Proceedings Paper:
Maestre, J.M., Trodden, P.A. and Ishii, H. (2019) A distributed model predictive control scheme with robustness against noncompliant controllers. In: 2018 IEEE Conference on Decision and Control (CDC). 57th IEEE Conference on Decision and Control (CDC 2018), 17-19 Dec 2018, Florida, USA. IEEE. ISBN: 978-1-5386-1395-5. ISSN: 0743-1546.

https://doi.org/10.1109/CDC.2018.8619079

A Distributed Model Predictive Control Scheme with Robustness Against Noncompliant Controllers

José M. Maestre[1], Paul A. Trodden[2] and Hideaki Ishii[3]

***Abstract*— A tube-based distributed model predictive control (DMPC) scheme is proposed for dynamically coupled linear systems. The control scheme is designed to guarantee local performance even when neighboring controllers are not complying with the requirements of the algorithm (e.g., they are malicious or faulty). The resulting conservativeness is minimized, for controllers aim to minimize their state and input constraint sets to reduce mutual disturbances. Also, sufficient conditions for feasibility and exponential stability are given. Finally, these ideas are illustrated and assessed with respect to other robust DMPC via a simulated example.**

I. Introduction

In standard MPC, a model of a system is used to build a finite horizon optimization problem (FHOP) in which the sequence of inputs to be implemented and the resulting predicted states are optimized with respect to a performance index [1]. The FHOP can deal explicitly with complex issues such as uncertainties, constraints, and delays, which is very convenient in many industrial applications [2]. When it is implemented in a distributed fashion, the control architecture is composed of a set of local MPC controllers —also known as *agents*— that exchange information to improve both local and overall performance. In addition, distributed MPC schemes must take into account aspects such as the organizational structure of the system and its information flows, constraints on the information exchange sources, among others. See for example [3], [4] for surveys on the topic.

As is common in interactive decision making problems, incentives may exist for agents to deviate with respect to their nominal or expected behavior. For example, strategic behavior in energy demand networks is studied in [5]. Another related work is [6], where economic incentives are introduced to promote truthful communication in load frequency control. A different mechanism design approach is that of [7], where a hierarchical structure is considered so that a coordinator with access to agents' private information computes a control law adjusted to the best interest of controllers. Also, the incentives for *misbehaving* agents might be other than economical, as it happens for example in cybersecurity problems [8], [9], where vulnerabilities in the elements that compose the system (sensors, communication channels, etc.) are often exploited to disrupt its normal operation. Even though this is a significant concern in networked applications such as the smart grid [10] and consensus problems [11], few attempts have been made to deal with it in a DMPC framework. For example, heuristic defense mechanisms for dual decomposition DMPC are proposed in [12], [13] to minimize the effects of attacks of the price based coordination mechanism. Finally, it must be noticed that problems due to mutual interaction can also arise as a consequence of faulty components [14], [15].

All the aforementioned issues have one thing in common: the existence of agents that do not operate as expected with consequences for the overall system that can range from the loss of performance to instability. This motivates us to extend the distributed MPC method presented in [16] to deal with noncompliant controllers, for it does not matter whether the undesired behavior stems from a malicious attack or is due to faulty events. In particular, the proposed approach is a tube-based distributed MPC scheme with guaranteed recursive feasibility and stability that is based on the optimization and exchange of the input and state constraint sets to minimize the mutual disturbances. The presence of noncompliant agents in the system is dealt with by the robustification of the disturbances expected by local controllers, so that feasibility and stability are preserved. A final improvement with respect to [16] is the relaxation of the conditions required for stability.

The outline of the rest of the paper is as follows: Sections II and III present, respectively, the preliminaries of the problem setting and the distributed control problem. Section IV focuses on the detection and defense against noncompliant agents. Implementation details of the algorithm are given in Section V and its main theoretical properties are discussed in Section VI. Finally, Section VII presents an illustrative example and Section VIII concludes the paper with closing remarks.

Notation: The sets of non-negative and positive reals are denoted, respectively, $\mathbb{R}_{0+}$ and $\mathbb{R}_{+}$. The notation $[a,b]^n$ means the n-dimensional product set $[a,b]\times[a,b]\times\cdots\times[a,b]$, where $a,b\in\mathbb{R}$. For $a,b\in\mathbb{R}^n$, $a\leq b$ applies element by element. The distance of a point $x\in\mathbb{R}^n$ from a set $X\subset\mathbb{R}^n$ is $|x|_X \triangleq \inf_{y\in X}|x-y|$. AX denotes the image of a set $X\subset\mathbb{R}^n$ under the linear mapping $A:\mathbb{R}^n\to\mathbb{R}^p$, and is given by $\{Ax : x\in X\}$. For $X,Y\subset\mathbb{R}^n$, the Minkowski sum is $X\oplus Y \triangleq \{x+y : x\in X, y\in Y\}$; for $Y\subset X$, the Minkowski difference is $X\ominus Y \triangleq \{x\in\mathbb{R}^n : Y\oplus\{x\}\subset X\}$. For $X\subset\mathbb{R}^n$ and $a\in\mathbb{R}^n$, $X\oplus a$ means $X\oplus\{a\}$. The column vectors of zeros and ones are denoted $\mathbf{0}$ and $\mathbf{1}$ respectively, the length of which will be clear from the context.

*Financial support by the Spanish MINECO (project DPI2017-86918-R), the Japanese Society for the Promotion of Science (scholarship PE16048) and the ERC-ADG OCONTSOLAR (Project ID: 789051) is gratefully acknowledged.

[1]J. M. Maestre is with the Department of Systems and Automation Engineering, University of Seville, Seville, Spain pepemaestre@us.es

[2]P. A. Trodden is with the Department of Automatic Control & Systems Engineering, University of Sheffield, Sheffield, England p.trodden@sheffield.ac.uk

[3]H. Ishii is with the Department of Computer Science, School of Computing, Tokyo Institute of Technology, Tokyo, Japan ishii@c.titech.ac.jp

II. Preliminaries

We consider a set $\mathcal{N} = \{1, \dots, M\}$ of coupled systems whose dynamics in discrete time can be described as

$$x_i^+ = A_{ii}x_i + B_{ii}u_i + w_i, \tag{1}$$

where $x_i \in \mathbb{R}^{n_i}$, $u_i \in \mathbb{R}^{m_i}$, $w_i \in \mathbb{R}^{n_i}$ are the state, input and disturbances of system $i \in \mathcal{N}$. Hence, $A_{ij} \in \mathbb{R}^{n_i \times n_j}$ and $B_{ij} \in \mathbb{R}^{n_i \times m_j}$. The successor state is denoted as x_i^+.

Assumption 1: Each (A_{ii}, B_{ii}), $i \in \mathcal{N}$ is stabilizable.

The local disturbance vector includes disturbances due to interactions with neighboring agents and a safety term w_i^{s} to account for possible noncompliant events. That is,

$$w_i = \sum_{j \in \mathcal{N}_i} (A_{ij}x_j + B_{ij}u_j) + w_i^{\mathrm{s}},$$

where the set of *neighbours* of subsystem i are defined as

$$\mathcal{N}_i \triangleq \{j \in \mathcal{N} \setminus \{i\} : [A_{ij}\ B_{ij}] \neq 0\}.$$

Assumption 2: Unexpected disturbances are bounded by a closed polytope that contains the origin in its interior, i.e., $w_i^{\mathrm{s}} \in \mathbb{W}_i^{\mathrm{s}}$, which can be described by r^s inequalities as

$$\mathbb{W}_i^{\mathrm{s}} \triangleq \{w_i^{\mathrm{s}} \in \mathbb{R}^{n_i} : C_i^{\mathrm{s}} w_i^{\mathrm{s}} \leq g_i^{\mathrm{s}}\}, \text{with } g_i^{\mathrm{s}} \in \mathbb{R}_{0+}^{r_i^s}.$$

Also, let $x = (x_1, \dots, x_M)$, $u = (u_1, \dots, u_M)$, and $w = (w_1^{\mathrm{s}}, \dots, w_M^{\mathrm{s}})$ be respectively the aggregated state, input, and disturbance vectors. Then, the overall system model becomes

$$x^+ = Ax + Bu + w,$$

where the overall state and input matrices A and B are composed accordingly.

A. Constraints and invariance

Each system $i \in \mathcal{N}$ is subject to local polytopic state and input constraints, i.e., $x_i \in \mathbb{X}_i$ and $u_i \in \mathbb{U}_i$, that contain the origin in their interiors and are defined respectively by r_i^x and r_i^u linear inequalities as

$$\mathbb{X}_i(a_i) \triangleq \{x_i \in \mathbb{R}^{n_i} : C_i^x x_i \leq a_i\}, \forall a_i \in \mathbb{R}_{0+}^{r_i^x},$$
$$\mathbb{U}_i(b_i) \triangleq \{u_i \in \mathbb{R}^{m_i} : C_i^u u_i \leq b_i\}, \forall b_i \in \mathbb{R}_{0+}^{r_i^u},$$

with $a_i \leq \mathbf{1}, b_i \leq \mathbf{1}$. In particular, $\mathbb{X}_i \triangleq \mathbb{X}_i(\mathbf{1})$ and $\mathbb{U}_i \triangleq \mathbb{U}_i(\mathbf{1})$ define hard constraint sets on the system variables while $\mathbb{X}_i(a_i)$ and $\mathbb{U}_i(b_i)$ are tightened versions that the local controllers may decide to use to minimize mutual disturbances. Since input and state local constraints and unexpected disturbances are assumed to be polytopic, it can be seen that

$$w_i \in \mathbb{W}_i \triangleq \mathbb{W}_i^{\mathrm{s}} \oplus \mathbb{W}_i^0 = \mathbb{W}_i^{\mathrm{s}} \oplus \bigoplus_{j \in \mathcal{N}_i} \mathbb{W}_{ij},$$

where $\mathbb{W}_i^0 = \bigoplus_{j \in \mathcal{N}_i} \mathbb{W}_{ij}$ is defined as the set of nominal disturbances, with $\mathbb{W}_{ij} = A_{ij}\mathbb{X}_j \oplus B_{ij}\mathbb{U}_j$ being the contribution of subsystem j to the disturbance of subsystem i. The set $\mathbb{W}_i^0$ contains the origin in its interior and can be described by a set of $r_i^{w^0}$ inequalities

$$\mathbb{W}_i^0 \triangleq \mathbb{W}_i^0(g_i^0) \triangleq \{w_i \in \mathbb{R}^{n_i} : C_i^{w^0} w_i \leq g_i\}, \forall g_i \in \mathbb{R}_{0+}^{r_i^{w^0}},$$

where $C_i^{w^0}$ is defined so that $\mathbb{W}_i^0(\mathbf{1})$ is formed from the full sized constraint sets, i.e.,

$$\mathbb{W}_i^0(\mathbf{1}) = \bigoplus_{j \in \mathcal{N}_i} \mathbb{W}_{ij}(\mathbf{1}) = \bigoplus_{j \in \mathcal{N}_i} A_{ij}\mathbb{X}_j(\mathbf{1}) \oplus B_{ij}\mathbb{U}_j(\mathbf{1}). \tag{2}$$

Also, $\mathbb{W}_i$ is described by a set of r_i^w inequalities:

$$\mathbb{W}_i \triangleq \mathbb{W}_i(g_i) \triangleq \{w_i \in \mathbb{R}^{n_i} : C_i^w w_i \leq g_i\}, \forall g_i \in \mathbb{R}_{0+}^{r_i^w}.$$

Again, C_i^w is defined so that $\mathbb{W}_i = \mathbb{W}_i(\mathbf{1})$ is formed from the full sized constraint sets $\mathbb{X}_i(\mathbf{1})$ and $\mathbb{U}_i(\mathbf{1})$, i.e.,

$$\begin{aligned} \mathbb{W}_i(\mathbf{1}) &= \mathbb{W}_i^{\mathrm{s}} \oplus \left(\textstyle\bigoplus_{j \in \mathcal{N}_i} \mathbb{W}_{ij}(\mathbf{1})\right) \\ &= \mathbb{W}_i^{\mathrm{s}} \oplus \left(\textstyle\bigoplus_{j \in \mathcal{N}_i} A_{ij}\mathbb{X}_j(\mathbf{1}) \oplus B_{ij}\mathbb{U}_j(\mathbf{1})\right). \end{aligned} \tag{3}$$

According to Assumption 1, it is possible to find, for each i, a local feedback K_i that stabilizes the local subsystem so that all the eigenvalues of $A_{ii} + B_{ii}K_i$ are within the unit circle. Hence, there also exists a polytopic robust positively invariant (RPI) set, $\mathcal{R}_i$, which satisfies:

$$(A_{ii} + B_{ii}K_i)\mathcal{R}_i \oplus \mathbb{W}_i \subseteq \mathcal{R}_i. \tag{4}$$

In particular, $\mathcal{R}_i$ can be represented by $r_i^{\mathcal{R}}$ inequalities as

$$\mathcal{R}_i(q_i) \triangleq \{x_i \in \mathbb{R}^{n_i} : C_i^{\mathcal{R}} x_i \leq q_i\},$$

and $q_i \in \mathbb{R}_{0+}^{r_i^{\mathcal{R}}}$. Moreover, following the previous definition of $\mathbb{W}_i(\mathbf{1})$, we can normalize $\mathcal{R}_i(q_i)$ so that $\mathcal{R}_i(\mathbf{1})$ is the RPI set that corresponds to the original disturbance set $\mathbb{W}_i(\mathbf{1})$, i.e.,

$$(A_{ii} + B_{ii}K_i)\mathcal{R}_i(\mathbf{1}) \oplus \mathbb{W}_i(\mathbf{1}) \subseteq \mathcal{R}_i(\mathbf{1}).$$

Finally, it is assumed that the strength of couplings is limited in such a way that the invariant set is compatible with local state and input constraint sets [17].

Assumption 3: For all $i \in \mathcal{N}$, $\mathcal{R}_i(\mathbf{1}) \subseteq \mathrm{interior}(\mathbb{X}_i(\mathbf{1}))$ and $K_i\mathcal{R}_i(\mathbf{1}) \subseteq \mathrm{interior}(\mathbb{U}_i(\mathbf{1}))$.

B. Control objective

The goal of local controllers is to minimize the following global infinite-horizon cost

$$\sum_{k=0}^{\infty} \sum_{i \in \mathcal{N}} \ell_i\big(x_i(k), u_i(k)\big) = \sum_{k=0}^{\infty} \sum_{i \in \mathcal{N}} (x_i^\top Q_i x_i + u_i^\top R_i u_i), \tag{5}$$

where $\ell_i(x_i, u_i)$ is the stage cost defined by positive definite weighting matrices Q_i and R_i.

III. Distributed optimal control problem

Local controllers regulate a *nominal* subsystem without interactions $z_i^+ = A_{ii}z_i + B_{ii}v_i$, with z_i and v_i being the corresponding nominal state and input. To this end, $v_i = \bar{\kappa}_i(z_i)$, where $\bar{\kappa}_i(z_i)$ is a MPC-based control law that implements the first element of the optimized sequence $\mathbf{v}_i^*(z_i)$. The MPC optimization also minimizes mutual disturbance sets by optimizing the corresponding parameters a_i and b_i in such a way that local performance is not affected. This information is transmitted to neighbors, which benefit from a decrease of their local uncertainty.

Regarding the *real* subsystem, the following input is applied:

$$u_i^* = \kappa_i(x_i, z_i) = \bar{\kappa}_i(z_i) + K_i(x_i - z_i), \tag{6}$$

where the second term is included to reduce mismatch between the nominal and perturbed trajectories.

A. Tube-based distributed optimal control problem

At nominal state z_i, an optimized sequence of controls $\mathbf{v}_i = (v_i(0), \dots, v_i(N-1))$ is obtained by local controller i by solving a FHOP $\bar{\mathbb{P}}_i(z_i; a_i, b_i, q_i)$ defined as

$$\min_{(\mathbf{v}_i, a_i, b_i)} V_i^f\big(z_i(N)\big) + \sum_{j=0}^{N-1} \ell_i\big(z_i(j), v_i(j)\big) + \rho_a \|a_i\|_1 + \rho_b \|b_i\|_1,$$

where V_i^f is a terminal cost and $\rho_a > 0$ and $\rho_b > 0$ are constant weighting parameters. The optimization is subject to the following constraints: $(a_i, b_i) \in [0,1]^{r_i^x} \times [0,1]^{r_i^u}$ and $\mathbf{v}_i \in \mathcal{V}_i(z_i; a_i, b_i, q_i)$, where $\mathcal{V}_i(z_i; a_i, b_i, q_i)$ is defined by

$$z_i(j+1) = A_{ii} z_i(j) + B_{ii} v_i(j), j = 1, \dots, N-1, \tag{7a}$$
$$z_i(0) = z_i, \tag{7b}$$
$$z_i(j) \in \mathbb{X}_i(a_i) \ominus \mathcal{R}_i(q_i), j = 0, \dots, N-1, \tag{7c}$$
$$v_i(j) \in \mathbb{U}_i(b_i) \ominus K_i \mathcal{R}_i(q_i), j = 0, \dots, N-1, \tag{7d}$$
$$z_i(N) \in \mathbb{X}_i^f(a_i, b_i; q_i). \tag{7e}$$

Here, $\mathbb{X}_i^f(a_i, b_i; q_i)$ is a terminal set and q_i is a parameter rather than an optimization variable. The domain $z_i \in \mathcal{Z}_i(q_i)$ for which $\bar{\mathbb{P}}_i(z_i; a_i, b_i, q_i)$ has a feasible solution can be computed using standard methods [17] and is defined as

$$\big\{z_i : \exists (a_i, b_i) \in [0,1]^{r_i^x} \times [0,1]^{r_i^u} \text{ s.t. } \mathcal{V}_i(z_i, a_i, b_i; q_i) \neq \emptyset\big\}.$$

B. Parametric terminal set and cost design

Recursive feasibility and closed-loop stability is attained following a standard terminal cost/constraint approach by means of V_i^f and $\mathbb{X}_i^f$ [17]. The terminal cost function is defined as $V_i^f(z_i) = (1/2) z_i^\top P_i z_i$, with $P_i > 0$ satisfying

$$\Phi_i^\top P_i \Phi_i - P_i \leq -Q_i - (K_i^f)^\top R_i K_i^f,$$

where $\Phi_i \triangleq A_{ii} + B_{ii} K_i^f$.

The terminal constraint set $\mathbb{X}_i^f$ is constructed to be invariant for local nominal dynamics when they are stabilized by a feedback $v_i = K_i^f z_i$ and admissible for tightened constraints, i.e.,

$$\mathbb{X}_i^f \subseteq \mathbb{X}_i(a_i) \ominus \mathcal{R}_i(q_i), \tag{8a}$$
$$K_i^f \mathbb{X}_i^f \subseteq \mathbb{U}_i(b_i) \ominus K_i \mathcal{R}_i(q_i). \tag{8b}$$

The terminal set $\mathbb{X}_i^f$ has to be recomputed as $\mathbb{X}_i(a_i)$ and $\mathbb{U}_i(b_i)$ change. To this end, an inner approximation $\mathcal{X}_i^f(a_i, b_i; q_i)$ to the maximal constraint admissible set $\mathbb{X}_i^f$ is parameterized by the state and input constraint vectors a_i and b_i as in [16].

IV. Noncompliant agents

A noncompliance happens when an agent j violates its broadcasted limits a_j and b_j, which provide its neighbors with information regarding the bounds of their local disturbance sets. This can render the computations of neighbors infeasible.

It is possible to employ the sets exchanged to perform a noncompliance detection based on a set-membership approach. To this end, neighbors in $\mathcal{N}_i$ are classified to be in either one of following disjoint sets:

- Compliant neighbor set $\mathcal{N}_i^{\mathrm{C}}$, which comprises neighboring subsystems whose announced disturbance sets can be trusted, which allows reducing conservatism.
- Uncertain compliance neighbor set $\mathcal{N}_i^{\mathrm{UC}}$, which comprises neighboring subsystems whose disturbance sets are compatible with the received disturbances. Initially, all agents are considered in this group.
- Noncompliant neighbor set $\mathcal{N}_i^{\mathrm{NC}}$, which comprises agents not to be trusted so that the controller should be prepared for the worst possible case (i.e., that of maximum coupling).

Note that $\mathcal{N}_i = \mathcal{N}_i^{\mathrm{C}} \cup \mathcal{N}_i^{\mathrm{UC}} \cup \mathcal{N}_i^{\mathrm{NC}}$, with $\mathcal{N}_i^{\mathrm{C}} \cap \mathcal{N}_i^{\mathrm{NC}} = \mathcal{N}_i^{\mathrm{C}} \cap \mathcal{N}_i^{\mathrm{UC}} = \mathcal{N}_i^{\mathrm{UC}} \cap \mathcal{N}_i^{\mathrm{NC}} = \emptyset$.

To reduce conservatism we limit the number of noncompliant agents:

Assumption 4: The maximum number of noncompliant agents in the neighborhood is known to be bounded by $N_{\max}^{\mathrm{NC}}$.

A. Noncompliance Detection

Given that we can measure x_i and x_i^+, it is possible to detect any noncompliance with respect to the transmitted values if

$$w_i = x_i^+ - A_{ii} x_i - B_{ii} u_i \notin \mathbb{W}_i$$

holds. Any noncompliance not fulfilling this condition goes undetected, although it does not compromise the local controller, for the disturbance received can be tolerated.

B. Identification

Under our approach, constrained disturbance sets are broadcasted to neighbors and maximum disturbance sets are known by each agent from the beginning. The challenge is to classify neighbors using this information and measuring only aggregate disturbances. Three situations are possible:

1) Neighbors not compatible with disturbance: It is possible to identify whether a disturbance is compatible with a neighbor $j \in \mathcal{N}_i$ by checking whether

$$w_i \notin \mathbb{W}_i \oplus \tilde{\mathbb{W}}_{ij} \oplus \bigcup_{\mathcal{A} \subseteq \mathcal{N}_i^{\mathrm{NC}} \cup \mathcal{N}_i^{\mathrm{UC}} \setminus \{j\} : |\mathcal{A}| = N_{\max}^{\mathrm{NC}} - 1} \bigoplus_{l \in \mathcal{A}} \tilde{\mathbb{W}}_{il}$$

holds. The fulfillment of this condition implies that j is not compatible with the disturbance received, for there is no set of neighbors $\mathcal{A} \subseteq \mathcal{N}_i^{\mathrm{NC}} \cup \mathcal{N}_i^{\mathrm{UC}}$ with $|\mathcal{A}| = N_{\max}^{\mathrm{NC}} - 1$ that can generate the disturbance received in combination with that of j. This condition should be checked for all neighbors. If the number of agents compatible with the disturbance is lower than or equal to $N_{\max}^{\mathrm{NC}}$, then noncompliant agents can be identified.

2) Neighbors responsible of disturbance: A neighbor j is responsible for the unexpected disturbance received if

$$w_i \notin \mathbb{W}_i \oplus \bigcup_{\mathcal{A}\subseteq\mathcal{N}_i^{\mathrm{NC}}\cup\mathcal{N}_i^{\mathrm{UC}}\setminus\{j\}:|\mathcal{A}|=N_{\max}^{\mathrm{NC}}} \bigoplus_{l\in\mathcal{A}} \tilde{\mathbb{W}}_{il}$$

holds. That is, there is no set of noncompliant neighbors $\mathcal{A} \subseteq \mathcal{N}_i^{\mathrm{NC}} \setminus \{j\}$ that is compatible with the disturbance received. If this condition is fulfilled, then a noncompliant agent is identified. Once $N_{\max}^{\mathrm{NC}}$ noncompliant agents are identified, the rest can be taken as compliant agents and be moved to N_i^{C}.

3) Neighbors compatible with disturbance: The compliance of neighbor j is uncertain, i.e., the disturbance received can be generated by combinations of neighbors that can involve j. In this case, j remains in $\mathcal{N}_i^{\mathrm{UC}}$.

C. Robustification against malicious agents

The maximum impact that a noncompliant neighbor j can have into the disturbances of subsystem i is given by

$$\tilde{\mathbb{W}}_{ij} = (A_{ij}\mathbb{X}_j(\mathbf{1}) \oplus B_{ij}\mathbb{U}_j(\mathbf{1})) \ominus (A_{ij}\mathbb{X}_j(a_j) \oplus B_{ij}\mathbb{U}_j(b_j)). \tag{9}$$

To avoid problems, agent i can use the set $\mathbb{W}_i^{\mathrm{s}}$ introduced in Assumption 2 to get an additional degree of robustness.

Proposition 1: A subsystem i is robust against $N_{\max}^{\mathrm{NC}}$ noncompliant controllers if

$$\mathbb{W}_i^{\mathrm{s}} \supseteq \bigcup_{\mathcal{A}\subseteq\mathcal{N}_i^{\mathrm{NC}}\cup\mathcal{N}_i^{\mathrm{UC}}:|\mathcal{A}|=N_{\max}^{\mathrm{NC}}} \bigoplus_{j\in\mathcal{A}} \tilde{\mathbb{W}}_{ij}$$

holds.

The proof is omitted but the rationale of the proposition is clear: robustness is guaranteed as long as unexpected disturbances stay within the safety set $\mathbb{W}_i^{\mathrm{s}}$. According to Proposition 1, since agent i does not know which are the malicious agents $\mathcal{A} \subseteq \mathcal{N}_i$, it has to be prepared for all the

$$\binom{|\mathcal{N}_i|}{\min(N_{\max}^{\mathrm{NC}}, |\mathcal{N}_i|)}$$

possibilities that can arise when there is a maximum of $N_{\max}^{\mathrm{NC}}$ noncompliant agents in the neighborhood.

V. Distributed control algorithm and implementation

In this section, we present an algorithm with defense mechanisms against noncompliant neighbors. In particular, it combines a set-membership detection mechanism to classify neighbors either as compliant/noncompliant and the optimal control problem $\mathbb{P}_i(z_i; q_i)$ to provide robustness.

Algorithm 1:

Initial data: Sets $\mathbb{X}_i(\mathbf{1})$, $\mathbb{U}_i(\mathbf{1})$, $\mathbb{W}_i(\mathbf{1})$, $\mathcal{R}_i(\mathbf{1})$, $\mathbb{X}_i^f(a_i, b_i; q_i)$; matrices K_i and K_i^f, reconfiguration period T; maximum number of noncompliant controllers in the neighborhood $N_{\max}^{\mathrm{NC}}$.

Initialization: At $k = 0$, set $x_i = z_i = x_i(0)$, $q_i = \mathbf{1}$, $p = 0$, and $\mathcal{N}_i^{\mathrm{UC}} = \mathcal{N}_i$ and $\mathcal{N}_i^{\mathrm{C}} = \mathcal{N}_i^{\mathrm{NC}} = \emptyset$.

Online routine:

1) At time k and state (x_i, z_i), solve $\mathbb{P}_i(z_i; q_i)$ to obtain $v_i^* = \bar{\kappa}_i(z_i)$ and (a_i^*, b_i^*).
2) Apply $u_i = v_i^* + K_i(x_i - z_i)$ to subsystem i.
3) Measure x_i^+, compute $z^+ = A_{ii}z_i + B_{ii}v_i^*$ and $\tilde{w}_i = x_i^+ - A_{ii}x_i - B_{ii}u_i$.
4) If $\tilde{w}_i \notin \mathbb{W}_i^0$
   a) Set $\mathcal{A} = \emptyset$.
   b) For each neighbor $j \in \mathcal{N}_i^{\mathrm{UC}}$
      - If j is *responsible* for $\tilde{w}_i$, $\mathcal{N}_i^{\mathrm{UC}} = \mathcal{N}_i^{\mathrm{UC}} \setminus \{j\}$, $\mathcal{N}_i^{\mathrm{NC}} = \mathcal{N}_i^{\mathrm{NC}} \cup \{j\}$.
      - Else if $\tilde{w}_i$ is compatible with j, $\mathcal{A} = \mathcal{A} \cup \{j\}$.
   c) If $|\mathcal{A}| \leq N_{\max}^{\mathrm{NC}}$, $\mathcal{N}_i^{\mathrm{NC}} = \mathcal{N}_i^{\mathrm{NC}} \cup \mathcal{A}$, $\mathcal{N}_i^{\mathrm{UC}} = \mathcal{N}_i^{\mathrm{UC}} \setminus \mathcal{A}$.
   d) If $|\mathcal{N}_i^{\mathrm{NC}}| = N_{\max}^{\mathrm{NC}}$, $\mathcal{N}_i^{\mathrm{C}} = \mathcal{N}_i \setminus \mathcal{N}_i^{\mathrm{NC}}$, update $\mathbb{W}_i^{\mathrm{s}}$ and compute $\mathbb{W}_i(g_i^+)$.
5) If $k = pT$,
   a) Transmit a_i^*, b_i^* to subsystems $j \in \mathcal{N}_i$.
   b) Compute $\mathbb{W}_i(g_i^+)$.
   c) Set $p = p + 1$.
6) Compute $\mathcal{R}_i(q_i^+)$.
7) Set $(x_i, z_i) = (x_i^+, z_i^+)$, set $k = k + 1$, go to Step 1.

A. Implementation: the polytopic case

Here, we provide implementation details of the algorithm.

1) Computing $\mathbb{W}_i(g_i^+)$: Given a safety disturbance set $\mathbb{W}_i^{\mathrm{s}}(g_i^{\mathrm{s}})$ described by $\{w_i^{\mathrm{s}} : C_i^{\mathrm{s}} w_i^{\mathrm{s}} \leq g_i^{\mathrm{s}}\}$, the local disturbance set $\mathbb{W}_i(g_i)$ –defined by $\{w_i : C_i^w w_i \leq g_i\}$– can be calculated by updating g_i^+ as

$$\begin{aligned} g_{il}^+ = &\max\{C_{il}^w w^l : w^l \in \mathbb{W}^{\mathrm{s}}\} \\ &+ \sum_{j\in\mathcal{N}_i} \max\{C_{il}^w A_{ij} x_j^l : x_j^l \in \mathbb{X}_j(a_j^*)\} \\ &+ \sum_{j\in\mathcal{N}_i} \max\{C_{il}^w B_{ij} u_j^l : u_j^l \in \mathbb{U}_j(b_j^*)\}. \end{aligned}$$

for each entry l of g_i^+.

2) Computing $\mathcal{R}_i(q_i^+)$ given $\mathbb{W}_i(g_i^+)$: Step 6 requires the on-line calculation of a new a minimal RPI set to reduce conservatism and take advantage of the updated information regarding the disturbance set $\mathbb{W}_i(g_i^+)$ and the knowledge regarding the state. To this end, the LP proposed in [18] is used, which allows computing an updated q_i^+ to form the minimal RPI set characterized by the given set of inequalities $C_i^{\mathcal{R}}$ that contains the state. In particular, $\mathcal{R}_i(\mathbf{1})$ is assumed to be designed off-line by a proper method as those in [19], [18]. Then, given $\mathbb{W}_i(g_i^+)$, it suffices to solve the following LP to calculate q_i^+:

$$q_i^+ = c_i^* + d_i^* \text{ where } (c_i^*, d_i^*) = \arg \max_{\substack{\{c_{il}, d_{il}, \xi_i^l, \omega_i^l\} \\ \forall l \in \{1,\ldots,r_i^{\mathcal{R}}\}}} \sum_{l=1}^{r_i^{\mathcal{R}}} c_{il} + d_{il}$$

subject to, for all $l \in \{1, \ldots, r_i^{\mathcal{R}}\}$,

$$\begin{aligned} c_{il} &\leq C_{il}^{\mathcal{R}}(A_{ii} + B_{ii}K_i)\xi_i^l, \\ C_{il}^{\mathcal{R}}(x_i^+ - z_i^+) &\leq C_i^{\mathcal{R}}\xi_i^l, \\ C_i^{\mathcal{R}}\xi_i^l &\leq c_i + d_i, \\ d_{il} &\leq C_{il}^{\mathcal{R}}\omega_i^l, \\ C_i^w\omega_i^l &\leq g_i^+. \end{aligned}$$

VI. Recursive feasibility and stability

Given $x_i \in z_i \oplus \mathcal{R}_i$, a feasible solution $\mathbf{v}_i^*(z_i)$ for $\mathbb{P}_i(z_i; q_i)$ guarantees that $x_i^+ \in z_i^+ \oplus \mathcal{R}_i$ and the satisfaction of the local true state and input constraints. Moreover, the sequence

$$\tilde{\mathbf{v}}_i(z_i^+) = \{v_i^*(1; z_i), \dots, v_i^*(N-1; z_i), K_i^f z_i^*(N; z_i)\} \tag{10}$$

is also feasible for $\mathbb{P}_i(z_i^+)$, which provides the controlled system with recursive feasibility as long as the constraint and invariant sets remain constant, i.e., the constraints of the true subsystem are satisfied for all future $x_i^+ \in (A_{ii}x_i + B_{ii}\kappa_i(x_i, z_i)) \oplus \mathbb{W}_i$.

Nevertheless, the fact that the RPI set changes, i.e., $\mathcal{R}_i(q_i^+) \neq \mathcal{R}_i(q_i)$, demands special attention to avoid the loss of recursive feasibility, for $\tilde{\mathbf{v}}_i(z_i^+)$ may not be feasible for $\mathbb{P}_i(z_i^+; q_i^+)$. Here we make a conservative assumption that requires that a feasible solution can always be found for the initial setup of the control scheme.

Assumption 5: Problem $\mathbb{P}_i(z_i; \mathbf{1})$ is feasible.

A. Conditions for recursive feasibility

Next, we discuss the different situations that can come up after the update of $\mathcal{R}_i$:

- $\mathcal{R}_i(q_i^+) \subseteq \mathcal{R}_i(q_i)$: every decrease $\mathcal{R}_i$ makes the domain of the optimization problem $\mathcal{Z}_i$ larger, as shown in [16]. Hence, the sequence is still feasible in future optimizations. Since the optimization promotes the reduction of $\mathbb{X}_i(a_i) \ominus \mathcal{R}_i(q_i)$ and $\mathbb{U}_i(b_i) \ominus K_i\mathcal{R}_i(q_i)$ until these constraints become active, a_i and b_i must decrease, which reduces $\mathbb{W}_{ji}$ for any j with $i \in \mathcal{N}_j$ and allows $\mathcal{R}_i(q_j)$, a_j and b_j to decrease and hence reduce $\mathbb{W}_{ij}$ and $\mathcal{R}_i(q_i)$. In this way, exponential stability towards the origin can be achieved if all agents comply with the scheme, as it was shown in [16] provided that a_i and b_i are non-increasing over time. If there are noncompliant agents, then agents state must remain inside a bounded region around the origin.
- $\mathcal{R}_i(q_i^+) \supset \mathcal{R}_i(q_i)$: $\mathcal{R}_i(q_i^+) = \mathcal{R}_i(q_i)$ should always be a feasible solution for the minimal RPI calculation step, that is, this case should not happen. Nevertheless, let us assume this situation for the sake of analysis. In this case, the sequence $\tilde{\mathbf{v}}_i(z_i^+)$ may not be feasible for $\mathbb{P}_i(z_i^+)$ and two situations can arise:
  - A new solution can be found for $\mathbb{P}_i(z_i^+)$ in such a way that a_i and b_i are lower or equal to the last *broadcasted* values. In this case, neighbors are not affected and everything is handled internally by the local controller.
  - A new solution can be found for $\mathbb{P}_i(z_i^+)$ but a_i and b_i must be increased with respect to the last transmitted values. For example, in the worst case the controller can resort to the initial case, which is assumed to be feasible. Here, it is necessary to communicate the new values *before* taking any control action. An iterative process could take place until agents converge on the values of their new bounds, which in the worst case are those corresponding to full sized constraints.

VII. Illustrative example

A modification of the four-truck system presented in [20] is used as test bench. Here, trucks have mass $m_1 = 3\,\mathrm{kg}$, $m_2 = 2\,\mathrm{kg}$, $m_3 = 3\,\mathrm{kg}$, and $m_4 = 6\,\mathrm{kg}$ and dynamics

$$\begin{bmatrix}\dot{r}_i \\ \dot{v}_i\end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 \\ -\frac{1}{m_i}\sum_{j\in\mathcal{N}_i} k_{ij} & -\frac{1}{m_i}\sum_{j\in\mathcal{N}_i} h_{ij}\end{bmatrix}}_{A_{ii}} \begin{bmatrix} r_i \\ v_i\end{bmatrix} + \underbrace{\begin{bmatrix} 0 \\ 100\end{bmatrix}}_{B_{ii}} u_i + \underbrace{\sum_{j\in\mathcal{N}_i} \underbrace{\begin{bmatrix} 0 & 0 \\ \frac{1}{m_i}\sum_{j\in\mathcal{N}_i} k_{ij} & \frac{1}{m_i}\sum_{j\in\mathcal{N}_i} h_{ij}\end{bmatrix}}_{A_{ij}} \begin{bmatrix} r_j \\ v_j\end{bmatrix}}_{w_i}$$

where r_i, v_i, u_i and w_i are respectively the displacement of truck i with respect to its equilibrium position, its velocity, the acceleration, which is the control input, and the disturbance due to neighbors, which is generated in the following way:

- trucks 1 and 2 are coupled via a spring (stiffness $k_{12} = 0.5\,\mathrm{N\,m^{-1}}$) and damper ($h_{12} = 0.2\,\mathrm{N\,m^{-1}\,s^{-1}}$);
- trucks 2 and 3 are coupled via a spring (stiffness $k_{23} = 0.75\,\mathrm{N\,m^{-1}}$) and damper ($h_{23} = 0.25\,\mathrm{N\,m^{-1}\,s^{-1}}$);
- trucks 3 and 4 are coupled via a spring (stiffness $k_{34} = 1\,\mathrm{N\,m^{-1}}$) and damper ($h_{34} = 0.3\,\mathrm{N\,m^{-1}\,s^{-1}}$);

Initial states are $x_1^{\mathrm{T}} = [1.8, 0]$, $x_2^{\mathrm{T}} = [-1, 0]$, $x_3^{\mathrm{T}} = [1, 0]$ and $x_4^{\mathrm{T}} = [-1, 0]$. The goal is to take trucks to the origin while satisfying state and input constraints $\mathbb{X}_i(\mathbf{1})$ and $\mathbb{U}_i(\mathbf{1})$, which are defined as $|r_i| \leq 4$, $|v_i| \leq 1$ and $|u_i| \leq 1$ for trucks 1, 2, and 3; the constraints of truck 4 are simply $|r_4| \leq 4$, $|v_4| \leq 1$ and $|u_4| \leq 2$. Also, recall that initial disturbance sets are assumed to be known by all affected agents, which allow them to compute $\mathbb{W}_i(\mathbf{1})$.

Local controllers approximate the continuous-time dynamics with a sampling time of 0.1 seconds to obtain a discrete-time model by using zero-order hold. Cost matrices are defined as $Q_i = I$ and $R_i = 100$ and $\rho_a = 0.0001$, and the horizon is $N = 25$. Note that there is no need for b_i in this case study, for there is only state coupling. Also, a deadbeat controller is used for the tube control law, K_i, of each truck, so that the minimal RPI set is finitely determined. Finally, an LQR $K_i^f = K_\infty(A_{ii}, B_i, Q_i, R_i)$ is used as a terminal controller, which allows us to calculate the terminal cost matrix P_i as the solution of the corresponding Lyapunov equation and the maximal parametric terminal set that guarantees the satisfaction of $\mathbb{X}_i(a_i)$ and $\mathbb{U}$.

We assume that $N_{\max}^{\mathrm{NC}} = 1$ and set agent 2 as noncompliant. In particular, we consider that its state remains constant at $x_2^{\mathrm{T}} = [4, 1]$ and also that it broadcasts that its state constraint set is empty so that neighbors will not expect any disturbances from it. Also, given the couplings, agents 1 and 4 are going to work in a pure decentralized tube MPC mode, for they have only one neighbor. Hence, we focus exclusively on agent 3, which is the only one that can benefit by applying the proposed method. Nevertheless, no detection can be carried

out because the disturbance set that agent 3 can receive from its neighbor 2 is a subset of that generated by agent 4.

In a 50 time step simulation, the cumulated cost of agent 3 when the method proposed in [16] was 8.1859. This result was obtained allowing agents to reconfigure their disturbance sets at each time step and without accounting for disturbances received from agent 2, for this is the information broadcasted by this agent. When standard decentralized tube MPC is applied, performance improves slightly and cumulated cost becomes 8.1830. In this case, agent 3 assumes worst case disturbances from agents 2 and 4 in its calculations. This improvement increases when the proposed method is used and cumulated cost becomes 8.1824. Here, it is considered that either agent 2 or agent 4 broadcasts false information, which allows local controller 3 to reduce conservatism. Figure 1 illustrates the conservatism of each approach by plotting simultaneously the evolution of the state of this agent and the size of the minimal RPI that corresponds to the information available from neighbors' disturbances. Nevertheless, note that costs can be misleading, for disturbances generated by the noncompliant neighbor might be beneficial for some of its neighbors. For this reason we must stress that the most relevant contribution of the proposed approach is to preserve theoretical properties such as stability even when noncompliant neighbors might exist.

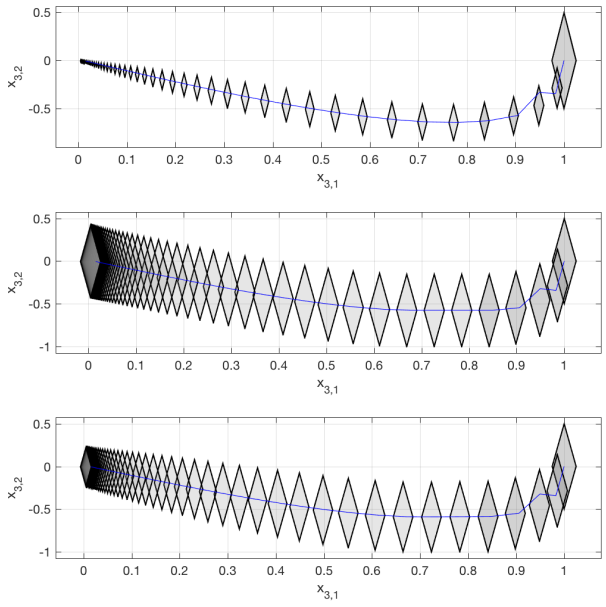

Fig. 1. Evolution of the state of agent 3 for the tested methods (up: DMPC with minimization of dual disturbances [16]; mid: decentralized tube MPC; down: proposed approach.).

VIII. Conclusions

A distributed MPC scheme with robustness with respect to noncompliant agents has been presented. To this end, local controllers deal explicitly with the possible deviations of neighbors with respect to their broadcasted bounds. To avoid resorting to the conservative decentralized tube-based MPC, it is assumed that there is a maximum number of noncompliant agents. Also, the proposed scheme has interesting theoretical properties as recursive feasibility and stability. In the simulation example, the rationale of the proposed method has been illustrated by showing how the conservativeness of the calculations lies between those of the method presented in [16] and standard decentralized tube MPC. Future work will extend the theoretical properties of the scheme, which will also be tested in a larger size example.

References

[1] J. M. Maciejowski, Predictive Control with Constraints, Prentice Hall, 2002.

[2] S. J. Qin, T. A. Badgwell, A survey of industrial model predictive control technology, Control Engineering Practice 11 (2003) 733–764. doi:10.1016/S0967-0661(02)00186-7.

[3] P. D. Christofides, R. Scattolini, D. Muñoz del la Peña, J. Liu, Distributed model predictive control: A tutorial review and future research directions, Computers and Chemical Engineering 51 (2013) 21–41. doi:10.1016/j.compchemeng.2012.05.011.

[4] J. M. Maestre, R. R. Negenborn (Eds.), Distributed Model Predictive Control Made Easy, Springer, 2014.

[5] Y. Okajima, K. Hirata, T. Murao, T. Hatanaka, V. Gupta, K. Uchida, Strategic behavior and market power of aggregators in energy demand networks, in: Proceedings of the 56th IEEE Conference on Decision and Control, IEEE, 2017.

[6] T. Tanaka, V. Gupta, Incentivizing truth-telling in mpc-based load frequency control, in: Proceedings of the 55th IEEE Conference on Decision and Control, 2016.

[7] A. Gupta, T. Başar, Dynamic incentive design in multi-stage linear-gaussian games with asymmetric information: A common information based approach, in: Proceedings of the 53rd IEEE Conference on Decision and Control, 2014.

[8] H. Sandberg, S. Amin, K. H. Johansson, Special issue on cyberphysical security in networked control system, IEEE Control Systems Magazine 35 (1) (2015) 20 – 23.

[9] P. Cheng, L. Shi, B. Sinopoli, Special issue on secure control of cyber-physical systems, IEEE Trans on Control of Network Systems 4 (1) (2017) 1 – 3.

[10] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, Cyber security and privacy issues in smart grids, IEEE Communications Surveys & Tutorials 14 (4) (2012) 981–997.

[11] W. Zeng, M.-Y. Chow, Resilient distributed control in the presence of misbehaving agents in networked control systems, IEEE Transactions on Cybernetics 44 (11) (2014) 2038–2049.

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

[13] P. Velarde, J. M. Maestre, H. Ishii, R. R. Negenborn, Scenario based defense mechanism for distributed model predictive control, in: Proceedings of the 56th IEEE Conference on Decision and Control, 2017.

[14] T. Wang, H. Gao, J. Qiu, A combined fault-tolerant and predictive control for network-based industrial processes, IEEE Transactions on Industrial Electronics 63 (4) (2016) 2529–2536.

[15] S. V. Naghavi, A. A. Safavi, M. Kazerooni, Decentralized fault tolerant model predictive control of discrete-time interconnected nonlinear systems, Journal of the Franklin Institute 351 (3) (2014) 1644–1656.

[16] P. A. Trodden, J. M. Maestre, Distributed predictive control with minimization of mutual disturbances, Automatica 77 (2017) 31–43.

[17] J. B. Rawlings, D. Q. Mayne, Model Predictive Control: Theory and Design, Nob Hill Publishing, 2009.

[18] P. A. Trodden, A one-step approach to computing a polytopic robust positively invariant set, IEEE Transactions on Automatic Control (in press). doi:10.1109/TAC.2016.2541300.

[19] S. V. Raković, E. C. Kerrigan, K. I. Kouramas, D. Q. Mayne, Invariant approximations of the minimal robust positively invariant set, IEEE Transactions on Automatic Control 50 (4) (2005) 406–410. doi:10.1109/TAC.2005.843854.

[20] S. Riverso, G. Ferrari-Trecate, Tube-based distributed control of linear constrained systems, Automatica 48 (2012) 2860–2865. doi:10.1016/j.automatica.2012.08.024.