Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 55-16 (2022) 296–301

A Tree-Based Multi-Scenario Approach to Networked MPC under Packet Losses and Disturbances[★]

T. Arauz[*] J. M. Maestre[*] A. Cetinkaya[**]
C. Stoica Maniu[***]

[*] *Systems and Automation Engineering Department, University of Seville, Spain (e-mail: marauz@us.es, pepemaestre@us.es).*
[**] *Graduate School of Engineering and Science, Shibaura Institute of Technology, Tokyo 135-8548, Japan (e-mail: ahmet@shibaura-it.ac.jp).*
[***] *Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, 91190, Gif-sur-Yvette, France (e-mail: cristina.stoica@l2s.centralesupelec.fr).*

Abstract: Systems with elements linked via a communication network are vulnerable to communication problems and attacks of malicious agents, with potentially harmful consequences for performance and stability. This paper proposes a stochastic Model Predictive Control (MPC) scheme to deal with two different sources of uncertainties simultaneously, namely, packet losses and external disturbances. In particular, the controller deals with packet losses using a tree-based approach and is robustified against external disturbances using a multiple scenario approach. Finally, the algorithm performance is compared via simulation with other MPC alternatives and a feedback control law.

Keywords: Model-based Predictive Control, Linear Control Systems, Cyber-Physical Systems, Robust Control and Stabilization, Stochastic Optimization.

1. INTRODUCTION

Control systems are getting ubiquitously entwined with physical systems thanks to the new possibilities of instrumentation and interconnection, giving rise to the so-called Cyber-Physical Systems (CPS), which are composed of computing devices that interact with physical processes (Lee, 2008). In a CPS, the physical components and the software are closely linked, generally within a communication network that makes such interrelation possible. Nevertheless, the network represents a source of weakness because data packets can be lost due to communication problems and malicious agents (Shu and Krunz, 2014).

A review of the state of the art of CPS security and a comparison of different works, from both industry and academia, explaining how security is addressed is given in Lun et al. (2019). Also, in Sandberg et al. (2015), potential attack models and defense strategies in the context of network control system theory are explored. Furthermore, many studies implement control algorithms applying Model Predictive Control (MPC) in this context. MPC is a model-based control strategy that, at each control time, computes an input sequence for the succeeding time instants (Camacho and Bordons, 2004), presenting many advantages to deal with cyber-attacks and packet losses. Some MPC applications in this situation are given in Velarde et al. (2017, 2018), which study different mechanisms to provide resilience in distributed MPC schemes with respect to malicious agents. In Quevedo et al. (2015), random packet dropouts are explicitly taken into account using a stochastic cost function for an MPC scheme. Besides, in Mishra et al. (2018), packet dropouts are also addressed using the MPC strategy, but assuming the system also affected by additive stochastic noise.

Regarding system stability, different strategies are proposed when the system is exposed to cyber-attacks. For instance, in Romagnoli et al. (2019), the communication network is open for a determined time and the system periodically refreshes its original control software. Similarly, in Abdi et al. (2018), full platform-wide restarts are combined with safe operational windows computed in runtime. Another case is presented in Trodden et al. (2020), where the attacker is only allowed to take a maximum proportion of the input constraint space, leaving the defender the remaining proportion to react. In Shoukry et al. (2015), the state reconstruction problem when measurements may have been corrupted by an adversarial attack is addressed.

External disturbances are also relevant in cybersecurity contexts. When these disturbances are bounded, they can be directly included in the controller, e.g., in Maestre et al.

[★] This project has received funding from the Spanish Training Program for Academic Staff (FPU19/00127), the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 789051)-OCONTSOLAR, the project GESVIP funded by Junta de Andalucía (ref. US-1265917) and MCIN/AEI/ 10.13039/501100011033 under project C3PO-R2D2 (PID2020-119476RB-I00). Also, support from the JST ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603) and JSPS Kakenhi Grant (No. JP20K14771) are acknowledged.

10.1016/j.ifacol.2022.09.040

(2018), a distributed MPC dynamically exploits boundedness to identify and mitigate attacks. However, there are also strategies to manage unbounded disturbances, such as the algorithm presented in Calafiore and Campi (2006), which computes the total number of disturbance scenarios required to ensure constraints satisfaction. Furthermore, some assumptions can be established to enable bounded disturbances. This is the case of Cannon et al. (2012), where a stochastic MPC problem is solved for systems with random additive disturbances by assuming that they are derived from a normally distributed random variable and bounded by truncating the maximum absolute value.

The main contribution of the current paper is to propose a Tree-Based Model Predictive Control (TBMPC) to deal with packet losses, which represents an improvement w.r.t. (Pierron et al., 2020). More precisely, TBMPC provides an optimal rooted tree of actions at each time instant, but only the action corresponding to the current instant is applied to the system. In particular, the TBMPC proposed in Pierron et al. (2020) is a type of scenario-based MPC which can consider different possibilities for the system evolution in terms of the packet losses caused by malicious attacks and unreliable transmissions. The key idea is to build a binary tree that contains all possible scenarios regarding packets losses and receptions. Since each scenario has a certain probability of occurrence, the input sequence is calculated according to the weighted cost function. Another contribution of the current paper relies on enhancing robustness to external disturbances simultaneously: different scenarios of noise are added to the binary tree, thus giving rise to a stochastic MPC controller.

The outline of the rest of the paper is as follows. In Section II, the problem formulation is introduced. Section III provides the fundamentals of the TBMPC formulation. Section IV outlines the features that the enhanced TBMPC includes related to the basic TBMPC. Section V presents the application of this control model to a case study, and results are discussed in Section VI. Finally, concluding remarks are given in Section VII.

2. PROBLEM FORMULATION

2.1 System dynamics

We consider the following system dynamics:

$$x(k+1) = Ax(k) + Bu(k) + Dw(k), \tag{1}$$

where $x(k) \in \mathbb{R}^n$, $u(k) \in \mathbb{R}^m$, and $w(k) \in \mathbb{R}^n$ are the states, inputs, and external disturbances, respectively. The state is assumed to be measurable and otherwise, it can be estimated. The system is assumed to be subject to polytopic state and input constraints, i.e.,

$$x \in \mathbb{X} \triangleq \{x \in \mathbb{R}^n \mid C^x x \leq a\}, \tag{2}$$

$$u \in \mathbb{U} \triangleq \{u \in \mathbb{R}^m \mid C^u u \leq b\}, \tag{3}$$

which contain the origin in their interiors and where $C^x \in \mathbb{R}^{r_x \times n}$, $a \in \mathbb{R}^{r_x}$, $C^u \in \mathbb{R}^{r_u \times m}$, and $b \in \mathbb{R}^{r_u}$. External disturbances are assumed to be bounded and random, following the probability of a truncated normal distribution. For simplicity, they are also assumed to lie in a polytopic, compact and convex set $\mathbb{W}$ that also contains the origin in its interior, $\mathbb{W} \triangleq \{w \in \mathbb{R}^n \mid C^w w \leq d\}$.

2.2 Packet losses

The system communicates with its controller via a network that is vulnerable to suffer packet losses, e.g., due to the unreliability of transmissions and the actuation of malicious attackers as in jamming attacks. In case of failed reception, the actuation of the plant has to be defined, e.g., by setting the input as zero.

We use $\theta(k) \in \{0, 1\}$ to indicate packet losses. In particular, we have $\theta(k) = 1$ when there is a packet loss, and $\theta(k) = 0$ otherwise.

This paper addresses two realistic packet loss characterizations. In the first case, the probability of packet losses is time-invariant and given by $p_{\text{PL}} \in [0, 1]$. In other words, $\mathbb{P}[\theta(k) = 1] = p_{\text{PL}}$ for $k \in \{0, 1, \ldots\}$. This case can represent the setting where an attacker attacks a wireless channel with the same interference power at all time instants. We call this setting *unbounded consecutive attacks*.

The second case that we consider represents *bounded consecutive attacks*. In this case the number of consecutive packet losses due to attacks is upper-bounded by a positive integer N_{attack}. More specifically, the probability of a packet loss at time k becomes zero if there are packet losses in the preceeding N_{attack} time instants, that is, $\mathbb{P}[\theta(k) = 1 | \theta(k - N_{\text{attack}}) = 1, \ldots, \theta(k-1) = 1] = 0$. In all other scenarios, packet loss probability remains to be p_{PL}. This modeling approach captures the scenarios where the attacker tries to prevent too many consecutive packet losses to avoid being detected.

The two cases above can be modeled similarly by generalizing Bernoulli packet losses and defining the probability of a packet loss as a function of the Signal to Interference plus Noise Ratio (SINR), commonly used in wireless channel models (Hamdi, 2009).

2.3 Control objective

The TBMPC controller goal is to minimize the following expected cost value along the prediction horizon N:

$$\begin{aligned} V_t(k) &= \sum_{i=1}^{N_s} p_i(p_{\text{PL}}) V_i(k) \\ &= \sum_{i=1}^{N_s} p_i(p_{\text{PL}}) \sum_{l=0}^{N-1} \big(x_i(k+l+1)^{\mathrm{T}} Q x_i(k+l+1) \\ &\qquad + u(k+l)^{\mathrm{T}} R u(k+l)\big), \end{aligned} \tag{4}$$

while respecting the constraints (2), (3), where $Q \in \mathbb{R}^{n \times n}$ and $R \in \mathbb{R}^{m \times m}$ are positive-definite weighting matrices. The scalar $p_i(p_{\text{PL}}) \in [0, 1]$ represents the probability of scenario i, which is calculated accordingly to the packet loss probability p_{PL} by multiplying all step individual probabilities of the corresponding scenario.

3. STOCHASTIC MPC

3.1 Tree-Based MPC for Packet Losses

TBMPC is an MPC strategy that computes the input signal $u(k)$ according to the $N_s = 2^{N-1}$ possible packet losses scenarios in a horizon of length N. That is, the

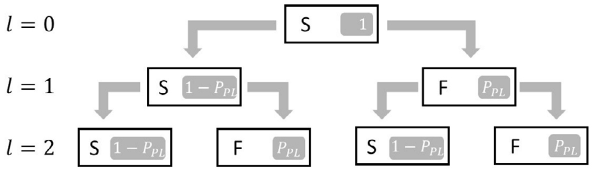

Fig. 1. Example of the binary tree for $N = 3$.

controller lets the input sequence follow different trajectories along the prediction horizon and provides the best response for each scenario. To this end, a scenario tree is built with branches representing all possible scenarios and bifurcations that stem from the two possible events after sending a packet: success or failure. This tree is built from the controller point of view by always assuming that the system would apply a zero input when losses occur, regardless of the strategy chosen by the plant.

Example 1. *The binary tree from Fig. 1 represents the tree for a prediction horizon of length 3: S means a success of packet reception and F a failure. Each step has a specific probability of occurrence that depends on the packet loss probability, except for the first step, where the data is assumed that is always received, so its probability is 1.*

Therefore, the system model of (1) must be extended to integrate all the tree scenarios. Thereby, the state evolution of each scenario $i \in [1, N_\mathrm{s}]$ is:

$$x_i(k+1) = Ax_i(k) + B_i(k)u_i(k) + Dw_i(k), \qquad (5)$$

where $x_i \in \mathbb{R}^n$, $u_i \in \mathbb{R}^m$ and $w_i \in \mathbb{R}^n$ represent the states, inputs and disturbances of the corresponding scenario, respectively. Notice that matrix B_i is *scenario- and time-dependent* because it models the packets loss pattern of each scenario.

Non anticipatory constraints All input signals of the different scenarios must be equal along the horizon until a tree bifurcation happens. In this way, the first input signal of all scenarios must be the same; in the second time step, the input takes one possible value for half of the scenarios and another value for the rest; and so on. They can be generally expressed as: for each instant $l \in [0, N-1]$, the following equalities must be imposed

$$\begin{aligned} u_{(2^{N-1-l})j+1} = u_{(2^{N-1-l})j+2} = \ldots \\ = u_{(2^{N-1-l})(j+1)} \end{aligned} \qquad (6)$$

for all $j \in [0, 2^{l-1}]$.

These constraints reduce the number of optimization variables of the input sequence $U_\mathrm{TBMPC} \in \mathbb{R}^{mN2^{N-1}}$. The reduced vector, $U_\mathrm{red} \in \mathbb{R}^{m(2^N-1)}$, is associated with the full vector U_TBMPC by the expression $U_\mathrm{TBMPC} = MU_\mathrm{red}$, where the suitable mapping matrix $M \in \mathbb{R}^{N2^{N-1}m \times m(2^N-1)}$ is defined to comply with the non-anticipatory constraints.

Example 2. *The reduced vector U_red corresponding to Fig. 1 is designed such that:*

$$\begin{aligned} U_\mathrm{red} = [&u_{1234}(0),\ u_{12}(1),\ u_{34}(1), \\ &u_1(2),\ u_2(2),\ u_3(2),\ u_4(2)]^\mathrm{T}. \end{aligned}$$

Notice that in this case U_red has a reduced size, i.e., $U_\mathrm{red} \in \mathbb{R}^{m(2^N-1)} = \mathbb{R}^7$, compared to $U_\mathrm{TBMPC} \in \mathbb{R}^{mN2^{N-1}} = \mathbb{R}^{12}$. Notice that this difference becomes greater as the prediction horizon length increases.

3.2 Scenario-Based MPC for external disturbances

Multiple scenarios of noise are added for system robustness. This way, the complete tree is composed of as many instances as noise scenarios considered. Therefore, the total number of scenarios is $N_\mathrm{Snoise} = N_\mathrm{noise}N_\mathrm{s} = N_\mathrm{noise}2^{N-1}$, where N_noise is the total number of possibilities of external noise considered.

Example 3. *For the binary tree of Fig. 1, if $N_\mathrm{noise} = 10$, there are $N_\mathrm{Snoise} = 40$ scenarios.*

Remark. *Depending on the inherent instability of the considered system, TBMPC may be unable to comply with the terminal constraint for all scenarios. Since the packet loss is probabilistic, there is a chance (with non-zero probability) that the packet transmissions fail during many consecutive time steps and some scenarios cannot be controlled at all. To avoid feasibility issues in the optimization problem, soft constraints can be used.*

3.3 Stochastic control law

The optimization problem is based on the prediction of the system evolution considering all scenarios along the prediction horizon. Hence, at each time step, the quadratic problem solved is

$$U^*_\mathrm{TBMPC} = \arg \min_{U_\mathrm{TBMPC}} V_t(k) \qquad (7)$$

subject to the global system dynamics of (5), the state and input constraints of (2) and (3), the non-anticipatory constraints of (6), and $x_\mathrm{TB} = \hat{x}_\mathrm{TB}$, where $\hat{x}_\mathrm{TB}$ corresponds to the state measurement (common for all scenarios). The vector U_TBMPC denotes the vector of all optimization variables.

The TBMPC control law implements the first component of the input sequence U_TBMPC:

$$u(k) = U_\mathrm{TBMPC}(k)[1]. \qquad (8)$$

This value represents the input applied in case the data packet is successfully received. In case of packet loss, the actuator must follow a predefined strategy to select which input value applies. In this article, the following two strategies have been considered:

- **Strategy 1:** Set the input value as zero.
- **Strategy 2:** Take the corresponding input from the last input sequence successfully received.

4. RESULTS

The system proposed to illustrate the efficiency of the developed TBMPC approach is a discrete-time version of a cart-pendulum system (Akashi et al., 2018; Pierron et al., 2020). Since the system is nonlinear, the dynamics have been linearized and discretized with $T_\mathrm{s} = 0.005$s. The state vector is composed of 4 elements: $x = [x\ \dot{x}\ \theta\ \dot{\theta}]^\mathrm{T}$, where x is the position of the cart and θ the tilt angle of the rod with respect to the vertical line. The matrices values of the corresponding discrete-time linear model of (1) are:

$$A = \begin{bmatrix} 1 & 0.005 & 0 & 0 \\ 0 & 1 & -0.01 & 0 \\ 0 & 0 & 1 & 0.005 \\ 0 & 0 & 0.1175 & 1 \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 0.01 \\ 0 \\ -0.02 \end{bmatrix},\ D = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Regarding the controller setup, the weight matrices of the cost function of Eq. (4) are fixed as: $Q = \text{diag}(0, 0, 1, 0)$ and $R = 2 \cdot 10^{-9}$. This configuration promotes that the tilt angle reaches zero regardless of any other variable. The prediction horizon has been chosen as $N = 4$, and the number of scenarios of noise $N_{\text{noise}} = 10$. Thus, the total number of scenarios according to packet losses pattern is $N_{\text{s}} = 2^{N-1} = 8$, and the total number of scenarios considering all scenarios of noise is $N_{\text{Snoise}} = N_{\text{noise}} N_{\text{s}} = 80$.

The initial state is set to $x_0 = [0.2 \;\; -0.01 \;\; -0.3 \;\; -0.1]^{\text{T}}$, and their elements are bounded as $|x(1)| \leq 1$, $|x(2)| \leq 5$, $|x(3)| \leq 0.4$ and $|x(4)| \leq 9$. The magnitude of the force applied is bounded as $|u| \leq 50$. The external disturbances are assumed to follow a normal distribution with zero mean and variance given by $\sigma^2 = 0.002$. However, they are assumed to be within the range of $\pm 3\sigma$, i.e. $|w| \leq 3\sqrt{0.002}$.

The packet loss probability has been set as $p_{\text{PL}} = 0.24$, which means that, in the long run, 24% of the packets are lost along the way (regardless of the reason). In addition, $N_{\text{attack}} = N - 2 = 2$ for the case when the consecutive attacks are bounded. In this way, it is always ensured that the number of consecutive attacks received is lower than the controller prediction horizon.

The system is designed to act in two different ways when the input data is not received by the plant: Strategy 1 and 2. Note that it has to be initially configured which Strategy must be followed. The proposed TBMPC algorithm has been simulated following both strategies.

Furthermore, this method is compared by simulations with other three control methods: the basic TBMPC, the standard MPC and the feedback controller with gain: $K = [71.1932 \;\; 38.0538 \;\; 111.0227 \;\; 24.6853]^T$, computed following the method of Cetinkaya et al. (2016). However, the comparison with the latter is only possible when a zero input is applied in case of loss, as it computes the input signal just for the current time step.

In addition, some Key Performance Indicators (KPIs) have also been calculated from each simulation: the *Integral Absolute Error* (IAE), the *Integral Time Absolute Error* (ITAE), the *Mean Squared Error* (MSE), and the *Mean value of input values* (Mean U).

Finally, the cost function values for the three MPC approaches have also been computed. However, in case soft constraints are considered for the developed TBMPC, the cost value for computations differs from (4), so it is unsuitable for comparison with the other cases. Instead, the value presented corresponds to the sum of the cost mean values from all noise scenario possibilities for each scenario of the packet loss pattern.

In the following, simulation results are presented for the two versions considered: the case when there is no limit of the consecutive attacks received, and the one with bounded consecutive attacks.

4.1 Unbounded consecutive attacks

Simulation results of the developed TBMPC algorithm in comparison with other algorithms are presented in Fig. 2 for Strategy 1 and in Fig. 3 for Strategy 2, when the consecutive attacks are not bounded. For simplicity, only the tilt angle and input signal performances are depicted. All KPI values are presented in Table 1 for both simulations. Also, Table 2 presents the cost function values for the three MPC approaches.

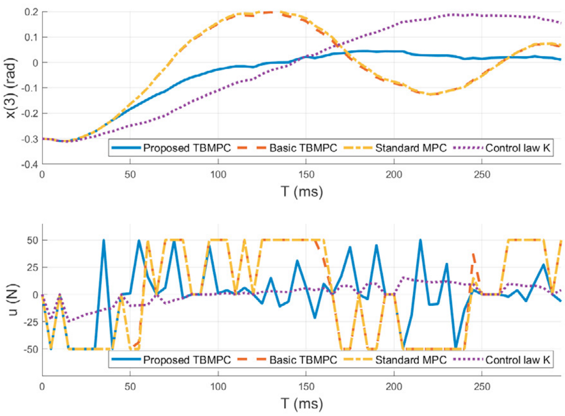

Fig. 2. Simulation results with Strategy 1 in the case of unbounded consecutive attacks for comparison.

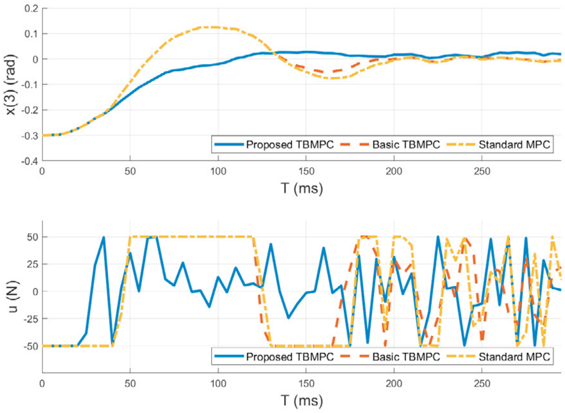

Fig. 3. Simulation results with Strategy 2 in the case of unbounded consecutive attacks for comparison.

Table 1. KPI values for unbounded consecutive attacks simulations.

Methods	IAE (rad)	ITAE (ms rad)	MSE (10^{-3} rad^2)	Mean U (N)
Simulation with Strategy 1				
Proposed TBMPC	4.73	335.46	15.59	17.35
Basic TBMPC	7.68	860.77	23.58	36.04
Standard MPC	7.82	882.75	24.32	36.08
State feedback K	9.67	1313.01	32.96	6.59
Simulation with Strategy 2				
Proposed TBMPC	3.84	244.79	12.08	24.97
Basic TBMPC	4.36	283.93	13.37	40.16
Standard MPC	4.62	332.36	13.72	44.81

4.2 Bounded consecutive attacks

The results for comparison between the developed TBMPC method with the other algorithms when the consecutive attacks are bounded are presented in Fig. 4-5 for Strategies 1 and 2, respectively. For simplicity, only the tilt angle and

Table 2. Cost function values for unbounded consecutive attacks simulations.

Simulations	Proposed TBMPC	Basic TBMPC	Standard MPC
Strategy 1	2.80	4.76	4.92
Strategy 2	2.01	2.32	2.33

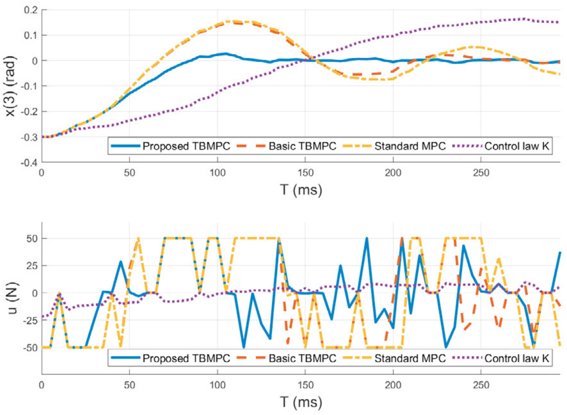

Fig. 4. Simulation results with Strategy 1 in the case of bounded consecutive attacks for comparison.

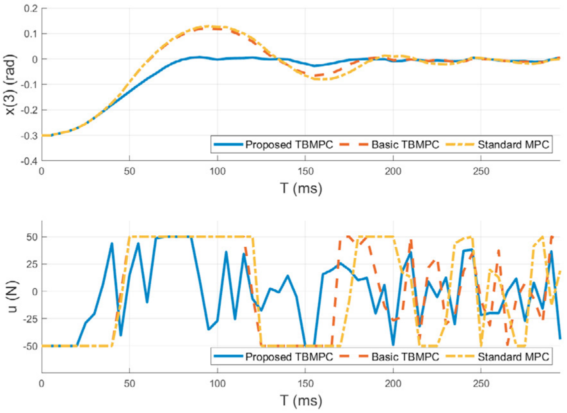

Fig. 5. Simulation results with Strategy 2 in the case of bounded consecutive attacks for comparison.

input signal performances are depicted. All KPI values are presented in Table 3 for both simulations, and the cost function values are given in Table 4.

Table 3. KPI values for bounded consecutive attacks simulations.

Methods	IAE (rad)	ITAE (ms rad)	MSE (10^{-3} rad^2)	Mean U (N)
Simulation with Strategy 1				
Proposed TBMPC	3.14	130.47	11.00	22.13
Basic TBMPC	4.94	392.59	14.13	32.54
Standard MPC	5.63	549.63	15.20	35.02
State feedback K	8.65	1112.36	27.22	5.47
Simulation with Strategy 2				
Proposed TBMPC	3.17	141.49	11.31	27.09
Basic TBMPC	4.26	281.76	12.84	40.06
Standard MPC	4.61	340.23	13.45	44.05

Table 4. Cost function values for bounded consecutive attacks simulations.

Simulations	Proposed TBMPC	Basic TBMPC	Standard MPC
Strategy 1	1.81	2.51	2.78
Strategy 2	1.79	2.15	2.29

5. DISCUSSION

The results show the better performance of the proposed TBMPC algorithm according to several aspects analyzed below.

Firstly, considering results when consecutive attacks are bounded or not, the main difference is that the proposed TBMPC algorithm stabilizes in the reference value in the bounded case (Fig. 4-5). However, in the unbounded case this is no longer guaranteed (Fig. 2-3). Therefore, system performances are better in case of bounded consecutive attacks independently of the strategy used. This can be quantitatively checked by comparing values of Tables 1–4.

Secondly, all MPC algorithms achieve better performances than the feedback controller, as Fig. 2 and 4 highlight. Besides, KPIs values for Strategy 1 of Tables 1 and 3 underline this fact. Its reason may be that the feedback controller has no prediction of the possible near future evolution as the MPC has, so it yields slower and softer performances as it is reflected in Fig. 2 and 4, and in the lowest mean U values in Tables 1 and 3.

Thirdly, the three MPC algorithms are analyzed. To facilitate this comparison, only the case of bounded consecutive attacks is considered (its superiority with the unbounded case has already been concluded). It is clearly seen in Fig. 4 and 5 and in Table 3 that the proposed TBMPC algorithm has the best performance regadless of the strategy followed. The following aspects support this statement:

- The angle evolution of the proposed TBMPC has less fluctuations than the others, as the IAE values of Table 3 show.
- The proposed TBMPC reaches the reference value before than the others, and also, presenting most errors in the initial time steps, as it is reflected in the ITAE values of Table 3.
- Furthermore, the absolute error values of the proposed TBMPC are lower, as Fig. 4 and 5 show and the MSE values of Table 3 reveal.
- Regarding input performances depicted in Fig. 4 and 5, the proposed TBMPC input signal is saturated only at a very few instants, whereas in the other two cases almost all the time, as the mean input values of Table 3 reveal.
- Finally, the cost function values of Table 4 also support the proposed TBMPC technique.

Therefore, with respect to the three MPC algorithms, the proposed TBMPC has the best performance, which is much better than the second best, which is the basic TBMPC. The worst is the standard MPC, although it has similar performance to the standard TBMPC.

Lastly, the two different control strategies followed in case of packet losses are separately analyzed depending on the unbounded or bounded case:

- In the case of unbounded consecutive attacks: the Strategy 1 (Fig. 2) provides a worse performance than the second one (Fig. 3). IAE, ITAE and MSE values of Table 1 are lower in simulation with Strategy 2, but for the mean U value, it is the opposite. Regarding the cost values of Table 2, Strategy 2 yields the lowest values in all methods.
- In the case of bounded consecutive attacks: for the basic TBMPC and the standard MPC the comparison between strategies is the same as in the unbounded case. However, for the proposed TBMPC the superiority of Strategy 2 is not as clear, as the IAE, ITAE and MSE values of Table 3 for both strategies are very similar. On the other hand, the cost values of Table 4 are lower for Strategy 2 for all methods.

To sum up, the best performance is achieved by the proposed TBMPC algorithm regardless of which of the two control strategies tested is followed. The second best performance belongs to the basic TBMPC algorithm but under the second control strategy. And the third result corresponds to the standard MPC also under the second control strategy. The algorithm based on the feedback control provides the worst performance.

6. CONCLUSION

A stochastic TBMPC has been designed by defining a binary tree for dealing with random packet losses and including a classical scenario approach to robustify the system against external disturbances. Two different control strategies have been studied when there are packet losses: the first one considers a zero input in case of loss, and the second takes advantage of the last input sequence received from the MPC controller in case of loss.

The designed algorithm has been analysed in two different situations: when the total number of consecutive attacks that can be received by the plant is unbounded and bounded. It has been tested by simulations along with the standard MPC, the basic TBMPC of Pierron et al. (2020), and the feedback controller defined according to Cetinkaya et al. (2016). Simulation results show better performance of the proposed TBMPC algorithm. In particular, the best performance for both strategies is achieved when the consecutive attacks are bounded.

REFERENCES

Abdi, F., Chen, C.Y., Hasan, M., Liu, S., Mohan, S., and Caccamo, M. (2018). Preserving physical safety under cyber attacks. *IEEE Internet of Things Journal*, 6(4), 6285–6300.

Akashi, S., Ishii, H., and Cetinkaya, A. (2018). Self-triggered control with tradeoffs in communication and computation. *Automatica*, 94, 373–380.

Calafiore, G.C. and Campi, M.C. (2006). The scenario approach to robust control design. *IEEE Transactions on Automatic Control*, 51(5), 742–753.

Camacho, E.F. and Bordons, C. (2004). *Model predictive control*. Springer-Verlag.

Cannon, M., Cheng, Q., Kouvaritakis, B., and Raković, S.V. (2012). Stochastic tube MPC with state estimation. *Automatica*, 48(3), 536–541.

Cetinkaya, A., Ishii, H., and Hayakawa, T. (2016). Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 62(5), 2434–2449.

Hamdi, K.A. (2009). On the statistics of signal-to-interference plus noise ratio in wireless communications. *IEEE transactions on communications*, 57(11), 3199–3204.

Lee, E.A. (2008). Cyber physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–369.

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

Maestre, J.M., Trodden, P.A., and Ishii, H. (2018). A distributed model predictive control scheme with robustness against noncompliant controllers. In Proc. *57th IEEE Conference on Decision and Control (CDC)*, 3704–3709.

Mishra, P.K., Chatterjee, D., and Quevedo, D.E. (2018). Sparse and constrained stochastic predictive control for networked systems. *Automatica*, 87, 40–51.

Pierron, T., Arauz, T., Maestre, J.M., Cetinkaya, A., and Maniu, C.S. (2020). Tree-based model predictive control for jamming attacks. In Proc. *European Control Conference,* Sankt Petersburg, Russia, 948–953.

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

Romagnoli, R., Krogh, B.H., and Sinopoli, B. (2019). Design of software rejuvenation for CPS security using invariant sets. In Proc. *American Control Conference (ACC)*, 3740–3745.

Sandberg, H., Amin, S., and Johansson, K.H. (2015). Cyberphysical security in networked control systems: An introduction to the issue. *IEEE Control Systems Magazine*, 35(1), 20–23.

Shoukry, Y., Nuzzo, P., Bezzo, N., Sangiovanni-Vincentelli, A.L., Seshia, S.A., and Tabuada, P. (2015). Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In Proc. *54th IEEE Conference on Decision and Control (CDC)*, 3804–3809.

Shu, T. and Krunz, M. (2014). Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. *IEEE Transactions on mobile computing*, 14(4), 813–828.

Trodden, P.A., Maestre, J.M., and Ishii, H. (2020). Actuation attacks on constrained linear systems: A set-theoretic analysis. In Proc. *21st IFAC Wold Conference,* Berlin, Germany, 7045–7050.

Velarde, P., Maestre, J.M., Ishii, H., and Negenborn, R.R. (2017). Scenario-based defense mechanism for distributed model predictive control. In Proc. *56th IEEE Conference on Decision and Control (CDC)*, 6171–6176.

Velarde, P., Maestre, J.M., Ishii, H., and Negenborn, R.R. (2018). Vulnerabilities in Lagrange-based distributed model predictive control. *Optimal Control Applications and Methods*, 39(2), 601–621.