Received <day> <Month>, <year>; | Revised <day> <Month>, <year>; | Accepted <day> <Month>, <year>

DOI: xxx/xxxx

RESEARCH ARTICLE

Resilient Distributed Model Predictive Control for Energy Management of Interconnected Microgrids[†]

Wicak Ananduta*[1] | José María Maestre[2] | Carlos Ocampo-Martinez[1] | Hideaki Ishii[3]

[1] Institut de Ròbotica i Informàtica Industrial, CSIC-UPC, Carrer Llorens i Artigas 4-6, 08028 Barcelona, Spain
[2] Department of System and Automation Engineering, University of Seville, Seville, Spain
[3] Department of Computer Science, Tokyo Institute of Technology, Yokohama, Japan

Correspondence
*Wicak Ananduta, Institut de Ròbotica i Informàtica Industrial, CSIC-UPC, Carrer Llorens i Artigas 4-6, 08028 Barcelona, Spain. Email: wananduta@iri.upc.edu

Summary

Distributed energy management of interconnected microgrids that is based on Model Predictive Control (MPC) relies on the cooperation of all agents (microgrids). This paper discusses the case in which some of the agents might perform one type of adversarial actions (attacks) and they do not comply with the decisions computed by performing a distributed MPC algorithm. In this regard, these agents could obtain a better performance at the cost of degrading the performance of the network as a whole. A resilient distributed method that can deal with such issues is proposed in this paper. The method consists of two parts. The first part is to ensure that the decisions obtained from the algorithm are robustly feasible against most of the attacks with high confidence. In this part, we formulate the economic dispatch problem, taking into account the attacks as a chance-constrained problem and employ a two-step randomization-based approach to obtain a feasible solution with a predefined level of confidence. The second part consists in the identification and mitigation of the adversarial agents, which utilizes hypothesis testing with Bayesian inference and requires each agent to solve a mixed-integer problem to decide the connections with its neighbors. In addition, an analysis of the decisions computed using the stochastic approach and the outcome of the identification and mitigation method is provided. The performance of the proposed approach is also shown through numerical simulations.

KEYWORDS:
Distributed MPC, economic dispatch, distributed optimization, resilient algorithm, microgrids

1 | INTRODUCTION

Recently, distributed approaches for energy management and control of electrical power systems, including economic dispatch, have drawn a lot of attention[1,2]. On one hand, the technological shifting of power generation towards distributed production, particularly power generation that is based on renewable sources, requires a different control approach than the conventional centralized one and results in the development of distributed approaches. For example, in order to deal with the intermittency issue of renewable energy production, storage units might be utilized[2]. In addition to dispatchable distributed generation units,

[†] 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) and has been also supported by the Spanish State Research Agency through the María de Maeztu Seal of Excellence to IRI (MDM-2016-0656). 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. The authors also acknowledge JST CREST Grants No. JPMJCR15K3 and JPMJCR15K5.

these storage devices must also be controlled. Therefore, the dimension of control inputs/decisions might become very large and a centralized control scheme might not be able to handle the computational loads. On the other hand, the advancement of supporting technologies, such as information and communication infrastructures, helps to improve the feasibility of distributed approaches for real and practical applications.

A distribution network that consists of a number of distributed generation units as well as storages may be perceived as a system of interconnected microgrids[2,3]. A microgrid is regarded as an entity that is capable of managing and operating itself[2,4]. When a distributed approach is applied to an economic dispatch problem for such a system, the microgrids in the system cooperatively optimize a global economic objective, by interacting among each other through a communication network. A distributed optimization approach requires the agents in the system, which are microgrids, to exchange certain information. The main advantages of such approaches include the optimality/suboptimality of the solutions, the distribution of computational burden, the plug-and-play ability, the improvement of the privacy and cybersecurity, and the reliability against failures[1].

Model predictive control (MPC) has also been proposed as a suitable solution for the economic dispatch problem of the present electrical networks, particularly, due to the high uncertainty of power generation from renewable generation units and the utilization of storage units, which have slow dynamics that must be taken into account. Different from the conventional economic dispatch that computes a power production plan, which typically consists of hourly decisions spanned over one day, MPC-based economic dispatch keeps optimizing the decision of several time steps ahead based on the measurement at each time instant. In this regard, different distributed MPC (DMPC) approaches, such as dual decomposition[5], alternating direction method of multipliers (ADMM)[6,7], optimality condition decomposition (OCD)[4,8] and population dynamics[9], have been proposed to solve economic dispatch problems. These distributed optimization approaches are suitable since they are able to obtain an optimal solution given that the related optimization problem is convex, with some mild assumptions.

As previously mentioned, one of the main requirements for implementing a distributed approach is the cooperation among all agents, which must operate in compliance with the algorithm. However, it might happen that some agents in the network do not cooperate because they selfishly want to have a better performance or suffer from failures. This paper discusses the case in which there are agents that might perform a certain adversarial behavior. In particular, we consider that the adversarial agents do not comply with the decisions that are obtained from the distributed algorithm implemented in the network. In other words, the adversarial agents might implement a different decision/control input than the one that has been computed by using the distributed algorithm.

Non-compliance of some agents in a network that applies a distributed approach has been discussed in some papers[10,11]. For instance, a secure dual-decomposition-based DMPC, in which each agent should monitor two neighbors that provide extreme control input values and disregard these extreme values, has been proposed[10]. Furthermore, a cyber-attack problem of a consensus-based distributed control scheme for distributed energy storage systems has also been addressed[11], where the approach involves a fuzzy-logic-based detection and a consensus-based leader-follower distributed control scheme. Related to the cyber-security issue of cyber-physical systems, the work of Pasqualetti et al.[12] provides a mathematical framework for attack detection and monitoring, particularly for deterministic systems. Moreover, consensus problems in which some of the agents perform an adversarial behavior to prevent convergence have also been investigated[13,14,15]. In the DMPC framework, the issue that some agents might provide false information, which is a different type of adversarial behaviors, has also been discussed[16,17]. A scenario-based defense mechanism[16] and a compensation scheme to incentivize truth telling among agents[17] have been proposed to deal with false information problems.

The main contribution of this paper is the distributed energy management algorithm for interconnected microgrids that is resilient with respect to the non-compliance of some microgrids. The proposed approach combines both passive and active mechanisms to deal with the issue of unexpected disturbances. On the one hand, we robustify the controllers via constraints with a stochastic method and on the other hand we use an active mechanism to disconnect some agents. Specifically, we formulate the economic dispatch problem, which takes into account the adversarial behavior, as a chance-constrained problem in which attacks, loads, and renewable power generation are regarded as uncertain disturbances. In order to solve the problem, we apply a stochastic two-step approach. The first step of the approach is to compute probabilistic bounds using a randomization-based program while the second step is to solve a robust program that takes into account the probabilistic bounds. As a result, we can guarantee that the obtained solution is also a feasible solution of the chance-constrained problem. Furthermore, we also propose an active methodology based on hypothesis testing using Bayesian inference to identify and disconnect from the agents that perform adversarial actions. In order to decide the connection with the neighbors, each agent must solve a local mixed-integer problem. Note that the probabilistic bounds computed in the passive mechanism are necessary ingredients for the identification scheme. Additionally, we present the robustness characteristics of the solutions and show how the attack identification and mitigation method works analytically and by means of simulation.

This paper is developed based on reported preliminary results[18,19], in which we limit the adversaries by only assuming there is only at most one adversarial neighbor per agent. Initially, we propose to solve a robust program to deal with the attacks[18]. However, here we consider a stochastic approach[19] to deal with the attacks and other uncertainties. In this regard, we do not assume the knowledge of the bounds of attacks or uncertain loads and power generation. Furthermore, we could also then obtain a less conservative solution than the robust program proposed in the preliminary paper[18] at the cost of allowing constraint violation with small probability. Moreover, in this paper, we also provide a convergence analysis of the attack identification and mitigation method. Since the control approach considered in this paper is based on MPC, it is more related to the work of Velarde et al.[10], than that of Sharma et al.[11] However, different from the method proposed by Velarde et al.[10], our methodology deals with the attacks by computing control inputs that are robust with respect to such attacks. Furthermore, our approach is also able to identify the adversarial agents in certain cases and can also deal with more general systems in which there are more than one adversarial agent in the network.

The remaining of the paper is structured as follows. Section 2 introduces the economic dispatch problem and the distributed scheme considered in this paper, and presents the adversary model. Afterward, the stochastic approach is proposed in Section 3 whereas the methodology to identify the adversarial agents is presented in Section 4. Furthermore, Section 5 provides the analysis of the overall control algorithm, which includes the characterization of the decisions computed by the algorithm and the outcome of the attack identification method. Numerical simulations that show the effectiveness in the performance of the proposed method are discussed in Section 6. Finally, Section 7 provides some concluding remarks and discussion of future work.

Notations

The sets of real numbers and integers are denoted by $\mathbb{R}$ and $\mathbb{Z}$, respectively. Moreover, for any $a \in \mathbb{R}$, $\mathbb{R}_{\geq a}$ denotes the subset of $\mathbb{R}$ that is defined by $\{b : b \geq a,\ b \in \mathbb{R}\}$ and, for any $a \in \mathbb{Z}$, $\mathbb{Z}_{\geq a}$ denotes the subset of $\mathbb{Z}$ that is defined by $\{b : b \geq a,\ b \in \mathbb{Z}\}$. A similar definition is used for the strict inequality cases. For column vectors v_i with $i \in \mathcal{L} = \{l_1, \dots, l_m\}$, the operator $[v_i^\top]_{i\in\mathcal{L}}^\top$ denotes the column-wise concatenation, i.e., $[v_i^\top]_{i\in\mathcal{L}}^\top = [v_{l_1}^\top \ \cdots \ v_{l_m}^\top]^\top$. The vector $\mathbb{1}_n$ denotes $[1\ 1\ \cdots\ 1]^\top \in \mathbb{R}^n$. The set cardinality and Euclidean norm are denoted by $|\cdot|$ and $\|\cdot\|_2$, respectively. Supposing that Ω_i, for $i = 1, 2, \dots, n$, is a subset of $\mathbb{R}^{n_i}$, then the Cartesian product over the sets Ω_i is defined by $\prod_{i=1}^n \Omega_i = \Omega_1 \times \cdots \times \Omega_n$. Furthermore, $\mathbb{P}(\cdot)$ denotes the probability measure, and $\mathbb{P}(\cdot|\cdot)$ denotes the conditional probability measure. Finally, discrete-time instants are denoted by the subscript k and the list of symbols is given in Appendix A.

2 | DISTRIBUTED ECONOMIC DISPATCH AND ADVERSARY MODEL

Firstly, the economic dispatch problem of interconnected microgrids is formulated in Section 2.1. Secondly, the distributed approach based on dual decomposition is presented in Section 2.2. Finally, Section 2.3 describes the adversary model that may be present in the system.

2.1 | Dynamic Economic Dispatch Problem

Consider the undirected graph $\mathcal{S} = (\mathcal{N}, \mathcal{E})$, where $\mathcal{N} = \{1, 2, \dots, n\}$ is the set of nodes and $\mathcal{E} \subseteq \mathcal{N} \times \mathcal{N}$ is the set of edges. It represents a system of n interconnected microgrids. Each node, $i \in \mathcal{N}$, represents a microgrid and an edge, $(i, j) \in \mathcal{E}$, describes that microgrids i and j are physically connected. Moreover, denote the set of neighbors of microgrid i by $\mathcal{N}_i$, i.e., $\mathcal{N}_i = \{j : (i, j) \in \mathcal{E}\}$.

Here, each microgrid, $i \in \mathcal{N}$, consists of a set of dispatchable distributed generation (DG) units, a set of generation units based on renewable energy sources (RES) that are non-dispatchable, a storage unit, and an aggregated load. Furthermore, consider that each microgrid is also able to import power from the main grid if it is connected to it, while two microgrids that are connected can exchange power with each other. In addition, we also consider that each microgrid has the capability to be in the island mode, i.e., it is able to meet the local loads independently using its own generators though this may be costly. A simple example of the system is shown in Figure 1 .

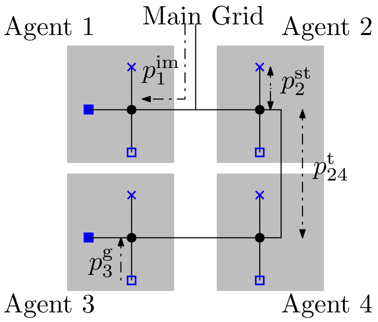

FIGURE 1 A 4-microgrid system as an example. Squares indicate the distributed generation units, i.e., filled squares, ■, and empty squares, □, represent renewable generation units and dispatchable generators, respectively, whereas crosses, ×, indicate the storage units.

In the economic dispatch problem of interconnected microgrids, economically optimal operating points of dispatchable generation and storage units are computed so that the power injected to a microgrid is equal to its load, while satisfying the operational constraints of the system. The economic dispatch problem can be described as a constrained optimization problem, where an economical cost function is considered and the constraints come from the power balance equations, the dynamics of the storage units, and the operational limits of the system components. Note that we assume that the storage and dispatchable generation units have low-level controllers[20] that control the units such that the computed operating points are met.

The power balance equations of each microgrid, $i \in \mathcal{N}$, are written as follows:

$$\rho_{i,k}^{\mathrm{d}} - \rho_{i,k}^{\mathrm{st}} - \rho_{i,k}^{\mathrm{g}} - \rho_{i,k}^{\mathrm{im}} - \sum_{j \in \mathcal{N}_i} \rho_{ji,k}^{\mathrm{t}} = 0, \tag{1}$$

$$\rho_{ij,k}^{\mathrm{t}} + \rho_{ji,k}^{\mathrm{t}} = 0, \quad \forall j \in \mathcal{N}_i, \tag{2}$$

where $\rho_{i,k}^{\mathrm{d}} \in \mathbb{R}$ denotes the power disturbance, which is an uncertain variable that represents the difference between the uncertain load and uncertain power generation from non-dispatchable generation units, such as wind- or solar- powered units. Moreover, $\rho_{i,k}^{\mathrm{g}} \in \mathbb{R}_{\geq 0}$ denotes the total power generated by the dispatchable DG units; $\rho_{i,k}^{\mathrm{st}} \in \mathbb{R}$ denotes the power delivered by or to the storage; $\rho_{i,k}^{\mathrm{im}} \in \mathbb{R}_{\geq 0}$ denotes the imported power from the main grid; and $\rho_{ji,k}^{\mathrm{t}} \in \mathbb{R}$, for all $j \in \mathcal{N}_i$, denote the power transferred between microgrids i and j. Equation (1) describes the local power balance of microgrid i whereas (2) describes the power balance between microgrid i and its neighbors.

The dynamics of the storage unit in microgrid i are described as the discrete-time state-space model as follows:

$$x_{i,k+1} = a_i x_{i,k} + b_i \rho_{i,k}^{\mathrm{st}}, \tag{3}$$

where $x_{i,k}$ denotes the state of charge (SoC) of the storage unit, $a_i \in (0, 1]$ denotes its efficiency and $b_i = -\frac{T_{\mathrm{s}}}{e_{\mathrm{cap},i}}$, where T_{s} and $e_{\mathrm{cap},i}$ denote the sampling period and the maximum capacity of the storage unit, respectively. Note that the input is normalized by $e_{\mathrm{cap},i}$ since we consider the SoC level as a percentage of the maximum capacity.

Furthermore, the operational limits of the components of microgrid i are described as follows:

$$x_i^{\min} \leq x_{i,k} \leq x_i^{\max}, \tag{4}$$

$$-\rho_i^{\mathrm{ch}} \leq \rho_{i,k}^{\mathrm{st}} \leq \rho_i^{\mathrm{dh}}, \tag{5}$$

$$\rho_i^{\mathrm{g,min}} \leq \rho_{i,k}^{\mathrm{g}} \leq \rho_i^{\mathrm{g,max}}, \tag{6}$$

$$\rho_{i,k}^{\mathrm{im}} \leq \rho_i^{\mathrm{im,max}}, \tag{7}$$

$$-\rho_i^{\mathrm{t,max}} \leq \rho_{ji,k}^{\mathrm{t}} \leq \rho_i^{\mathrm{t,max}}, \quad \forall j \in \mathcal{N}_i, \tag{8}$$

where $x_i^{\min}, x_i^{\max} \in [0, 1]$, denote the minimum and the maximum SoC of the storage unit, respectively; $\rho_i^{\mathrm{ch}} \in \mathbb{R}_{\geq 0}$ and $\rho_i^{\mathrm{dh}} \in \mathbb{R}_{\geq 0}$ denote the maximum charging and discharging power of the storage; $\rho_i^{\mathrm{g,min}}$, $\rho_i^{\mathrm{g,max}} \in \mathbb{R}_{\geq 0}$ denote the minimum and the maximum of the total power generated by the DG units of microgrid i, respectively; $\rho_i^{\mathrm{im,max}} \in \mathbb{R}_{\geq 0}$ denotes the maximum imported power from the main grid, which is 0 if microgrid i is not connected to the main grid; and $\rho_i^{\mathrm{t,max}} \in \mathbb{R}_{>0}$ denotes the maximum energy that can be transferred between microgrid i and j. Notice that $\rho_i^{\mathrm{t,max}}$ is a local bound and it can be different from one microgrid to another.

Remark 1. When two neighboring agents i and j have different maximum limits of the allowable transferred power, i.e., $\rho_i^{\mathrm{t,max}} \neq \rho_j^{\mathrm{t,max}}$, then the more restrictive constraint is naturally imposed. In order to clarify further, consider that agent i and j are neighboring agents. Thus, we have the following bounds on $\rho_{ji,k}^{t}$ and $\rho_{ij,k}^{t}$:

$$-\rho_i^{t,\max} \leq \rho_{ji,k}^{t} \leq \rho_i^{t,\max}, \; -\rho_j^{t,\max} \leq \rho_{ij,k}^{t} \leq \rho_j^{t,\max}.$$

Furthermore, since we also have the power balance equation among neighboring microgrids (2) the variables $\rho_{ji,k}^{t}$ and $\rho_{ij,k}^{t}$ in the centralized problem are then bounded as follows:

$$\begin{aligned} -\min\left(\rho_i^{t,\max}, \rho_j^{t,\max}\right) &\leq \rho_{ji,k}^{t} \leq \min\left(\rho_i^{t,\max}, \rho_j^{t,\max}\right), \\ -\min\left(\rho_i^{t,\max}, \rho_j^{t,\max}\right) &\leq \rho_{ij,k}^{t} \leq \min\left(\rho_i^{t,\max}, \rho_j^{t,\max}\right). \end{aligned}$$

The above equations show that the bounds of the power transferred between two neighboring agents depend on both agents. □

By defining the control input of microgrid i as $\boldsymbol{u}_{i,k} = [\rho_{i,k}^{\mathrm{st}} \; \rho_{i,k}^{\mathrm{g}} \; \rho_{i,k}^{\mathrm{im}} \; \boldsymbol{u}_{i,k}^{\mathrm{c}\top}]^\top \in \mathbb{R}^{3+|\mathcal{N}_i|}$, where $\boldsymbol{u}_{i,k}^{\mathrm{c}} = [\rho_{ji,k}^{\mathrm{t}}]_{j\in\mathcal{N}_i}^\top$ is the vector of coupled control input variables, we consider the quadratic stage cost function of each microgrid as follows:

$$J_{i,k} = \boldsymbol{u}_{i,k}^\top \boldsymbol{R}_i \boldsymbol{u}_{i,k}, \tag{9}$$

where $\boldsymbol{R}_i = \mathrm{diag}([c_i^{\mathrm{st}} \; c_i^{\mathrm{g}} \; c_i^{\mathrm{im}} \; c_i^{\mathrm{t}}\mathbb{1}_{|\mathcal{N}_i|}^\top]) > 0$, in which c_i^{st}, c_i^{g}, $c_i^{\mathrm{im}}, c_i^{\mathrm{t}} \in \mathbb{R}_{>0}$ denote the per-unit cost of storage operation, the per-unit cost of producing energy, the per-unit cost of buying energy from the main grid, and the per-unit cost of transferring energy to/from the neighbor due to losses, respectively[7].

Remark 2. The per-unit cost of transferring energy is considered to be equal for all neighbors, i.e., with a common c_i^{t}, for simplicity of the exposition in the proposed attack identification and mitigation approach. However, in general, this cost can be different from one neighbor to another. □

Based on the preceding description of the system and the stage cost defined in (9), the finite-time open-loop optimization problem that underlies an MPC strategy for the dynamic economic dispatch of this system is stated as follows:

$$\underset{\{\{\boldsymbol{u}_{i,\ell|k}\}_{i\in\mathcal{N}}\}_{\ell=k}^{k+h_p-1}}{\mathrm{minimize}} \sum_{i\in\mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) \tag{10a}$$

$$\text{subject to} \quad \boldsymbol{F}_i \boldsymbol{u}_{i,\ell|k} \leq \boldsymbol{f}_{i,\ell}, \; \forall i \in \mathcal{N}, \tag{10b}$$

$$\boldsymbol{u}_{i,\ell|k}^{\mathrm{c}} + \sum_{j\in\mathcal{N}_i} \boldsymbol{G}_{ij} \boldsymbol{u}_{j,\ell|k}^{\mathrm{c}} = \boldsymbol{0}, \; \forall i \in \mathcal{N}, \tag{10c}$$

for all $\ell \in \{k, \dots, k+h_p-1\}$, where $h_p \in \mathbb{Z}_{\geq 1}$ denotes the prediction horizon, the local constraints (10b) that only include local control inputs are constructed from (1), (3)-(8), whereas the coupled constraints (10c) are constructed from (2). Since $\boldsymbol{R}_i$, for all $i \in \mathcal{N}$, are positive definite, the cost function (10a) is strictly convex. Furthermore, the constraints (10b)–(10c) form a compact polyhedral set. Hence, Problem (10) is convex.

Remark 3. We consider that the power injected to the storage and the power extracted from the storage units as a single decision variable, i.e., $\rho_{i,k}^{\mathrm{st}}$, in order to obtain a convex optimization problem. When charging and discharging efficiencies are taken into account and the injected and drawn power are distinguished, the dynamics become hybrid and the economic dispatch problem (10) becomes non-convex. In this case, there is no guarantee that distributed methods considered in this paper can provide a solution that converges to the optimal one. Nevertheless, the resilient methods that we propose in this paper can also be extended to this case.

2.2 | Distributed Optimization Method

Distributed optimization methods have been considered as suitable approaches to solve large-scale economic dispatch problems[5,6,7,8]. One of the main reasons is the fact that the solution obtained by applying a distributed optimization algorithm approximates the optimal solution obtained from the centralized approach. The main challenge when one wants to solve an economic dispatch problem, such as Problem (10), in a distributed manner is that the problem is not trivially separable. In Problem (10), the equality constraints (10c) couple neighboring microgrids. One of the methods to deal with the couplings is by considering its dual problem, which is decomposable[21]. This approach is called the *dual decomposition method* and an iterative distributed algorithm such as the dual-ascent algorithm[21] or the accelerated gradient algorithm[22] can be applied to solve the dual problem.

We apply the dual decomposition approach and the dual-ascent algorithm to compute the control inputs. In this regard, Lemma 1 states the result of the dual-ascent algorithm based on the duality theory of convex optimization[21, §5.2.3].

Lemma 1. Let $\mathcal{U} \subset \mathbb{R}^n$ be a compact polyhedral set, $f : \mathbb{R}^n \to \mathbb{R}$ be a strictly convex quadratic function, and $A \in \mathbb{R}^{m \times n}$ be any matrix. Consider the optimization problem defined as follows:

$$\min_{\boldsymbol{u} \in \mathcal{U}} \ f(\boldsymbol{u}), \ \text{subject to} \ \ A\boldsymbol{u} = 0, \tag{11}$$

whose feasible set is nonempty, and the dual ascent algorithm that has the following iteration rules:

1. $\boldsymbol{u}^{(r+1)} = \arg\min_{\boldsymbol{u} \in \mathcal{U}} \quad f(\boldsymbol{u}) + \lambda^{(r)\top} A\boldsymbol{u}$,
2. $\lambda^{(r+1)} = \lambda^{(r)} + \gamma A\boldsymbol{u}^{(r+1)}$,

where $\lambda \in \mathbb{R}^m$ is the Lagrange multiplier vector associated to the equality constraint $A\boldsymbol{u} = 0$, $\gamma \in (0, 1)$ is the step size, and the superscript (r) indicates the iteration step. Then, $\boldsymbol{u}^{(r)}$ converges to the optimal solution of (11) with the dual-ascent algorithm. □

The dual problem of (10) is derived by introducing the Lagrange multipliers associated to (10c) and denoted by $\lambda_{i,\ell} \in \mathbb{R}^{|\mathcal{N}_i|}$, for all $\ell \in \{k, \dots, k + h_p - 1\}$ and $i \in \mathcal{N}$. Note that the dimension of $\lambda_{i,\ell}$ is the same as the dimension of the coupled decision variable $\boldsymbol{u}^{\mathrm{c}}_{i,k}$, due to the association with (10c). As a result, the distributed dual-ascent algorithm that solves Problem (10) is presented in Algorithm 1, where $\mathcal{U}_{i,\ell} \in \mathbb{R}^{3+|\mathcal{N}_i|}$ in step 4 is the local polyhedral set defined from the local constraint (10b) and ζ_i is a small positive scalar that determines the stopping criterion of the algorithm. Note that the step of the dual-ascent method for computing the decision variables, is carried out in step 4 and the step of the dual-ascent method for updating the Lagrange multipliers, is carried out in step 6. Based on Lemma 1, since (10b) forms a compact polyhedral set, and (10a) is strictly convex, the solutions coming from Algorithm 1, which are denoted by $\boldsymbol{u}^{\star}_{i,\ell|k}$, for all $i \in \mathcal{N}$ and $\ell \in \{k, \dots, k + h_p - 1\}$, converge to the optimal solution of Problem (10). Note that in order to implement the algorithm (performing steps 3 and 5), it has been assumed that there exists a bidirectional communication between two neighboring agents, i.e., for all i and j, where $(i, j) \in \mathcal{E}$.

Algorithm 1 Distributed dual-ascent algorithm, for each agent $i \in \mathcal{N}$

```
1: Set $r = 1$, $\zeta_i \in \mathbb{R}_{>0}$, and initialize $\lambda^{(r)}_{i,\ell}$.
2: do
3:     Receive $\lambda^{(r)}_{j,\ell}$ for all $\ell \in \{k, \dots, k + h_p - 1\}$ from all neighbors $j \in \mathcal{N}_i$, and send $\lambda^{(r)}_{i,\ell}$ for all $\ell \in \{k, \dots, k + h_p - 1\}$ to the neighbors.
4:     Solve the local optimization problem
       $$\begin{aligned} \underset{\{\boldsymbol{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \ & \sum_{\ell=k}^{k+h_p-1} \left( \boldsymbol{J}_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) + \left( \boldsymbol{\lambda}^{(r)\top}_{i,\ell} + \sum_{j \in \mathcal{N}_i} \boldsymbol{\lambda}^{(r)\top}_{j,\ell} \boldsymbol{G}_{ji} \right) \boldsymbol{u}^{c}_{i,\ell|k} \right) \\ \text{subject to} \quad & \boldsymbol{u}_{i,\ell|k} \in \mathcal{U}_{i,\ell}, \quad \forall \ell \in \{k, \dots, k + h_p - 1\}. \end{aligned}$$
5:     Receive the decision $\boldsymbol{u}^{\mathrm{c}}_{j,\ell|k}$ for all $\ell \in \{k, \dots, k + h_p - 1\}$ from all neighbors $j \in \mathcal{N}_i$, and send $\boldsymbol{u}^{\mathrm{c}}_{i,\ell|k}$ for all $\ell \in \{k, \cdots, k + h_p - 1\}$ to the neighbors.
6:     Update $\lambda_{i,\ell}$ for all $\ell \in \{k, \dots, k + h_p - 1\}$ as
       $$\lambda^{(r+1)}_{i,\ell} = \lambda^{(r)}_{i,\ell} + \alpha_i \boldsymbol{\psi}_{i,\ell},$$
       where $\boldsymbol{\psi}_{i,\ell} = \boldsymbol{u}^{\mathrm{c}}_{i,\ell|k} + \sum_{j \in \mathcal{N}_i} \boldsymbol{G}_{ij} \boldsymbol{u}^{\mathrm{c}}_{j,\ell|k}$ and $0 < \alpha_i < 1$.
7:     $r \leftarrow r + 1$
8: while $\left\| \begin{bmatrix} \boldsymbol{\psi}^{\top}_{i,k} & \cdots & \boldsymbol{\psi}^{\top}_{i,k+h_p-1} \end{bmatrix} \right\|_2 > \zeta_i$
```

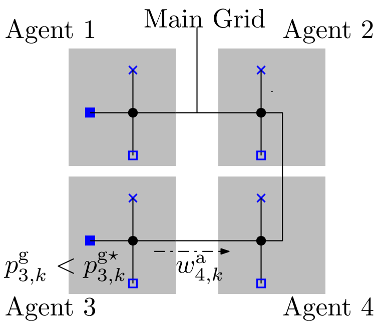

FIGURE 2 An attack received by Agent 4 from Agent 3, which is adversarial.

R2-2

2.3 | Adversary Model

It is considered that some of the agents (microgrids) might perform adversarial actions. Definition 1 classifies the regular and the adversarial agents in the network.

Definition 1. An agent i is regular if it always implements its control input $\boldsymbol{u}_{i,k}$ according to the decision obtained from the DMPC strategy, i.e., $\boldsymbol{u}_{i,k} = \boldsymbol{u}^{\star}_{i,k|k}$, for all $k \geq 0$. Otherwise, agent i is adversarial. □

Furthermore, denote the set of regular agents by $\mathcal{R}$ and the set of adversarial agents by $\mathcal{A}$. We consider the f-local model of adversaries that is stated in Definition 2 [13].

Definition 2. Given $f \in \mathbb{Z}_{\geq 1}$, the set of adversarial agents is f-local if $|\mathcal{A} \cap \mathcal{N}_i| \leq f$, for all $i \in \mathcal{N}$. □

Based on Definition 1, an attack is defined as follows.

Definition 3. An attack is an event at which an adversarial agent $i \in \mathcal{A}$ implements a control input that is different than the decision obtained from the distributed strategy, i.e., $\boldsymbol{u}_{i,k} \neq \boldsymbol{u}^{\star}_{i,k|k}$ for some k. □

We assume that the attacks occur in a probabilistic manner at each time k and thus consider the following assumption.

Assumption 1. The probability of an attack to occur at each time step k, for each $i \in \mathcal{A}$, can be time-varying with a uniform lower bound, denoted by $p^{\mathrm{a}}_i > 0$. □

By performing an attack defined in Definition 3, an adversarial agent might gain benefit from its neighbors. For instance, an adversarial agent may produce an energy quantity smaller than the amount that has been decided from the distributed algorithm. It then asks its neighbor to compensate the deficiency of power. This attack is possible since these agents are connected and the power balance equations must be met. In this circumstance, the economic cost of the adversarial agent might be less than what it was supposed to be, but its neighbors must pay an extra cost to produce and deliver the energy compensation. An illustration of an attack in the 4-microgrid system is given in Figure 2 . We assume that if an adversarial agent attacks, it attacks all of its neighbors equally at the same time. Clearly, different distribution schemes can also be considered, but the study of how each adversarial agent attacks is out of the scope of this paper and is left for future work. The proposed methods presented in Sections 3 and 4 can deal with this issue and for this reason we choose this simple assumption without loss of generality. In the next sections, we propose a distributed strategy to deal with such attacks.

3 | TWO-STEP STOCHASTIC APPROACH

The optimization problem (10) considers the power balance constraint (1) over the prediction horizon h_p. However, the power disturbances of each microgrid, $\rho^{\mathrm{d}}_{i,\ell}$, for all $\ell \in \{k, \dots, k+h_p-1\}$, cannot be known in advance. Therefore, we can only consider the forecast of $\rho^{\mathrm{d}}_{i,\ell}$, for all $\ell \in \{k, \dots, k+h_p-1\}$, and assume the difference between the forecast and the actual value as an uncertain variable. In this regard, denote the forecast of the power disturbance of microgrid i at time k by $\hat{\rho}^{\mathrm{d}}_{i,k}$ and let the uncertain variable $w^{\mathrm{d}}_{i,k} \in \mathbb{R}$ be defined as

$$w^{\mathrm{d}}_{i,k} = \rho^{\mathrm{d}}_{i,k} - \hat{\rho}^{\mathrm{d}}_{i,k}. \tag{12}$$

Furthermore, we denote the amount of attack that agent i receives by $w^{\mathrm{a}}_{i,k} \in \mathbb{R}$ and consider it as another source of uncertainty. Hence, the uncertainties of microgrid i can be denoted by $\boldsymbol{w}_{i,k} = [w^{\mathrm{d}}_{i,k}\ w^{\mathrm{a}}_{i,k}]^{\top}$ and we introduce Assumption 2 on the uncertain vector $\boldsymbol{w}_{i,k}$. Assumption 2 is necessary for a randomization-based method and commonly considered[23,24]. Note that we do not need any assumption on the distribution function of $\boldsymbol{w}_{i,k}$, although any type of distribution could be considered as well.

Assumption 2. Let $\Omega_i \subseteq \mathbb{R}^2$, for each $i \in \mathcal{N}$, be an uncertain set that is endowed with a Borel σ-algebra. For each microgrid $i \in \mathcal{N}$ and for any $k \in \mathbb{Z}_{\geq 0}$, $\boldsymbol{w}_{i,k} \in \Omega_i$ is a random process that is independent and identically distributed (i.i.d.). □

The energy storage units can help not only to deal with the intermittency issue of renewable energy sources but also to deal with the uncertain disturbance, which is due to the forecast mismatch or an attack from adversarial agents, by providing power reserves[25]. In other words, if there is unforeseen extra load, i.e., the disturbance is positive, it is met by the power taken from the storage units or if there is unforeseen extra power generated, i.e., the disturbance is negative, it is stored to the storage units. In this regard, we assume that each storage unit has a low-level control, which acts similarly as an automatic generation control[20,24], to balance the mismatches. We consider this strategy in order to have less reliance on the main grid. In order to take into account this strategy, as well as the disturbance, the formulation of the dynamic economic dispatch problem in Section 2.1 is adjusted as follows. Let $\hat{\rho}^{\mathrm{st}}_{i,k}$ denote the nominal power delivered to/from the storage unit and consider that

$$\rho^{\mathrm{st}}_{i,k} = \hat{\rho}^{\mathrm{st}}_{i,k} + \mathbb{1}^{\top}\boldsymbol{w}_{i,k}, \quad \forall i \in \mathcal{N}. \tag{13}$$

By introducing $w^{\mathrm{a}}_{i,k}$ in (1) and from (12) and (13), we obtain the local power balance equation as follows:

$$\hat{\rho}^{\mathrm{d}}_{i,k} - \hat{\rho}^{\mathrm{st}}_{i,k} - \rho^{\mathrm{g}}_{i,k} - \rho^{\mathrm{im}}_{i,k} - \sum_{j \in \mathcal{N}_i} \rho^{\mathrm{t}}_{ji,k} = 0. \tag{14}$$

By considering (13) as additional constraints, as well as (14) instead of (1), we specify how the disturbance affects the system. In particular, it can be seen that the satisfaction of constraints (4)-(5) depends on the disturbance.

Hence, in order to take into account the disturbance, we reformulate Problem (10) as a chance-constrained problem as follows:

$$\underset{\{\{\boldsymbol{u}_{i,\ell|k}\}_{i\in\mathcal{N}}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \sum_{i\in\mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) \tag{15a}$$

subject to

$$\mathbb{P}(\boldsymbol{F}_i \boldsymbol{u}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{w},i}\boldsymbol{w}_{i,\ell} \leq \boldsymbol{f}_{i,\ell} | \boldsymbol{w}_{i,\ell} \in \Omega_i,\ \forall \ell \in \{k, \dots, k+h_p-1\}) \geq 1 - \varepsilon_i,\ \forall i \in \mathcal{N}, \tag{15b}$$

$$\boldsymbol{u}^{\mathrm{c}}_{i,\ell|k} + \sum_{j\in\mathcal{N}_i} \boldsymbol{G}_{ij}\boldsymbol{u}^{\mathrm{c}}_{j,\ell|k} = \boldsymbol{0},\ \forall \ell \in \{k, \dots, k+h_p-1\},\ \forall i \in \mathcal{N}, \tag{15c}$$

where $\boldsymbol{u}_i = [\hat{\rho}^{\mathrm{st}}_{i,k}\ \rho^{\mathrm{g}}_{i,k}\ \rho^{\mathrm{im}}_{i,k}\ \boldsymbol{u}^{\mathrm{c}\top}_{i,k}]^{\top} \in \mathbb{R}^{3+|\mathcal{N}_i|}$; the inequality $\boldsymbol{F}_i\boldsymbol{u}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{w},i}\boldsymbol{w}_{i,\ell} \leq \boldsymbol{f}_{i,\ell}$ is a compact form of the local constraints (3)-(8), (13), and (14), with appropriate $\boldsymbol{F}_i$ and $\boldsymbol{F}_{\mathrm{w},i}$ matrices and $\boldsymbol{f}_{i,\ell}$ vector; (15b) are the chance constraints where $\varepsilon_i \in (0,1)$ is the maximum level of violation; and (15c) is the coupled constraints as in (10c). By having a chance-constrained problem, we allow small probability of violation of the local constraints $\boldsymbol{F}_i\boldsymbol{u}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{w},i}\boldsymbol{w}_{i,\ell} \leq \boldsymbol{f}_{i,\ell}$. Violation, with small probability, in this control level is tolerable since it will only imply suboptimality of the performance. Any solution of Problem (15) is referred to as an ε-level feasible solution, where $\varepsilon = \sum \varepsilon_i$.

To solve Problem (15), we follow a two-step stochastic approach[26]. The methodology consists of two steps: first, we compute a probabilistic bound of the disturbance and then, we solve a robust programming problem that takes into account the bound that we compute in the first step. The solutions obtained using this approach are feasible solutions of the corresponding chance-constrained problem with certain confidence[26]. One of the advantages of applying this approach, compared to the standard scenario approach[27], is that since the dimension of the uncertain vector $\boldsymbol{w}_{i,k}$ is smaller than the dimension of the decision vector $\boldsymbol{u}_{i,k}$, the number of scenarios that must be generated is smaller when applying this approach than when directly applying the scenario approach to Problem (15)[26]. Furthermore, since the local constraints are convex, the second step of this approach is tractable. The steps of this approach are explained in Sections 3.1 and 3.2.

3.1 | Computing Probabilistic Bounds

In this step, we solve a randomized program in which a number of scenarios of the disturbance is generated and considered in the constraints of the problem, to compute a set that probabilistically bounds the uncertainty of the chance-constrained problem. Since in Problem (15), each microgrid has a sequence of uncertain variables, i.e., $\boldsymbol{w}_{i,\ell}$, for all $\ell \in \{k,\dots,k+h_p-1\}$, let the set that bounds a portion of the probability mass of $[\boldsymbol{w}_{i,k}^\top \cdots \boldsymbol{w}_{i,k+h_p-1}^\top]^\top$ be denoted by $\mathcal{B}_{i,k}^\star$. We define $\mathcal{B}_{i,k}^\star$ to be a polyhedral set, i.e., $\mathcal{B}_{i,k}^\star = \prod_{\ell=k}^{k+h_p-1}\{\boldsymbol{\tau}\in\mathbb{R}^2 : \underline{\boldsymbol{\tau}}_{i,\ell|k}^\star \leq \boldsymbol{\tau} \leq \overline{\boldsymbol{\tau}}_{i,\ell|k}^\star\}$, where the inequality relations are component-wise, and $\underline{\boldsymbol{\tau}}_{i,\ell|k}^\star, \overline{\boldsymbol{\tau}}_{i,\ell|k}^\star \in \mathbb{R}^2$ denote the lower and upper bounds of $\boldsymbol{w}_{i,\ell}$, respectively, and consist of two components since there are two sources of uncertainty, i.e., the system disturbance, $w_{i,k}^{\mathrm{d}}$, and the attack, $w_{i,k}^{\mathrm{a}}$.

In order to compute $\mathcal{B}_{i,k}^\star$, we pose a chance-constrained problem for each microgrid, $i\in\mathcal{N}$, as follows:

$$\begin{aligned} &\underset{\{\underline{\boldsymbol{\tau}}_{i,\ell|k},\overline{\boldsymbol{\tau}}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \sum_{\ell=k}^{k+h_p-1} \mathbb{1}^\top \left(\overline{\boldsymbol{\tau}}_{i,\ell|k} - \underline{\boldsymbol{\tau}}_{i,\ell|k}\right)\\ &\text{subject to}\\ &\mathbb{P}\left(\boldsymbol{w}_{i,\ell} \in [\underline{\boldsymbol{\tau}}_{i,\ell|k},\overline{\boldsymbol{\tau}}_{i,\ell|k}] | \boldsymbol{w}_{i,\ell}\in\Omega_i,\ \forall \ell \in\{k,\dots,k+h_p-1\}\right) \geq 1-\varepsilon_i. \end{aligned} \tag{16}$$

Now, we are in a position to solve (16) with the scenario approach, which can be stated as follows:

$$\begin{aligned} &\underset{\{\underline{\boldsymbol{\tau}}_{i,\ell|k},\overline{\boldsymbol{\tau}}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \sum_{\ell=k}^{k+h_p-1} \mathbb{1}^\top \left(\overline{\boldsymbol{\tau}}_{i,\ell|k} - \underline{\boldsymbol{\tau}}_{i,\ell|k}\right)\\ &\text{subject to}\\ &\boldsymbol{w}_{i,\ell}^{(s)} \in [\underline{\boldsymbol{\tau}}_{i,\ell|k},\overline{\boldsymbol{\tau}}_{i,\ell|k}], \quad s=1,\dots,n_{s,i},\ \forall \ell \in\{k,\dots,k+h_p-1\}, \end{aligned} \tag{17}$$

where $\boldsymbol{w}_{i,\ell}^{(s)}$ denote a scenario of $\boldsymbol{w}_{i,\ell}$, generated according to the probability measure for $\boldsymbol{w}_{i,\ell}$ in an i.i.d. manner, and $n_{s,i}$ is the number of scenarios, which satisfies[26]

$$n_{s,i} \geq \frac{e}{\varepsilon_i(e-1)}\left(4h_p - 1 + \ln\frac{1}{\beta_i}\right), \tag{18}$$

where $\beta_i \in (0,1)$ indicates the desired level of confidence and e is the Euler constant. With some abuse of notation, let the set $\mathcal{B}_{i,k}^\star$ be constructed from the solution of Problem (17). This set is a feasible solution of (16) with probability at least $1-\beta_i$.

Remark 4. The level of violation (ε_i) and the level of confidence (β_i) are predefined variables that determine the number of scenarios needed to be generated. □

3.2 | Robust Reformulation

Upon obtaining the bounds $\mathcal{B}_{i,k}^\star$, for all $i\in\mathcal{N}$, we can derive a robust counterpart of Problem (15). Since the local constraints are convex, we can apply the vertex enumeration method, i.e., substituting the uncertain variable $\boldsymbol{w}_{i,\ell}$ with the vertices of $\mathcal{B}_{i,k}^\star$ [26]. The robust formulation associated to Problem (15) is stated as follows:

$$\underset{\{\{\boldsymbol{u}_{i,\ell|k}\}_{i\in\mathcal{N}}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \sum_{i\in\mathcal{N}}\sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) \tag{19a}$$

subject to

$$\boldsymbol{F}_i\boldsymbol{u}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{w},i}\boldsymbol{w}_{i,\ell|k} \leq \boldsymbol{f}_{i,\ell}, \tag{19b}$$

$$\boldsymbol{w}_{i,\ell|k} \in \mathcal{V}(\mathcal{B}_{i,k}^\star,\ell), \tag{19c}$$

$$\boldsymbol{u}_{i,\ell|k}^{\mathrm{c}} + \sum_{j\in\mathcal{N}_i}\boldsymbol{G}_{ij}\boldsymbol{u}_{j,\ell|k}^{\mathrm{c}} = \boldsymbol{0}, \tag{19d}$$

for all $\ell\in\{k,\dots,k+h_p-1\}$ and $i\in\mathcal{N}$, where $\mathcal{V}(\mathcal{B}_{i,k}^\star,\ell) = \{\underline{\boldsymbol{\tau}}_{i,\ell|k}^\star, \overline{\boldsymbol{\tau}}_{i,\ell|k}^\star\}$ is the vertex set computed in the previous step (Section 3.1). Problem (19) is convex, with a strictly convex cost function and local non-empty compact polyhedral constraint sets. Therefore, based on Lemma 1, we can obtain the optimal solution of Problem (19) using the distributed approach presented in Algorithm 1, where $\mathcal{U}_{i,k}$ is defined by constraints (19b)-(19c).

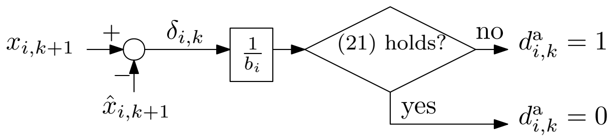

FIGURE 3 The attack detection scheme. The predicted SoC, $\hat{x}_{i,k+1}$, is computed based on (3).

4 | ATTACK IDENTIFICATION AND MITIGATION

Besides employing the stochastic approach outlined in Section 3, we also propose an active methodology to identify the adversarial agents and mitigate the attacks. The identification methodology is a hypothesis testing using Bayesian inference. Furthermore, the identification method requires regular agents to actively disconnect the links with their neighbors. To decide from which neighbors an agent should disconnect, a local mixed-integer optimization problem is solved.

4.1 | Attack Detection

In order to identify the adversarial neighbors, a regular agent (microgrid) must be able to detect an attack in the first place. To this end, a regular agent uses its SoC, which is assumed to be measurable, and compares the measured value with the predicted value using its nominal dynamics to compute the total disturbance, denoted by $\delta_{i,k}$, as follows:

$$\delta_{i,k} = x_{i,k+1} - \left(x_{i,k} + \boldsymbol{b}_i^\top \boldsymbol{u}_{i,k|k}\right), \quad \forall k \in \mathbb{Z}_{\geq 0}, \tag{20}$$

where $\boldsymbol{b}_i = [b_i \; \mathbf{0}^\top_{2+|\mathcal{N}_i|}]^\top$. Note that, by definition, $\delta_{i,k} = b_i \mathbb{1}^\top \boldsymbol{w}_{i,k}$. The probabilistic bound $\mathcal{B}^\star_{i,k}$ can now be used as the threshold to define whether an attack occurs. Recall that $\underline{\boldsymbol{\tau}}^\star_{i,k|k} = [\underline{\tau}^{\mathrm{d}\star}_{i,k|k} \; \underline{\tau}^{\mathrm{a}\star}_{i,k|k}]^\top$, where $\underline{\tau}^{\mathrm{d}\star}_{i,k|k}$ and $\underline{\tau}^{\mathrm{a}\star}_{i,k|k}$ denote the lower bounds of the disturbance associated to the load and to an attack, respectively, and similarly $\overline{\boldsymbol{\tau}}^\star_{i,k|k} = [\overline{\tau}^{\mathrm{d}\star}_{i,k|k} \; \overline{\tau}^{\mathrm{a}\star}_{i,k|k}]^\top$, where $\overline{\tau}^{\mathrm{d}\star}_{i,k|k}$ and $\overline{\tau}^{\mathrm{a}\star}_{i,k|k}$ denote the corresponding upper bounds. Then, the attack detection is defined as follows.

Definition 4. Let $d^{\mathrm{a}}_{i,k} \in \{0, 1\}$, for each regular agent $i \in \mathcal{R}$ and $k \in \mathbb{Z}_{\geq 0}$, be the indicator that detects attacks. If

$$\underline{\tau}^{\mathrm{d}\star}_{i,k|k} \leq \delta_{i,k}/b_i \leq \overline{\tau}^{\mathrm{d}\star}_{i,k|k}, \tag{21}$$

then there is no attack detected and $d^{\mathrm{a}}_{i,k} = 0$. Otherwise, $d^{\mathrm{a}}_{i,k} = 1$, implying an attack is detected. □

The attack detection scheme based on Definition 4 is given in Figure 3 . Based on Definition 4, the following definitions of an undetectable attack and a false attack detection are given. Furthermore, we also consider Assumption 3.

R2-1 **Definition 5.** An attack is detectable if $w^{\mathrm{a}}_{i,k} \neq 0$ such that (21) does not hold. On the other hand, an attack is undetectable if $w^{\mathrm{a}}_{i,k} \neq 0$ such that (21) holds. □

Assumption 3. The probability of the undetectable attacks that are received by agent $i \in \mathcal{R}$, denoted by p^{ua}_i, is less than 1. □

Definition 6. A false attack detection occurs when $w^{\mathrm{a}}_{i,k} = 0$ and $d^{\mathrm{a}}_{i,k} = 1$, i.e., if $w^{\mathrm{d}}_{i,k} < \underline{\tau}^{\mathrm{d}\star}_{i,k|k}$ or $w^{\mathrm{d}}_{i,k} > \overline{\tau}^{\mathrm{d}\star}_{i,k|k}$ when $w^{\mathrm{a}}_{i,k} = 0$. □

When an attack is undetectable, the regular agent i cannot distinguish the attack from the load disturbance. Such an attack is tolerable since the *total* disturbance is within the bounds of the *power* disturbance, $w^{\mathrm{d}}_{i,k}$. For systems without disturbances, undetectable attacks are also defined similarly[12]. Furthermore, Assumption 3 implies that some attacks are detectable by agent i, which is necessary in order to identify the adversarial neighbor. On the other hand, a false detection occurs when the disturbance $w^{\mathrm{d}}_{i,k}$ is outside of the computed bounds. It is worth mentioning that the detection scheme is similar to the passive fault detection method[28].

4.2 | Identification and Mitigation Method

A regular agent that has more than one neighbor is not able to identify which ones are adversarial although it could detect an attack based on Definition 4. Therefore, a hypothesis testing scheme that is based on Bayesian inference is formulated as the method to identify the adversarial neighbors. In this method, we assume that regular agents do not have prior knowledge of the occurrence of the attacks, but each agent $i \in \mathcal{R}$ has an initial expectation on the probability of attacks received, denoted by $\hat{p}_i^{\mathrm{a}}$. The parameter $\hat{p}_i^{\mathrm{a}}$ is a positive constant smaller than one that is used to update the hypothesis probability as shown in (22)-(23) below. It does not need to reflect the actual probability of the received attacks and only affects the convergence of the identification process as we will see in Section 5.

Based on the f-local adversary model, each regular agent, $i \in \mathcal{R}$, where $|\mathcal{N}_i| \geq f$, considers all the sets that are the elements of the power set of $\mathcal{N}_i$ and have the cardinality f. Let these sets be denoted by $\Theta_i^m \subseteq \mathcal{N}_i$, for $m = 1, 2, \dots, n_i^{\mathrm{H}}$, where $n_i^{\mathrm{H}} = \binom{|\mathcal{N}_i|}{f}$. Note that $\Theta_i^{m_1} \neq \Theta_i^{m_2}$ if $m_1 \neq m_2$. Now, consider a set of hypotheses, $\mathcal{H}_i = \{\mathbf{H}_i^m : m = 0, 1, \dots, n_i^{\mathrm{H}}\}$, where the hypotheses are defined as follows:

- $\mathbf{H}_i^0$: There is no adversarial neighbor,
- $\mathbf{H}_i^m$: The set Θ_i^m contains all the adversarial neighbors,

for $m = 1, \dots, n_i^{\mathrm{H}}$. Hence, we associate each set Θ_i^m to one hypothesis. Furthermore, recall the attack indicator variable $d_{i,k}^{\mathrm{a}}$, which is defined in Definition 4. The Bayesian inference is used as the model to update the probability of the hypothesis as follows:

$$\mathbb{P}_{k+1}(\mathbf{H}_i^m) = \frac{\mathbb{P}_k(\mathbf{H}_i^m)\mathbb{P}_k(d_{i,k}^{\mathrm{a}}|\mathbf{H}_i^m)}{\mathbb{P}_k(d_{i,k}^{\mathrm{a}})}, \quad \forall \mathbf{H}_i^m \in \mathcal{H}_i, \tag{22}$$

where $\mathbb{P}_{k+1}(\mathbf{H}_i^m)$ is the a posteriori probability of $\mathbf{H}_i^m$ given the event $d_{i,k}^{\mathrm{a}}$, i.e., $\mathbb{P}_{k+1}(\mathbf{H}_i^m) = \mathbb{P}(\mathbf{H}_i^m|d_{i,k}^{\mathrm{a}})$; $\mathbb{P}_k(\mathbf{H}_i^m)$ denotes the probability of hypothesis $\mathbf{H}_i^m$ at time instant k; $\mathbb{P}_k(d_{i,k}^{\mathrm{a}})$ denotes the marginal likelihood of $d_{i,k}^{\mathrm{a}}$; and $\mathbb{P}_k(d_{i,k}^{\mathrm{a}}|\mathbf{H}_i^m)$ denotes the probability of observing $d_{i,k}^{\mathrm{a}}$ given hypothesis $\mathbf{H}_i^m$. The probability $\mathbb{P}_k(d_{i,k}^{\mathrm{a}}|\mathbf{H}_i^j)$ is formulated as follows:

$$\begin{aligned}
\mathbb{P}_k(d_{i,k}^{\mathrm{a}} = 0|\mathbf{H}_i^m) &= \begin{cases} 1, & \text{for } m = 0, \\ 1 - \left(\max_{j \in \Theta_i^m} v_{i,k}^j\right)\hat{p}_i^{\mathrm{a}}, & \text{for } m = 1, \dots, n_i^{\mathrm{H}}, \end{cases} \\
\mathbb{P}_k(d_{i,k}^{\mathrm{a}} = 1|\mathbf{H}_i^m) &= \begin{cases} 0, & \text{for } m = 0, \\ \left(\max_{j \in \Theta_i^m} v_{i,k}^j\right)\hat{p}_i^{\mathrm{a}}, & \text{for } m = 1, \dots, n_i^{\mathrm{H}}, \end{cases}
\end{aligned} \tag{23}$$

where $v_{i,k}^j \in \{0, 1\}$, for all $j \in \mathcal{N}_i$, denote the decision whether agent i both 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. Additionally, the initial probabilities of all hypotheses are defined as

$$\mathbb{P}_0(\mathbf{H}_i^m) = \begin{cases} 1 - \hat{p}_i^{\mathrm{a}}, & \text{for } m = 0, \\ \hat{p}_i^{\mathrm{a}}/n_i^{\mathrm{H}} & \text{for } m = 1, \dots, n_i^{\mathrm{H}}, \end{cases} \tag{24}$$

implying that agent i initially considers each neighbor has an equal chance of attacking. Note that $\hat{p}_i^{\mathrm{a}}$ does not need to be equal to any p_j^{a}, for $j \in \mathcal{N}_i \cap \mathcal{A}$. In addition, for agent $i \in \mathcal{R}$, where $|\mathcal{N}_i| < f$, two hypotheses are considered, i.e., $\mathbf{H}_i^0$ and $\mathbf{H}_i^1$, where $\Theta_i^1 = \mathcal{N}_i$.

In order to compute $v_{i,k}^j$, for all $j \in \mathcal{N}_i$, i.e., the decision to connect with neighbor j, agent i solves a local mixed-integer optimization problem as follows:

$$\underset{\boldsymbol{v}_{i,k}, \{\boldsymbol{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \quad \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) + J_i^{\mathrm{v}}(\boldsymbol{v}_{i,k}) \tag{25a}$$

subject to

$$\boldsymbol{F}_i \boldsymbol{u}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{w},i}\boldsymbol{w}_{i,\ell|k} + \boldsymbol{F}_{\mathrm{v},i}\boldsymbol{v}_{i,k} \leq \boldsymbol{f}_{i,\ell}^{\mathrm{lc}}, \tag{25b}$$

$$\boldsymbol{w}_{i,\ell|k} \in \mathcal{V}(\mathcal{B}_{i,k}^{\star}, \ell), \tag{25c}$$

$$\boldsymbol{v}_{i,k} \in \{\mathbb{1}_{|\mathcal{N}_i|}\} \cup \{\boldsymbol{v} \in \{0, 1\}^{|\mathcal{N}_i|} : \mathbb{1}^{\top}\boldsymbol{v} = |\mathcal{N}_i| - f\}, \tag{25d}$$

for all $\ell \in \{k, \dots, k + h_p - 1\}$, where $\boldsymbol{v}_{i,k} = [v_{i,k}^j]_{j \in \mathcal{N}_i}^{\top} \in \{0, 1\}^{|\mathcal{N}_i|}$. The cost function $J_i^{\mathrm{v}}(\boldsymbol{v}_{i,k}) : \mathbb{R}^{|\mathcal{N}_i|} \to \mathbb{R}$ penalizes the decision of having a connection with the neighbors, i.e.,

$$J_i^{\mathrm{v}}(\boldsymbol{v}_{i,k}) = \gamma_i n_{i,k}^{\mathrm{a}} \sum_{j \in \mathcal{N}_i} c_{i,k}^j v_{i,k}^j, \tag{26}$$

where $c_{i,k}^j = \sum_{m_j \in \{m : j \in \Theta_i^m\}} \mathbb{P}_k(\mathbf{H}_i^{m_j})$, for each $j \in \mathcal{N}_i$, denotes the individual weight associated to $v_{i,k}^j$, $\gamma_i \in \mathbb{R}_{>0}$ denotes a weight that must be predefined and $n_{i,k}^{\mathrm{a}}$ denotes the number of attacks that agent i has detected, i.e., $n_{i,k}^{\mathrm{a}} = \sum_{\ell=0}^{k} d_{i,\ell}^{\mathrm{a}}$. By having $n_{i,k}^{\mathrm{a}}$

as a weight, establishing a connection with a neighbor is penalized more if the number of attacks detected increases. Moreover, (25b) is obtained from (3)-(7), (13), (14) and from the following expression:

$$-\rho_i^{\mathrm{t,max}} v_{i,k}^j \le \rho_{ji,\ell}^{\mathrm{t}} \le \rho_i^{\mathrm{t,max}} v_{i,k}^j, \quad \forall j \in \mathcal{N}_i, \tag{27}$$

for all $\ell \in \{k, \dots, k+h_p-1\}$, whereas, the constraint (25d) implies that agent i can either connect to all neighbors or disconnect from any f neighbors. It can be seen that Problem (25) considers the same local constraints of Problem (19), except that (8) is replaced by (27), which includes the Boolean variables.

Problem (25) is a mixed-integer quadratic program (MIQP). Notice that we penalize the Boolean variable $v_{i,k}^j$, for each $j \in \mathcal{N}_i$, by adding weight $c_{i,k}^j$, proportionally to the sum of probability measures of the hypotheses associated to neighbor j. Furthermore, having constraint (25d) means that there are only $n_i^{\mathrm{H}} + 1$ possible solutions of $\boldsymbol{v}_{i,k}$. Therefore, if n_i^{H} is relatively small, agent i might solve $n_i^{\mathrm{H}} + 1$ convex problems, i.e., Problem (25) without (25d) and a fixed $\boldsymbol{v}_{i,k}$ that satisfies (25d), and then obtain the minimizers, i.e., all $\boldsymbol{v}_{i,k}$, that provide the minimum cost (25a). Another way to solve Problem (25) is by directly employing a mixed-integer optimization method such as the branch-and-bound algorithm. Finally, let $\mathcal{V}_{i,k}^\star \in \{0,1\}^{|\mathcal{N}_i|}$ be the set of minimizers of Problem (25) and suppose that the decision $\boldsymbol{v}_{i,k}^\star = [v_{i,k}^{j\star}]_{j\in\mathcal{N}_i}^\top$ is chosen from $\mathcal{V}_{i,k}^\star$, i.e., $\boldsymbol{v}_{i,k}^\star \in \mathcal{V}_{i,k}^\star$. Hence, in order to include the connection decision in the robust problem (19), the local constraints (19b) are switched by (25b) with $\boldsymbol{v}_{i,k} = \boldsymbol{v}_{i,k}^\star$, for all $i \in \mathcal{N}$.

Remark 5. One might set γ_i large enough such that $\mathbb{1}_{|\mathcal{N}_i|} \in \mathcal{V}_{i,k}^\star$ only if $n_{i,k}^{\mathrm{a}} = 0$. In this case, once an attack is detected, some of the neighbors are always disconnected. □

5 | ANALYSIS OF THE OVERALL APPROACH

The methodologies to robustify the control inputs with respect to uncertain attacks (Section 3) and to identify the adversarial agents (Section 4) are summarized in Algorithm 2. First, each regular agent $i \in \mathcal{R}$ computes the probabilistic bounds of the disturbance and decides the connections with the neighbors. Then, it performs the distributed algorithm to compute the decisions. After the decisions are applied, the agent detects the occurrence of an attack and performs the identification method. Note that $\mathbb{P}(\mathbf{H}_i^{\hat{m}})$ in step 9 is associated to the set $\Theta_i^{\hat{m}} = \{j \in \mathcal{N}_i : v_{i,k}^{j\star} = 0\}$. Related to step 12 of Algorithm 2, in particular the part of implementing $\boldsymbol{v}_{i,k}^\star$, we consider that any agent can temporarily disconnect the physical link between itself and its neighbors, respecting the decision of $\boldsymbol{v}_{i,k}^\star$. Note that two agents, i and j, where $(i,j) \in \mathcal{E}$, can only exchange energy if and only if $v_{i,k}^{j\star} = v_{j,k}^{i\star} = 1$. Therefore, although there exists a connection between agents i and j, either of them can block the influence by closing the connection. Furthermore, due to constraints (27), when one of two neighboring agents decides to disconnect, the negotiation of the power transferred is forced towards a common solution $\rho_{ij,k}^{\mathrm{t}} = \rho_{ji,k}^{\mathrm{t}} = 0$ (see Remark 1). Although this assumption is not suitable in a conventional power network, considering the framework of microgrids, which can work in the island mode, disconnecting two neighboring microgrids can be done. In addition, two neighboring agents must also be able to exchange information in order to apply the distributed algorithm. The analysis of the algorithm, in terms of the characteristics of the obtained solution and the result of the identification method, is presented next in Sections 5.1 and 5.2, respectively.

Remark 6. In our problem setting, for simplicity, the probability distribution of the uncertainties $\boldsymbol{w}_{i,k}$ remains the same over time under Assumption 2. In this case, to reduce the computational effort at each iteration in Algorithm 2, steps 3 and 4 can actually be carried out only once offline[23]. In this case, suppose that the probabilistic bounds that are computed by solving (17) in an offline manner are denoted by $\mathcal{B}_i^\star$, for all $i \in \mathcal{N}$. Then, at each time instant k, we have that $\mathcal{B}_{i,k}^\star = \mathcal{B}_i^\star$. In general, however, the distribution of $\boldsymbol{w}_{i,k}$ can be time-varying, and with sufficient computational resources and knowledge regarding the variables, steps 3 and 4 can be executed online.

Remark 7. Recall that the disturbance $\boldsymbol{w}_{i,k}$ is compensated by the storage unit. However, a different strategy to deal with that disturbance can also be implemented, for instance, by using the dispatchable generation unit. In this case, the distribution of the compensation between the storage and the dispatchable unit must be determined. Additionally, the low-level controller might need to use the droop method[20,25]. Then, in the robust reformulation (Section 3), the distribution must be taken into account, i.e., (13) becomes $\rho_{i,k}^{\mathrm{st}} = \hat{\rho}_{i,k}^{\mathrm{st}} + \mu\mathbb{1}^\top \boldsymbol{w}_{i,k}$, where μ denotes the proportion of the disturbance that is handled by the storage unit. Additionally, re-denote the nominal decision of the dispatchable generation unit by $\hat{\rho}_{i,k}^{\mathrm{st}}$, then we must also include $\rho_{i,k}^{\mathrm{g}} = \hat{\rho}_{i,k}^{\mathrm{g}} + (1-\mu)\mathbb{1}^\top \boldsymbol{w}_{i,k}$ in the chance-constrained problem (15c). Furthermore, in the attack detection scheme, we need to

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

```
1: Initialize the hypothesis probabilities according to (24).
2: for $k = 0, 1, 2, \dots$ do
3:     Choose $n_{s,i}$ according to (18).
4:     Compute the probabilistic bound $\mathcal{B}^{\star}_{i,k}$ by solving (17).
5:     Compute $\mathcal{V}^{\star}_{i,k}$ by solving (25).
6:     if $\mathbb{1}_{|\mathcal{N}_i|} \in \mathcal{V}^{\star}_{i,k}$ then
7:         Choose $\boldsymbol{v}^{\star}_{i,k} = \mathbb{1}_{|\mathcal{N}_i|}$.
8:     else
9:         Choose randomly $\boldsymbol{v}^{\star}_{i,k} \in \mathcal{V}^{\star}_{i,k}$ such that $\mathbb{P}(\mathbf{H}_i^{\hat{m}}) \neq 0$.
10:    end if
11:    Compute $\boldsymbol{u}^{\star}_{i,k|k}$ using Algorithm 1, considering $\mathcal{U}_i$ is formed by the constraints defined in (25b)-(25c), where $\boldsymbol{v}^{j}_{i,k} = \boldsymbol{v}^{j\star}_{i,k}$.
12:    Implement $\boldsymbol{u}^{\star}_{i,k|k}$ and $\boldsymbol{v}^{\star}_{i,k}$.
13:    Measure $x_{i,k+1}$.
14:    Compute $d^{\mathrm{a}}_{i,k}$ based on Definition 4.
15:    Update the probability values of the hypotheses according to (22).
16: end for
```

evaluate not only the SoC as in (21) but also the difference between the nominal set point of the dispatchable generation and the actual one to determine the indicator of attack signal, $d^{\mathrm{a}}_{i,k}$.

5.1 | Analysis of the Solutions

Prior to stating the outcome of Algorithm 2, we establish the following assumption.

Assumption 4. The set of feasible solutions of Problem (19) is nonempty. Furthermore, this set contains a subset in which $\rho^{\mathrm{t}}_{ij,\ell} = \rho^{\mathrm{t}}_{ji,\ell} = 0$, for all $\ell \in \{k, \dots, k + h_p - 1\}$, and $(i, j) \in \mathcal{E}$.

The existence of nonempty feasible region in Problem (19) depends on the scenario realization, which determines the construction of the probabilistic bounds. Therefore, each agent can compute the bounds such that Assumption 4 holds. Furthermore, the second part of Assumption 4 follows from the consideration that each microgrid can operate in the island mode. Based on this assumption, we can state the feasibility of Problem (25), which is solved in step 5, as follows.

Proposition 1. Suppose that Assumption 4 holds. Then, Problem (25) has feasible solutions. □

Proof. The existence of nonempty feasible region of Problem (19) (Assumption 4) implies the feasibility of Problem (25) for the case $\boldsymbol{v}_{i,k} = \mathbb{1}_{|\mathcal{N}_i|}$ since constraint (25b) is also a constraint in Problem (19). When some of the neighbors are disconnected, i.e., $\boldsymbol{v}_{i,k} \in \{\boldsymbol{v} \in \{0,1\}^{|\mathcal{N}_i|} : \mathbb{1}^{\top}\boldsymbol{v} = |\mathcal{N}_i| - f\}$, there exist some vectors $\{\boldsymbol{u}_{i,\ell|k}\}_{\ell=k}^{k+h_p-1}$, where $\rho^{\mathrm{t}}_{ji,\ell} = 0$, for j only if $v^{j}_{i,k} = 0$ and all $\ell \in \{k, \dots, k+h_p-1\}$, that satisfy (27) and are also feasible solutions of Problem (19) due to the second part of Assumption 4. □

The characteristics of the decision implemented by each regular agent $i \in \mathcal{R}$ are stated in Proposition 2.

Proposition 2. Suppose that Assumptions 2 and 4 hold. Furthermore, suppose that each agent $i \in \mathcal{N}$ applies steps 4, 5, and 11 of Algorithm 2 to compute $\boldsymbol{u}^{\star}_{i,k|k}$. Then, the implemented decision, $\boldsymbol{u}^{\star}_{i,k|k}$, for each $i \in \mathcal{R}$, is an ε-level feasible solution of Problem (15), with level of inexactness ζ_i and probability at least $1 - \beta$, where $\varepsilon = \sum_{i\in\mathcal{N}} \varepsilon_i$ and $\beta = \sum_{i\in\mathcal{N}} \beta_i$. □

Proof. Consider the following minimization problem:

$$\begin{aligned} &\underset{\{\{\boldsymbol{u}_{i,\ell|k}\}_{i\in\mathcal{N}}\}_{\ell=k}^{k+h_p-1}}{\text{minimize}} \sum_{i\in\mathcal{N}} \sum_{\ell=k}^{k+h_p-1} J_{i,\ell}(\boldsymbol{u}_{i,\ell|k}) \\ &\text{subject to (25b), (25c), (19d), } \forall \ell \in \{k, \dots, k + h_p - 1\},\ \forall i \in \mathcal{N}. \end{aligned} \tag{28}$$

It can be seen that the decision $\boldsymbol{u}^{\star}_{i,k|k}$ is computed in step 11 of Algorithm 2, where all agents, $i \in \mathcal{N}$, cooperatively solve Problem (28), which has the same property as Problem (19), i.e., convex with strictly convex cost. The set of feasible solutions of Problem (28) is a nonempty subset of that of Problem (19) since Assumption 4 holds (see the proof of Proposition 1). Furthermore, the dual-ascent algorithm (Algorithm 1) is applied to solve Problem (28). Based on Lemma 1, the solution of Algorithm 1 converges to the optimal solution of Problem (28), i.e., $\left\|\left[\boldsymbol{\psi}^{\top}_{i,k} \ \cdots \ \boldsymbol{\psi}^{\top}_{i,k+h_p-1}\right]\right\|_2 \to 0$, for all $i \in \mathcal{N}$, as $r \to \infty$. Since Algorithm 1 is stopped prematurely, i.e., when the condition $\left\|\left[\boldsymbol{\psi}^{\top}_{i,k} \ \cdots \ \boldsymbol{\psi}^{\top}_{i,k+h_p-1}\right]\right\|_2 \leq \zeta_i$ is satisfied, the solution obtained, $\boldsymbol{u}^{\star}_{i,k|k}$, is inexact with the level of inexactness ζ_i. On the other hand, since Assumption 2 holds and since the bound sets $\mathcal{B}^{\star}_{i,k}$, for all $i \in \mathcal{N}$, are generated by solving (17), where the number of generated scenarios satisfies (18), the optimal solution of Problem (28) is an ε-level feasible solution of Problem (15), with probability at least $1 - \beta$[26, Proposition 1]. □

Remark 8. Since $\boldsymbol{u}^{\star}_{i,k|k}$, for each $i \in \mathcal{R}$, is an ε-level feasible solution of Problem (15), it might happen, with small probability ε, that one of the constraints imposed on the SoC level is violated after implementing $\boldsymbol{u}^{\star}_{i,k|k}$. Then, this fact might lead to an infeasibility issue when computing $\boldsymbol{u}^{\star}_{i,k+1|k+1}$ at the next time instant. When it is not feasible for agent i to improve its SoC level such that it is within the bounds at one time instant, agent i might relax the corresponding constraint such that its SoC level will be back within the original bounds after several time instants. Furthermore, in general, when the storage unit cannot handle the disturbances because of its physical limitation, the low level controller of the dispatchable generation unit might respond when there is a local imbalance in the microgrid.

5.2 | Analysis of the Identification Method

In this section, we show how each regular agent can correctly identify the adversarial agent in the case $f = 1$ and, in general, for any f-local adversary model, can block the influence of all adversarial neighbors by employing Algorithm 2. Note that in this model, the total number of adversarial agents in the network might be more than f. The analysis is divided into two parts, for the case $f = 1$ and for the case $f > 1$. Firstly, it is worth to note that the identification method works inseparably with the robustification method, as shown in Proposition 1. Secondly, we establish the following lemmas, which are useful in the analysis.

Lemma 2. Suppose that Assumptions 1-3 hold. If a regular agent, $i \in \mathcal{R}$, is connected to any adversarial neighbor, then the probability that infinitely many detectable attacks are received by agent i is 1. □

Proof. Since Assumptions 1 and 3 hold, the probability that detectable attacks occur is a positive scalar that is lower bounded by $\min_{j \in \mathcal{N}_i \cap \mathcal{A}} p^{\mathrm{a}}_j (1 - p^{\mathrm{ua}}_i) > 0$. Furthermore, the connection between agent i and an adversarial neighbor implies that agent i can receive an attack from the adversarial neighbor. As a result, based on the Borel-Cantelli lemma[29, Section 8.2.3] and since Assumption 2 holds, the claimed statement follows. □

Lemma 3. Let Assumption 4 hold. Suppose that at time step κ, the minimizer $\boldsymbol{v}^{\star}_{i,\kappa}$ chosen from the set of minimizers $\mathcal{V}^{\star}_{i,\kappa}$ of Problem (25) is such that some of the neighbors are disconnected, i.e., there exists some $j^{\star} \in \Theta^{\hat{m}}_i = \{j \in \mathcal{N}_i : v^{j\star}_{i,k} = 0\}$, $|\Theta^{\hat{m}}_i| = f$. Furthermore, suppose that for $k \geq \kappa$, $\mathbb{1}_{|\mathcal{N}_i|} \notin \mathcal{V}^{\star}_{i,k}$. If $d^{\mathrm{a}}_{i,\kappa} = 0$, then $\mathcal{V}^{\star}_{i,\kappa+1} = \{\boldsymbol{v}^{\star}_{i,\kappa}\}$.

Proof. The decision about which neighbors should be disconnected by agent i is based on the weight of $v^{j}_{i,k}$ in (26). For the case $f = 1$, the weight depends on the probability measure of each hypothesis, i.e., $c^{j}_{i,\kappa} = \mathbb{P}_{\kappa}(\mathbf{H}^{m_j}_i)$, where $\mathbf{H}^{m_j}_i$, for each $j \in \mathcal{N}_i$, is associated to $\Theta^{m_j}_i = \{j\}$ (see (26)). Therefore, $v^{j^{\star}}_{i,\kappa} = 0$ implies that $\mathbb{P}_{\kappa}(\mathbf{H}^{m_{j^{\star}}}_i) \in \arg\max_{j \in \mathcal{N}_i}(\mathbb{P}_{\kappa}(\mathbf{H}^{m_j}_i))$. Observe that $\mathbb{P}_k(d^{\mathrm{a}}_{i,k}) = 1$ only if $\mathbb{P}_{\kappa}(\mathbf{H}^{m_{j^{\star}}}_i) = 1$, implying $\mathbb{P}_{\kappa}(\mathbf{H}^{m_j}_i) = 0$ for $j \neq j^{\star}$. Thus in this case the claimed statement follows immediately. Now consider the case where $\mathbb{P}_{\kappa}(\mathbf{H}^{m_{j^{\star}}}_i) < 1$. Since $d^{\mathrm{a}}_{i,\kappa} = 0$ and $\mathbb{P}_k(d^{\mathrm{a}}_{i,k}) \in (0,1)$, by applying (22), we obtain that $\mathbb{P}_{\kappa+1}(\mathbf{H}^{m_{j^{\star}}}_i) > \mathbb{P}_{\kappa}(\mathbf{H}^{m_{j^{\star}}}_i)$ and $\mathbb{P}_{\kappa+1}(\mathbf{H}^{m_j}_i) \leq \mathbb{P}_{\kappa}(\mathbf{H}^{m_j}_i) \leq \mathbb{P}_{\kappa}(\mathbf{H}^{m_{j^{\star}}}_i)$, for any $j \in \mathcal{N}_i \backslash \{j^{\star}\}$. Therefore, $\mathbb{P}_{\kappa+1}(\mathbf{H}^{m_{j^{\star}}}_i) = \arg\max_{j \in \mathcal{N}_i}(\mathbb{P}_{\kappa+1}(\mathbf{H}^{m_j}_i))$ and the claimed statement follows.

For the case $f > 1$, let $\Theta^{\hat{m}}_{i,\kappa}$ be the set of all neighbors that are disconnected from agent i at time $k = \kappa$, i.e., $\Theta^{\hat{m}}_{i,\kappa} = \{j \in \mathcal{N}_i : v^{j\star}_{i,\kappa} = 0\}$. Note that there is a hypothesis that is associated to $\Theta^{\hat{m}}_{i,\kappa}$, denoted by $\mathbf{H}^{\hat{m}}_i$, and the probability measure of this hypothesis is denoted by $\mathbb{P}_k(\mathbf{H}^{\hat{m}}_i)$. Consider any $j^{\star} \in \Theta^{\hat{m}}_{i,\kappa}$ and $j \in \mathcal{N}_i \backslash \Theta^{\hat{m}}_{i,\kappa}$. Since $j^{\star} \in \Theta^{\hat{m}}_{i,\kappa}$ are disconnected at $k = \kappa$, we have $c^{j^{\star}}_{i,\kappa} \geq c^{j}_{i,\kappa}$. Now, we will show that $c^{j^{\star}}_{i,\kappa+1} > c^{j}_{i,\kappa+1}$ by updating $\mathbb{P}_{\kappa+1}(\mathbf{H}^{m}_i)$ for all $\mathbf{H}^{m}_i \in \mathcal{H}_i$ with (22) when $d^{\mathrm{a}}_{i,\kappa} = 0$. Similarly to the case $f = 1$, if for any $j \in \mathcal{N}_i \backslash \Theta^{\hat{m}}_{i,\kappa}$, $c^{j}_{i,\kappa} = 0$, we have that $c^{j^{\star}}_{i,\kappa+1} > c^{j}_{i,\kappa+1} = c^{j}_{i,\kappa} = 0$. In the case that $c^{j}_{i,\kappa} > 0$, for some $j \in \mathcal{N}_i \backslash \Theta^{\hat{m}}_{i,\kappa}$, we also have $c^{j^{\star}}_{i,\kappa+1} > c^{j}_{i,\kappa+1}$, which is shown as follows.

From the fact that $c^{j^\star}_{i,\kappa} \geq c^{j}_{i,\kappa}$, we observe that

$$\begin{aligned} c^{j^\star}_{i,\kappa} \geq c^{j}_{i,\kappa} &\Leftrightarrow \mathbb{P}_\kappa(\mathbf{H}^{\hat{m}}_i) + \sum_{m\in\mathcal{M}\setminus\{\hat{m}\}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) + \sum_{m\in\hat{\mathcal{M}}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) \geq \sum_{m\in\mathcal{M}'} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) + \sum_{m\in\hat{\mathcal{M}}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) \\ &\Leftrightarrow \mathbb{P}_\kappa(\mathbf{H}^{\hat{m}}_i) + \sum_{m\in\mathcal{M}\setminus\{\hat{m}\}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) - \sum_{m\in\mathcal{M}'} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) \geq 0, \end{aligned} \tag{29}$$

where $\mathcal{M} = \{m : j^\star \in \Theta^m_i, j \notin \Theta^m_i\}$, $\mathcal{M}' = \{m : j \in \Theta^m_i, j^\star \notin \Theta^m_i\}$, and $\hat{\mathcal{M}} = \{m : j \in \Theta^m_i, j^\star \in \Theta^m_i\}$. The second inequality is obtained directly from the definition of the weight $c^{j}_{i,k}$. Furthermore, observing at $k = \kappa + 1$, we have that

$$\begin{aligned} c^{j^\star}_{i,\kappa+1} - c^{j}_{i,\kappa+1} &= \mathbb{P}_{\kappa+1}(\mathbf{H}^{\hat{m}}_i) + \sum_{m\in\mathcal{M}\setminus\{\hat{m}\}} \mathbb{P}_{\kappa+1}(\mathbf{H}^{m}_i) - \sum_{m\in\mathcal{M}'} \mathbb{P}_{\kappa+1}(\mathbf{H}^{m}_i) \\ &= \alpha_1 \mathbb{P}_\kappa(\mathbf{H}^{\hat{m}}_i) + \alpha_2 \sum_{m\in\mathcal{M}\setminus\{\hat{m}\}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) - \alpha_2 \sum_{m\in\mathcal{M}'} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) \\ &= \alpha_2 \left(\frac{\alpha_1}{\alpha_2} \mathbb{P}_\kappa(\mathbf{H}^{\hat{m}}_i) + \sum_{m\in\mathcal{M}\setminus\{\hat{m}\}} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) - \sum_{m\in\mathcal{M}'} \mathbb{P}_\kappa(\mathbf{H}^{m}_i) \right) > 0, \end{aligned}$$

where $\alpha_1 = 1/\mathbb{P}_k(d^{\mathrm{a}}_{i,k})$ and $\alpha_2 = (1 - \hat{p}^{\mathrm{a}}_i)/\mathbb{P}_k(d^{\mathrm{a}}_{i,k})$. The last inequality follows from the fact that $\alpha_1 > \alpha_2$ and (29) holds. □

Lemma 2 indicates that when a regular agent is connected to an adversarial agent, a detectable attack will occur almost surely. Meanwhile, Lemma 3 shows how a regular agent decides the connection under certain conditions. Both lemmas are used to show how the attack identification and mitigation method works.

5.2.1 | The Case where $f = 1$

When $f = 1$, there exist $|\mathcal{N}_i|+1$ hypotheses, where Θ^m_i, for $m = 1, \dots, |\mathcal{N}_i|$, have one element. The outcome of the identification method for $f = 1$ is characterized in Proposition 3 as follows.

Proposition 3. Suppose that Assumptions 1-4 hold, a regular agent $i \in \mathcal{R}$ applies Algorithm 2 with $f = 1$, and there exists an adversarial neighbor of agent i. If there is no false detection, then agent i correctly identifies the adversarial neighbor. □

Proof. A regular agent $i \in \mathcal{R}$ identifies its adversarial neighbor by concluding from the probability measures of its hypotheses. In particular, let the adversarial neighbor be denoted by $j_{\mathrm{a}} \in \mathcal{N}_i \cap \mathcal{A}$ and the hypothesis associated to j_{a} is denoted by $\mathbf{H}^{m_{\mathrm{a}}}_i$. Then, we will show that $\mathbb{P}_k(\mathbf{H}^{m_{\mathrm{a}}}_i)$ eventually becomes 1. Note that when one of the hypothesis probabilities equals 1, the others equal 0 since $\sum_{m=0}^{|\mathcal{N}_i|} \mathbb{P}_k(\mathbf{H}^m_i) = 1$, for any $k \in \mathbb{Z}_{\geq 0}$.

Recall that $\mathbb{P}_k(\mathbf{H}^m_i)$, for all $\mathbf{H}^m_i \in \mathcal{H}_i$, evolve based on Bayesian inference given in (22). From (23), the dynamics (22) can be seen as hybrid dynamics since $d^{\mathrm{a}}_{i,k}, v^{j}_{i,k} \in \{0, 1\}$. Note that when $d^{\mathrm{a}}_{i,k} = 1$, a detectable attack occurs, whereas, when $d^{\mathrm{a}}_{i,k} = 0$, no attack is detected because the adversarial neighbor either does not attack or performs an undetectable attack. Furthermore, recall also that $v^{j}_{i,k} = 0$ implies agent j is blocked, so that if $j = j_{\mathrm{a}}$, it cannot attack. Otherwise, agent j is not blocked. At each k, there is only at most one neighbor that is blocked due to constraint (25d) in Problem (25), which is solved to determine $\boldsymbol{v}^\star_{i,k}$ (step 10 of Algorithm 2).

We analyze the dynamics of all $\mathbb{P}_k(\mathbf{H}^m_i)$ based on the decision $\boldsymbol{v}^\star_{i,k}$. During the period at which $\boldsymbol{v}^\star_{i,k} = \mathbb{1}_{|\mathcal{N}_i|}$, the adversarial agent can attack. Note that the number of detectable attacks, $n^{\mathrm{a}}_{i,k}$, is unbounded due to Lemma 2. As a result, depending on the weight γ_i, for some k where $n^{\mathrm{a}}_{i,k}$ is sufficiently large, $\mathbb{1}_{|\mathcal{N}_i|} \notin \mathcal{V}^\star_{i,k}$, e.g., see Remark 5. Additionally, it is observed from (22) and (23) that starting for the first time instant that $d^{\mathrm{a}}_{i,k} = 1$, $\mathbb{P}_{k+1}(\mathbf{H}^0_i) = 0$. If agent i only has one neighbor, a detectable attack immediately leads to the identification that the neighbor is adversarial. In the following, we consider the case where $|\mathcal{N}_i| > 1$. We observe the dynamics of $\mathbb{P}_k(\mathbf{H}^m_i)$, for which $\mathbb{1}_{|\mathcal{N}_i|} \notin \mathcal{V}^\star_{i,k}$. In particular, we consider two cases: (a) when the adversarial agent is blocked and (b) when a regular neighbor is blocked.

In case (a), suppose that at time step $\underline{k}$, the adversarial agent is blocked, i.e., $v^{j_{\mathrm{a}}\star}_{i,\underline{k}} = 0$. Therefore, $d^{\mathrm{a}}_{i,\underline{k}} = 0$. Moreover, according to Lemma 3, $v^{j_{\mathrm{a}}\star}_{i,\underline{k}+1} = 0$, implying $d^{\mathrm{a}}_{i,\underline{k}+1} = 0$. In fact, $v^{j_{\mathrm{a}}\star}_{i,k} = 0$ and $d^{\mathrm{a}}_{i,k} = 0$, for all $k \geq \underline{k}$. Hence, since $d^{\mathrm{a}}_{i,k}$ and $\boldsymbol{v}^\star_{i,k}$, for $k \geq \underline{k}$, are fixed, the dynamics (22) are smooth. By recursively applying (22), starting from $\underline{k}$, and considering fixed $d^{\mathrm{a}}_{i,k}$ and $\boldsymbol{v}^\star_{i,k}$, we have, for $k > \underline{k}$,

$$\mathbb{P}_k(\mathbf{H}_i^m) = \frac{(p_{\mathbf{H}_i^m})^{k-\underline{k}}}{\sum\limits_{m=0}^{|\mathcal{N}_i|} (p_{\mathbf{H}_i^m})^{k-\underline{k}} \mathbb{P}_{\underline{k}}(\mathbf{H}_i^m)} \mathbb{P}_{\underline{k}}(\mathbf{H}_i^m), \ \forall \mathbf{H}_i^m \in \mathcal{H}_i,$$

where $p_{\mathbf{H}_i^m} = \mathbb{P}_k(d^{\mathrm{a}}_{i,k} = 0 | \mathbf{H}_i^m)$, i.e.,

$$p_{\mathbf{H}_i^m} = \begin{cases} 1, & \text{for } m \in \{0, m_{\mathrm{a}}\}, \\ 1 - \hat{p}_{\mathrm{at}}, & \text{for all } m \notin \{0, m_{\mathrm{a}}\}. \end{cases}$$

Hence, for $\mathbf{H}_i^{m_{\mathrm{a}}}$,

$$\mathbb{P}_k(\mathbf{H}_i^{m_{\mathrm{a}}}) = \frac{1}{\mathbb{P}_{\underline{k}}(\mathbf{H}_i^{m_{\mathrm{a}}}) + \sum\limits_{m \neq m_{\mathrm{a}}} (p_{\mathbf{H}_i^m})^{k-\underline{k}} \mathbb{P}_{\underline{k}}(\mathbf{H}_i^m)} \mathbb{P}_{\underline{k}}(\mathbf{H}_i^{m_{\mathrm{a}}}).$$

Thus, we have $\lim_{k\to\infty} \mathbb{P}_k(\mathbf{H}_i^{m_{\mathrm{a}}}) = 1$, since $p_{\mathbf{H}_i^m} < 1$ for all $m \neq m_{\mathrm{a}}$. Furthermore, we also have that $\lim_{k\to\infty} \mathbb{P}_k(\mathbf{H}_i^m) = 0$ for $m \neq m_{\mathrm{a}}$.

In case (b), suppose that at time step $\underline{k}$, a regular neighbor $j \in \mathcal{N}_i \backslash \{j_{\mathrm{a}}\}$ is blocked, i.e., $v^{j\star}_{i,\underline{k}} = 0$. According to Lemma 3 and the dynamics (22) and (23), the neighbor j is blocked as long as $d^{\mathrm{a}}_{i,k} = 0$, for $k \geq \underline{k}$. However, consider that at some $\overline{k} \geq \underline{k}$, $d^{\mathrm{a}}_{i,\overline{k}} = 1$. Then, based on (22) and (23), $\mathbb{P}_{\overline{k}+1}(\mathbf{H}_i^{m_j}) = 0$. Note that since j_{a} is not blocked for $\underline{k} \leq k \leq \overline{k}$, a detectable attack will occur almost surely (Lemma 2). Thus, if any regular neighbor $j \in \mathcal{N}_i \backslash \{j_{\mathrm{a}}\}$ is being blocked, its probability $\mathbb{P}_k(\mathbf{H}_i^{m_j})$ will eventually become 0. As a result, if another regular neighbor is blocked at $k = \overline{k} + 1$, we have case (b) again, whereas if the adversarial neighbor is blocked, we have case (a). □

Remark 9. Based on Proposition 3, each regular agent that applies Algorithm 2 can identify its adversarial neighbor correctly for the case $f = 1$ provided that there is no false detection. Based on Definition 6, a false detection occurs when the uncertainty from the load, $w^{\mathrm{d}}_{i,k}$, is outside of the probabilistic bounds. Since the computed decision $\boldsymbol{u}^\star_{i,k|k}$ is an ε-level solution (Proposition 2), we know that the probability of $w^{\mathrm{d}}_{i,k}$ being outside of the bounds is at most ε, which can be set to be small. If false detections are made during the operation, then all hypothesis probabilities will eventually become zero. When they are all zero, the identification process can then be restarted. □

5.2.2 | The Case where $f > 1$

In the case that $f > 1$, a regular agent might not be able to identify the adversarial neighbors. However, it can block all adversarial neighbors, as presented in Proposition 4.

Proposition 4. Suppose that Assumptions 1-4 hold, regular agent $i \in \mathcal{R}$ applies Algorithm 2 with $f > 1$, and there exist at most f adversarial neighbors of agent i. If there is no false detection, then the hypothesis probability associated to one of the sets of neighbors that contain all adversarial neighbors converges to one and, when all hypothesis probabilities $\mathbb{P}_k(\mathbf{H}_i^m)$ have converged, agent i blocks all adversarial neighbors. □

Proof. The lines of proof are similar to those of Proposition 3. Let $\mathcal{A}_i$ denote the set of adversarial neighbors of agent i, i.e., $\mathcal{A}_i = \mathcal{N}_i \cap \mathcal{A}$. Note that by Definition 2, $|\mathcal{A}_i| \leq f$. We analyze the dynamics of $\mathbb{P}_k(\mathbf{H}_i^m)$, for all $\mathbf{H}_i^m \in \mathcal{H}_i$, at $k \geq k_0$, for which $\mathbb{1}_{|\mathcal{N}_i|} \notin \mathcal{V}^\star_{i,k}$. Firstly, observe that, if $f \geq |\mathcal{N}_i|$, then there are only two hypotheses. The assertion immediately holds since when there is a detectable attack, $\mathbb{P}(\mathbf{H}_i^0) = 0$. Furthermore, since $\mathbb{1}_{|\mathcal{N}_i|} \notin \mathcal{V}^\star_{i,k}$, all neighbors are disconnected. Now we observe two possible cases on the decision of $\boldsymbol{v}^\star_{i,k}$ for $f < |\mathcal{N}_i|$. The cases are similar to those that are explained in the proof of Proposition 3.

In case (a), we suppose that at $\underline{k}$, agent i blocks all adversarial neighbors, $j \in \mathcal{A}_i$, i.e., $v^{j\star}_{i,\underline{k}} = 0$ for all $j \in \mathcal{A}_i$. Since agent i is disconnected from all adversarial neighbors, at $k = \underline{k}$, $d^{\mathrm{a}}_{i,\underline{k}} = 0$. Furthermore, based on Lemma 3, the decision to block all adversarial neighbors hold for $k \geq \underline{k}$. Therefore, $\mathbb{P}_k(\mathbf{H}_i^m)$, for all $m = 0, 1, \dots, n_i^{\mathrm{H}}$, evolve smoothly for $k \geq \underline{k}$. Let $\Theta^{\hat{m}}_{i,\underline{k}}$ denotes the set of neighbors that are disconnected by agent i at time $\underline{k}$, i.e., $\Theta^{\hat{m}}_{i,\underline{k}} = \{j \in \mathcal{N}_i : v^{j\star}_{i,\underline{k}} = 0\}$ and $\mathbf{H}_i^{\hat{m}}$ denotes the hypothesis associated to $\Theta^{\hat{m}}_{i,\underline{k}}$. Note that $\mathcal{A}_i \subseteq \Theta^{\hat{m}}_{i,\underline{k}}$, where the equality holds if $|\mathcal{A}_i| = f$. By evaluating the dynamics (22), it holds that $\lim_{k\to\infty} \mathbb{P}_k(\mathbf{H}_i^{\hat{m}}) = 1$ whereas the other hypothesis probabilities converge to 0.

In case (b), we suppose that at $\underline{k}$, some adversarial neighbors are not blocked, i.e., the set $\{j \in \mathcal{A}_i : j \notin \Theta^{\hat{m}}_{i,\underline{k}}\}$ is nonempty. As in the case $f = 1$, if there is no attack, due to Lemma 3, the set of neighbors $\Theta^{\hat{m}}_{i,\underline{k}}$ will still be blocked at the next time step, $k = \underline{k} + 1$. Furthermore, since $\mathbb{P}_k(\mathbf{H}_i^m)$ for all $m = 1, \dots, n_i^{\mathrm{H}}$ are initialized equally, only $\mathbb{P}_k(\mathbf{H}_i^{\hat{m}})$ evolves differently, for $k \geq \underline{k}$.

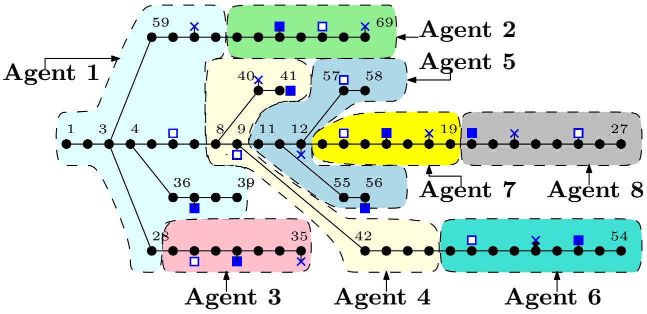

FIGURE 4 The PG&E 69-bus distribution network partitioned into a group of interconnected microgrids[3]. Squares indicate the distributed generation units, i.e., filled squares, ■, and empty squares, □, represent renewable generation units and dispatchable generators, respectively, whereas crosses, ×, indicate the storage units.

The other probabilities, $\mathbb{P}_k(\mathbf{H}_i^m)$, for $m \neq \hat{m}$ such that $\mathbb{P}_k(\mathbf{H}_i^m) \neq 0$, are equal, for $k \geq \underline{k}$, since they are multiplied by the same factor, which is either $(1-\hat{p}_i^{\mathrm{a}})/\mathbb{P}(d_{i,k}^{\mathrm{a}})$ when there is no attack, or $\hat{p}_i^{\mathrm{a}}/\mathbb{P}(d_{i,k}^{\mathrm{a}})$ when there is an attack. However, the occurrence of the next attack is with probability 1 (Lemma 2). Suppose that the next attack occurs at $\overline{k}$. Therefore, $\mathbb{P}_{\overline{k}}(\mathbf{H}_i^{\hat{m}}) = 0$, while other hypotheses that have probability strictly larger than zero at $k = \overline{k} - 1$, have an equal value at $k = \overline{k}$, denoted by $\pi_{\overline{k}}$. Note that the number of these hypotheses is $1/\pi_{\overline{k}}$. The decision $\boldsymbol{v}^{\star}_{i,\overline{k}+1}$ depends on solving Problem (25) and step 9 in Algorithm 2. Due to step 9 in Algorithm 2, a different set of neighbors, i.e., $\Theta^{\hat{m}}_{i,\overline{k}+1} \neq \Theta^{\hat{m}}_{i,\underline{k}}$, is disconnected at $k = \overline{k} + 1$. If $\mathcal{A}_i \subseteq \Theta^{\hat{m}}_{i,\overline{k}+1}$, we have case (a), otherwise we have case (b). Note that, since the number of sets of disconnected neighbors that do not include all adversarial agents is limited and such a set cannot be chosen twice, eventually a set of neighbors, Θ_i^m, which includes all adversarial neighbors, i.e., $\mathcal{A}_i \subseteq \Theta_i^m$, is disconnected. Thus, eventually we have case (a). □

Remark 10. Proposition 4 shows that each regular agent that applies Algorithm 2 can eventually block all adversarial neighbors for any $f \geq 1$, provided that there is no false detection. Therefore, similar to the case $f = 1$, setting a small desired level of violation ε implies a high probability of blocking all adversarial neighbors. Furthermore, when false detections occur, then the identification and mitigation process can be restarted after all hypothesis probabilities have become zero. □

6 | CASE STUDY

In order to show the effectiveness of the proposed approach in mitigating attacks and identifying adversarial agents, we consider the PG&E 69-bus distribution network with additional dispatchable generation, renewable generation, and storage units, which is partitioned into eight microgrids (agents)[3]. The topology of this interconnected-microgrid system is shown in Figure 4 . Furthermore, the parameter values of the components of each microgrid are given in Table 1 . We consider that there are two types of load profiles, which are residential and industrial loads. We suppose that microgrids 1, 2, 5, and 6 have industrial load profiles whereas the others have residential profiles. In addition, we consider that agents 2, 6, and 7 are adversarial.

Two simulation studies are carried out. The first study shows how the overall scheme works in two scenarios, which correspond to the conditions in Propositions 3 and 4, while the second study emphasizes on the attack detection scheme. The simulations are carried out in MATLAB with YALMIP[30] using a computer with 2.6 GHz Intel Core i7 CPU and 16 GB of RAM. In addition, it is set that the sampling time is 15 minutes, the prediction horizon is four time steps and the level of inexactness for Algorithm 1 is $\zeta_i = 5$, for all $i \in \mathcal{N}$. We assume that there exist low-level local controllers at each microgrid that control the dispatchable generation and storage units such that the set points computed are met at each time instant.

6.1 | Performance of the Overall Scheme

In this simulation, where the simulation time is one day (96 steps), the adversarial agents, $i = 2, 6, 7$, attack with $p_i^{\mathrm{a}} = 0.3$. The industrial and the residential load profiles are based on realistic data collected in a large-scale study[31,32]. Furthermore, the network has solar-based energy sources, the profiles of which are also based on realistic data[32]. The attack strategy of the adversarial agents is to reduce the production of their dispatchable generation units randomly. Here, we apply Algorithm 2 to

TABLE 1 Parameters of the Microgrids

Parameters	Value	Unit	Agent (i)
x_i^{min}, x_i^{max}, $x_{i,0}$	30, 80, 50	%	all
ρ_i^{ch}, ρ_i^{dh}	300, 300	kW	all
$\rho_i^{\text{g,min}}$, $\rho_i^{\text{g,max}}$	0, 1000 0, 2000	kW	3, 4, 7, 8 1, 2, 5, 6
$\rho_i^{\text{t,max}}$	110	kW	all
$\rho_i^{\text{im,max}}$	2000 0	kW	1 else
$e_{\text{cap},i}$	500 1000	kWh	3, 4, 7, 8 1, 2, 5, 6
a_i	0.98	-	all
c_i^{st}, c_i^{im}, c_i^{t}	1, 250, 0.1	-	all
c_i^{g}	5 10	-	2, 4, 6, 7 1, 3, 5, 8
ε_i, β_i	0.01, 0.05	-	all

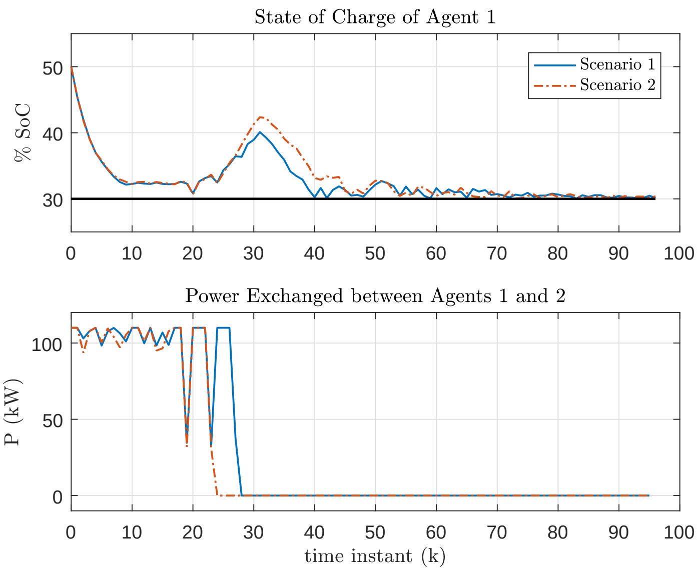

FIGURE 5 The evolution of SoC of agent 1 (top plot) and the power exchanged between agent 1 and its adversarial neighbor, agent 2 (bottom plot).

the previously described system. Two simulation scenarios are considered, where we consider that false detection never occurs. In the first scenario, it is assumed that $f = 1$, whereas in the second scenario $f = 2$. Figures 5 –7 show some plots of the simulation results. From the top plot of Figure 5 , it is observed that the SoC value of agent 1 stays in the limit for all time steps in both scenarios, showing the robustness of the decisions with respect to the attacks and system disturbance. Figures 6 and 7 show how agent 1 manages to disconnect from its adversarial neighbor (agent 2). Particularly in Scenario 1, agent 1 identifies that agent 2 is an adversarial agent. Moreover, once one of the hypothesis probability values converge to 1, the bottom plot of Figure 5 shows that agent 1 stops exchanging power with agent 2.

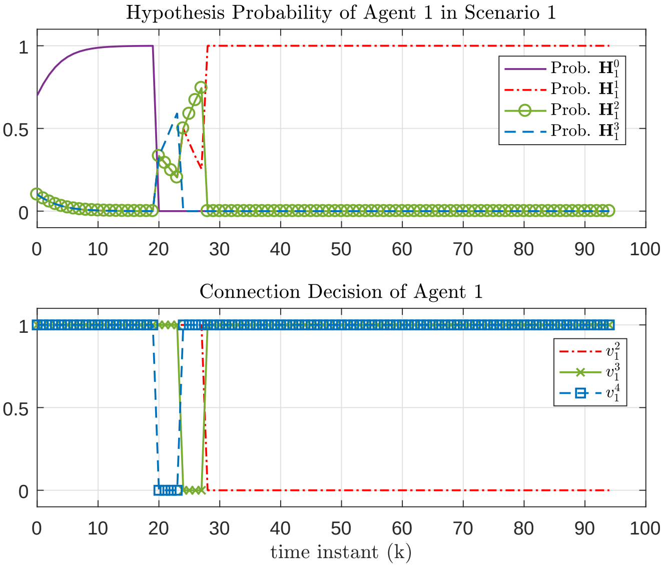

FIGURE 6 The evolution of each hypothesis probability of agent 1 (top plot) and the connection decision of agent 1 at each time instant (bottom plot) in Scenario 1. Note that $\Theta_1^1 = \{2\}, \Theta_1^2 = \{3\}, \Theta_1^3 = \{4\}$.

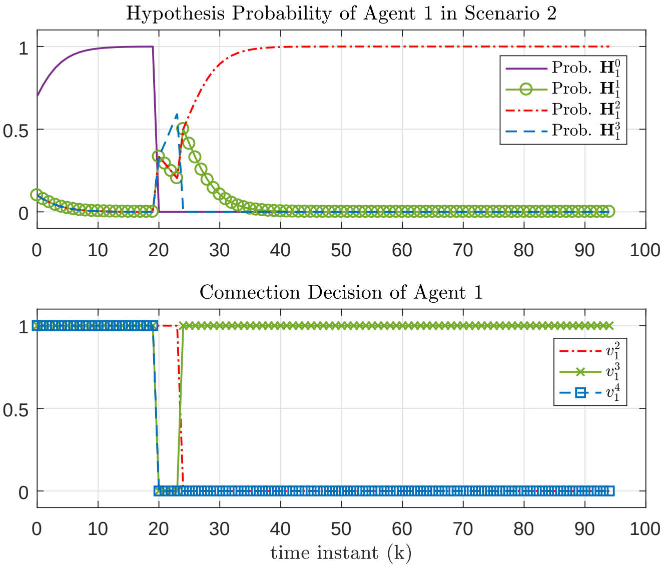

FIGURE 7 The evolution of each hypothesis probability of agent 1 (top plot) and the connection decision of agent 1 at each time instant (bottom plot) in Scenario 1. Note that $\Theta_1^1 = \{2,3\}, \Theta_1^2 = \{2,4\}, \Theta_1^3 = \{3,4\}$.

6.2 | Performance of the Attack Detection Scheme

In the second simulation study, we perform Monte Carlo simulations to observe the attack detection scheme. We suppose that the adversarial agents $i = 2, 6, 7$ attack with $p_i^{\mathrm{a}} = 0.5$ and the regular agents do not apply the active strategy of disconnecting their neighbors so that the regular agents are always subject to attacks. Note that the probability of attack is set to be quite high in order to observe more attacks, particularly undetectable ones. For these simulations, load and renewable power generation profiles from the first simulation study are perturbed. We carried out seven simulations, each of which is 96 time steps length. Therefore, we observe 672 detection instants for each regular agent. Table 2 shows the summary of the attack detection outcomes whereas Figure 8 shows the attack detection of agent 1 in some time steps of one simulation. Correct detection means that an agent

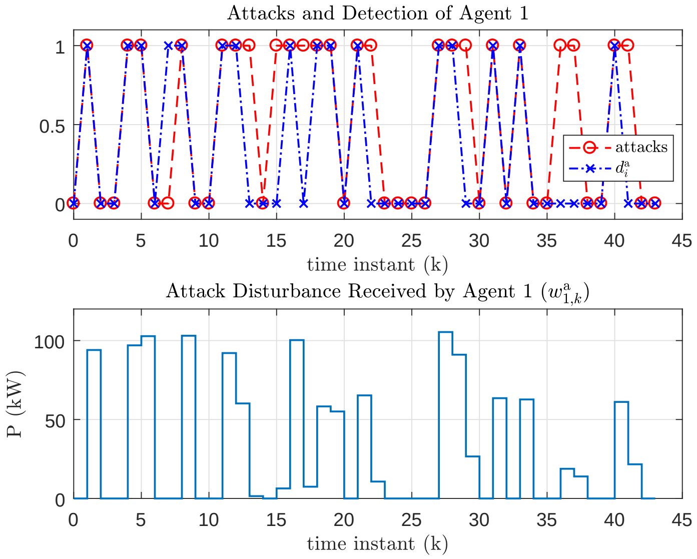

FIGURE 8 Top plot shows the detection variable $d^{\mathrm{a}}_{1,k}$ (dot-dashed blue plot with cross markers) and the actual event, i.e., whether there is an attack (1) or not (0) (dashed red plot with circle markers). Bottom plot shows the attack disturbance of agent 1, $w^{\mathrm{a}}_{1,k}$. These plots are taken from one simulation.

TABLE 2 Detection Results of the Regular Agents

Agent	Correct Detection (%)	Undetectable Attack (%)	False Detection (%)
1	82.74	16.82	0.44
3	99.40	0.00	0.60
4	82.59	17.11	0.30
5	79.61	20.09	0.30
8	49.85	50.15	0.00
Total	78.84	20.83	0.33

TABLE 3 The Average Local Performance Change During the Attacks

Case Study	Adversarial Agent			Regular Agent			
	2	6	7	1	4	5	8
6.1	19.7%	1.5%	4.5%	0.0%	−0.3%	−0.1%	−0.2%
6.2	35.2%	8.9%	53.3%	−0.4%	−1.1%	−0.6%	−3.7%

Note: Agent 3 does not have any adversarial neighbors.

correctly detects whether there is an attack or not. As expected from the stochastic method that we applied, the probability of false detection is less than ε. One can see a false detection in the top plot of Figure 8 at time step $k = 7$.

6.3 | Discussions

The local performance improvements obtained by each adversarial agent when performing successful attacks in both simulation studies presented in Sections 6.1 and 6.2 are shown in Table 3 . Furthermore, as can be seen in Table 3 , the performance of the regular agents are degraded by the attacks. The degradation is relatively low compared to the improvement obtained by the adversarial agents since most of the attacks can still be handled by the storage unit, whose cost per unit is cheaper than using the dispatchable generator, whereas the adversarial agents manage to reduce the power production of their generators by performing the attacks. However, note that the available power in the storage unit of a regular agent is lower after an attack occurs. Therefore, the performance of a regular agent after an attack might still deteriorate and this performance degradation is not captured in Table 3 .

It is also worth mentioning that an adversarial agent might actually perform an undetectable attack. Although the performance improvement obtained by an undetectable attack is less than a detectable one since undetectable attack is limited, it will make the identification process to take longer time to finish. For instance, as can be seen in Table 2 , the probability of correct detections of agent 8 is 49.85%, implying that the adversarial neighbor of agent 8 has successfully performed undetectable attacks half of the time. Note that, in the case study of Section 6.2, the average performance improvements obtained by the adversarial agents 2, 6, and 7 by performing undetectable attacks are lower than the total average shown in Table 3 (9.7%, 0.1%, and 52.61%, respectively). Similarly, the performance degradation of each regular agent by undetectable attacks is also quite low (less than 0.6%). Nevertheless, in order to guarantee that the performed attack is undetectable, an adversarial agent will require local information of its neighbors, which is not shared in the presented problem setting. Therefore, it might be difficult for the adversarial agents to keep attacking without being detected.

7 | CONCLUSION AND FUTURE WORK

A distributed approach for an economic dispatch problem of interconnected microgrids in the presence of adversaries has been proposed. The adversarial actions are considered as uncertain disturbances and the economic dispatch problem is formulated as a chance-constrained problem. Thus, we propose to apply a two-step stochastic approach so that the control inputs computed are robustly feasible against the adversarial behavior. Furthermore, the proposed approach also includes a methodology to identify the adversarial agents and mitigate the attacks from these agents. The methodology is based on hypothesis testing using Bayesian inference and requires each regular agent to solve a local mixed-integer problem to decide the connection with its neighbors. Therefore, our proposal is a combination of active and passive methods to deal with unexpected disturbances.

As future work, we will consider analyzing potential clever attacks from adversarial agents such that the attacks are hard to be detected. In this regard, the interaction between regular and adversarial agents might also be analyzed from the perspective of game theory. Moreover, we will also consider to improve the identification scheme by employing an information-sharing scheme of the hypothesis probability among the agents. In addition, a more accurate model of the system should also be taken into account in the future work. Since it will likely lead to a non-convex formulation, we will also investigate whether the present results hold.

ACKNOWLEDGMENT

The authors would like to thank Yasuhiro Hayashi and Shinya Yoshizawa for providing us the load and solar power generation data used[31,32] in the case study.

How to cite this article: W Ananduta, JM Maestre, C Ocampo-Martinez, and H Ishii (2019), Resilient Distributed Model Predictive Control for Energy Management of Interconnected Microgrids, *Optim. Control Appl. Meth.*.

APPENDIX

A LIST OF SYMBOLS

The symbols used in this paper are summarized in Table A1 .

References

1. Molzahn DK, Dörfler F, Sandberg H, et al. A Survey of Distributed Optimization and Control Algorithms for Electric Power Systems. *IEEE Transactions on Smart Grid.* 2017;8(6):2941–2962.

2. Morstyn T, Hredzak B, Agelidis VG. Control Strategies for Microgrids with Distributed Energy Storage Systems: An Overview. *IEEE Transactions on Smart Grid.* 2018;9(4):3652–3666.

3. Arefifar SA, Mohamed YARI, El-Fouly THM. Supply-Adequacy-Based Optimal Construction of Microgrids in Smart Distribution Systems. *IEEE Transactions on Smart Grid.* 2012;3(3):1491–1502.

4. Hug G, Kar S, Wu C. Consensus + Innovations Approach for Distributed Multiagent Coordination in a Microgrid. *IEEE Transactions on Smart Grid.* 2015;6(4):1893–1903.

5. Larsen GKH, Foreest ND, Scherpen JMA. Distributed MPC Applied to a Network of Households With Micro-CHP and Heat Storage. *IEEE Transactions on Smart Grid.* 2014;5(4):2106–2114.

6. Wang T, O'Neill D, Kamath H. Dynamic Control and Optimization of Distributed Energy Resources in a Microgrid. *IEEE Transactions on Smart Grid.* 2015;6(6):2884–2894.

7. Hans C A, Braun P, Raisch J, Grune L, Reincke-Collon C. Hierarchical Distributed Model Predictive Control of Interconnected Microgrids. *IEEE Trans. Sustainable Energy.* 2019;10(1):407–416.

8. Baker K, Guo J, Hug G, Li X. Distributed MPC for Efficient Coordination of Storage and Renewable Energy Sources Across Control Areas. *IEEE Transactions on Smart Grid.* 2016;7(2):992–1001.

9. Quijano N, Ocampo-Martinez C, Barreiro-Gomez J, Obando G, Pantoja A, Mojica-Nava E. The Role of Population Games and Evolutionary Dynamics in Distributed Control Systems: The Advantages of Evolutionary Game Theory. *IEEE Control Systems.* 2017;37(1):70–97.

10. Velarde P, Maestre JM, Ishii H, Negenborn RR. Vulnerabilities in Lagrange-based Distributed Model Predictive Control. *Optimal Control Applications and Methods.* 2018;39(2):601-621.

11. Sharma DD, Singh SN, Lin J, Foruzan E. Agent-Based Distributed Control Schemes for Distributed Energy Storage Systems Under Cyber Attacks. *IEEE Transactions on Emerging and Selected Topics in Circuits and Systems.* 2017;7(2):307–318.

12. Pasqualetti F, Dörfler F, Bullo F. Attack Detection and Identification in Cyber-Physical Systems. *IEEE Transactions on Automatic Control.* 2013;58(11):2715–2729.

13. LeBlanc HJ, Zhang H, Koutsoukos X, Sundaram S. Resilient Asymptotic Consensus in Robust Networks. *IEEE Journal on Selected Areas in Communications.* 2013;31(4):766–781.

14. Dibaji SM, Ishii H, Tempo R. Resilient Randomized Quantized Consensus. *IEEE Transactions on Automatic Control.* 2018;63(8):2508–2522.

15. Feng Z, Wen G, Hu G. Distributed Secure Coordinated Control for Multiagent Systems Under Strategic Attacks. *IEEE Transactions on Cybernetics.* 2017;47(5):1273–1284.

16. Velarde P, Maestre JM, Ishii H, Negenborn RR. Scenario-based Defense Mechanism for Distributed Model Predictive Control. In: Proceedings of the IEEE 56th Conference on Decision and Control (CDC):6171–6176; 2017; Melbourne, Australia.

17. Tanaka T, Gupta V. Incentivizing Truth-telling in MPC-based Load Frequency Control. In: Proceedings of the IEEE 55th Conference on Decision and Control (CDC):1549–1555; 2016; Las Vegas, USA.

18. Ananduta W, Maestre JM, Ocampo-Martinez C, Ishii H. Resilient Distributed Energy Management for Systems of Interconnected Microgrids. In: Proceedings of the IEEE 57th Conference on Decision and Control (CDC):6159–6164; 2018; Miami, USA.

19. Ananduta W, Maestre JM, Ocampo-Martinez C, Ishii H. A Resilient Approach for Distributed MPC-Based Economic Dispatch in Interconnected Microgrids. In: Proceedings of the European Control Conference; 2019; Naples, Italy. to appear.

20. Guerrero JM, Vasquez JC, Matas J, de Vicuna LG, Castilla M. Hierarchical Control of Droop-Controlled AC and DC Microgrids–A General Approach Toward Standardization. *IEEE Transactions on Industrial Electronics.* 2011;58(1):158-0172.

21. Boyd S, Vandenberghe L. *Convex Optimization*. Cambridge University Press; 2010.

22. Giselsson P, Doan MD, Keviczky T, De Schutter B, Rantzer A. Accelerated Gradient Methods and Dual Decomposition in Distributed Model Predictive Control. *Automatica.* 2013;49(3):829–833.

23. Margellos K, Rostampour V, Vrakopoulou M, Prandini M, Andersson G, Lygeros J. Stochastic Unit Commitment and Reserve Scheduling: A Tractable Formulation with Probabilistic Certificates. In: Proceedings of European Control Conference:2513–2518; 2013.

24. Vrakopoulou M, Margellos K, Lygeros J, Andersson G. A Probabilistic Framework for Reserve Scheduling and $N-1$ Security Assessment of Systems With High Wind Power Penetration. *IEEE Transactions on Power Systems.* 2013;28(4):3885-3896.

25. Olivares DE, Mehrizi-Sani A, Etemadi AH, et al. Trends in Microgrid Control. *IEEE Transactions on Smart Grid.* 2014;5(4):1905–1919.

26. Margellos K, Goulart P, Lygeros J. On the Road Between Robust Optimization and the Scenario Approach for Chance Constrained Optimization Problems. *IEEE Transactions on Automatic Control.* 2014;59(8):2258–2263.

27. Calafiore GC, Campi MC. The Scenario Approach to Robust Control Design. *IEEE Transactions on Automatic Control.* 2006;51(5):742–753.

28. Ingimundarson A, Bravo JM, Puig V, Alamo T, Guerra P. Robust Fault Detection Using Zonotope–based Set–membership Consistency Test. *International Journal of Adaptive Control and Signal Processing.* 2008;23(4):311–330.

29. Capinski M, Kopp PE. *Measure, Integral and Probability*. Springer; 2013.

30. Lofberg J. YALMIP: A Toolbox for Modeling and Optimization in MATLAB. In: Proceedings of the CACSD Conference:284–289; 2004; Taipei, Taiwan.

31. Hayashi Y, Fujimoto Y, Ishii H, et al. Versatile Modeling Platform for Cooperative Energy Management Systems in Smart Cities. *Proceedings of the IEEE.* 2018;106(4):594–612.

32. New Energy Industrial Technology Development Organization (NEDO) . Demonstrative Research on Grid-Interconnection of Clustered Photovoltaic Power Generation Systems .

TABLE A1 The List of Symbols

Symbol	Definition
$\mathcal{S}$	Graph representation of the system
$\mathcal{N}$	Set of nodes
$\mathcal{E}$	Set of edges
$\mathcal{N}_i$	Set of neighbors of agent *i*
$\mathcal{A}$	Set of adversarial agents
$\mathcal{R}$	Set of regular agents
$\rho^{\mathrm{d}}_{i,k}$	Power disturbance (the difference between power load and power generated from non-dispatchable units) of agent *i*
ρ^{st}	Power delivered from/to the storage unit
ρ^{g}	Power generated by the dispatchable generators
ρ^{im}	Power imported from the main grid
ρ^{t}	Power transferred between two neighboring microgrids
ρ^{ch}_i	Maximum charging power of the storage unit
ρ^{dh}_i	Maximum discharging power of the storage unit
$\rho^{\mathrm{g,min}}_i$	Minimum power can be generated by the dispatchable generator
$\rho^{\mathrm{g,max}}_i$	Maximum power can be generated by the dispatchable generator
$\rho^{\mathrm{im,max}}_i$	Maximum power can be imported from the main grid
$\rho^{\mathrm{t,max}}_i$	Maximum power can be transferred
$x_{i,k}$	State of charge (SoC) of the storage unit
$x^{\min}_i$	Minimum level of SoC
$x^{\max}_i$	Maximum level of SoC
a_i	efficiency of the storage unit
c^{st}_i	Per-unit cost of using storage unit
c^{g}_i	Per-unit cost of using the dispatchable generator
c^{im}_i	Per-unit cost of importing power from the main grid
c^{t}_i	Per-unit cost of transferring power with neighboring microgrids
h_p	Prediction horizon
$\lambda_{i,k}$	Lagrange multipliers associated to the coupling constraints
$^{(r)}$	Iteration in the distributed optimization algorithm
p^a_i	The probability of attacks performed by agent *i*
$\hat{p}^a_i$	The predicted probability of attacks received by agent *i*
$w^{\mathrm{d}}_{i,k}$	Disturbance of the system due to the difference between forecast and actual power disturbance
$w^{\mathrm{a}}_{i,k}$	Attack disturbance
ε_i	Maximum level of violation
β_i	Level of confidence
$\mathcal{B}_i$	Probabilistic set that bounds the disturbances
$\overline{\tau}_i$	Upper bound of the disturbances (parameter of hyper-rectangular $\mathcal{B}_i$)
$\underline{\tau}_i$	Lower bound of the disturbances (parameter of hyper-rectangular $\mathcal{B}_i$)
$d^{\mathrm{a}}_{i,k}$	Indicator of attack
n^{H}_i	Number of attacks received
$\mathbf{H}^m_i$	The m^{th} hypothesis of agent *i*
$\mathbb{P}_k(\mathbf{H}^m_i)$	The probability of the m^{th} hypothesis of agent *i* at time instance *k*
$\upsilon^j_{i,k}$	Indicator of connection between agent *i* and its neighbor $j \in \mathcal{N}_i$