOI: 10.1016/j.automatica.2006.03.011.

[19] Daniel E. Quevedo, Prabhat K. Mishra, Rolf Findeisen, and Debasish Chatterjee. "A Stochastic Model Predictive Controller for Systems with Unreliable Communications". In: *IFAC-PapersOnLine* 48.23 (2015), pp. 57–64. DOI: 10.1016/j.ifacol.2015.11.262.

[20] Daniel E. Quevedo and Dragan Nešić. "Robust stability of packetized predictive control of nonlinear systems with disturbances and Markovian packet losses". In: *Automatica* 48.8 (2012), pp. 1803–1811. DOI: 10.1016/j.automatica.2012.05.046.

[21] Liang Hu, Zidong Wang, Qing-Long Han, and Xiaohui Liu. "State estimation under false data injection attacks: Security analysis and system protection". In: *Automatica* 87 (2018), pp. 176–183. DOI: 10.1016/j.automatica.2017.09.028.

[22] Albert Rosich, Holger Voos, Yumei Li, and Mohamed Darouach. "A model predictive approach for cyber-attack detection and mitigation in control systems". In: *52nd IEEE Conference on Decision and Control*. IEEE, 2013. DOI: 10.1109/cdc.2013.6760937.

[23] Angelo Barboni, Francesca Boem, and Thomas Parisini. "Model-based Detection of Cyber-Attacks in Networked MPC-based Control Systems". In: *IFAC-PapersOnLine* 51.24 (2018), pp. 963–968. DOI: 10.1016/j.ifacol.2018.09.691.

[24] James B. Rawlings and Mayne David Q. *Model Predictive Control Theory and Design*. Nob Hill Pub, Llc, 2009. ISBN: 9780975937709.

[25] Rossiter J.A. *Model-Based Predictive Control. CRC Press. 2003.* CRC Press Inc, 2003. ISBN: 0-203-50396-1.

[26] Jan Maciejowski. *Predictive Control with Constraints*. Prentice Hall, 2000. ISBN: 978-0201398236.

[27] Saurabh Amin, Alvaro A. Cárdenas, and S. Shankar Sastry. “Safe and Secure Networked Control Systems under Denial-of-Service Attacks”. In: *Hybrid Systems: Computation and Control*. Springer Berlin Heidelberg, 2009, pp. 31–45. DOI: 10.1007/978-3-642-00602-9_3.

The University Of Sheffield.

Automatic Control & Systems Engineering.

ACS6200: Individual Project – Aim and Objectives

Student name: Paulo Roberto Loma Marconi

Student Reg No: 180123717

Project code and Title: PT1 – Study of the robustness and stability of Model Predictive Control (MPC) against cyber-attacks.

Supervisor: Dr. P. Trodden

Second Reader:

Project Aim:

The project aim is study the robustness and stability of a Model Predictive Control (MPC) system against different types of cyber-attacks in the feedback loop.

Project Objectives, to be described as:

Basic Objectives:

- Review the literature of cyber-attacks on MPC systems.
- Stablish the framework of study of the MPC system.
- Determine the types of cyber-attacks to be used in the evaluation.
- Formulate the MPC scheme with the selected cyber-attacks.
- Analyse the robustness and stability of the case-study.
- Evaluate the performance of the case-study by software simulation.

Advanced Objectives:

- Propose an attack detection/rejection method and a resilient control strategy for MPC.

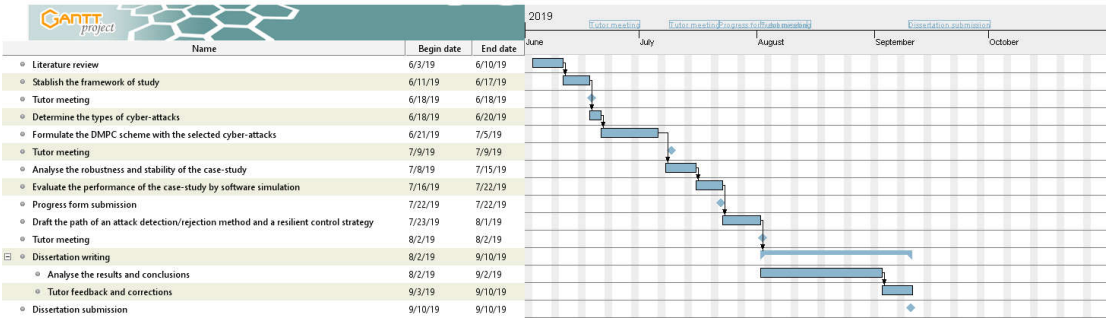
My project requires components/items to be purchased and I confirm that I have completed the budget request form on MOLE (please answer yes/no in the box on the right)	No
Will (or do you anticipate) that any part of your project will require **ethics** approval? – (please check with your supervisor and answer yes/no in the box on the right)	No
Will (or do you anticipate) that any part of your project will be **confidential**? – (please check with your supervisor and answer yes/no in the box on the right)	No

Please attach (as an additional sheet) your project work plan in the form of Gantt chart

Student name (Print): ...Paulo Roberto Loma Marconi .....

Date:..... 13 – 05 – 19 .....

It is the student's responsibility to complete this form in consultation with the project supervisor and handbook. Please submit the completed form by the due date. Failure to do so will incur a penalty for the project mark.



Name	Begin date	End date
Literature review	6/3/19	6/10/19
Stablish the framework of study	6/11/19	6/17/19
Tutor meeting	6/18/19	6/18/19
Determine the types of cyber-attacks	6/18/19	6/20/19
Formulate the DMPC scheme with the selected cyber-attacks	6/21/19	7/5/19
Tutor meeting	7/9/19	7/9/19
Analyse the robustness and stability of the case-study	7/8/19	7/15/19
Evaluate the performance of the case-study by software simulation	7/16/19	7/22/19
Progress form submission	7/22/19	7/22/19
Draft the path of an attack detection/rejection method and a resilient control strategy	7/23/19	8/1/19
Tutor meeting	8/2/19	8/2/19
Dissertation writing	8/2/19	9/10/19
Analyse the results and conclusions	8/2/19	9/2/19
Tutor feedback and corrections	9/3/19	9/10/19
Dissertation submission	9/10/19	9/10/19

The University Of Sheffield.

Automatic Control & Systems Engineering.

ACS6200: Individual Project – Progress Review Form

It is the student's responsibility to complete this form

The student should discuss their progress with their supervisor when completing the form

After submission of this form, the supervisor will be asked to check and mark progress as satisfactory or unsatisfactory – if unsatisfactory the module leader will be notified

The completed form should be included in the student's submitted dissertation (in the Appendix)

Student name: Paulo Roberto Loma Marconi

Student Reg No: 180123717

Project code and Title: – Study of the robustness and stability of Model Predictive Control systems against cyber-attacks

Supervisor: Dr. P. Trodden

Second Reader:

Project Progress against objectives (in bullet-points):

- Review the literature of cyber-attacks on MPC systems.
- Stablish the framework of study of the MPC system.
- Determine the types of cyber-attacks to be used in the evaluation.

Main tasks to be completed in the next 4 weeks (in bullet-points):

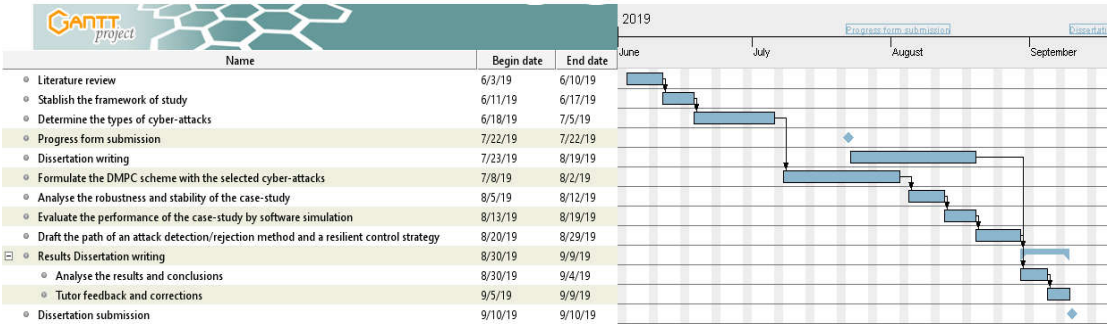
- Formulate the MPC scheme with the selected cyber-attacks.
- Analyse the robustness and stability of the case-study.
- Evaluate the performance of the case-study by software simulation.

(any barriers preventing you to progress as planned?)

None

Please attach (as an additional sheet) your updated project work plan in the form of a Gantt chart

Student name (Print): ... Paulo Roberto Loma Marconi ..... Date: ... 22 – 07 – 19 .....



Name	Begin date	End date
Literature review	6/3/19	6/10/19
Stablish the framework of study	6/11/19	6/17/19
Determine the types of cyber-attacks	6/18/19	7/5/19
Progress form submission	7/22/19	7/22/19
Dissertation writing	7/23/19	8/19/19
Formulate the DMPC scheme with the selected cyber-attacks	7/8/19	8/2/19
Analyse the robustness and stability of the case-study	8/5/19	8/12/19
Evaluate the performance of the case-study by software simulation	8/13/19	8/19/19
Draft the path of an attack detection/rejection method and a resilient control strategy	8/20/19	8/29/19
Results Dissertation writing	8/30/19	9/9/19
Analyse the results and conclusions	8/30/19	9/4/19
Tutor feedback and corrections	9/5/19	9/9/19
Dissertation submission	9/10/19	9/10/19