

Resilient Distributed Energy Management for Systems of Interconnected Microgrids

Wicak Ananduta, José María Maestre, *Member, IEEE*, Carlos Ocampo-Martinez, *Senior Member, IEEE*, and Hideaki Ishii, *Senior Member, IEEE*

Abstract—In this paper, distributed energy management of interconnected microgrids, which is stated as a dynamic economic dispatch problem, is studied. Since the distributed approach requires cooperation of all local controllers, when some of them do not comply with the distributed algorithm that is applied to the system, the performance of the system might be compromised. Specifically, it is considered that adversarial agents (microgrids with their controllers) might implement control inputs that are different than the ones obtained from the distributed algorithm. By performing such behavior, these agents might have better performance at the expense of deteriorating the performance of the regular agents. This paper proposes a methodology to deal with this type of adversarial agents such that we can still guarantee that the regular agents can still obtain feasible, though suboptimal, control inputs in the presence of adversarial behaviors. The methodology consists of two steps: (i) the robustification of the underlying optimization problem and (ii) the identification of adversarial agents, which uses hypothesis testing with Bayesian inference and requires to solve a local mixed-integer optimization problem. Furthermore, the proposed methodology also prevents the regular agents to be affected by the adversaries once the adversarial agents are identified. In addition, we also provide a sub-optimality certificate of the proposed methodology.

Index Terms—Economic dispatch, distributed MPC, distributed optimization, resilient algorithm

I. INTRODUCTION

In order to face the increasing penetration of distributed generation units, either dispatchable or non-dispatchable ones, and energy storages, such as batteries, supercapacitors, and fuel cells, in electrical networks, distributed approaches for energy management system currently gain a lot of attention, e.g., as discussed in [1]–[4]. The advantages of employing a distributed approach for this task include avoiding significant increase of information, communication, and modeling resources used for a centralized dispatch as well as distributing high computational burden [1].

W. Ananduta and C. Ocampo-Martinez are with the Automatic Control Department, Universitat Politècnica de Catalunya, Institut de Robòtica i Informàtica Industrial (CSIC-UPC), Barcelona, Spain (emails: {wananduta, cocampo}@iri.upc.edu).

J. M. Maestre and H. Ishii are with Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan (emails: pepemaestre@us.es, ishii@c.titech.ac.jp).

J. M. Maestre is also with Department of System and Automation Engineering, University of Seville, Seville, Spain.

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675318 (INCITE). Financial support by the Spanish MINECO project DPI2017-86918-R and the Japanese Society for the Promotion of Science (scholarship PE16048) is also gratefully acknowledged.

In a distributed scheme, a distribution electrical network can be viewed as a system of interconnected microgrids [1], [5], each of which is a controllable entity that has its own local controller. Therefore, the economic dispatch problem of the network must be decomposed and assigned to the local controllers. A distributed optimization approach can then be formulated and applied to solve the problem. In this regard, Model Predictive Control (MPC) strategy, with receding horizon principle, is suitable, particularly when the dynamics of the storages are considered, since the decisions/control inputs are always updated at each sampling time according to the measurement of the states. Distributed MPC (DMPC) methods that have been proposed to solve economic dispatch problems include those that are based on dual decomposition [4], alternating direction method of multipliers (ADMM) [2], optimality condition decomposition (OCD) [3] and population dynamics [6]. These approaches are suitable since they are able to obtain an optimal solution given that the related optimization problem is convex.

Two important features in such distributed approaches are the necessity to share information among the agents (in this case the microgrids) and the cooperation of the agents to apply the algorithm and to comply with the decisions obtained from the distributed algorithm. In this work, we deal with the problem of agent compliance, in which some of the agents do not always implement the decision obtained from the distributed algorithm. Instead, they may implement a different decision that is more beneficial for them but compromise the performance of the other agents and hence the entire system.

Agents with such adversarial behaviors are identified in [7] as *liar agents* or in [8] as *misbehaving agents*. The authors of [7] propose a secure dual-decomposition-based DMPC, in which the agents that provide extreme control input values are monitored and disregarded, to deal with this issue. Furthermore, [8] addresses a cyber-attack problem of a consensus-based distributed control scheme for distributed energy storage systems. The proposed approach in [8] includes a fuzzy-logic-based detection and a consensus based leader-follower distributed control scheme. Related to the cyber-security issue of cyber physical systems, in particular power systems, the work of [9] provides a mathematical framework for attack detection and monitoring. In addition, [10]–[12] and some of their references also discuss consensus problems in which some of the agents perform adversarial behavior to prevent convergence.

The contributions of this paper is as follows. We study the

impact of an adversarial behavior in the distributed energy management system that is based on a DMPC scheme and propose to actively use the storage system and the possibility to establish/disestablish connections between agents to deal with this behavior. To this end, we propose an approach that consists of two main steps. The first step is the robustification of the economic dispatch problem. By considering the robust reformulation, we ensure that the regular agents always obtain a solution that satisfies all the constraints defined in the economic dispatch problem even though there are some agents that do not comply with the decisions. In the second step, we propose an active strategy to identify the adversarial agents that is based on hypothesis testing using Bayesian inference (e.g., [13]). In this method, each regular agent must solve a local mixed-integer problem to decide the connections with its neighbors at each time instant. By actively connecting/disconnecting with neighbors, regular agents can then assess their hypothesis. Additionally, we also provide a decentralized sub-optimality certificate of our proposed approach.

Differently from [8], we consider a DMPC scheme to act as an energy management. Thus, our work is more related to [7] than the approaches discussed in [8], [10]–[12]. However, the methodology that we propose in this paper is different than that proposed in [7], in a way that it is more specific for the aforementioned problem and particularly for power systems. Moreover, unlike [7], our approach can deal with more than one adversarial agent in a network.

This paper is structured as follows. In Section II, the dynamic economic dispatch problem of interconnected microgrids is formulated. Moreover, a distributed approach that is based on dual decomposition and the adversary model are presented. In Section III, the approach to deal with the adversarial behavior is proposed. Section IV provides the numerical simulations and Section V concludes the paper.

Notations: The set of real numbers and integers are denoted by \mathbb{R} and \mathbb{Z} , respectively. Moreover, $\mathbb{R}_{\geq a}$ denotes all real numbers in the set $\{b : b \geq a, b, a \in \mathbb{R}\}$ and $\mathbb{Z}_{\geq a}$ denotes all integers in the set $\{b : b \geq a, b, a \in \mathbb{Z}\}$. A similar definition can be used for the strict inequality case. For column vectors v_i with $i \in \mathcal{L} = \{l_1, \dots, l_{|\mathcal{L}|}\}$, the operator $[v_i^\top]_{i \in \mathcal{L}}^\top$ denotes the column-wise concatenation, i.e., $[v_i^\top]_{i \in \mathcal{L}}^\top = [v_{l_1}^\top, \dots, v_{l_{|\mathcal{L}|}}^\top]^\top$. The vector $\mathbb{1}_n$ denotes $[1 \ 1 \ \dots \ 1]^\top \in \mathbb{R}^n$. The set cardinality and Euclidean norm are denoted by $|\cdot|$ and $\|\cdot\|_2$. Furthermore, $\mathbb{P}(\cdot)$ denotes the probability measure. Finally, discrete-time instants are denoted by the subscript k .

II. PROBLEM FORMULATION & DISTRIBUTED APPROACH

In this section, the dynamic economic dispatch is formulated as an MPC problem. Afterward, a DMPC strategy based on a distributed optimization approach is formulated for this problem. Finally, the adversaries are defined.

A. Dynamic Economic Dispatch Problem

Consider a network of interconnected microgrids, which can be represented as an undirected graph $\mathcal{S} = (\mathcal{N}, \mathcal{E})$,

where $\mathcal{N} = \{1, 2, \dots, |\mathcal{N}|\}$ denotes the set of microgrids and $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ denotes the set of physical links among the microgrids. In this regard, the link $(i, j) \in \mathcal{E}$ implies that it is possible to exchange energy between microgrids i and j . Furthermore, denote the set of neighbors of microgrid i by \mathcal{N}_i , i.e., $\mathcal{N}_i = \{j : (i, j) \in \mathcal{E}\}$. Each microgrid $i \in \mathcal{N}$ consists of an aggregated local load, denoted by $p_{i,k}^d \in \mathbb{R}_{\geq 0}$, a set of dispatchable distributed generators, denoted by \mathcal{G}_i , and a storage system from which electrical energy can be stored and retrieved. Each microgrid can also obtain power by buying it from the main grid. In this economic dispatch problem, optimal power generation of the generators and storage usage are sought by considering their economical costs such that the loads are satisfied. Additionally, $p_{i,k}^d$ is assumed to be bounded as follows:

$$|p_{i,k}^d - \hat{p}_{i,k}^d| \leq d_i^{\max}, \quad (1)$$

where $\hat{p}_{i,k}^d, d_i^{\max} \in \mathbb{R}_{\geq 0}$ denote the forecast and the upper bound, respectively, which are assumed to be known a priori. Note that the forecast and bound can be obtained from historical data.

The power balance equations that must be satisfied by each microgrid $i \in \mathcal{N}$ at each time instant $k \in \mathbb{Z}_{\geq 0}$ are as follows [2], [3]:

$$\hat{p}_{i,k}^d - p_{i,k}^G - p_{i,k}^{\text{st}} - p_{i,k}^{\text{im}} - \sum_{j \in \mathcal{N}_i} p_{j,i,k}^t = 0, \quad (2)$$

$$p_{i,j,k}^t + p_{j,i,k}^t = 0, \quad \forall j \in \mathcal{N}_i, \quad (3)$$

where $p_{i,k}^G = \sum_{m \in \mathcal{G}_i} p_{m,k}^g \in \mathbb{R}_{\geq 0}$ denotes the total power generation in microgrid i , with $p_{m,k}^g$ being the power generation of distributed generator m ; $p_{i,k}^{\text{st}} \in \mathbb{R}$ denotes the power delivered by or to the storage; $p_{i,k}^{\text{im}} \in \mathbb{R}_{\geq 0}$ denotes the imported power from the main grid; and $p_{j,i,k}^t \in \mathbb{R}$, for all $j \in \mathcal{N}_i$, denote the power flows between microgrids i and j and can be regarded as a coupled variable. Note that (2) resembles the DC approximation of the power flow equation, in which $p_{j,i,k}^t$ is a function of the voltage angles. Furthermore, (3) ensures that there is an agreement between two neighboring microgrids in terms of the power exchanged between them.

The dynamics of the storage system, for each $i \in \mathcal{N}$, is represented as follows:

$$x_{i,k+1} = a_i x_{i,k} + b_i p_{i,k}^{\text{st}}, \quad (4)$$

where $x_{i,k}$ denotes the state-of-charge (SoC) of storage i , $a_i \in (0, 1]$ denotes the efficiency of the storage and $b_i = -\frac{T_s}{e_{\text{cap},i}}$, where T_s and $e_{\text{cap},i}$ denote the sampling time and the maximum capacity of the storage, respectively.

Additionally, for each microgrid $i \in \mathcal{N}$, some local operational constraints are also considered as follows:

$$x_i^{\min} \leq x_{i,k} \leq x_i^{\max}, \quad (5)$$

$$-p_i^{\text{ch}} \leq p_{i,k}^{\text{st}} \leq p_i^{\text{dh}}, \quad (6)$$

$$p_i^{\text{G},\min} \leq p_{i,k}^G \leq p_i^{\text{G},\max}, \quad (7)$$

$$p_{i,k}^{\text{im}} \leq p_i^{\text{im},\max} \quad (8)$$

$$-p_{ji}^{\text{t},\max} \leq p_{j,i,k}^t \leq p_{ji}^{\text{t},\max}, \quad \forall j \in \mathcal{N}_i, \quad (9)$$

where $x_i^{\min}, x_i^{\max} \in \mathbb{R}_{\geq 0}$ denote the minimum and the maximum SoC of the storage of microgrid i , respectively. Note that $0 \leq x_i^{\min} \leq x_i^{\max} \leq 1$. Moreover, $p_i^{\text{ch}} \in \mathbb{R}_{\geq 0}$ and $p_i^{\text{dh}} \in \mathbb{R}_{\geq 0}$ denote the maximum charging and discharging power of the storage. Furthermore, $p_i^{\text{G},\min}, p_i^{\text{G},\max} \in \mathbb{R}_{\geq 0}$ denote the minimum and the maximum power generated by the distributed generators of microgrid i , respectively, $p_i^{\text{im},\max}$ denotes the maximum imported power from the main grid, and $p_{ji}^{\text{t},\max}$ denotes the maximum energy that can be transferred between microgrid i and j . Notice that (9) is symmetric and $p_{ji}^{\text{t},\max} = p_{ij}^{\text{t},\max}$, for all $(i, j) \in \mathcal{E}$.

Now, denote the control input vector of microgrid i by $\mathbf{u}_{i,k} = [p_{i,k}^{\text{st}}, p_{i,k}^{\text{G}}, p_{i,k}^{\text{im}}, \mathbf{u}_{i,k}^{\text{c}\top}]^\top \in \mathbb{R}^{3+|\mathcal{N}_i|}$, where $\mathbf{u}_{i,k}^{\text{c}} = [p_{ji,k}^{\text{t}}]_{j \in \mathcal{N}_i}^\top$ is the vector of coupled control input variables. We denote h_p as the prediction horizon and consider the quadratic cost function

$$J_{i,k} = \mathbf{u}_{i,k}^\top R_i \mathbf{u}_{i,k}, \quad (10)$$

where $R_i = \text{diag}([c_i^{\text{st}}, c_i^{\text{G}}, c_i^{\text{im}}, c_i^{\text{t}} \mathbf{1}_{|\mathcal{N}_i|}^\top]) > 0$, in which $c_i^{\text{st}}, c_i^{\text{G}}, c_i^{\text{im}}, c_i^{\text{t}} \in \mathbb{R}_{>0}$ denote the cost of storage operation, the cost of producing energy, the cost of buying energy from the main grid, and the cost of transferring energy to/from the neighbor due to losses [2]. Thus, the finite-time optimization problem that underlies an MPC strategy for the dynamic economic dispatch of this system can be written as

$$\begin{aligned} & \text{minimize} && \sum_{i \in \mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell|k}) && (11a) \\ & \text{subject to} && \mathbf{F}_i \mathbf{u}_{i,\ell|k} \leq \mathbf{f}_{i,\ell}, \quad \forall i \in \mathcal{N}, && (11b) \end{aligned}$$

$$\mathbf{u}_{i,\ell|k}^{\text{c}} + \sum_{j \in \mathcal{N}_i} \mathbf{G}_{ij} \mathbf{u}_{j,\ell|k}^{\text{c}} = \mathbf{0}, \quad \forall i \in \mathcal{N}, \quad (11c)$$

for all $\ell \in \{k, \dots, k+h_p-1\}$, where the local constraints (11b) that only include local control inputs are constructed from (2), (4)-(9), while the coupled constraints (11c) are constructed from (3).

Remark 1: Without loss of generality, $p_{i,k}^{\text{G}}$ is considered as one of the control input instead of $p_{m,k}^{\text{G}}$, for all $m \in \mathcal{G}_i$, for simplicity of the exposition. Considering $p_{m,k}^{\text{G}}$, for all $m \in \mathcal{G}_i$, in \mathbf{u}_i is also straightforward and only increases the dimension of \mathbf{u}_i . \square

Remark 2: In the matrix R_i , the weight/cost of exchanging energy, c_i^{t} , is considered to be smaller than the other weights. \square

Remark 3: Problem (11) considers the load forecast, which does not always match with the actual load. Therefore, the proposed robust reformulation in Section III-A takes into account the fact that $p_{i,k}^{\text{d}}$, for all $i \in \mathcal{N}$, are bounded, as expressed in (1). \square

Problem (11) is convex since the inequality constraints form a polyhedron, the coupled equality constraints are affine, and the cost function (10) is strictly convex. Furthermore, the following assumption is considered.

Assumption 1: For Problem (11), there exists a nonempty set of feasible solutions and it includes a subset in which $p_{ij,k}^{\text{t}} = p_{ji,k}^{\text{t}} = 0$, for any $(i, j) \in \mathcal{E}$ and $k \in \mathbb{Z}_{\geq 0}$. \square

Note that $p_{ij,k}^{\text{t}} = p_{ji,k}^{\text{t}} = 0$ implies that there is no power exchanged between microgrids i and j . Based on this assumption, it is considered that each microgrid is able to satisfy its load independently, e.g., in the island mode. However, it is more cost efficient if the microgrids exchange power among them when they are connected.

B. Distributed Energy Management based on Dual Decomposition

In general, many distributed optimization algorithm can be applied as a DMPC strategy to solve Problem (11). However, for the clarity of the explanation, a DMPC algorithm based on dual decomposition is considered in this paper. It is known that the solution obtained from a distributed algorithm based on dual decomposition converges to the optimal solution if the problem is convex with strictly convex cost function [14]. In order to design the mentioned algorithm, the Lagrangian function associated to Problem (11) is derived and its dual problem [15] is decomposed into smaller problems that are assigned to the agents (microgrids). The DMPC strategy based on dual decomposition is stated in Algorithm 1, where $\lambda_{i,\ell} \in \mathbb{R}^{|\mathcal{N}_i|}$, for all $\ell \in \{k, \dots, k+h_p-1\}$ and all $i \in \mathcal{N}$, are the Lagrange multipliers associated to the coupled constraints (11c). In this algorithm, each agent should solve the local optimization problem in step 4 and update its Lagrange multipliers via the gradient-ascent method at each iteration. Finally, denote the optimal decisions obtained by the DMPC strategy for time k by $\mathbf{u}_{i,k|k}^*$, for all $i \in \mathcal{N}$.

Algorithm 1 DMPC algorithm based on dual decomposition, for each agent $i \in \mathcal{N}$

- 1: Set $r = 1$, $\varepsilon \in \mathbb{R}_{>0}$, and initialize $\lambda_{i,\ell}^{(r)}$
- 2: **while** $\|[\psi_{i,k}^\top \ \dots \ \psi_{i,k+h_p-1}^\top]\|_2 > \varepsilon$ **do**
- 3: Receive $\lambda_{j,\ell}^{(r)}$ for all $\ell \in \{k, \dots, k+h_p-1\}$ from the neighbors, all $j \in \mathcal{N}_i$, and send $\lambda_{i,\ell}^{(r)}$ for all $\ell \in \{k, \dots, k+h_p-1\}$ to the neighbors
- 4: Solve the local optimization problem:

$$\begin{aligned} & \text{minimize} && \sum_{\ell=k}^{k+h_p-1} \left(J_{i,\ell}(\mathbf{u}_{i,\ell|k}) + \mathbf{y}_{i,\ell}^\top \mathbf{u}_{i,\ell|k}^{\text{c}} \right) \\ & \text{subject to} && (11b), \quad \forall \ell \in \{k, \dots, k+h_p-1\}, \end{aligned}$$

where $\mathbf{y}_{i,\ell}^\top = \lambda_{i,\ell}^{(r)\top} + \sum_{j \in \mathcal{N}_i} \lambda_{j,\ell}^{(r)\top} \mathbf{G}_{ji}$

- 5: Receive the decision $\mathbf{u}_{j,\ell|k}^{\text{c}}$ for all $\ell \in \{k, \dots, k+h_p-1\}$ from the neighbors, all $j \in \mathcal{N}_i$, and send $\mathbf{u}_{i,\ell|k}^{\text{c}}$ for all $\ell \in \{k, \dots, k+h_p-1\}$ to the neighbors
- 6: Update $\lambda_{i,\ell}$ for all $\ell \in \{k, \dots, k+h_p-1\}$ as

$$\lambda_{i,\ell}^{(r+1)} = \lambda_{i,\ell}^{(r)} + \gamma \psi_{i,\ell},$$

where $\psi_{i,\ell} = \left(\mathbf{u}_{i,\ell|k}^{\text{c}} + \sum_{j \in \mathcal{N}_i} \mathbf{G}_{ij} \mathbf{u}_{j,\ell|k}^{\text{c}} \right)$ and $0 < \gamma < 1$

- 7: $r \leftarrow r + 1$
 - 8: **end while**
-

C. Adversary Model

The agents are classified as regular and adversarial agents based on the following definitions.

Definition 1: Agent i belongs to the set of regular agents, denoted by \mathcal{R} , if it always implements its control input $\mathbf{u}_{i,k}$ according to the decision obtained from the DMPC strategy, i.e., $\mathbf{u}_{i,k} = \mathbf{u}_{i,k|k}^*$, for all $k \geq 0$. Otherwise, agent i belongs to the set of adversarial agents, denoted by \mathcal{A} . \square

Definition 2: An attack is defined as the event at one time instant when at least one adversarial agent implements its control input that is different than the decision obtained from the DMPC strategy. \square

We consider the f -local model of adversaries, which is stated in Definition 3.

Definition 3 ([10]): The set of adversarial agents is f -local if $|\mathcal{A} \cap \mathcal{N}_i| \leq f$, for $f \in \mathbb{Z}_{\geq 1}$ and all $i \in \mathcal{N}$. \square

In this paper, the case is restricted for $f = 1$, as stated in the following Assumption 2.

Assumption 2: Each agent has at most one adversarial neighbor. \square

Assumption 3: Regular agents do not have prior knowledge of the occurrence of the attacks, but they have an initial expectation on the probability of attacks, denoted by $P_{\text{at}} \in (0, 1]$. \square

The adversarial agents may try to gain advantage by implementing a different decision that benefits these agents. In the economic dispatch problem, the adversarial agents may get benefit if they decide to reduce the energy production and/or store more energy to their storages. Therefore, in order to meet their power balance equation, they ask their neighbors to provide the deficiency i.e., $p_{ij,k}^{\dagger} > p_{ij,k|k}^{\dagger*}$, for $j \in \mathcal{A}$ and $i \in \mathcal{R}$, where $p_{ij,k|k}^{\dagger*}$ denotes the decision obtained from the DMPC method. Although it leads to a global suboptimal solution, the adversarial agents gain an advantage locally by performing this action. In other words, the adversarial agents are not willing to cooperate for their own interest. It is also possible that this behavior is observed due to a fault in the adversarial agents.

III. PROPOSED APPROACH

In this section, the problem is reformulated such that the regular agents are robust against attacks and propose a methodology to identify the adversarial neighbors and to prevent an attack from them once they are identified.

A. Robustification Against Attacks

Regular agents might be affected negatively from the attacks of their adversarial neighbors. Due to the coupled constraints (3), regular agents must conform with the actions taken by their adversarial neighbors. For instance, if the adversarial neighbor $j \in \mathcal{A}$ requests more power than the agreed solution, then the regular microgrids $i \in \mathcal{N}_j$ must adjust their decision (control inputs $\mathbf{u}_{i,k}$) in order to satisfy their power balance (2). In this regard, the existence of a storage unit at each microgrid could help to mitigate this issue without affecting the operation of the distributed generators. Additionally, uncertain loads might have similar

effect to all microgrids and we consider that the deviation between the forecast and the actual load is compensated by the storage units.

In order to meet the power balance (2) when an attack occurs, more power from the storage ($p_{i,k}^{\text{st}}$) is taken. However, it implies that the evolution of the SoC is different than the one that is predicted by the dynamic model (4). Due to this circumstance, it may happen that the minimum limit of the storage capacity (5) is violated.

In order to ensure that there is no violation on the constraints, a formulation that robustifies Problem (11) against such attacks as well as the uncertainty of the load is proposed. To this end, we consider the attack as disturbance, denoted by $w_{i,k}^{\text{a}}$, and denote the load disturbance by $w_{i,k}^{\text{d}}$. These disturbances affect the power balance (2) as follows:

$$\hat{p}_{i,k}^{\text{d}} - p_{i,k}^{\text{G}} - p_{i,k}^{\text{st}} - p_{i,k}^{\text{im}} - w_{i,k}^{\text{d}} - w_{i,k}^{\text{a}} - \sum_{j \in \mathcal{N}_i} p_{ji,k}^{\text{t}} = 0. \quad (12)$$

Although $w_{i,k}^{\text{d}}$ and $w_{i,k}^{\text{a}}$ are uncertain, they are bounded by (1) and (9), respectively. Therefore, agent $i \in \mathcal{R}$ might consider the worst case of the total disturbance, denoted by $w_{i,k} = w_{i,k}^{\text{a}} + w_{i,k}^{\text{d}}$, which is stated as follows:

$$w_{i,k}^{\text{max}} = \max_{j \in \mathcal{N}_i} (2p_{ji}^{\text{t,max}}) + d_i^{\text{max}}, \quad (13)$$

due to (9) and Assumption 2. Since $w_{i,k}$ is compensated by the power delivered by/to the storage $p_{i,k}^{\text{st}}$, the constraints related to $p_{i,k}^{\text{st}}$, i.e., (5) and (6), might be violated. Therefore, these constraints are tightened to accommodate the worst case disturbance $w_{i,k}^{\text{max}}$ as follows:

$$x_i^{\text{min}} - b_i w_{i,k}^{\text{max}} \leq a_i x_{i,\ell} + b_i p_{i,\ell}^{\text{st}} \leq x_i^{\text{max}} + b_i w_{i,k}^{\text{max}}, \quad (14)$$

$$-p_i^{\text{ch}} + w_{i,k}^{\text{max}} \leq p_{i,\ell}^{\text{st}} \leq p_i^{\text{dh}} - w_{i,k}^{\text{max}}, \quad (15)$$

for all $\ell \in \{k, \dots, k + h_p - 1\}$. Hence, the robust reformulation of Problem (11) is stated as follows:

$$\begin{aligned} & \text{minimize} && \sum_{i \in \mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell|k}) && (16a) \\ & \text{subject to} && \mathbf{F}_i^{\text{r}} \mathbf{u}_{i,\ell|k} \leq \mathbf{f}_{i,\ell}^{\text{r}}, \quad \forall i \in \mathcal{N}, && (16b) \end{aligned}$$

$$\mathbf{u}_{i,\ell|k}^{\text{c}} + \sum_{j \in \mathcal{N}_i} \mathbf{G}_{ij} \mathbf{u}_{j,\ell|k}^{\text{c}} = \mathbf{0}, \quad \forall i \in \mathcal{N}, \quad (16c)$$

for all $\ell \in \{k, \dots, k + h_p - 1\}$, where (16b) with the appropriate \mathbf{F}_i^{r} and $\mathbf{f}_{i,\ell}^{\text{r}}$ is defined according to (2), (4), (7)-(9), and (13)-(15).

Proposition 1: Suppose that Assumption 1 holds. Problem (16) has feasible solutions if and only if

$$w_{i,k}^{\text{max}} \leq \min \left(\frac{1}{2} (p_i^{\text{ch}} + p_i^{\text{dh}}), -\frac{1}{2b_i} (x_i^{\text{max}} - x_i^{\text{min}}) \right). \quad (17)$$

Furthermore, suppose that both Assumption 2 and (17) hold. Then, any feasible solution of Problem (16) does not violate operational constraints (2)-(9) even though an attack, which is defined in Definition 2, occurs. \square

Proof: The difference between Problems (11) and (16) is the fact that the tightened constraints (14) and (15) are

considered in Problem (16). Thus, a feasible region exists if and only if $x_i^{\min} - b_i w_{i,k}^{\max} \leq x_i^{\max} + b_i w_{i,k}^{\max}$ and $-p_i^{\text{ch}} + w_{i,k}^{\max} \leq p_i^{\text{dh}} - w_{i,k}^{\max}$. The necessary and sufficient condition (17) is obtained from these two inequalities. Provided that a feasible solution of Problem (16) exists, the second claim follows from the formulation of Problem (16). ■

If the condition of $w_{i,k}^{\max}$ stated in Proposition 1 is not satisfied, then $p_{i,k}^{\text{G}}$ and/or $p_{i,k}^{\text{im}}$ must also be involved in compensating $w_{i,k}$. In this regard, the constraints related to $p_{i,k}^{\text{G}}$ and $p_{i,k}^{\text{im}}$ must be tightened with similar procedure as that previously explained. For the remaining of the paper, suppose that the next assumption holds.

Assumption 4: Condition (17) holds true, implying the existence of feasible solutions of Problem (16). □

Therefore, the DMPC method presented in Algorithm 1 can be then applied to solve Problem (16) by simply substituting (11b) with (16b) in the local optimization problem, i.e., step 5.

Remark 4: Problem (16) can also be expressed as a min-max problem [16]. However, in this robust reformulation (16), the computational complexity is lower than that in the min-max counterpart. □

B. Attack Identification and Mitigation

In this section, the methodology to identify the adversarial agents in the system and, at the same time, to block the attacks is presented. It is an active detection strategy, where regular agents test their hypothesis to find their adversarial neighbors by deciding to open/close their connections with their neighbors. The methodology involves applying Bayesian inference for hypothesis testing (e.g., [13]) and solving mixed-integer optimization problems. Note that in the control literature, Bayesian inference has also been applied to system identification [17] and fault detection [18], while hypothesis testing has been used within the framework of fault diagnosis and robust control [19].

Firstly, a regular agent, $i \in \mathcal{R}$, detects an attack performed by one of its neighbors by evaluating its own SoC at the current time instant as follows:

$$\Delta_{i,k} = |x_{i,k} - (x_{i,k-1} + \mathbf{b}_i^\top \mathbf{u}_{i,k-1}^* + b_i \hat{p}_{i,k-1}^{\text{d}})|, \quad (18)$$

where $\mathbf{b}_i = b_i [0 \quad -\mathbf{1}_{2+|\mathcal{N}_i|}^\top]^\top$. If $\Delta_{i,k} > b_i d_i^{\max}$, then at k , agent i is considered to be attacked, otherwise agent i is not attacked.

Remark 5: An attack $w_{i,k}^{\text{a}}$ such that $|w_{i,k}^{\text{a}} + w_{i,k}^{\text{d}}| \leq d_i^{\max}$ is undetectable since the regular agents cannot distinguish it from the load disturbance. However, such an attack is tolerable since the agents consider the bound of load disturbance as d_i^{\max} in the first place. □

Although an attack can be detected, for $|\mathcal{N}_i| > 1$, it is not possible to determine which neighbor is the adversarial one by only evaluating (18). Therefore, in order to identify the adversarial neighbors, we apply a hypothesis testing method that is based on Bayesian inference [13].

Each agent, $i \in \mathcal{R}$, considers the following set of hypotheses, $\mathcal{H}_i = \{\mathbf{H}_i^0, \mathbf{H}_i^j : j \in \mathcal{N}_i\}$, where the hypotheses are defined as follows:

- \mathbf{H}_i^0 : There is no attack,
- \mathbf{H}_i^j : Neighbor j is an adversarial agent,

for all $j \in \mathcal{N}_i$. The Bayesian inference is used as the model to update the probability of the hypotheses as follows:

$$\mathbb{P}_{k+1}(\mathbf{H}_i^j) = \frac{\mathbb{P}_k(\mathbf{H}_i^j) \mathbb{P}_k(\Delta_{i,k} | \mathbf{H}_i^j)}{\mathbb{P}_k(\Delta_{i,k})}, \quad (19)$$

for all $\mathbf{H}_i^j \in \mathcal{H}_i$, where $\mathbb{P}_k(\mathbf{H}_i^j)$ denotes the probability of hypothesis \mathbf{H}_i^j at time instant k , $\mathbb{P}_k(\Delta_{i,k})$ denotes the marginal likelihood of $\Delta_{i,k}$, and $\mathbb{P}_k(\Delta_{i,k} | \mathbf{H}_i^j)$ denotes the probability of observing $\Delta_{i,k}$ given hypothesis \mathbf{H}_i^j and is formulated as follows:

$$\mathbb{P}_k(\Delta_{i,k} \leq b_i d_i^{\max} | \mathbf{H}_i^j) = \begin{cases} 1, & \text{for } j = 0, \\ 1 - v_{i,k}^j P_{\text{at}}, & \text{for all } j \in \mathcal{N}_i, \end{cases}$$

$$\mathbb{P}_k(\Delta_{i,k} > b_i d_i^{\max} | \mathbf{H}_i^j) = \begin{cases} 0, & \text{for } j = 0, \\ v_{i,k}^j P_{\text{at}}, & \text{for all } j \in \mathcal{N}_i, \end{cases}$$

where $v_{i,k}^j \in \{0, 1\}$, for all $j \in \mathcal{N}_i$, denote the decision whether agent i connects to and negotiates with neighbor j , i.e., $v_{i,k}^j = 1$ implies agent i connects to neighbor j , whereas $v_{i,k}^j = 0$ implies agent i does not connect to neighbor j . Note that $\mathbb{P}_{k+1}(\mathbf{H}_i^j)$ is the a posteriori probability of \mathbf{H}_i^j given the event $\Delta_{i,k}$, i.e., $\mathbb{P}_{k+1}(\mathbf{H}_i^j) = \mathbb{P}(\mathbf{H}_i^j | \Delta_{i,k})$. The initial probabilities of all hypotheses are defined as

$$\mathbb{P}_0(\mathbf{H}_i^j) = \begin{cases} 1 - P_{\text{at}}, & \text{for } j = 0, \\ P_{\text{at}}/|\mathcal{N}_i| & \text{for all } j \in \mathcal{N}_i, \end{cases} \quad (20)$$

implying that it is initially considered that each neighbor is equally likely to be adversarial.

In order to decide the connection that a regular agent $i \in \mathcal{R}$ will have with its neighbors at each time instant, each agent $i \in \mathcal{R}$ solves a local mixed-integer optimization problem of the form:

$$\text{minimize}_{\mathbf{v}_{i,k}, \{\mathbf{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell|k}) + J_i^{\text{Y}}(\mathbf{v}_{i,k}) \quad (21\text{a})$$

$$\text{subject to } \mathbf{F}_{i,k}^{\text{lc}} \mathbf{u}_{i,\ell|k} + \mathbf{F}_{\text{v},i}^{\text{lc}} \mathbf{v}_{i,k} \leq \mathbf{f}_{i,\ell}^{\text{lc}}, \quad (21\text{b})$$

$$\mathbf{v}_{i,k} \in \mathcal{C}_i \cup \{\mathbf{1}_{|\mathcal{N}_i|}\}, \quad (21\text{c})$$

where $\mathbf{v}_{i,k} = [v_{i,k}^j]_{j \in \mathcal{N}_i}^\top$. Here, the cost function $J_i^{\text{Y}}(\mathbf{v}_{i,k}) : \mathbb{R}^{|\mathcal{N}_i|} \rightarrow \mathbb{R}$ penalizes the decision of having a connection with the neighbors. It is expressed as follows:

$$J_i^{\text{Y}}(\mathbf{v}_{i,k}) = \gamma n_{\text{at}} \sum_{j \in \mathcal{N}_i} \mathbb{P}_k(\mathbf{H}_i^j) (v_{i,k}^j)^2,$$

where $\gamma \in \mathbb{R}_{>0}$ denotes a weight that can be tuned and n_{at} denotes the number of attacks that agent i has received, i.e., the number of time instants at which $\Delta_{i,k} > b_i d_i^{\max}$. By having n_{at} as a weight, establishing a connection with a neighbor is penalized more if the number of received attacks increases. Moreover, (21b) is obtained from (2), (4), (7), (8), (14), and (15) as well as from the following expressions:

$$w_{i,k}^{\max} = \max_{j \in \mathcal{N}_i} \left(2p_{ji}^{\text{t,max}} v_{i,k}^j \right) + d_i^{\max}, \quad (22)$$

$$-p_{ji}^{\text{t,max}} v_{i,k}^j \leq p_{ji}^{\text{t}} \leq p_{ji}^{\text{t,max}} v_{i,k}^j, \quad \forall j \in \mathcal{N}_i, \quad (23)$$

for all $\ell \in \{k, \dots, k + h_p - 1\}$, whereas, in the constraint (21c), $\mathcal{C}_i = \{\mathbf{z}_j = \mathbb{1}_{|\mathcal{N}_i|} - \mathbf{e}_j, j = 1, 2, \dots, |\mathcal{N}_i|\}$, where \mathbf{e}_j , for all $j = 1, 2, \dots, |\mathcal{N}_i|$, are the standard basis vectors of $|\mathcal{N}_i|$ -dimensional Euclidean space.

Problem (21) is a mixed-integer quadratic program (MIQP) due to the existence of $\mathbf{v}_{i,k}$. Notice that we penalize $v_{i,k}^j$, for each $j \in \mathcal{N}_i$, proportionally to the probability value of the hypothesis associated to neighbor j , $\mathbb{P}_k(\mathbf{H}_i^j)$. Furthermore, (21c) implies that agent i only allows that it is disconnected from at most one neighbor. This means that there are only $|\mathcal{N}_i| + 1$ possible solutions of $\mathbf{v}_{i,k}$. In addition, this constraint is added based on Assumption 2.

Proposition 2: Suppose that Assumptions 1 and 4 hold. Then, Problem (21) has feasible solutions. \square

Proof: Any solution of $\mathbf{v}_{i,k} \in \mathcal{C}_i \cup \{\mathbb{1}_{|\mathcal{N}_i|}\}$ implies the satisfaction of (17) since Assumption 4 holds and yields a feasible solution of $\{\mathbf{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}$ by choosing $p_{j,i,\ell}^t = 0$, for all $j \in \mathcal{N}_i$ and $\ell \in \{k, \dots, k + h_p - 1\}$ since this solution satisfies (23) and, according to Assumption 1, also satisfies (2),(4)-(8). \blacksquare

Finally, suppose that the decision $\mathbf{v}_{i,k}^* = [v_{i,k}^{j*}]_{j \in \mathcal{N}_i}^\top$ is the solution obtained from solving Problem (21). Now, instead of using (13), each agent $i \in \mathcal{R}$ computes the worst case of the disturbance by plugging $\mathbf{v}_{i,k}^*$ into (22). Thus, in the robust problem (16), the local constraints (16b) are switched by (21b) with $\mathbf{v}_{i,k} = \mathbf{v}_{i,k}^*$, for all $i \in \mathcal{N}$.

C. Overall Scheme and Sub-optimality Bound

The overall scheme of the proposed method is given in Algorithm 2.

Algorithm 2 Resilient distributed algorithm, for $i \in \mathcal{R}$

- 1: Initialize the hypothesis probabilities according to (20)
 - 2: **for** $k = 1, 2, \dots$ **do**
 - 3: Evaluate (18) to detect an attack
 - 4: Update the probability value of the hypotheses according to (19)
 - 5: **if** $\mathbb{P}_k(\mathbf{H}_i^j) = 1, j \in \mathcal{N}_i$, **then**
 - 6: $v_{i,k}^{j*} = \begin{cases} 0, & \text{for } \mathbb{P}_k(\mathbf{H}_i^j) = 1, \\ 1, & \text{for } \mathbb{P}_k(\mathbf{H}_i^j) = 0 \end{cases}$
 - 7: Compute $\mathbf{u}_{i,k|k}^*$ by solving (16), considering (16b) is formed by (2), (4), (7), (8), (14), (15), (23) with $\mathbf{v}_{i,k} = \mathbf{v}_{i,k}^*$, and $w_{i,k}^{\max} = d_i^{\max}$, using Algorithm 1
 - 8: **else**
 - 9: Compute $v_{i,k}^{j*}$, for all $j \in \mathcal{N}_i$, by solving (21)
 - 10: Compute $\mathbf{u}_{i,k|k}^*$ by solving (16), considering (16b) is formed by (2), (4), (7), (8), (14), (15), (22) and (23), with $\mathbf{v}_{i,k} = \mathbf{v}_{i,k}^*$, using Algorithm 1
 - 11: **end if**
 - 12: Apply $\mathbf{u}_{i,k|k}^*$ and $\mathbf{v}_{i,k}^*$
 - 13: **end for**
-

Assumption 5: Any agent can temporarily disconnect the physical link between itself and its neighbors, respecting the decision of $\mathbf{v}_{i,k}^*$. Two agents, i and j , where $(i, j) \in \mathcal{E}$, can only exchange energy if and only if $v_{i,k}^{j*} = v_{j,k}^{i*} = 1$. \square

Assumption 5 implies that, although there exists a connection between agents i and j , either of them can block the influence by closing the connection. The decisions obtained by performing Algorithm 2 are characterized by the following Proposition 3.

Proposition 3: Suppose that Assumptions 1-5 hold. If the regular agents, i.e. all $i \in \mathcal{R}$, apply Algorithm 2, then the obtained decision $\mathbf{u}_{i,k}^*$, for all $i \in \mathcal{R}$, do not violate the operational constraints (2)-(9) under an attack that is defined by Definition 2, for all $k \in \mathbb{Z}_{\geq 0}$. \square

Proof: A regular agent $i \in \mathcal{R}$ obtains its control inputs $\mathbf{u}_{i,k|k}^*$ in either step 7 or 10, based on whether the adversarial neighbor has been identified or not. The difference between steps 7 and 10 is the definition of $w_{i,k}^{\max}$, and it is seen that d_i^{\max} is smaller than or equal to $w_{i,k}^{\max}$ that is expressed in (22). By Assumption 4, $w_{i,k}^{\max}$, expressed in (22) or in step 7, satisfy (17). In the case that $\mathbf{v}_{i,k}^* = \mathbb{1}_{|\mathcal{N}_i|}$, we obtain the original robustified problem (16) and the claim follows immediately from Proposition 1. Now, we consider the case that one of the neighbor is blocked. Suppose that agent $j \in \mathcal{N}_i$ is blocked, i.e., $v_{i,k}^{j*} = 0$. The constraint (23) yields the following equality constraint: $p_{j,i,\ell}^t = 0$, for all $\ell \in \{k, \dots, k + h_p - 1\}$. Assumptions 1 and 4 result in a feasible solution $\mathbf{u}_{i,k}^*$, where $p_{j,i,k}^{t*} = 0$. Thus, the claim follows from Proposition 1. Furthermore, by Assumption 5, agent i is physically disconnected from agent j . Therefore, if agent j is adversarial, then it cannot attack agent i . \blacksquare

Remark 6: The proposed attack identification and mitigation methods can be implemented along with any distributed optimization algorithm that is able to solve Problems (11) and (16). \square

We also provide a sub-optimality certificate of the control inputs obtained by performing Algorithm 2, which is stated in Proposition 4.

Proposition 4: Suppose that $\{\mathbf{u}_{i,\ell}^o\}_{\ell=k}^{k+h_p-1}$, for all $i \in \mathcal{N}$, are the minimizers of the following problem:

$$\text{minimize} \quad \sum_{i \in \mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell|k}) \quad (24a)$$

$$\text{subject to} \quad \mathbf{F}_i \mathbf{u}_{i,\ell|k} \leq \mathbf{f}_{i,\ell}, \quad \forall i \in \mathcal{N}, \quad (24b)$$

for all $\ell \in \{k, \dots, k + h_p - 1\}$, $\{\mathbf{u}_{i,\ell}^*\}_{\ell=k}^{k+h_p-1}$ denotes the solution obtained from Algorithm 2 in step 7 or 10, and $\{\tilde{\mathbf{u}}_{i,\ell}^*\}_{\ell=k}^{k+h_p-1}$ denotes the solution obtained from solving Problem (11). Then, the sub-optimality of the solution, i.e. $\Delta J_{i,k} = \sum_{\ell=k}^{k+h_p-1} (J_{i,\ell}(\mathbf{u}_{i,\ell}^*) - J_{i,\ell}(\tilde{\mathbf{u}}_{i,\ell}^*))$, is bounded as follows:

$$\Delta J_{i,k} \leq \sum_{\ell=k}^{k+h_p-1} (J_{i,\ell}(\mathbf{u}_{i,\ell}^*) - J_{i,\ell}(\mathbf{u}_{i,\ell}^o)).$$

\square

Proof: The system achieves global optimal performance if all agents $i \in \mathcal{N}$ apply the solution obtained from solving (11), implying the adversarial agents do not attack, and the forecast loads are equal to the actual ones. We prove the

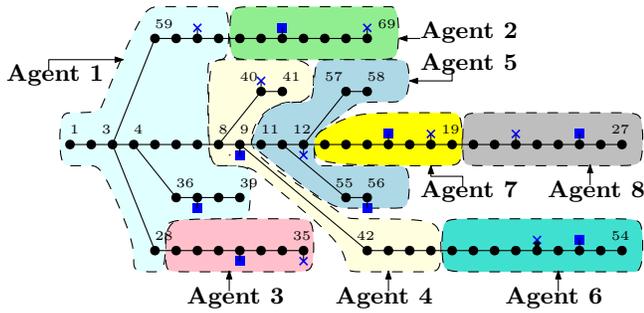


Fig. 1. The topology of the PG&E 69-bus distribution system and its 8-agent resulting partition. Blue crosses and squares indicate the distributed generators and storages, respectively.

proposition by showing that the following inequalities hold:

$$\sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell}^*) \geq \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\tilde{\mathbf{u}}_{i,\ell}^*) \geq \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell}^o).$$

Notice that Problem (24) is actually a relaxed formulation of Problem (11), i.e., Problem (11) without constraint (11c). Therefore, any feasible solution of Problem (11) is also a feasible solution of Problem (24), but not necessarily vice versa. Furthermore, the constraints imposed in the problem that is solved either in steps 7 or 10 of Algorithm 2 are tighter than those in Problem (11), implying any feasible solution obtained from applying Algorithm 2 is also feasible for Problem (11), but not necessarily vice versa. ■

Remark 7: Problem (24) is trivially separable since there is no coupling constraint. Therefore, each agent $i \in \mathcal{N}$ can compute $\{\mathbf{u}_{i,k}^o\}_{\ell=k}^{k+h_p-1}$ independently as follows:

$$\begin{aligned} \{\mathbf{u}_{i,k}^o\}_{\ell=k}^{k+h_p-1} &= \arg \min_{\{\mathbf{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\mathbf{u}_{i,\ell|k}) \\ &\text{subject to } \mathbf{F}_i \mathbf{u}_{i,\ell|k} \leq \mathbf{f}_{i,\ell}, \end{aligned}$$

for all $\ell \in \{k, \dots, k+h_p-1\}$. □

IV. CASE STUDY

As a case study, we use the PG&E 69-bus distribution network, which has been modified by adding distributed generators and energy storages [5], as depicted in Fig. 1. We follow the partition given by [5] to divide the network into eight interconnected microgrids (agents). The operational parameters of each microgrid are given in Table I. Furthermore, we consider two types of load profiles, which are industrial and residential, and assign each microgrid to one of the profiles randomly. Moreover, we generate the load profile and load forecast of each microgrid by considering the available load data as the maximum loads. In this case study, microgrids 2, 6, and 7 are chosen to be adversarial and the probability of attacks is set to be 0.3, which is known by the regular agents. Furthermore, the prediction horizon of each agent is $h_p = 4$ steps and we consider one-day simulation with sampling time of 15 minutes.

TABLE I
PARAMETERS OF THE MICROGRIDS

Parameters	Value	Unit	Agent (i)
$x_i^{\min}, x_i^{\max}, x_{i,0}$	40, 70, 55	%	all
$p_i^{\text{ch}}, p_i^{\text{dh}}$	300, 300	kW	all
$p_i^{\text{G},\min}, p_i^{\text{G},\max}$	0, 1500	kW	all
$p_i^{\text{t},\max}, p_i^{\text{im},\max}$	100, 2000	kW	all
$e_{\text{cap},i}$	1000	kWh	all
a_i	1.0	-	all
$c_i^{\text{st}}, c_i^{\text{im}}, c_i^{\text{t}}$	1, 250, 0.1	-	all
c_i^{g}	5	-	2, 3, 6, 7
c_i^{g}	10	-	1, 4, 5, 8

TABLE II
TOTAL COST OF THE SYSTEM

Scenario	Dist. Strategy	Attack/Load Disturbance	Cost (Proportional)	Constraint Satisfaction
1	Nominal	No	1.00	Yes
2	Nominal	Yes	1.06	No
3	Alg. 3	Yes	1.91	Yes
4	Alg. 2	Yes	1.18	Yes

Algorithm 3 Distributed robust algorithm, for $i \in \mathcal{R}$

- 1: **for** $k = 1, 2, \dots$ **do**
- 2: Compute $\mathbf{u}_{i,k}$ by solving Problem (16), considering (16b) is formed by (2), (4), (7)-(9), and (13)-(15), with Algorithm 1
- 3: Apply $\mathbf{u}_{i,k}$
- 4: **end for**

We consider four simulation scenarios, in each of which a different distributed strategy is applied (see Table II). As the baseline performance, in Scenario 1, the nominal approach, i.e., applying Algorithm 1 to solve Problem (11), is implemented for the case in which the adversarial agents do not attack and there is no load disturbance, whereas, in Scenario 2, the nominal approach is applied to the case with attacks and load disturbance. In Scenario 3, we apply the robustified approach without attack identification and mitigation as shown in Algorithm 3, while in Scenario 4, we apply the proposed approach. Table II shows the overall performance of the network over the whole simulation time. The proposed approach achieves a better performance than the robustified approach while ensuring the satisfaction of the constraints. As shown in Fig. 2, in Scenario 2, the minimum limit of the SoC is violated. However, this violation does not occur in Scenarios 3 and 4. Moreover, Fig. 3 shows how agent 1 detects agent 2 as the adversarial neighbor in Scenario 4. Once detected, i.e., at $k = 8$, agent 1 disconnects from agent 2. Additionally, the average sub-optimality bound of the proposed approach is 49% of the nominal performance (Scenario 1), whereas the measured sub-optimality is 18%.

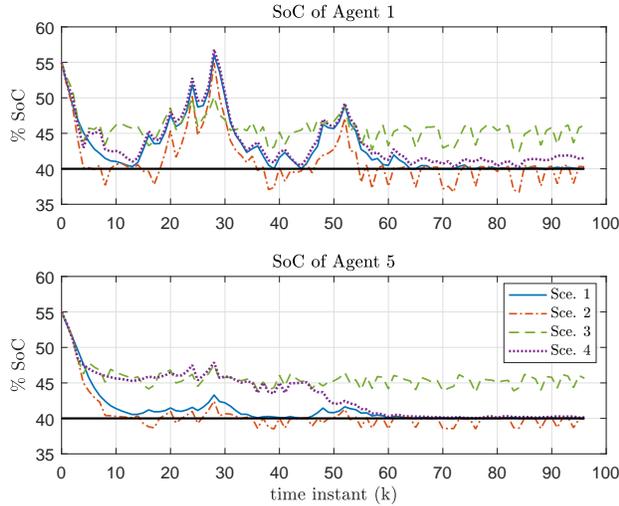


Fig. 2. The evolution of the SoC of agents 1 (top) and 5 (bottom). The black horizontal line indicates the minimum limit of SoC, x_i^{\min} .

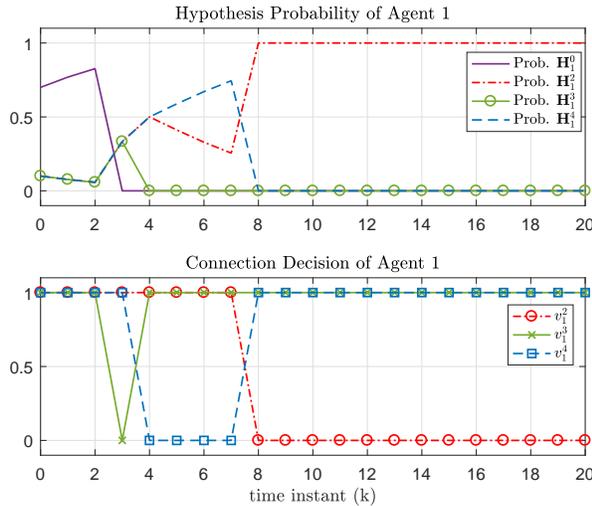


Fig. 3. The evolution of the hypothesis probability (top) and the connection decision (bottom) of agent 1. Note that the decision $v_{1,k}^*$ are the same for $k = 8, 9, \dots, 96$, since the adversarial neighbor is detected at $k = 8$.

V. CONCLUSION AND FUTURE WORK

A distributed energy management for interconnected microgrid systems that is based on dynamic economic dispatch problem is investigated. We analyze the case of having microgrids that perform an adversarial behavior, i.e., some microgrids do not comply with the decisions obtained from the distributed strategy. Furthermore, we propose a robustified formulation and an attack identification and mitigation method such that the distributed strategy can deal with such adversaries. Additionally, we also provide a sub-optimality certificate of the proposed approach.

Future work includes extending the proposed approach such that the stochasticity of the loads is taken into account explicitly in order to improve the performance and assumptions on the number of adversarial neighbors are

relaxed. Furthermore, we will also explore the possibility to improve the detection strategy as well as the attack mitigation method, e.g., by considering that the agents might exchange their hypothesis probability and by considering $v_{i,k}$, for all $i \in \mathcal{N}$, as continuous variables that determine the limit of the connections among agents.

REFERENCES

- [1] A. Pantoja and N. Quijano, "A population dynamics approach for the dispatch of distributed generators," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4559–4567, 2011.
- [2] C. A. Hans, P. Braun, J. Raisch, L. Grune, and C. Reincke-Collon, "Hierarchical distributed model predictive control of interconnected microgrids," *IEEE Trans. Sustain. Energy*, 2018, (in press, DOI: 10.1109/TSTE.2018.2802922).
- [3] K. Baker, J. Guo, G. Hug, and X. Li, "Distributed MPC for efficient coordination of storage and renewable energy sources across control areas," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 992–1001, 2016.
- [4] G. K. H. Larsen, N. D. van Foreest, and J. M. A. Scherpen, "Distributed MPC applied to a network of households with micro-CHP and heat storage," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 2106–2114, 2014.
- [5] S. A. Arefifar, Y. A. R. I. Mohamed, and T. H. M. El-Fouly, "Supply-adequacy-based optimal construction of microgrids in smart distribution systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1491–1502, 2012.
- [6] N. Quijano, C. Ocampo-Martinez, J. Barreiro-Gomez, G. Obando, A. Pantoja, and E. Mojica-Nava, "The role of population games and evolutionary dynamics in distributed control systems: The advantages of evolutionary game theory," *IEEE Control Syst.*, vol. 37, no. 1, pp. 70–97, 2017.
- [7] P. Velarde, J. M. Maestre, H. Ishii, and R. R. Negenborn, "Vulnerabilities in Lagrange-based distributed model predictive control," *Optimal Control Appl. and Methods*, 2017, in press. [Online]. Available: <http://dx.doi.org/10.1002/oca.2368>
- [8] D. Sharma, S. N. Singh, J. Lin, and E. Foruzan, "Agent-based distributed control schemes for distributed energy storage systems under cyber attacks," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 307–318, 2017.
- [9] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
- [10] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, 2013.
- [11] S. M. Dibaji and H. Ishii, "Resilient consensus of second-order agent networks: Asynchronous update rules with delays," *Automatica*, vol. 81, pp. 123–132, 2017.
- [12] Z. Feng, G. Wen, and G. Hu, "Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Trans. Cybern.*, vol. 47, no. 5, pp. 1273–1284, 2017.
- [13] P. D. Hoff, *A First Course in Bayesian Statistical Methods*. Springer Science & Business Media, 2009.
- [14] I. Necoara and J. A. K. Suykens, "Application of a smoothing technique to decomposition in convex optimization," *IEEE Trans. Autom. Control*, vol. 53, no. 11, pp. 2674–2679, 2008.
- [15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge university press, 2010, vol. 25, no. 3.
- [16] A. Bemporad and M. Morari, "Robust model predictive control: A survey," in *Robustness in Identification and Control*, A. Garulli and A. Tesi, Eds. Springer-Verlag, 1999, vol. 245, Lecture Notes in Control and Information Sciences.
- [17] B. Ninness and S. Henriksen, "Bayesian system identification via Markov chain Monte Carlo techniques," *Automatica*, vol. 46, no. 1, pp. 40–51, 2010.
- [18] R. M. Fernández-Cantí, J. Blesa, V. Puig, and S. Tornil-Sin, "Set-membership identification and fault detection using a Bayesian framework," *Int. J. Syst. Sci.*, vol. 47, no. 7, pp. 1710–1724, 2016.
- [19] C. Ocampo-Martinez, R. Sánchez-Peña, F. Bianchi, and A. Ingimundarson, "Data-driven fault diagnosis and robust control: Application to PEM fuel cell systems," *Int. J. Robust and Nonlinear Control*, 2018, (in press, DOI: 10.1002/rnc.3820).