Resilient Control of Interconnected Microgrids Under Attack by Robust Nonlinear MPC

Sarah Braun[1][a], Sebastian Albrecht[1][b] and Sergio Lucia[2][c]
[1]*Siemens AG, Otto-Hahn-Ring 6, 81739 München, Germany*
[2]*TU Dortmund University, August-Schmidt-Straße 1, 44227 Dortmund, Germany*

Keywords: Robust Control, Attack Identification, Mathematical Modeling, Nonlinear Model Predictive Control, Distributed Control.

Abstract: With the growing share of renewable energy sources, the uncertainty in power supply is increasing, on the one hand because of fluctuations in the renewables, but on the other hand also due to the threat of deliberate malicious attacks, which may become more prevalent due to the growing number of distributed generation units. It is thus essential that local microgrids are controlled in a robust manner in order to ensure stability and supply security even in the event of disturbances. To this end, we introduce a mathematical model for interconnected, physically coupled microgrids with renewable generation that are exposed to the risk of attacks. For optimal energy management and control, we present a resilient framework that combines a model-based method to identify occurring attacks and a model predictive control scheme to compute robust control inputs. We demonstrate the efficiency of the method for microgrid control in numerical experiments.

1 INTRODUCTION

In the course of the energy transition, power generation is undergoing a technological shift toward distributed generation, mainly from renewable energy sources. This requires distributed control methods that can be applied to safety-critical systems in real time. Decentralized microgrids, combining local demands, generation, and often storage units, increase the security of supply within the microgrid area, but create new challenges: Under the uncertainty of renewables, one has to address optimal control tasks like economic generator dispatch, efficient battery use, or optimal power import and export strategies to benefit from fluctuating energy prices, see (Olivares et al., 2014; Mohammed et al., 2019). For the design of such control schemes, one has to be aware that distributed systems with many local generators and consumers provide attackers with many targets. Distributed control like the tertiary control tasks above should thus be approached in a robust and secure manner to provide viable solutions even under uncertainty or in the event of an attack.

An important tool for flexible energy management in microgrids is model predictive control (MPC), since it repeatedly computes optimal inputs to the system based on measurements at each sampling time, while it allows to include constraints and economic costs into consideration. *Robust* MPC schemes explicitly take uncertainty into account and typically use tube-based ideas, see (Mayne et al., 2005), or multi-stage approaches, see (Lucia et al., 2013), which consider a discrete set of possible scenarios. Robust MPC cannot only be applied to parametric uncertainties, but also to malicious attacks as illustrated in (Braun et al., 2021a). Also distributed MPC schemes for large systems under attack have been proposed, e.g., in (Wang and Ishii, 2019; Braun et al., 2020). While robust control can mitigate the impact of unknown attacks, appropriate countermeasures require detecting and identifying the attack. (Pasqualetti et al., 2013) define attack detection and identification (ADI) as the tasks to uncover the presence of an attack and localize all attacked components, respectively. They also establish a widely used mathematical framework for control systems under attack. An overview of physics-based ADI methods for both linear and nonlinear dynamics is given by (Giraldo et al., 2018; Arauz et al., 2021). Some approaches like (Pasqualetti et al., 2013; Gallo et al., 2020) design

[a] https://orcid.org/0000-0002-7032-6116
[b] https://orcid.org/0000-0002-3647-4043
[c] https://orcid.org/0000-0002-3347-5593

Braun, S., Albrecht, S. and Lucia, S.
Resilient Control of Interconnected Microgrids Under Attack by Robust Nonlinear MPC.
DOI: 10.5220/0011316500003271
In *Proceedings of the 19th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2022)*, pages 58-66
ISBN: 978-989-758-585-2; ISSN: 2184-2809

unknown-input observers for ADI, where identification typically requires the use of one observer for each possible attack scenario. To avoid the resulting combinatorial nature, others propose optimization-based methods and compute suspicious attackers by solving sparse optimization problems like (Pan et al., 2015; Braun et al., 2021b). Similar to the present work, several authors examine their methods for robust control or ADI using the example of interconnected microgrids such as (Gallo et al., 2020; Ananduta et al., 2020), which underlines the need for resilient methods in microgrid control. While (Gallo et al., 2020) consider low-voltage control and focus on attack *detection*, (Ananduta et al., 2020) solve economic dispatch problems similar to those in this work. They propose an ADI method based on hypothesis testing that, however, requires full enumeration of all possible attack scenarios, which again results in a combinatorial complexity. Both use linear dynamic models, whereas we consider nonlinear battery dynamics.

The contribution of this work consists of a mathematical model for tertiary control of interconnected microgrids, a novel approach for local attack identification, and a numerical case study to illustrate a resilient control framework for attacked microgrids with uncertain generation. The model, described in Section 2, includes nonlinear battery dynamics, takes into account the physical coupling of neighboring microgrids through dispatchable power exchange, and covers the possible threat of attacks. To the new microgrid model, we apply the methods developed in prior work for attack identification based on sparse optimization and for robust control against uncertainties and already identified attacks. All approaches are summarized in Section 3, where we also introduce a new method for *local* ADI. We illustrate the potential of these methods by numerical experiments in Section 4, using an example of interconnected microgrids with uncertain renewable generation under attack.

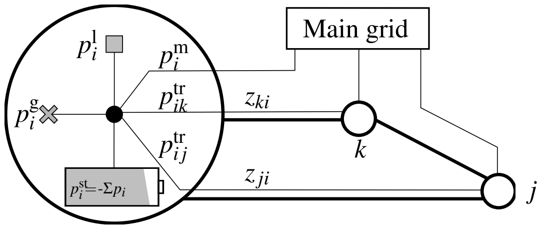

Figure 1: Schematic overview of the proposed model for interconnected microgrids, showing the local model components for microgrid i. Apart from internal power states, each microgrid only requires knowledge of its neighboring couplings $(z_{ji})_{j\in\mathcal{N}_i}$. Storage units are used as a buffer to maintain power balance.

2 A MODEL FOR INTERCONNECTED MICROGRIDS UNDER ATTACK

2.1 Microgrid Model

We consider a set of interconnected microgrids that are represented by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where each node $i \in \mathcal{V}$ corresponds to a microgrid and each edge $\{i, j\} \in \mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ describes two physically coupled microgrids. Such pairs are called neighbors and we denote the neighborhood of i as $\mathcal{N}_i := \{j | \{i, j\} \in \mathcal{E}\}$. Each microgrid contains dispatchable generation units, generating a total power output $p_i^{\mathrm{g}} \geq 0$, and an aggregated load $p_i^{\mathrm{l}} \leq 0$. Modeling uncertain load and nondispatchable generation from renewable energy sources is postponed to Section 2.3. Each microgrid is connected to the main grid, from or to which it can import or export power p_i^{m}. Import is modeled by non-negative values $p_i^{\mathrm{m}} \geq 0$, export by negative values $p_i^{\mathrm{m}} < 0$. In addition, we assume that neighboring microgrids i, j with $j \in \mathcal{N}_i$ can transfer power to each other. The power that microgrid i sends to a neighbor j is denoted by p_{ij}^{tr} and vice versa, and the resulting directed power flow from i to j is given as $p_{ij}^{\mathrm{flow}} = p_{ij}^{\mathrm{tr}} - p_{ji}^{\mathrm{tr}}$. Finally, each microgrid has a storage unit with state of charge (SoC) $s_i \in [0, 1]$, from which power $p_i^{\mathrm{st}} > 0$ is taken when discharged and which can be charged with power $p_i^{\mathrm{st}} < 0$. Unlike, e.g., (Ananduta et al., 2020), we assume that generation cannot change instantaneously and model p_i^{g} and, similarly, p_i^{m} and p_{ij}^{tr} as differential states, whose change over time is controlled by inputs u_i^{g}, u_i^{m}, and u_{ij}^{tr} according to

$$\begin{aligned}
\dot{p}_i^{\mathrm{g}} &= \frac{1}{T_i^{\mathrm{g}}} \left(u_i^{\mathrm{g}} - p_i^{\mathrm{g}}\right), \\
\dot{p}_i^{\mathrm{m}} &= \frac{1}{T_i^{\mathrm{m}}} \left(u_i^{\mathrm{m}} - p_i^{\mathrm{m}}\right), \qquad (1) \\
\dot{p}_{ij}^{\mathrm{tr}} &= \frac{1}{T_{ij}^{\mathrm{tr}}} \left(u_{ij}^{\mathrm{tr}} - p_{ij}^{\mathrm{tr}}\right).
\end{aligned}$$

The delay parameters $T_i^{\mathrm{g}}, T_i^{\mathrm{m}}$, and $T_{ij}^{\mathrm{tr}} \in \mathbb{R}$ describe how quickly a change in the input affects the state and depend on technical characteristics. Compared to T_i^{g}, for power transfers with the main grid or neighboring microgrids, typically smaller delay times T_i^{m} and T_{ij}^{tr} are chosen as we will see in our numerical example in Section 4. We assume that low-level controllers in all units ensure that the computed set points are met at all times. To make sure that the power balance in microgrid i is always satisfied, even when an attack occurs, the storage is used as a buffer that provides the required power reserves. To this end, the storage power

p_i^{st} is modeled as a dependent variable that is computed from the states p_i^{g}, p_i^{m} and p_{ij}^{tr} and the load p_i^{l} according to

$$p_i^{\mathrm{st}} = -p_i^{\mathrm{g}} - p_i^{\mathrm{m}} - p_i^{\mathrm{l}} - \sum_{j\in\mathcal{N}_i} \left(p_{ji}^{\mathrm{tr}} - p_{ij}^{\mathrm{tr}}\right).$$

It should be noted here that for microgrid i, p_{ij}^{tr} is a local state that can be controlled via u_{ij}^{tr} as in eq. (1), whereas the neighboring state p_{ji}^{tr} can neither be controlled by microgrid i nor is its dynamic behavior known to i. Instead, it represents a coupling variable $z_{ji} = p_{ji}^{\mathrm{tr}}$, that models the physical connection of neighboring microgrids and is treated locally as an uncertain parameter as we will explain in more detail in Section 3. Figure 1 illustrates that each microgrid only knows its local power variables and its neighboring couplings, allowing for distributed control. According to the storage power p_i^{st}, the storage is charged or discharged and the resulting change in the SoC s_i is modeled as

$$\dot{s}_i = b_i(s_i, p_i^{\mathrm{st}}),$$

with some function b_i modeling the battery dynamics, which is described in the next section.

2.2 Nonlinear Battery Model

If a microgrid is attacked, the battery may also be used at SoCs close to 0 or 1, which is avoided during normal operation. Therefore, the goal of this section is to derive a nonlinear function b_i that describes the battery dynamics for all states of charge in $[0,1]$ and not only in the middle range, where a linear approximation is often sufficient. With Q_i denoting the maximum capacity of the battery and I_i^{st} being the battery current, the dynamics of the SoC are given as

$$\dot{s}_i = -\frac{I_i^{\mathrm{st}}}{Q_i}, \tag{2}$$

see, e.g., (Mathieu and Taylor, 2016). With U_i^{st} denoting the battery voltage, the storage power p_i^{st} is given as $p_i^{\mathrm{st}} = U_i^{\mathrm{st}} I_i^{\mathrm{st}}$ and U_i^{st}, in turn, can be modeled as

$$U_i^{\mathrm{st}} = U_i^{\mathrm{OCV}}(s_i) + R_i I_i^{\mathrm{st}}.$$

The first term describes the open circuit voltage U_i^{OCV} and the second the ohmic effect with resistance R_i, see (Mathieu and Taylor, 2016). For the storage power p_i^{st}, this results in the following equation, which is quadratic in I_i^{st}

$$p_i^{\mathrm{st}} = U_i^{\mathrm{OCV}}(s_i) I_i^{\mathrm{st}} + R_i \left(I_i^{\mathrm{st}}\right)^2.$$

Solving it for I_i^{st}, the battery current I_i^{st} is obtained from s_i and p_i^{st} via $I_i^{\mathrm{st}} = \beta_i(s_i, p_i^{\mathrm{st}})$ for some nonlinear function β_i. Together with eq. (2), this results in a nonlinear function $b_i(s_i, p_i^{\mathrm{st}}) = -\beta_i(s_i, p_i^{\mathrm{st}})/Q_i$ describing the dynamic behavior of the battery. It remains open to specify $U_i^{\mathrm{OCV}}(s_i)$. Models for the open circuit voltage of batteries are typically obtained from electrochemical analyses and often fitted to linear curves. For low and high SoCs, however, this is inaccurate, which is why we use the model by (Zhang et al., 2016). With parameters A_i, B_i, C_i, D_i, M_i, and N_i that depend on the type of battery, their model includes a logarithmic, a linear, and an exponential function

$$U_i^{\mathrm{OCV}}(s_i) = A_i + B_i(-\ln(s_i))^{M_i} + C_i s_i + D_i e^{N_i(s_i-1)}.$$

2.3 Attack Model

In this work, we examine attacks on microgrid control and model an attack as an additional, unknown input like, e.g., (Ananduta et al., 2020). In microgrid i, we consider the possibility of attacks on the generation input u_i^{g}, on the power exchange u_i^{m} with the main grid, and on power transfers u_{ij}^{tr} with any neighbor $j \in \mathcal{N}_i$. If an attacker is present, the dynamics in eq. (1) of the affected state $p_i \in \{p_i^{\mathrm{g}}, p_i^{\mathrm{m}}, p_{ij}^{\mathrm{tr}}\}$ with input $u_i \in \{u_i^{\mathrm{g}}, u_i^{\mathrm{m}}, u_{ij}^{\mathrm{tr}}\}$ and delay parameter $T_i \in \{T_i^{\mathrm{g}}, T_i^{\mathrm{m}}, T_{ij}^{\mathrm{tr}}\}$ are changed to

$$\dot{p}_i = \frac{1}{T_i}(u_i + a_i - p_i), \tag{3}$$

where $a_i \in \{a_i^{\mathrm{g}}, a_i^{\mathrm{m}}, a_{ij}^{\mathrm{tr}}\}$ represents the modification in the dynamics caused by the attack. In other words, in case of an attack, not the computed controller command u_i is applied to the system, but some altered input $u_i + a_i$.

This model covers not only malicious attacks, but uncertain disturbances in general. If microgrid i includes nondispatchable generation from renewables or uncertain load, the input a_i^{g} also models the power difference between uncertain generation and load. We deliberately make no difference in modeling, but consider both attacks and renewable generation as uncertain influences, since the resilient control framework presented in Section 3 is robust against attacks as well as fluctuations in generation and load.

2.4 Cost Function

Each microgrid i is operated locally to meet the respective load at the lowest possible cost. For a time window $[0,T]$, we consider the following costs for economic dispatch

$$J_i(T) = \int_0^T q_i\left(p_i^{\mathrm{g}}, p_i^{\mathrm{tr}}, p_i^{\mathrm{st}}\right) + l_i\left(p_i^{\mathrm{flow}}, p_i^{\mathrm{m}}\right) dt + m_i(s_i(T)),$$

that consist of quadratic stage costs q_i, piecewise linear stage costs l_i, and terminal costs m_i. The costs q_i are defined as

$$q_i\left(p_i^{\mathrm{g}}, p_i^{\mathrm{tr}}, p_i^{\mathrm{st}}\right) = C_i^{\mathrm{g}}\left(p_i^{\mathrm{g}}\right)^2 + \sum_{j\in\mathcal{N}_i} C_i^{\mathrm{tr}}\left(p_{ij}^{\mathrm{tr}}\right)^2 + C_i^{\mathrm{st}}\left(p_i^{\mathrm{st}}\right)^2$$

with cost values $C_i^{\mathrm{g}}, C_i^{\mathrm{tr}}, C_i^{\mathrm{st}} \in \mathbb{R}_{\geq 0}$. They describe the per-unit costs of power generation, power transfers to neighbors, and storage operations, and model the costs that incur by the use of these units. The economic profit or loss from selling or buying energy in trade with neighbors or the main grid is modeled by piecewise linear costs l_i. Based on the positive and negative part functions

$$(x)_+ := \begin{cases} 0 \text{ if } x < 0, \\ x \text{ if } x \geq 0, \end{cases}$$

and

$$(x)_- = \begin{cases} x \text{ if } x < 0, \\ 0 \text{ if } x \geq 0, \end{cases}$$

the piecewise linear cost function l_i is defined as

$$l_i\left(p_i^{\mathrm{flow}}, p_i^{\mathrm{m}}\right) = \sum_{j\in\mathcal{N}_i} C_{ji}^{\mathrm{flow,ex}}\left(p_{ji}^{\mathrm{flow}}\right)_- + \sum_{j\in\mathcal{N}_i} C_{ji}^{\mathrm{flow,im}}\left(p_{ji}^{\mathrm{flow}}\right)_+ + C_i^{\mathrm{m,ex}}\left(p_i^{\mathrm{m}}\right)_- + C_i^{\mathrm{m,im}}\left(p_i^{\mathrm{m}}\right)_+$$

for each microgrid i, with export and import per-unit prices $C_{ji}^{\mathrm{flow,ex}}$, $C_{ji}^{\mathrm{flow,im}}$, $C_i^{\mathrm{m,ex}}$, $C_i^{\mathrm{m,im}} \in \mathbb{R}_{\geq 0}$, which may fluctuate throughout the day. We will explicitly allow export prices to be considerably lower than import prices since we focus on small producers, for which in reality it is often more profitable to generate power for their own demand than to import from the main grid. To account for degradation costs of the battery and to avoid that only the storage is discharged to fulfill the load, we introduce terminal costs m_i as

$$m_i(s_i) = C_i^{\mathrm{dis}}\left(s_i(0) - s_i(T)\right)_+ Q_i.$$

If the state of charge $s_i(T)$ at the end of the considered horizon is smaller than $s_i(0)$ at the beginning, each unit of power discharge is penalized by some cost $C_i^{\mathrm{dis}} \in \mathbb{R}_{\geq 0}$.

3 A FRAMEWORK FOR RESILIENT CONTROL

In this section, we outline three methods for resilient control of distributed systems under attack that have been proposed in recently published work, see (Braun et al., 2020; Braun et al., 2021b; Braun et al., 2021a): First, we describe an approach for robust distributed MPC in Section 3.1. Then, a global ADI method to identify unknown attacks is outlined in Section 3.2, and, finally, both methods are combined into an adaptively robust MPC scheme in Section 3.3 to compute control inputs that are robust against previously identified attacks. We also propose a novel approach for *local* ADI in Section 3.2. All methods are applicable to distributed control systems with several subsystems that behave according to discrete-time dynamics of the form

$$\begin{aligned} x_i^{k+1} &= f_i\left(x_i^k, u_i^k + a_i^k, z_{\mathcal{N}_i}^k\right), \\ z_i^{k+1} &= h_i(x_i^{k+1}), \\ y_i^{k+1} &= g_i(x_i^{k+1}), \end{aligned} \tag{4}$$

with local states x_i^k, inputs u_i^k, attacks a_i^k, and system outputs y_i^k in subsystem i. The physical interconnection of subsystems is modeled through coupling variables z_i^k, which depend on the local states. All functions f_i, h_i, and g_i may be nonlinear and are assumed to be sufficiently smooth. The microgrid model from Section 2 is of the same form as eq. (4) when we define local states

$$x_i = \left(s_i, p_i^{\mathrm{g}}, p_i^{\mathrm{m}}, \left(p_{ij}^{\mathrm{tr}}\right)_{j\in\mathcal{N}_i}\right)^{\mathrm{T}},$$

local inputs

$$u_i = \left(u_i^{\mathrm{g}}, u_i^{\mathrm{m}}, \left(u_{ij}^{\mathrm{tr}}\right)_{j\in\mathcal{N}_i}\right)^{\mathrm{T}},$$

local attacks

$$a_i = \left(a_i^{\mathrm{g}}, a_i^{\mathrm{m}}, \left(a_{ij}^{\mathrm{tr}}\right)_{j\in\mathcal{N}_i}\right)^{\mathrm{T}},$$

and local couplings

$$z_i = \left(p_{ij}^{\mathrm{tr}}\right)_{j\in\mathcal{N}_i} \text{ and } z_{\mathcal{N}_i} = \left(p_{ji}^{\mathrm{tr}}\right)_{j\in\mathcal{N}_i}.$$

The function f_i is obtained from the dynamics in eq. (1) by discretizing the equations in time, while the function g_i depends on the desired system output and can for example model measurement data.

3.1 Contract-based Robust Distributed MPC

An important aspect for the control of safety-critical systems is to compute inputs that are *robust* against uncertainties by ensuring that the constraints are fulfilled in all possible cases. To this end, (Lucia et al., 2013) propose a multi-stage scheme for robust MPC that assumes a discrete set of possible scenarios and represents all potential future states in a scenario tree. Taking into account that in a closed-loop approach future inputs can be adapted when new measurements are available, they compute control inputs that achieve constraint satisfaction in all scenarios and minimize a cost function weighted over all scenarios.

Robust MPC can be employed to design also *distributed* MPC schemes since in a distributed setting as in eq. (4), to the eyes of subsystem i, the neighboring couplings $z_{\mathcal{N}_i}$ behave in an uncertain manner. Since multi-stage MPC requires knowledge about the range of possible values for each uncertain quantity, (Lucia et al., 2015) introduce so-called *contracts* $\mathcal{Z}_i$, that contain predicted reachable values of the coupling variables z_i and are exchanged among neighbors. In (Braun et al., 2020), approximations of these contracts are proposed that can efficiently be obtained from local scenario trees and have been proven to work well in practice.

To apply multi-stage (distributed) MPC for robust control also against attacks, one has to provide suitable uncertainty sets $\mathcal{A}_i$ with possible values for local attacks a_i. To this end, one can choose suitable samples for attack values as in (Braun et al., 2020), or in a more general approach use available knowledge about the attackers gained from attack identification. The latter approach is introduced in (Braun et al., 2021a) and summarized in Section 3.3.

3.2 Attack Identification based on Sparse Optimization

Robust MPC schemes provide an important tool to manage the impact of a potential attack. Nevertheless, when an attack occurs, it is crucial to detect and identify it quickly to initiate appropriate countermeasures in order to eliminate the attacker or mitigate its impact. To avoid the combinatorial nature that is inherent to most identification methods relying on unknown-input observers, one can solve a continuous optimization problem to compute a suspected attack from an unknown, possibly infinite dimensional and unbounded set of potential attacks. Taking advantage of the observation that typical attacks in practical applications target only few network components, the optimization reveals a sparsest possible attack that explains the observed system output.

In (Braun et al., 2021b), this idea is implemented in a global ADI method with rigorous success guarantees for nonlinear networked systems. Since in a distributed setting, model information about the subsystems' dynamics is available only locally and should remain private, a linear approximation of the dynamics at the current iterate is used for identification. To this end, each subsystem locally evaluates first-order derivatives and makes them publicly available. Then, a global linear optimization problem is solved to identify a sparse suspected attack.

In this paper, we propose a novel identification problem for *local* attack identification, which is also based on sparse optimization. Since no information on local dynamics is published in this decentralized approach, the linearization from above is no longer necessary. Instead, each subsystem locally solves the following nonlinear identification problem with measurements $\tilde{y}_i$, $\tilde{x}_i$, and $\tilde{z}_{\mathcal{N}_i}$ of the output y_i, the state x_i, and the neighboring couplings $z_{\mathcal{N}_i}$:

$$\begin{aligned} \min_{a_i} \quad & \|a_i\|_1, \\ \text{s.t.} \quad & \left\| \tilde{y}_i - g_i \circ f_i(\tilde{x}_i, u_i + a_i, \tilde{z}_{\mathcal{N}_i}) \right\|_2 \leq \varepsilon_i, \end{aligned} \tag{5}$$

where the $\circ$-operator denotes the function composition of g_i and f_i. A solution of problem eq. (5) locally reveals a suspected attack, referred to as a_i^*, based on which the local model in eq. (4) with functions g_i, f_i explains the observed output $\tilde{y}_i$ up to an accuracy of ε_i. The choice of the tolerance ε_i is not trivial, even if perfect measurements were assumed, since the distributed model in eq. (4) only approximates the dynamic behavior of the global system. More specifically, the coupling variables $z_{\mathcal{N}_i}$ in the local models represent differential states of neighboring subsystems, but their dynamic behavior is unknown to subsystem i. In ongoing research, we investigate how different parametrization schemes of the coupling variables influence the resulting error between centralized and distributed numerical integration. Based on this error, a suitable value ε_i can be chosen. In the numerical experiments in this work, we use a fixed value, which is given in Section 4.

3.3 Attack Mitigation using Adaptively Robust MPC

In the previous sections, two important tools for distributed control systems under attack have been introduced: For one thing, robust MPC can limit the impact of a disturbance by ensuring satisfied constraints in all scenarios, but requires information about the uncertainty range. For another thing, attack identification provides suspicions about an attack, but is not able to mitigate its effects. To combine the advantages of both, an adaptively robust MPC scheme was proposed in (Braun et al., 2021a). It repeatedly adjusts the uncertainty sets $\mathcal{A}^k$ that involve possible attacks a^k at time k according to findings from attack identification. The method is designed for attacks that obey a probability distribution with unknown, time-invariant expected value μ and standard deviation σ, which are estimated at each time k from solutions $a^{*,l}$ of the identification problem in earlier times $l \leq k$. The mean μ^k and the sample standard deviation σ^k of all previously identified values $a^{*,l}$ serve as estimates for μ and σ according to

$$\mu^k = \frac{1}{k+1} \sum_{l=0}^{k} a^{*,l}$$

and

$$\sigma^k = \left(\frac{1}{k} \sum_{l=0}^{k} \left(a^{*,l} - \mu^k \right)^2 \right)^{\frac{1}{2}}.$$

The uncertainty of possible attacks a^k is now represented by three scenarios for each component a_i^k

$$\mathcal{A}_i^k = \left\{ \mu_i^k, \mu_i^k + \sigma_i^k, \mu_i^k - \sigma_i^k \right\}. \tag{6}$$

The total amount of scenarios considered in the multi-stage control scheme results from the product of all uncertainty sets $\mathcal{A}_i^k$ for each identified component a_i^k. The interplay of all methods presented in Section 3 is summarized in Algorithm 1.

Algorithm 1: A resilient control framework.

```
Input: Initial contracts $\mathcal{Z}_i^0 \ \forall i$, e.g., $\mathcal{Z}_i^0 = \{h_i(x_i(0))\}$
1: Set $\mathcal{A}_i^0 := \{\} \ \forall i$
2: for time step $k$ and microgrid $i$ do
3:     Set up local multi-stage problem and compute input $u_i^k$, robust against $\mathcal{Z}_{\mathcal{N}_i}^{k-1}$ and $\mathcal{A}_i^{k-1}$
4:     Derive new contract $\mathcal{Z}_i^k$ and transmit to all neighbors $j \in \mathcal{N}_i$
5:     Local ADI: Solve problem (5) to obtain a suspicion $a_i^{*,k}$
6:     Locally adapt uncertainty set $\mathcal{A}_i^k$ as in eq. (6)
7: end for
```

Table 1: This table lists all model and cost parameters, variable bounds, and initial values that are used in all experiments presented in this work.

Parameters	Values	Unit
T_i^{g}, T_i^{m}, T_{ij}^{tr} $\forall i,j$	0.1, 0.001, 0.001	h
Q_1, Q_2, Q_3	100, 200, 100	kAh
R_1, R_2, R_3	1.5, 2.0, 3.0	mΩ
$A_i, B_i \ \forall i$	2.23, -0.001	V
$C_i, D_i \ \forall i$	-0.35, 0.6851	V
$M_i, N_i \ \forall i$	3.0, 1.6	-
$C_1^{\mathrm{g}}, C_2^{\mathrm{g}}, C_3^{\mathrm{g}}$	0.2, 3.0, 2.0	-
$C_i^{\mathrm{tr}}, C_i^{\mathrm{st}}, C_i^{\mathrm{dis}} \ \forall i$	4.0, 1.0, 2000	-
$C_{ij}^{\mathrm{flow,im}}, C_{ij}^{\mathrm{flow,ex}} \ \forall i,j$	4.0, 0.04	-
$\underline{s}_i, \underline{p}_i^{\mathrm{g}}, \underline{p}_i^{\mathrm{m}}, \underline{p}_{ij}^{\mathrm{tr}} \ \forall i,j$	0, 0, -1000, -100	-, kW
$\overline{s}_i, \overline{p}_i^{\mathrm{g}}, \overline{p}_i^{\mathrm{m}}, \overline{p}_{ij}^{\mathrm{tr}} \ \forall i,j$	1, 1000, 2000, 100	-, kW
$\underline{u}_i^{\mathrm{g}}, \underline{u}_i^{\mathrm{m}}, \underline{u}_{ij}^{\mathrm{tr}} \ \forall i,j$	0, -1000, -100	kW
$\overline{u}_i^{\mathrm{g}}, \overline{u}_i^{\mathrm{m}}, \overline{u}_{ij}^{\mathrm{tr}} \ \forall i,j$	1000, 2000, 100	kW
$s_1(0), s_2(0), s_3(0)$	0.9, 0.5, 0.6	-
$p_i^{\mathrm{g}}(0), p_i^{\mathrm{m}}(0) \ \forall i$	0.0, 0.0	kW
$p_{ij}^{\mathrm{tr}}(0) \ \forall i,j$	0.0	kW
$p_i^{\mathrm{l}} \ \forall i$	-2.0	kW

4 NUMERICAL EXPERIMENTS

In this section, we perform a numerical case study to analyze how economic dispatch for microgrids can be achieved at minimum cost despite possible disturbances, using the methods from Section 3. We consider three microgrids with renewable generation that may be exposed to attacks, each connected to the other microgrids and the main grid as in Figure 1. According to Section 2, each microgrid $i \in \{1,2,3\}$ is modeled by five states $s_i, p_i^{\mathrm{g}}, p_i^{\mathrm{m}}, p_{ij}^{\mathrm{tr}}$ and four control inputs $u_i^{\mathrm{g}}, u_i^{\mathrm{m}}, u_{ij}^{\mathrm{tr}}$ for $j \in \{1,2,3\} \setminus \{i\}$. For all variables $v_i \in \left\{ s_i, p_i^{\mathrm{g}}, p_i^{\mathrm{m}}, p_{ij}^{\mathrm{tr}}, u_i^{\mathrm{g}}, u_i^{\mathrm{m}}, u_{ij}^{\mathrm{tr}} \right\}$, the initial values $v_i(0)$ and lower and upper bounds $\underline{v}_i$ and $\overline{v}_i$ are given in Table 1, which also contains the values of all model parameters as in Section 2. The parameters A_i, B_i, C_i, D_i, M_i, and N_i in the model for open circuit voltage by (Zhang et al., 2016) are chosen following their suggestion for LTO-batteries. During a time window of two days, each microgrid locally applies MPC with step size 0.25 h. At time $t \in [0,48]$ h, the local cost function J_i considers the time window $[t, t+N_p]$ with prediction horizon $N_p = 6$ h and is designed as in Section 2.4 with cost parameters from Table 1. The values $C_i^{\mathrm{m,im}}$ and $C_i^{\mathrm{m,ex}}$, that describe the cost or revenue of power imports from or exports to the main grid, vary in the course of the day. For all microgrids i, we use the following fictitious values, which reflect typical market fluctuations with rising prices in the morning and evening hours, based on real prices by (Bundesnetzagentur Deutschland, 2021):

$$C_i^{\mathrm{m,im}}(t) = \begin{cases} 275 & \text{if } t\,\%\,24\,\mathrm{h} \in [15,20)\,\mathrm{h}, \\ 200 & \text{if } t\,\%\,24\,\mathrm{h} \in [6,9) \cup [20,22)\,\mathrm{h}, \\ 150 & \text{if } t\,\%\,24\,\mathrm{h} \in [9,15) \cup [22,24)\,\mathrm{h}, \\ 100 & \text{otherwise,} \end{cases}$$

$$C_i^{\mathrm{m,ex}}(t) = \begin{cases} 15 & \text{if } t\,\%\,24\,\mathrm{h} \in [15,20)\,\mathrm{h}, \\ 10 & \text{if } t\,\%\,24\,\mathrm{h} \in [6,9) \cup [20,22)\,\mathrm{h}, \\ 0 & \text{otherwise.} \end{cases}$$

Here, % denotes the modulo operator and $t\,\%\,24\,\text{h}$ indicates the time of day. One possible strategy to maximize revenue is to store energy at times of low prices for later export. Toward a resilient operation, the system is controlled using the adaptively robust distributed MPC scheme described in Algorithm 1. Based on the local control problems, each microgrid computes contracts $\mathcal{Z}_i^k$ for its coupling variables $z_i = \left(p_{ij}^{\text{tr}}\right)_{j\in\mathcal{N}_i}$ at each time k and shares them with its neighbors. To locally identify the unknown attack, a nonlinear optimization problem of the form (5) is solved at each sampling time to an accuracy of $\varepsilon_i = 10^{-3}$. Only *partial* observability of the states $x_i = \left(s_i, p_i^{\text{g}}, p_i^{\text{m}}, p_{ij}^{\text{tr}}, p_{ik}^{\text{tr}}\right)^{\mathrm{T}}$ with $g_i(x_i) = \operatorname{diag}(1,1,1,0,0)x_i$ is assumed. That means, for each microgrid i the outputs $y_i = (s_i, p_i^{\text{g}}, p_i^{\text{m}})^{\mathrm{T}}$ are considered by the local identification process, but not the transfer variables p_{ij}^{tr}, p_{ik}^{tr}. Based on the suspected attacks $a_i^{*,k}$, we approximate the uncertainty sets $\mathcal{A}_i^k$ as in eq. (6). The local control problems are repeatedly adapted to new contracts and identification results that become available in course of time. As a consequence, the computed inputs at time $k+1$ are robust toward neighboring couplings in $\mathcal{Z}_{\mathcal{N}_i}^k$ and identified attacks in $\mathcal{A}_i^k$. For comparison, we repeat each experiment with non-robust distributed MPC, where neither contracts are exchanged nor attack identification is considered.

We examine the behavior of the system in two attack scenarios, each with adaptively robust versus non-robust control. First, we assume that all generation units are dispatchable and an attack $a_1^{\text{g}} = 10\,\text{kW}$ disturbs the generator dynamics in microgrid 1 as in eq. (3). Later we will also consider uncertain renewable generation. The attack is present over the entire time window $[0,48]\,\text{h}$ and causes the generated power p_1^{g} in the attacked microgrid to deviate strongly from the control input u_1^{g}, see Figure 2. The local ADI method successfully identifies the attack in every time step, computing suspected attack values $a_1^{\text{g},*} \approx 9.9989$, which allows the adaptively robust MPC scheme to adjust its prediction. As a result, the control inputs are adapted and the microgrid makes use of the additionally generated power by storing it into the battery and exporting it to the main grid during times with high profit. In contrast, in the solution computed with non-robust MPC, the battery reaches and violates its maximum state of charge of 1 after about 5 h, see Figure 2. This is because due to the attack, more power than planned is generated and charged into the storage to maintain power balance. Since SoC values larger than 1 are invalid, the next MPC step starts with $s_1 = 1$, but as the attack is not identified, the full battery continues to be charged, resulting in bound violations in 171 of 192 steps.

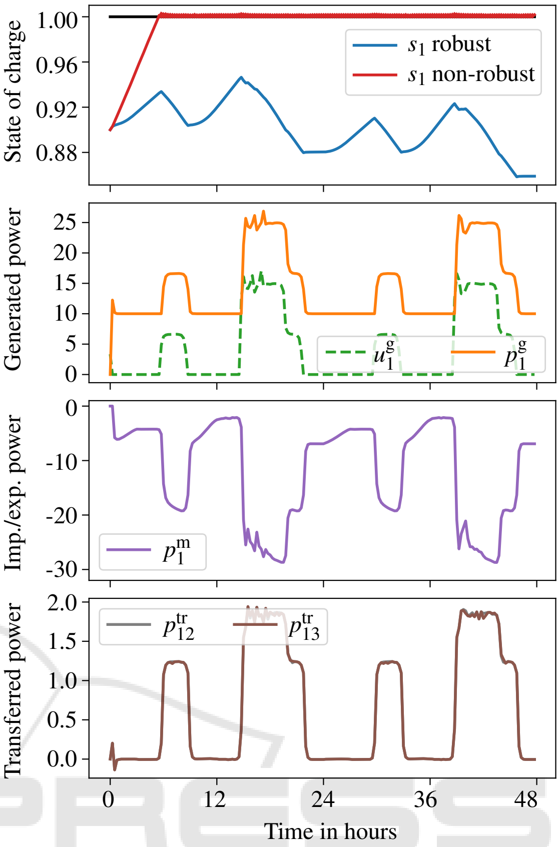

Figure 2: Selected state and input trajectories for microgrid 1 that is exposed to a generator attack, all powers in kW. The different SoC trajectories, computed by adaptively robust versus non-robust MPC, show the benefit of the proposed resilient control framework.

It should be mentioned that power balance can be ensured in other ways than using the storage as a buffer. If power exchange with the main grid is allowed at all times, using the main grid as a buffer would not cause bound violations like the above. However, this may result in very high costs if, for instance, power has to be imported at expensive prices in the evening. The battery, on the other hand, allows to store power until exports to the main grid become profitable. Indeed, over the entire time window, robust MPC achieves total costs of $-5.2\cdot 10^{3}$, thus making profit despite the attack, while non-robust MPC yields total costs of $2.3\cdot 10^{4}$, being orders of magnitudes larger.

In the second experiment, we modify the generator attack to $a_1^{\text{g}} = 10\,\text{kW} + r_1^{\text{g}}$ with renewable generation $r_1^{\text{g}} \sim \mathcal{N}(0,8)\,\text{kW}$, randomly drawn from a nor-

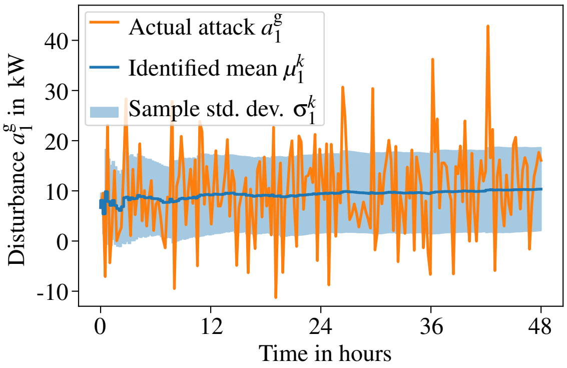

Figure 3: Course of the mean μ_1^k of identified values $a_1^{*,k}$ over time, with sample standard deviation σ_1^k. The actual disturbance $a_1^{\mathrm{g},k}$ at each time k is shown in orange.

mal distribution with mean 0 kW and standard deviation 8 kW, independently at each time. Attack and renewable generation together may cause more generated power than planned (if $a_1^{\mathrm{g}} > 0$) or less ($a_1^{\mathrm{g}} < 0$), but are chosen such that the total input $u_1^{\mathrm{g}} + a_1^{\mathrm{g}}$ is nonnegative. Due to the continually changing values for a_1^{g}, the ADI method identifies different values $a_1^{*,k}$ at each time step, but as Figure 3 shows, the mean value μ_1^k quickly settles at around 10 kW. Due to the fluctuating uncertainty, the three scenarios in multi-stage MPC are further apart than in the first experiment. Adaptively robust MPC computes a solution, shown in Figure 4, with total costs of $3.1 \cdot 10^3$ that is admissible for all scenarios, using the storage as a buffer to cope with the uncertainty. The non-robust approach again proves to be unsuitable to control the disturbed system as it computes a solution that violates state bounds in 113 steps and causes more than ten times higher total costs of $3.2 \cdot 10^4$.

5 CONCLUSION AND OUTLOOK

We introduced a distributed model for microgrids that are interconnected by dispatchable power transfers and influence neighboring systems through coupling variables. The model considers possible disturbances in the form of input attacks or uncertain renewable generation. We applied a previously presented resilient control framework, combining multi-stage robust MPC with optimization-based methods to identify unknown attacks. It is designed for distributed systems, where each component has (only) access to a local dynamic model and transmits information about predicted coupling values to its neighbors. In numerical experiments, the method has proven to be suitable for microgrids under attack, even if renewables cause additional uncertainty. We plan to extend existing ADI methods toward distributed identification schemes, where the exchange of suitable information allows microgrids to identify not only local disturbances, but even attacks on neighboring microgrids.

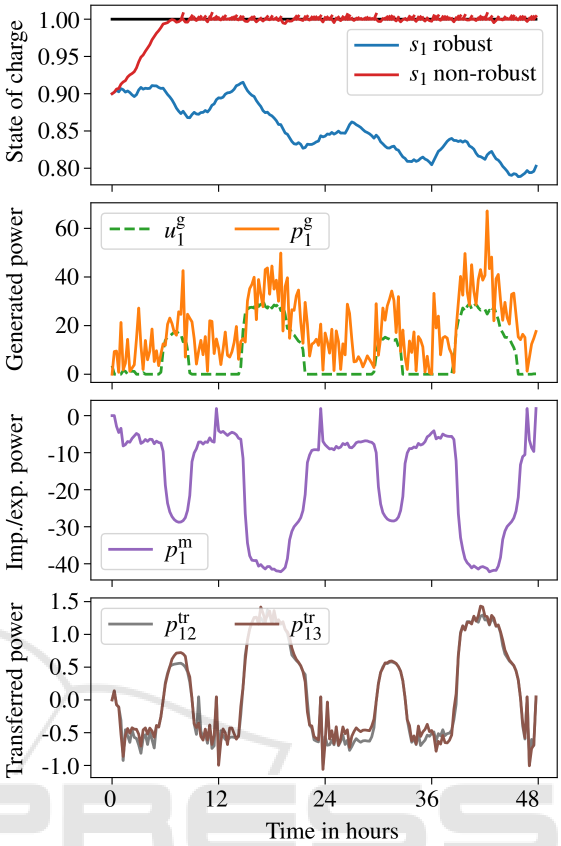

Figure 4: States and inputs in microgrid 1, which now contains renewable generation as another source of uncertainty in addition to the generator attack.

ACKNOWLEDGEMENTS

This work was supported by the German Federal Ministry of Education and Research (BMBF) via the funded research project AlgoRes (01S18066B).

REFERENCES

Ananduta, W., Maestre, J., Ocampo-Martinez, C., and Ishii, H. (2020). Resilient distributed model predictive control for energy management of interconnected microgrids. *Optimal Control Applications and Methods*, 41:146–169.

Arauz, T., Chanfreut, P., and Maestre, J. (2021). Cybersecurity in networked and distributed model predictive control. *Annual Reviews in Control*.

Braun, S., Albrecht, S., and Lucia, S. (2020). Hierarchical attack identification for distributed robust nonlinear control. In *21st IFAC World Congress*, pages 6191–6198.

Braun, S., Albrecht, S., and Lucia, S. (2021a). Adaptively robust nonlinear model predictive control based on attack identification. Accepted for publication in at-Automatisierungstechnik, preprint at https://tu-dortmund.sciebo.de/s/w8IPet5jfxJaEaW.

Braun, S., Albrecht, S., and Lucia, S. (2021b). Attack identification for nonlinear systems based on sparse optimization. *IEEE Transactions on Automatic Control*. early access.

Bundesnetzagentur Deutschland (2021). SMARD Strommarktdaten for Germany in November 2021. https://www.smard.de/home/downloadcenter/download-marktdaten. Online, last accessed: November 18th, 2021.

Gallo, A., Turan, M., Boem, F., Parisini, T., and Ferrari-Trecate, G. (2020). A distributed cyber-attack detection scheme with application to DC microgrids. *IEEE Transactions on Automatic Control*, pages 3800–3815.

Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N., Sandberg, H., and Candell, R. (2018). A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys*, 51:76:1–76:36.

Lucia, S., Finkler, T., and Engell, S. (2013). Multi-stage nonlinear model predictive control applied to a semi-batch polymerization reactor under uncertainty. *Journal of Process Control*, 23:1306–1319.

Lucia, S., Kögel, M., and Findeisen, R. (2015). Contract-based predictive control of distributed systems with plug and play capabilities. *IFAC-PapersOnLine*, 48:205–211.

Mathieu, J. and Taylor, J. (2016). Controlling nonlinear batteries for power systems: Trading off performance and battery life. In *IEEE Power Systems Computation Conference*, pages 1–7.

Mayne, D., Seron, M., and Raković, S. (2005). Robust model predictive control of constrained linear systems with bounded disturbances. *Automatica*, 41:219–224.

Mohammed, A., Refaat, S., Bayhan, S., and Abu-Rub, H. (2019). AC microgrid control and management strategies: evaluation and review. *IEEE Power Electronics Magazine*, 6:18–31.

Olivares, D., Mehrizi-Sani, A., Etemadi, A., Cañizares, C., Iravani, R., et al. (2014). Trends in microgrid control. *IEEE Transactions on Smart Grid*, 5:1905–1919.

Pan, W., Yuan, Y., Sandberg, H., Gonçalves, J., and Stan, G. (2015). Online fault diagnosis for nonlinear power systems. *Automatica*, 55:27–36.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58:2715–2729.

Wang, Y. and Ishii, H. (2019). A distributed model predictive scheme for resilient consensus with input constraints. In *IEEE Conference on Control Technology and Applications*, pages 349–354.

Zhang, C., Jiang, J., Zhang, L., Liu, S., Wang, L., and Loh, P. (2016). A generalized SOC-OCV model for lithium-ion batteries and the SOC estimation for LN-MCO battery. *Energies*, 9:900:1–900:16.