Security of the Distributed Model Predictive Control

Sylvain Chatel, Pierre Haessig, Romain Bourdais

Security of the Distributed Model Predictive Control

Sylvain Chatel, Pierre Haessig and Romain Bourdais.
CentraleSupélec - IETR - UMR 6164, France
Email : sylvain.chatel@supelec.fr, {pierre.haessig ; romain.bourdais}@centralesupelec.fr

***Résumé*—In this paper, we explore the security of a distributed model predictive control (DMPC) scheme. A global system is decomposed into several local subsystems which share a common resource. For instance a heating problem among several rooms with a limited amount of power. Each subsystem owns a model predictive control (MPC) controller which cooperates and works iteratively with all the other controllers in order to reach the system's objective. Here, we focus on the security of such a system. Indeed, we report that a user could disturb the DMPC through several attacks in order to destabilize the resource distribution. Hence, examples of cheating protocols and counter-cheat ideas are presented and discussed.**

I. Introduction

Model predictive control (MPC), also known as *receding horizon control*, is becoming more and more popular in the industrial process control [1], [2]. Among other benefits, the attractiveness of the MPC lies in its ability to represent clearly the constraints of the optimization problem [3]. Over the past decades, the MPC has become widespread and many successful applications have been developed in the process industry.

In an MPC, the objective is to get the optimal control input over a given horizon by solving a discrete-time optimal control problem. Traditionally, this kind of control is done by a controller in a centralized way. This controller have full knowledge of the system over the horizon. Although efficient, this schemes might sometimes be inadequate. For instance, for large-scale interconnected systems such as power and water distribution or even traffic systems (with plug and play), a centralized MPC might not be ideal or even technically feasible [3]. Moreover, the fact that the controller is omniscient and fully knowledgeable might be an obstacle because some agents might not be able to divulge information about their local subsystem. This might be the case as [2] points out for the newly regulated power markets in the United States.

Hence the idea of developing a distributed system. The global system is decomposed into several subsystems. Each subsystem has a MPC controller which communicates with the others. Local control inputs are then locally computed and determined with the few information shared. For instance, when a decentralized control scheme (where local control input are determined based on local measurements for instance) is needed, a distributed MPC is a better choice. For example, for water distribution systems, a centralized MPC is decomposed into a DMPC using a coordinator (e.g. augmented Lagrangian [2] or Uzawa method [4] depending on the type of dependence between the subsystems).

Several distributed MPC examples are available in the literature. DMPC frameworks were developed in [5], [6] and [7]. In the latest, a MPC framework is developed for a system with several independent subsystem dynamics but nonetheless linked through their cost functions.

In a DMPC, each agent communicates with the others via a simple coordinator. This latest, returns a simple information (e.g. a Lagrangian multiplier for an augmented Lagrangian technique). All the information required for the system to work efficiently is communicated through this small amount of data. As pointed out in [8], though efficient the DMPC still suffers from some risks. Indeed, DMPC might sometimes be harmful to the physical system. For instance in a complex system such as a power grid, human error, malicious and misleading agents could easily disturb the grid. According to Brooks in [8], one of the best ways to mitigate those security threats is to involve a combination of counter measures such as using fault detection softwares, limiting the size of each entity or even certifying aggregators. However, to the best of our knowledge, there has been no comprehensive study on security threats and counter measures at the level of DMPC algorithms (as opposed to the lower level layers like communication protocols). This article is a first attempt to bridge this gap.

The paper is organised as follow. Section II introduces the model of DMPC for power distribution we used in our study. In Section III, a study of the base cases is conducted. The security threats are implemented and studied in section IV. In Section V, the main contribution of this study are summarized.

II. Model

In this paper, we consider a linear time-invariant (LTI) system composed of m interconnected subsystems. Each subsystem represents a room with a thermal resistance R_{th_i} and a thermal conductivity C_{th_i}. Taking into account the exterior temperature T_{ext}, the objective is for the temperature of each room T_i to be as close as possible to the reference temperature T_{id}^i at each time. All rooms are getting their power from a limited global amount of power U_{max}, and each user has a maximum admissible power u_{max}^i due to its physical configuration. We note u_i the power consumed by user i. Since the consumed power cannot exceed the

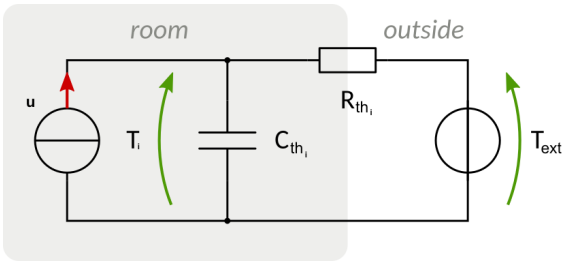

FIGURE 1. Thermal model of a room. R_{th_i} represents the thermal resistance and C_{th_i} the thermal conductivity of the room. U is the consumed power, T the temperature of the room and T_{ext} the external temperature.

maximum admissible power, and since the global power resource is limited, we have the first two constraints :

$$\forall i \in [\![0, m-1]\!],\ 0 \leq u_i \leq u^i_{max} \tag{1}$$

$$\sum_{i=0}^{m-1} u_i \leq U_{max} \tag{2}$$

The main objective is to minimize the consumed energy represented by the sum. In order to take into account the will of each user to reach its ideal temperature, we introduced a comfort factor α. Hence the optimization problem is to minimize the following cost function subjected to 1 and 2.

$$J_u = \sum_{i=0}^{m-1} u_i \ + \ \sum_{i=0}^{m-1} \alpha_i (T_i - T^i_{id})^2 \tag{3}$$

In order to determine the J_u, we used the thermal model presented in Figure 1.

With this model, it is possible to use the state-space representation of the problem. We can set $\boldsymbol{X}[t_k]$ as the temperature vector of each room. $\boldsymbol{U}[t_k]$ represents the consumed energy of each room and $\boldsymbol{U}_{ext}[t_k]$ the external temperature. With those notations, we can write :

$$\boldsymbol{X}[t_{k+1}] \ = \ A.\boldsymbol{X}[t_k] + B.\boldsymbol{U}[t_k] + B'.\boldsymbol{U}_{ext}[t_k] \tag{4}$$

Given equation (4), and the model, we can replace the temperature in equation (3). This enables us to have a quadratic problem in $\boldsymbol{U}$:

$$J_u = \boldsymbol{U}^T P \boldsymbol{U} + q^T \boldsymbol{U} + cst \tag{5}$$

In order to proceed to a centralized MPC, we just have to minimize 5 subjected to 1 and 2. However, in order to have a DMPC, we need to decompose the computation to all users. To this end, we used an Uzawa method. The idea is to unconstrain the optimization problem and relax the constraint in 2. Then, after solving the optimization problem, we iterate the Lagrangian multiplier λ.

$$\lambda_{k+1} = \lambda_k + p * (\sum_{i=0}^{m} u^*_i[t_k] - U_{max}) \tag{6}$$

In 6, p represents the step of the Uzawa iteration and $u^*_i[t_k]$ the optimal consumption of user i at t_k. This iterative procedure is done until the difference between $\sum_{i=0}^{m-1} u^*_i[t_k]$

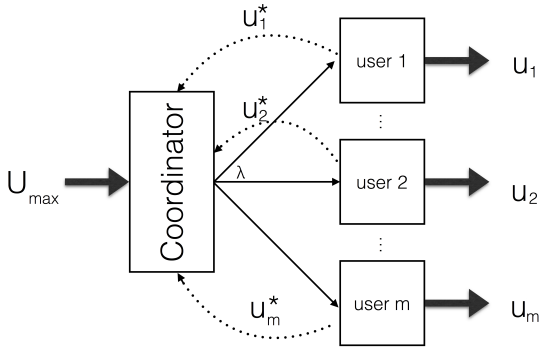

FIGURE 2. Structure of the distributed problem

and U_{max} is lower than a threshold. We note λ_{opt} the value of the multiplier fulfilling this condition.

To summarize, the DMPC requires to solve the following quadratic problem over a prediction horizon N for a simulation lasting over N_{sim} :

$$\begin{cases} \min J_u[t_k] = \boldsymbol{U}[t_k]^T P \boldsymbol{U}[t_k] + q^T \boldsymbol{U}[t_k] + cst[t_k] + \lambda[k_{opt}] \\ \text{subjected to} \\ \forall t_k \in [\![0, N_{sim}-1]\!], \forall i \in [\![0, m-1]\!],\ 0 \leq u_i \leq u^i_{max} \end{cases} \tag{7}$$

In our study, we simulate 24 hours, which is $N_{sim} = 240$ points with a time step $\Delta t = 0.1h$.

III. BASE CASES

In this section, we present the results for the nominal experiment of power distribution in several cases : the static case, the centralized dynamic case and the distributed dynamic case. All those simulations were made via the python module we developed. This package relies on M. Andersen, J.Dahl and L. Vandenberghe *cvxopt* package for convex optimization [9].

A. Static case

1) Centralized case: Let us consider a problem with three different users. We consider, at first, that all users are identical. We set the system so that $U_{max} = 3kW$ is inferior to the sum of all admissible temperature.

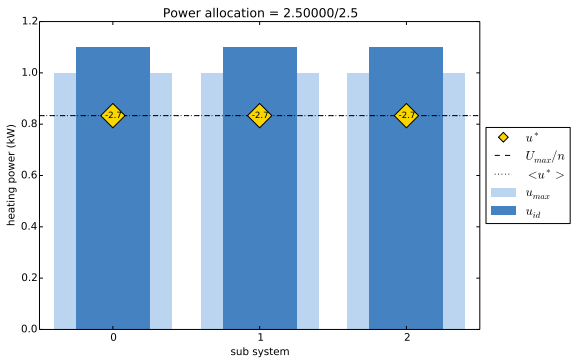

FIGURE 3. Optimal power distribution in a static symmetrical case

Now, if we change the comfort factor of user 2 in order for him to be more comfortable. To do so, let us take $\alpha_2 = 10 \times \alpha_0$.

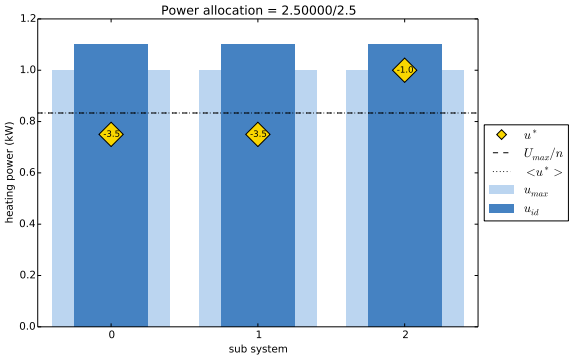

FIGURE 4. Optimal power distribution in a static case with different priorities, $\alpha_2/\alpha_0 = 10$

When comparing Figure 3 and 4, we notice that the third user ($n°2$ is indeed preferred in the power distribution and then its comfort becomes better to the disadvantage of the others (i.e. the square deviation to the ideal temperature of the third user ($n°2$ is the smallest of all users).

2) Distributed case: When we decompose the centralized computation with the Uzawa method, we are able to model a distributed optimization. At first we consider a symmetrical situation.

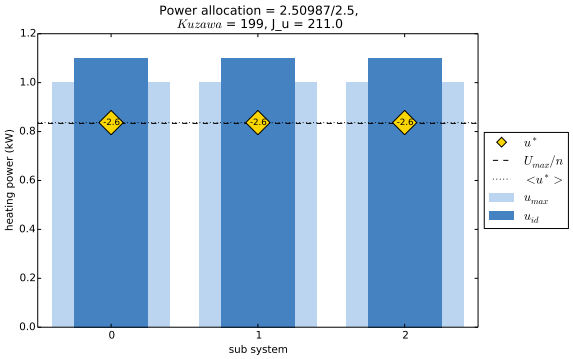

FIGURE 5. Optimal power distribution in a static symmetrical distributed case

Now, if we change the comfort factor of user 2 in order for him to more comfortable. To do so, let us take $\alpha_2 = 10 \times \alpha_0$.

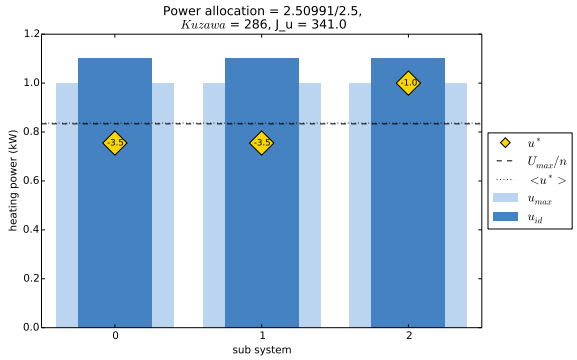

FIGURE 6. Optimal power distribution in a static distributed case with different priorities, $\alpha_2/\alpha_0 = 10$

When comparing Figure 5 and 6, we also notice that user 2 is more satisfied to the disadvantage of user 0 and 1. We notice as well that the total amount of consumed energy is superior to U_{max}. This phenomenon is due to the constraint relaxation executed in the Uzawa method.

Through this nominal static study, we were able to determine the influence of all the different parameters on the optimal solution among which the Uzawa step determination to have a convergence of the Uzawa iteration. We then used those results in the study and set $p = 1.5$.

B. Dynamic case

Now, we consider a dynamic simulation on a horizon of 24 hours. Three different users are using a limited amount of energy $U_{max} = 3kW$. The ideal temperature is determined with a time based profile : between 6:30-8:30 am and 18:00-22:00 pm the user wishes to have a temperature $T_{pres} = 22°C$ (people are present in the room), the rest of the time the temperature is set to $T_{abs} = 18°$.

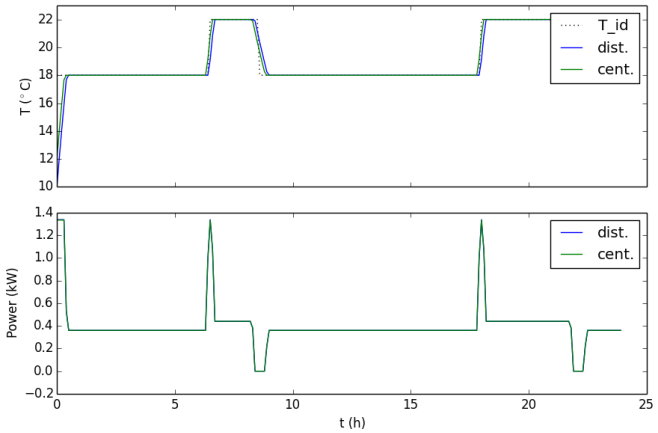

FIGURE 7. Optimal power distribution in a dynamic case for user 2 in a symmetrical problem

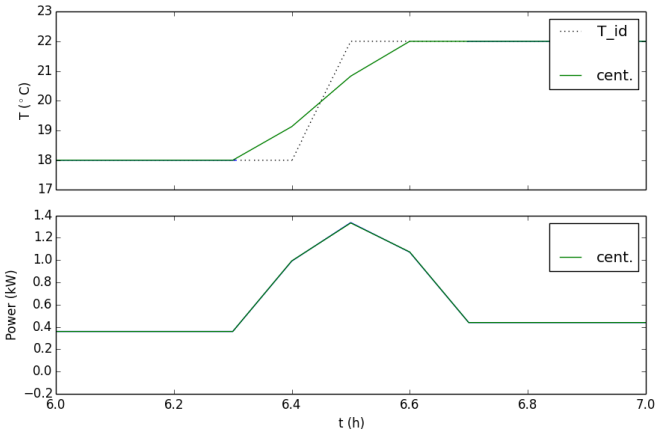

FIGURE 8. Optimal power distribution in a dynamic case for user 2 in a symmetrical problem, focus between 6:30-8:30 am

As before, we now consider a situation where user 2 is preferred and has a comfort factor ten times superior to others.

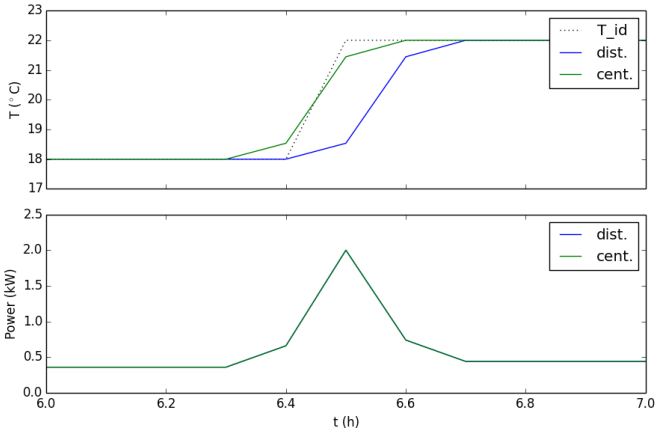

FIGURE 9. Optimal power distribution in a dynamic case for user 2 when it is preferred, $\alpha_2/\alpha_0 = 10$, focus between 6:30-8:30 am

We notice comparing Figures 8 and 9 that in the second case, user 2 is given mush more energy when needed and hence can reach its ideal temperature much faster.

From this point on, we are able to use this model to begin the study of cheating and misleading scenarios.

IV. SECURITY ISSUES : MISLEADING AND CHEATING USERS

In this section, we will focus on the security issues of the DMPC. First, we will analyse the different ways of cheating before putting it into application on static and then dynamic situations.

A. Security concepts

First of all, we must clarify the concept of security breach in a DMPC. Through our research, we were able to detect two kinds of threatening users : greedy users (whose objective is to maximize their comfort) and nihilist users (whose objective is to destroy the system).

In Figure 10, we can see an overview of the different threat we detected. The reader can note that even if other strategies might exist, we realized that all the other strategies can be somehow reduced to one of those we studied.

Moreover, for our study we considered that the transmission canal is ideal and that the communication cannot be altered. Indeed with the current knowledge, security protocols enable us to safely communicate and to change ones identity. This implies that in our model cheating by usurping ones identity or by altering the communication is not considered. Moreover, unless the demand profile of the users are complementary, the strategy of regrouping is ineffective.

To summarize, the base attack cases are as follow :

- Change its own comfort factor α_i.
- Do not listen to the DMPC talks ie the Uzawa iterations results to satisfy the global power limitation.
- Listen partially to the DMPC talks. This means the user only takes a fraction of the multiplier λ.
- Duplicate itself. In other words, a user broadcast to the others that he is two or more users in order to get more power.

B. Security in static situations

Now, we implement those strategies into the static model.

First, we implemented the influence of the comfort factor α. The idea was to determine to which extent this parameters changes the power distribution. In Figure 11, we represented the optimal power distribution and the temperature deviation for two users when the comfort factor is a parameter. We noticed that, as expected, when the one user comfort factor is superior to the one of the others, it receives much more energy and as therefore a better comfort.

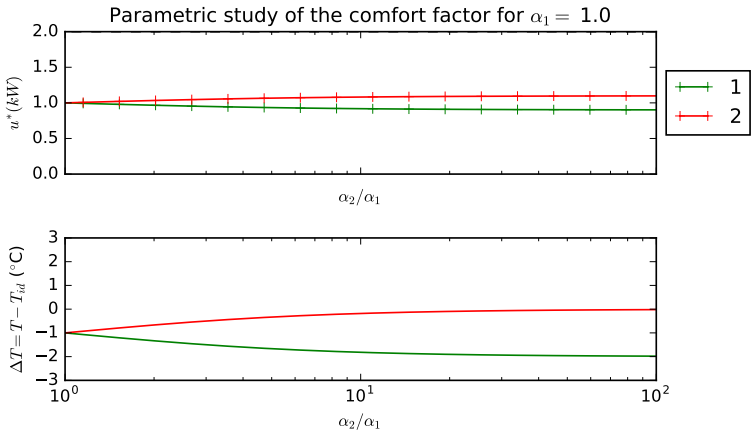

FIGURE 11. Parametric study of the comfort factor for two users

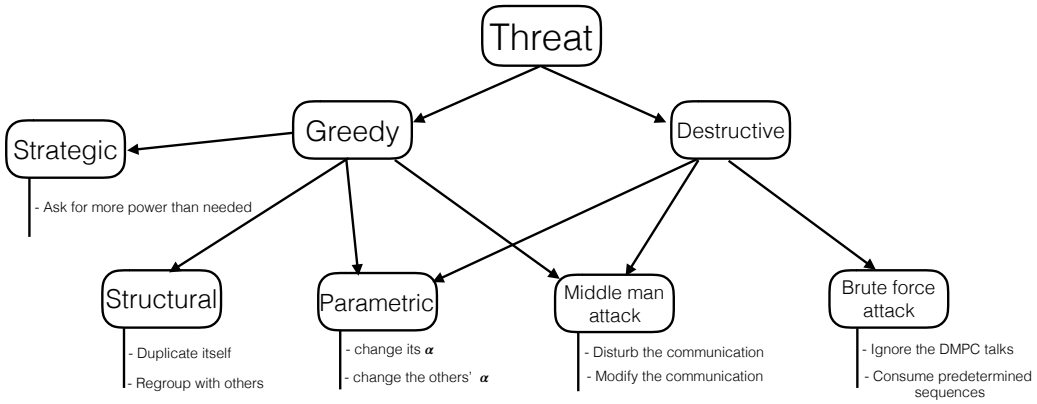

FIGURE 10. Overview of different threatening methods

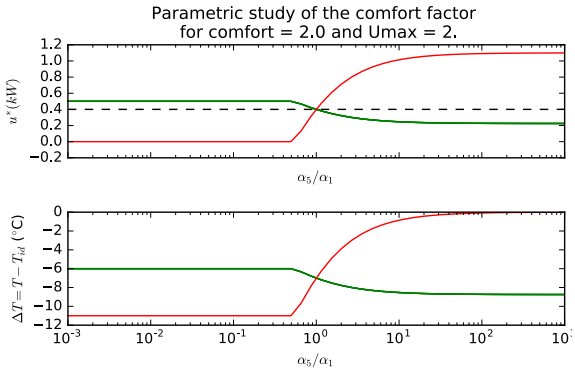

FIGURE 12. Parametric study of the comfort factor for five users

Then, we determine the influence of the ideal temperature on the distribution. In Figure 13 is represented the power distribution and the temperature deviation as functions of the broadcasted temperature. We notice that the higher this temperature is, the more energy the user receives and the less its deviation is. Please note that in our model if a user receives energy, this user has to consume it (hence the positive deviation in Figure 13).

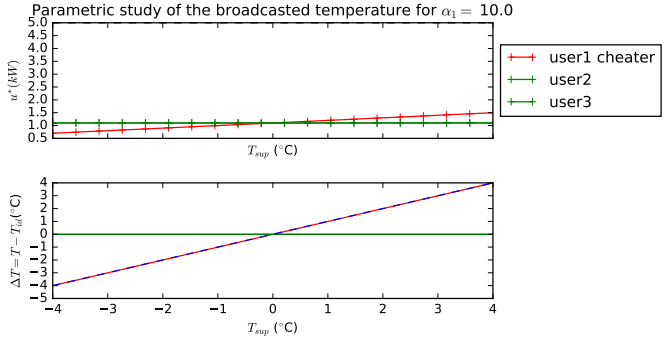

FIGURE 13. Parametric study of the broadcasted ideal temperature when different from the real ideal temperature for three users

Finally, we created a situation where a user could listen or not to the talks of the DMPC. This means the user can decide if it takes into account the Lagrangian multiplier returned by the coordinator. We introduced this notion as the deafness β. If the user behaves and listen, $\beta = 0$, but if he is deaf, and does not take the talk into account, $\beta = 1$.

$$\begin{cases} \min J_u[t_k] = \boldsymbol{U}[t_k]^T P \boldsymbol{U}[t_k] + q^T \boldsymbol{U}[t_k] + cst[t_k] + (1-\beta)\lambda[k_{opt}] \\ \text{subjected to} \\ \forall t_k \in [\![0, N_{sim}-1]\!], \forall i \in [\![0, m-1]\!],\ 0 \leq u_i \leq u^i_{max} \end{cases} \tag{8}$$

In Figure 14, the nominal situation is presented and in Figure 15 a situation were user 1 is deaf is presented. We do notice that when the user is deaf, its comfort is much better than when it listens to the talk.

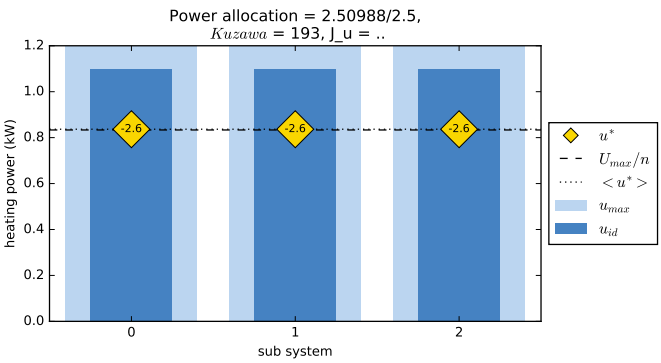

FIGURE 14. Power distribution for three user in the nominal case

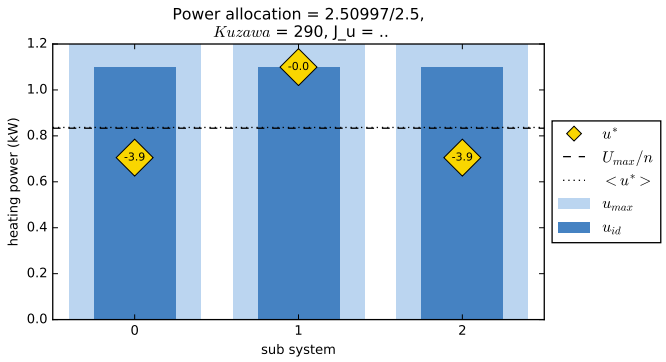

FIGURE 15. Power distribution for three users when user 1 does not listen to the talk

Of course this deafness factor β can be set between 0 and 1. Figure 16 shows the influence of the deafness factor of user 1 on the temperature deviation of both users. With no surprise, when a user is not listening to the talks all the others are penalized.

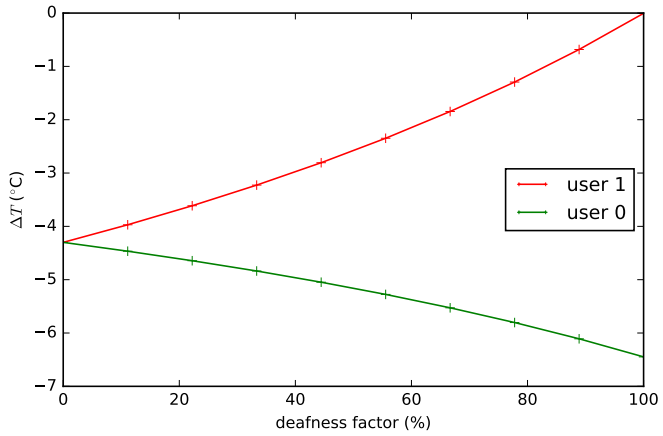

FIGURE 16. Parametric study of the deafness factor on the deviation to ideal temperature

All those studies have been executed on the static model, but all those results can easily be extended to the dynamic model and to the DMPC.

C. Security in dynamic situations

Now, let us consider the dynamic model. Our developed python module is able to deal with centralized MPC and distributed MPC. However, due to the complexity of the DMPC, its calculation requires more computation power. So for the sake of the simplicity the results of this part were obtained with a classic MPC but they can all be extended to the DMPC.

1) First, we consider a cheating user: We want to observe the influence of the comfort factor. In Figures 17 and 18 we can observe the situation with two users. In blue we can see the the distribution in the nominal case were $\alpha_1 = \alpha_2 = 10$. Then we change the value of the comfort factor for the second user. We notice that its comfort is drastically better (follows the reference temperature more than the green and the blue lines) to the detriment of the first user (in green).

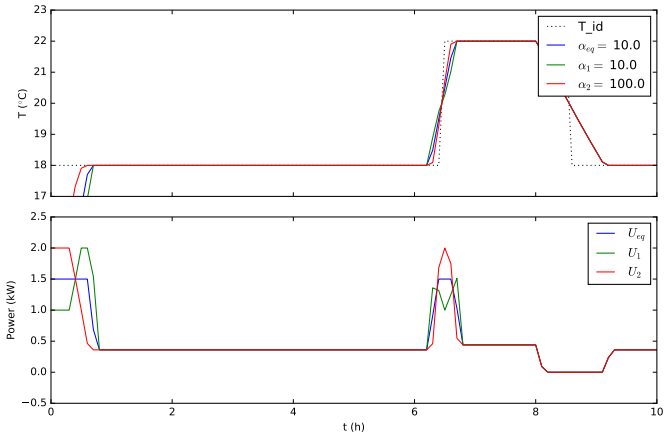

FIGURE 17. Power distribution through time for two users. In blue is the nominal situation with identical comfort factor.

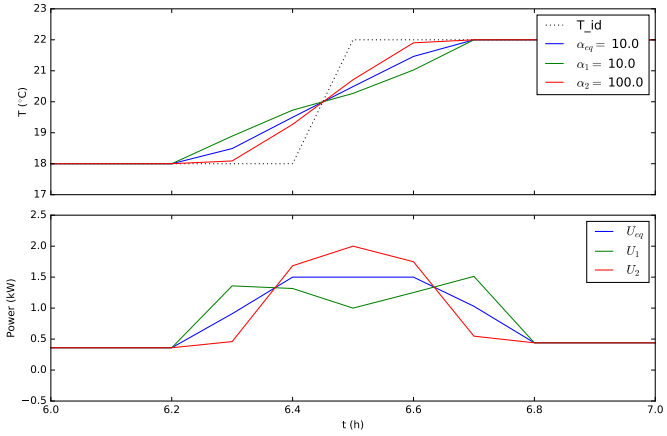

FIGURE 18. Power distribution through time for two users. In blue is the nominal situation with identical comfort factor. Focus between 6:00-7:00 am

Our study pointed out that the more $\alpha_2 > \alpha_1$, the more user 2 has a great comfort and the opposite for user 1. Hence, by modifying α, one could easily cheat the DMPC in order to gain access to more energy.

2) Then, we consider a nihilist user.: As previously stated, a nihilist user is a user whose objective is to disrupt the system and even destroy it. In our first subsection, we presented several strategies in order to disable the DMPC system. During this phase, we evaluated the influence of different parameters to detect if they could be a liability in the DMPC. We notice that by augmenting the comfort factor of all users, we could reach a threshold and make the Uzawa iteration not converging (or at least reaching the maximum admissible iteration k_{max}). Hence if a user succeeds to change the value of all the α, it might be able to break the DMPC.

Secondly, we tried the other method : to use a particular sequence of $u_i^*[t_k]$ and not the result of the optimization.

We created a sequence such as $u_2[t_k] = u^i_{max}$ if k is an odd number and $u_2[t_k] = 0$ else. In Figure 19, we show the distribution through time for the non-nihilist user (user 1). In Figure 20, we show the same but for the nihilist user (user 2).

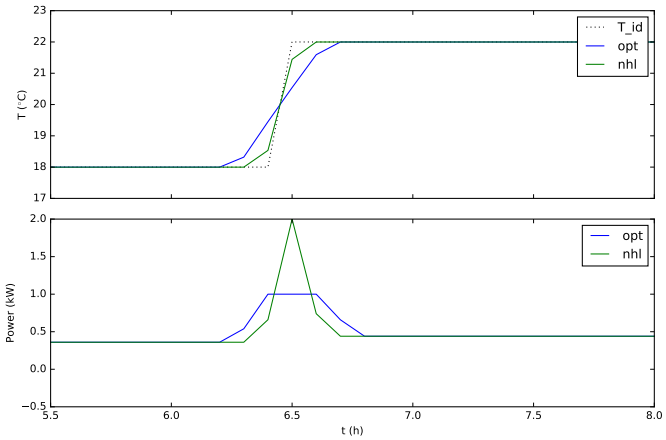

FIGURE 19. Power distribution through time for user 1 when applying a destroying sequence of consumed power for user 1

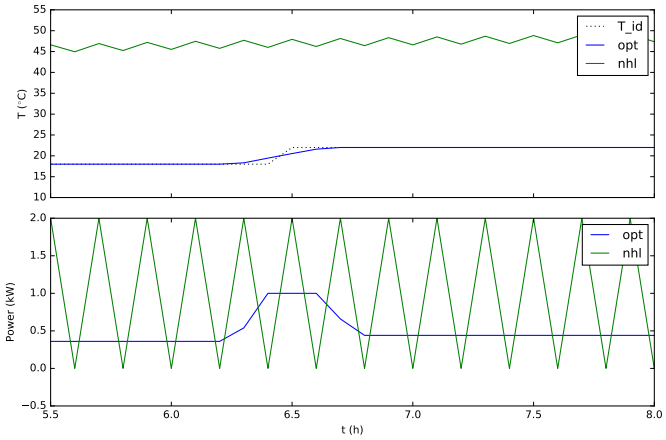

FIGURE 20. Power distribution through time for user 0 when applying a destroying sequence of consumed power for user 1

When summing u_1^* and u_2^* we notice that the max is superior to the amount of energy available U_{max}. This proves that this sequence disable the DMPC.

D. Protection

Finally, we studied security counter-measures against those threat. We noticed through our experiment that when we were altering the parameters, we modified as well the following functions :

- $k_{Uzawa} \rightarrow (u^*(k_{Uzawa})|_\alpha)$
- $\lambda \rightarrow (u^*(\lambda)|_\alpha)$
- $k_{Uzawa} \rightarrow (\lambda(k_{Uzawa})|_\alpha)$

In other words, the first (*resp.* second) function represents the power distribution (of one user for a given α) as a function of the number of iteration realized in the Uzawa method

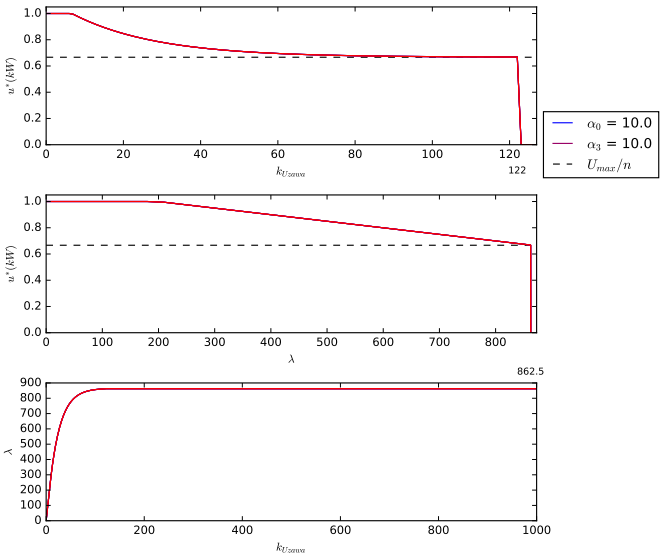

FIGURE 21. $u^*(k)$, $u^*(\lambda)$ and $\lambda(k)$ in nominal situation

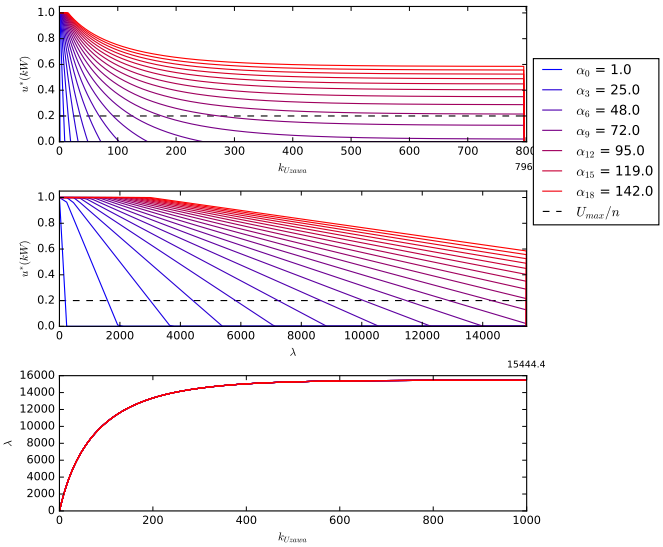

FIGURE 22. Parametric study of the influence of the comfort on different functions : the optimal distributed power as function of the Uzawa iteration and the Lagrange multiplier for the first two graphs and the Lagrange multiplier as a function of the Uzawa iteration.

(*resp.* the value of the Lagrangian multiplier). Similarly, the third one returns the value of the Lagrangian multiplier as a function of the number of iteration realized in the Uzawa method.

In Figure 21, we can observe the nominal situation. Then in Figure 22 we can see a cluster of lines created for different values of α.

We then decided to realize a large cluster of lines for alpha linearly distributed. The result is presented in Figure 22 for α in range 0 to 150.

Thanks to Figure 22, we can set a threshold (for instance on the line α_{12}), this will divide the space in two : above the line $(u^*(k_{Uzawa})|_{\alpha_{12}})$, user will be considered as cheaters,

else the users are cleared. Respectively below the line $(u^*(\lambda)|_{\alpha_{12}})$, user will be considered as cheaters, else the users are cleared.

This is a way to detect efficiently cheating and nihilist users using a comfort variation approach.

V. Conclusion

In this paper, we presented new results on security breach and measures for distributed model predictive control. By developing a thermal model we were able to experiment various approaches on, firstly, how to destroy or cheat, and secondly on how to detect such behaviours. By analysing all the different method, we managed to reduce those situation to a few base cases much easier to analyse and export to other situations. All those results are encouraging and call for further investigation on the subject.

Références

[1] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright, "Distributed mpc strategies with application to power system automatic generation control," *IEEE Transactions on Control Systems Technology*, vol. 16, pp. 1192–1206, Nov 2008.

[2] E. Camponogara, D. Jia, B. H. Krogh, and S. Talukdar, "Distributed model predictive control," *IEEE Control Systems*, vol. 22, pp. 44–52, Feb 2002.

[3] D. Jia and B. H. Krogh, "Distributed model predictive control," vol. 4, pp. 2767–2772 vol.4, 2001.

[4] G. Cohen, *Optimisation des grands systèmes*. DEA. Université de Paris-I 1994-2004, 2004.

[5] L. Acar, "Some examples for the decentralized receding horizon control," in *Decision and Control, 1992., Proceedings of the 31st IEEE Conference on*, pp. 1356–1359 vol.2, 1992.

[6] S. Sawadogo, R. M. Faye, P. O. Malaterre, and F. Mora-Camino, "Decentralized predictive controller for delivery canals," in *Systems, Man, and Cybernetics, 1998. 1998 IEEE International Conference on*, vol. 4, pp. 3880–3884 vol.4, Oct 1998.

[7] W. B. Dunbar and R. M. Murray, "Distributed receding horizon control for multi-vehicle formation stabilization," *Automatica*, vol. 42, no. 4, pp. 549 – 558, 2006.

[8] A. Brooks, E. Lu, D. Reicher, C. Spirakis, and B. Weihl, "Demand dispatch," *IEEE Power and Energy Magazine*, vol. 8, pp. 20–29, May 2010.

[9] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.