An Invariant Set Construction Method, Applied to Safe Coordination of Thermostatic Loads

Sunho Jang, Student Member, IEEE, Necmiye Ozay, Senior Member, IEEE, and Johanna L. Mathieu, Senior Member, IEEE

Abstract—We consider the problem of coordinating a collection of switched subsystems under both local and global constraints for safe operation of the system. Although an invariant set can be leveraged to construct a safety-guaranteed controller for this kind of problem, computing an invariant set is not scalable to high-dimensional systems. In this article, we introduce a strategy to obtain an implicit representation of a controlled invariant set for a collection of switched subsystems and construct a safety-guaranteed controller to coordinate the subsystems using the representation. Specifically, we incorporate the invariant set into a model predictive controller to coordinate the subsystems and global constraints on their collective behavior. In order to guarantee safety, we can use an algorithm that keeps the state inside a controlled invariant set [1], [2], [3]. Some previous works [4], [5], [6] have incorporated invariant sets into model predictive control (MPC), resulting in controllers with both safety and recursive feasibility guarantees, which means that actions taken over time by the controller will lead to feasible optimization problems in every time step.

However, these methods of invariant set computation are not scalable; obtaining an explicit form of an invariant set requires a projection from a higher dimensional state space to a lower-dimensional one, which is computationally burdensome. Some recent studies [7], [8] propose scalable algorithms to compute invariant sets for linear systems. However, these algorithms are neither scalable enough for high-dimensional systems nor applicable to switched systems, which have discrete inputs or modes. The method introduced in [9] computes an invariant set for a switched linear system; however, it is also not sufficiently scalable to deal with high-dimensional systems.

In this work, we develop a scalable method to construct a controlled invariant set for a large collection of switched subsystems and synthesize a control algorithm with formal safety guarantees by incorporating the invariant set. We develop an approach to obtain an implicit representation of an invariant set of a high-dimensional system and incorporate that representation into an MPC algorithm to provide guarantees on safety and recursive feasibility. Crucially, this strategy allows us to avoid the heavy computational burden imposed by the projection step so that our approach is applicable to a high-dimensional system.

Our problem is motivated by the application-domain problem of coordinating a collection of hundreds or thousands of thermostatically controlled loads (TCLs) to balance supply and demand on the grid. For safety, the controller should be designed to enforce not only local constraints on each TCL but also network-level safety constraints. Many previous papers [10], [11], [12], [13], [14] have proposed approaches that satisfy the local TCL constraints, but the safety of the distribution network (e.g., voltages maintained within their limits) is not generally considered. Some works [15], [16], [17] deal with network safety by incorporating network-level constraints using optimal power flow approaches, but the recursive feasibility of the optimization problem is not guaranteed. In contrast, our approach explicitly ensures recursive feasibility and, therefore, safety.

The main contributions of our article are threefold. First, we develop a method for finding an implicit representation of an invariant set of a system composed of a large number of heterogeneous subsystems with global constraints on their collective behavior and local constraints including lockout constraints, which require a subsystem to keep its current mode for a certain time duration after a switch. Second, we propose a control algorithm with safety guarantees by incorporating the implicit representation of the invariant set. Third, we apply the proposed approach to the coordination of TCLs for frequency regulation.
while limiting aggregate power consumption to ensure network safety. We use a distribution network model to demonstrate how our controller avoids voltage violations. This article significantly extends our preliminary work [18], which only considered homogeneous subsystems without lockout constraints and did not explicitly model the network. Here, we benchmark our results against several other control approaches, including the approach we proposed in [18] to demonstrate the importance of modeling lockout.

The rest of this article is organized as follows. In Section II, we describe the application-domain problem. In Section III, we detail the abstraction and aggregate system construction. In Section IV, we propose our novel invariant set construction method. In Section V, we propose our safety-guaranteed control algorithm. Numerical simulation results are given in Section VI. Finally, Section VII concludes this article. Proofs are presented in the Appendix.

**Notations:** We write row vectors of ones as 1. The lth element of vector $c$ is denoted as $c_j$. We denote the set of nonnegative integers as $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Also, $[X]$ refers to the set of the integers $\{1, \ldots, X\}$, and $[X]_0$ denotes $[X] \cup \{0\}$. Floor and ceiling functions are represented by $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$, respectively. The indicator function on set $A$ is denoted as $\mathbb{1}_A$. We denote the Minkowski sum by $A \oplus B = \{a + b \mid a \in A, b \in B\}$, and the subtraction $A \ominus B$ is defined as the largest solution to $X \ominus B = A$. Also, $\|\cdot\|$ refers to the infinity norm. The ball with radius $r$ centered at $\theta$ is denoted as $B(\theta, r) := \{x \mid \|x - \theta\| \leq r\}$. The identity function in space $\mathbb{R}^d$ is denoted as $\text{Id}_{\mathbb{R}^d}$.

**II. APPLICATION-DOMAIN PROBLEM SETTING**

We consider a power reference tracking control problem for a collection of TCLs, such as air conditioners, which switch ON/OFF to maintain a temperature within a dead-band, i.e., a small range around a setpoint. Most residential air conditioning systems in the USA are TCLs versus variable speed systems. Each TCL is a switched subsystem, which collectively makes up a system. The control problem is to switch ON/OFF individual TCLs to cause power consumption of the collection to track a signal, e.g., a scaled and shifted frequency regulation signal while ensuring local constraints are satisfied. First, the temperature of each TCL should remain within its dead-band. Second, the ON/OFF mode of each TCL should be maintained for a certain duration after a switch to ensure that the compressor is not damaged; this constraint is called a lockout constraint [14]. There are several approaches that have been developed to handle lockout, e.g., [13]; though to the best of the authors’ knowledge, none ensures recursive feasibility and safety.

Manipulating the aggregate power consumption of TCLs could cause constraint violations in the distribution network, e.g., over/undervoltages and transformer overloading. One way to avoid these violations is to impose minimum and maximum bounds on the aggregate power consumption of the collection of TCLs, i.e., network-level safety constraints. A variety of recent papers have developed approaches to compute bounds on network-safe changes in power consumption/production of distributed energy resources [19], [20], [21], [22]. Assuming that we can compute conservative bounds with one of these methods, controlling TCLs such that their aggregate power consumption remains within these bounds should guarantee network safety. Therefore, the collection of TCLs should commit to providing a regulation capacity (i.e., the range over which it can manipulate its aggregate power consumption) within the network-safe bounds. However, if the TCLs prioritize maintaining temperatures within dead-bands, attempting to track an aggressive signal within those bounds (e.g., a signal that stays at either bound for a long duration) can eventually render the signal untrackable and can cause the TCL aggregate power consumption to violate the bounds.

To clarify this issue, we must first describe our assumed control architecture. There are many possible architectures for network-safe TCL participation in electricity markets, but here, we consider one in which a third-party aggregator coordinates TCLs subject to network-safe power bounds provided by the utility. Fig. 1 shows the interaction of the aggregator, utility, and independent system operator (ISO). Based on the forecast of the network states, the utility uses its network model (which we assume it has) to compute the range of TCL power consumption that can be safely accommodated by the network and sends it to the aggregator. The bounds are used by the aggregator to make an offer for regulation capacity, which is expected to be safe. The ISO commits the aggregator at or below its offered capacity. In real time, the ISO generates a normalized regulation signal (ranging from $-1$ to $1$, with $0$ corresponding to a resource’s scheduled or nominal operating point), and the aggregator 1) scales it by its committed capacity, 2) shifts it by the TCL collection’s nominal load, and 3) controls the modes of TCLs to track it. Some U.S. ISOs have designed mechanisms to constrain regulation signals to reduce the chance of aggressive signals in an effort to support the use of energy-constrained resources, such as energy storage and TCLs [23], [24]. However, many ISOs do not have these mechanisms, and so a TCL collection attempting to track an aggressive signal with a simple tracking controller may violate the network-safe power bounds.

This is even more likely to happen if real-time network states differ from their forecasts and the actual network-safe bounds are tighter than those generated with the forecasts. Fig. 2 provides an example of this situation, where the dashed black lines are the power bounds obtained in advance that are used to determine the committed capacity, and the solid black lines are the actual network-safe power bounds computed in real time. The red reference signal (a scaled and shifted frequency regulation signal from the PJM interconnection [25]) is scaled to the committed power bounds and is impossible to track while ensuring network safety. We assume that network safety takes precedence over tracking performance; specifically, the aggregator should track the regulation signal as closely as possible within the tighter bounds, i.e., the blue signal in Fig. 2. PJM uses a mechanism to constrain the integral of the normalized signal (i.e., the energy
content of the signal), meaning that tracking the red signal is unlikely to cause power bound violations. However, the bound tightening in Fig. 2 makes the blue signal much harder to track; attempting to track it with a simple tracking controller would cause average aggregate power consumption to decrease from nominal, eventually rendering the signal untrackable as TCLs struggle to cool/heat sufficiently. Eventually, many TCLs may need to be on simultaneously violating the network-safe power bound. We will benchmark our approach against a simple tracking controller in Section V.

We next detail the problem formulation. We consider a collection of TCLs that are clustered into multiple groups based on their similarity in terms of thermal/electrical parameters and ambient temperatures, and we treat TCLs in the same group as homogeneous. To do this, the amount of deviations allowed between TCLs in the same group is small enough so that we can construct a bisimilar abstraction for each group; details are given in Section III-B. Our method also allows for sufficiently small process noise and variation in ambient temperature, but our mathematical development assumes no process noise and constant ambient temperature to simplify the exposition of the main results. Considering multiple groups allows us to deal with TCL heterogeneity, which we did not consider in our preliminary work [18].

Let the number of groups of homogeneous TCLs be \( g_{\text{TCL}} \), the total number of TCLs across all groups be \( N_{\text{TCL}} \), and the number of TCLs in group \( i \) be \( N_{\text{TCL}}^{(i)} \); hence, \( \sum_{i=1}^{g_{\text{TCL}}} N_{\text{TCL}}^{(i)} = N_{\text{TCL}} \). The internal temperature of the \( j \)th TCL in group \( i \) at time \( t \) is denoted by \( T_{j}^{(i)}(t) \), and its domain is \([T_{\text{min}}^{(i)}, T_{\text{max}}^{(i)}]\). Also, the ON/OFF mode of each TCL is \( \mu_{j}^{(i)}(t) \), which is 0 if it is not consuming power (OFF), and 1 if it is consuming power (ON). Then, we assume that the internal temperature evolution follows the affine model developed in [26] as follows:

\[
T_{j}^{(i)}(t+1) = a_{j}^{(i)} T_{j}^{(i)}(t) + \left(1 - a_{j}^{(i)}\right) \left(\bar{r}(i) - R(i) p_{a}^{(i)} \mu_{j}^{(i)}(t)\right).
\] (1)

Here, \( a^{(i)} \) is the ambient temperature (e.g., for air conditioners, this would be the outside temperature) of TCLs in group \( i \) and \( \bar{r}^{(i)} \) is \( \exp(-\Delta t/(R(i) C^{(i)}) \), where \( \Delta t \) is the sampling time, \( R(i) \) is the thermal resistance, and \( C^{(i)} \) is the thermal capacitance of every TCL in group \( i \). Parameter \( p_{a}^{(i)} \) is the thermal energy transfer rate, which is positive for a cooling TCL and negative for a heating TCL; since, here, we assume all TCLs are air conditioners, the value is positive. The power consumption of each TCL in group \( i \) when it is in ON mode, denoted as \( p^{(i)} \), equals \( p_{a}^{(i)}/\bar{r}^{(i)} \), where \( \bar{r}^{(i)} \) is the coefficient of performance. Then, the aggregate power consumption of all TCLs, denoted as \( P_{agg}(t) \), equals \( \sum_{i=1}^{g_{\text{TCL}}} \sum_{j=1}^{N_{\text{TCL}}^{(i)}} p_{j}^{(i)}(t) \).

We next define the local constraints. The temperature dead-band of group \( i \) is \([T_{\text{min}}^{(i)}, T_{\text{max}}^{(i)}]\), which leads to the constraint \( T_{j}^{(i)}(t) \in [T_{\text{min}}^{(i)}, T_{\text{max}}^{(i)}] \forall t \in \mathbb{N}_{0}, i \in [g_{\text{TCL}}], j \in [N_{\text{TCL}}^{(i)}] \). (2)

We assume that temperature setpoints and dead-bands are constant over time.

In addition, a lockout constraint on every TCL requires it to remain in the same mode for a specific duration after a switch; imposing this constraint is a key extension from our preliminary work [18]. Suppose that the mode of every TCL in group \( i \) should be kept for \( t_{\text{off}}^{(i)} \) after it is turned off and for \( t_{\text{on}}^{(i)} \) after it is turned on. Then, the number of time steps TCL should be locked after a switch for each mode is computed as

\[
\tau_{\text{off}}^{(i)} = \left[T_{\text{off}}^{(i)}, t_{\text{off}}^{(i)}\right] \quad \tau_{\text{on}}^{(i)} = \left[T_{\text{on}}^{(i)}, t_{\text{on}}^{(i)}\right].
\]

Now, let \( t_{\text{off}}^{(i)}(t) \) be the last step time the \( j \)th TCL in group \( i \) switched its mode to OFF/ON. Then, the input sequence \( \mu_{j}^{(i)}(t) \) should satisfy the following:

\[
\mu_{j}^{(i)}(t) = 0 \quad \text{if} \quad t < t_{\text{off}}^{(i)}(t) + \tau_{\text{off}}^{(i)} \quad \text{and} \quad \mu_{j}^{(i)}(t) = 1 \quad \text{if} \quad t < t_{\text{off}}^{(i)}(t) + \tau_{\text{on}}^{(i)}.
\]

Next, we define the global constraint, which ensures the safety of the distribution network. Specifically, we bound the aggregate power consumption

\[
P_{agg} \leq P_{agg}(t) = \sum_{i=1}^{g_{\text{TCL}}} \sum_{j=1}^{N_{\text{TCL}}^{(i)}} p_{j}^{(i)}(t) \leq P_{agg} \quad \forall t \in \mathbb{N}_{0} \quad (4)
\]

where \( P_{agg} \) and \( P_{agg} \) are the upper and lower power bounds, respectively.

Finally, our goal is to control the modes of the TCLs so that the aggregate power consumption \( P_{agg}(t) \) of all TCLs tracks the reference signal \( r(t) \) as closely as possible while satisfying all constraints. Then, the problem of interest is as follows.

**Problem 1:** Given the system described earlier, synthesize a controller to choose \( \mu_{j}^{(i)}(t) \) for all \( i = 1, \ldots, g_{\text{TCL}} \), \( j = 1, \ldots, N_{\text{TCL}}^{(i)} \), and \( t \in \mathbb{N}_{0} \) that guarantees the satisfaction of constraints (2)–(4) while trying to minimize the performance measure \( |P_{agg}(t) - r(t)| \).

**III. ABSTRACTION AND AGGREGATION OF A COLLECTION OF SWITCHED SUBSYSTEMS**

In this section, we consider an abstract problem where the goal is to coordinate a collection of switched subsystems, clustered into groups based on the similarity of their dynamics, subject to the constraints that are generalized versions of (2)–(4). After we introduce this general problem setup, we explain how to
construct an abstraction with discrete states from the original continuous-state subsystems in each group. This abstraction is then used to model an “aggregate system,” representing the dynamics, which we use to synthesize a safety-guaranteed controller.

Using aggregate dynamics to represent collections of TCLs is not a new idea [10], [11], but works that aim to characterize the relation between the aggregate dynamics and the actual collection are more recent. Soudjani and Abate [27] abstract a TCL as a Markov chain and probabilistically quantify the difference between the dynamics of the underlying collection and its aggregate model. In contrast, our approach provides deterministic bounds using approximate bisimulation relations. Furthermore, their model is different because the mode of each TCL is assumed to be uncontrollable; instead, their input is the temperature setpoint. Nilsson and Ozay [28] used a similar approach to ours to construct abstractions and an aggregate system, but it considers continuous-time subsystems and develops open-loop control signals, whereas we consider discrete-time subsystems and propose an algorithm to compute invariant sets, which can be used to ensure the safety of arbitrary feedback controllers. The abstraction and aggregation methods from our preliminary work [18] are only applicable to collections of homogeneous subsystems, whereas here we consider heterogeneous subsystems. In addition, none of the aforementioned approaches consider lockout constraints, as we do here.

A. Abstract Problem Formulation

First, the transition system formalism is introduced to model discrete-time dynamics. The definitions in this section follow the work in [29].

**Definition 1:** A transition system $T$ is a tuple $(X, U, Y)$, where $X$ is a set of states, $U$ is a set of actions, $X \times U \times X$ is a transition relation, and $Y : X \rightarrow \mathbb{R}^n$ is an output function.

We denote $(x, u, x') \in T$ as $x \xrightarrow{u} x'$ for short.

**Definition 2:** Given a transition system $T = (X, U, Y)$, a safe set $X_{\text{safe}} \subseteq X$, and a set of admissible input constraints $U_{\text{safe}} \subseteq U$, a set $X_{\text{inv}}$ is a controlled invariant set with respect to $(T, X_{\text{safe}}, U_{\text{safe}})$ if $X_{\text{inv}} \subseteq X_{\text{safe}}$, and for all $x \in X_{\text{inv}}$, there exists $u \in U_{\text{safe}}$ such that for all $x'$ with $x \xrightarrow{u} x'$, we have $x' \in X_{\text{inv}}$. The union of all controlled invariant sets with respect to $(T, X_{\text{safe}}, U_{\text{safe}})$ is called the maximal controlled invariant set for $(T, X_{\text{safe}}, U_{\text{safe}})$.

We consider a system that includes multiple groups of homogeneous switched subsystems. Here, the number of groups is $g$, the number of subsystems in group $i$ is $N(i)$, the total number of subsystems across all groups is $N = \sum_{i=1}^{g} N(i)$, and the number of modes is $M$.

For any $i \in [g]$ and $j \in [N(i)]$, let $S^{(i)}_j$ be the $j$th subsystem of group $i$, and $\theta^{(i)}_j(t)$ be its state at time step $t$, where $\Theta^{(i)} \subseteq \mathbb{R}^d$ is a compact domain. The difference equation governing the evolution of $\theta^{(i)}_j(t)$ is

$$S^{(i)}_j : \theta^{(i)}_j(t + 1) = f^{(i)}_j(\theta^{(i)}_j(t), \mu^{(i)}_j(t)), \quad \mu^{(i)}_j : \mathbb{N}_0 \rightarrow [M]$$

where $f^{(i)}_j(t)$ is the mode of $j$th subsystem in group $i$ at time $t$ and is also the control input. For TCLs, $\theta^{(i)}_j$ corresponds to $T^{(i)}_j$ and $f^{(i)}$ corresponds to the affine dynamics in (1). For the rest of this section, we drop the index $j$ for convenience.

The discrete-time dynamics $S^{(i)}_j$ in (5) can be equivalently represented as a transition system

$$S^{(i)}_j = \left( \Theta^{(i)}_j, [M], \rightarrow^{(i)}_j, \text{Id}_{R^d} \right)$$

where $\theta \xrightarrow{\mu^{(i)}_j} \theta'$ if and only if $\theta' = f^{(i)}(\theta, \mu)$.

To formally describe each group of subsystems, we introduce the following definition of a product transition system.

**Definition 3:** Given $N$ identical copies of a transition system $T = (X, U, Y)$, the product transition system is given by $T \times N = (X \times N, U \times N, Y \times N)$, where

$$(x_1, \ldots, x_N) \xrightarrow{u_{11}, \ldots, u_{NN}} (x_{1}', \ldots, x_{N}')$$

if and only if $x_i \xrightarrow{u_i} x_i'$ for all $i \in [N]$, and $Y \times N : (x_1, \ldots, x_N) \rightarrow (Y(x_1), \ldots, Y(x_N))$.

According to the definition before, group $i$ can be represented by the product transition system $S^{(i)} \times N^{(i)}$. Furthermore, the entire system can be represented as the product of those systems, denoted as $S := (S^{(1)} \times N^{(1)}) \times \cdots \times (S^{(g)} \times N^{(g)})$ with the set of states $\Theta := (\Theta^{(1)} \times N^{(1)}) \times \cdots \times (\Theta^{(g)} \times N^{(g)})$.

Now, we introduce the constraints imposed on $S$. First, the state $\theta_j^{(i)}$ of each subsystem in group $i$ should stay in the safe set $\Theta_{\text{safe}}^{(i)}$ which corresponds to (2) in the TCL problem, i.e.,

$$\theta_j^{(i)}(t) \in \Theta_{\text{safe}}^{(i)} \quad \forall j \in [N^{(i)}], t \in \mathbb{N}_0. \quad (7)$$

Second, each subsystem in group $i$ cannot switch again for $\tau_m^{(i)}$ time steps after its mode is switched to $m$ [which corresponds to the lockout constraints (3) in the TCL problem], and so the input sequence $\mu_j^{(i)}(t)$ of each subsystem should satisfy

$$\mu_j^{(i)}(t) = m \quad \text{if} \quad t < \tau_j^{(i),m}(t) + \tau^{(i)}_m \quad \forall m \in [M] \quad (8)$$

where $\tau_j^{(i),m}(t)$ is the last time step, and the subsystem $S_j^{(i)}$ switched its mode to $m$ (i.e., $\mu_j^{(i)}(\tau_j^{(i),m}(t)) = m, \mu_j^{(i)}(\tau_j^{(i),m}(t) - 1) \neq m$). Third and finally, we impose bounds on a linear combination of the number of subsystems in each mode $m$ in each group $i$ [which corresponds to (4) in the TCL problem] as follows:

$$P_m \leq \sum_{i=1}^{g} P_m^{(i)} \sum_{j=1}^{N^{(i)}} 1_m(\mu_j^{(i)}(t)) \leq P_m \quad \forall m \in [M], t \in \mathbb{N}_0 \quad (9)$$

where $p_m^{(i)}$ is a scalar corresponding to subsystems in mode $m$ in group $i$, and $\sum_{j=1}^{N^{(i)}} 1_m(\mu_j^{(i)}(t))$ is the number of subsystems in mode $m$ in group $i$.

In addition, we assume a time-varying cost function $c_t : \mathbb{N}_0^d \rightarrow \mathbb{R}$, which depends on the number of subsystems in each mode in each group. Then, the generalized problem is as follows.

**Problem 2:** Given a collection of subsystems $S_j^{(i)}$ as described earlier, synthesize a controller to choose $\mu_j^{(i)}(t)$ for all $i = 1, \ldots, g$, $j = 1, \ldots, N^{(i)}$, and $t \in \mathbb{N}_0$ that guarantees the
satisfaction of constraints (7)–(9) while trying to minimize a cost function $c_s$.

B. Abstracts

In this section, we introduce the abstraction of each subsystem $S_j^i$. We consider the following notion of closeness to the original subsystem.

**Definition 4**: Two transition systems $T_1 = (X_1, U, \rightarrow, Y_1)$ and $T_2 = (X_2, U, \rightarrow, Y_2)$ are $\epsilon$-approximately bisimilar if there exists a relation $R \subset X_1 \times X_2$ such that the sets $R_{1\rightarrow 2} = \{x_1 : (x_1, x_2) \in R\}$ and $R_{2\rightarrow 1} = \{x_2 : (x_1, x_2) \in R\}$ are nonempty for all $x_1$ and $x_2$, and such that for all $(x_1, x_2) \in R$, all of the following are satisfied.

1) $\|Y_1(x_1) - Y_2(x_2)\| \leq \epsilon$.
2) If $x_1 x_1' \in R$, there exists $x_2 x_2' \in R$ s.t. $(x'_1, x'_2) \in R$.
3) If $x_2 x_2' \in R$, there exists $x_1 x_1' \in R$ s.t. $(x'_1, x'_2) \in R$.

To guarantee the existence of a bisimilar abstraction for the subsystems in each group, the following assumption is made.

**Assumption 1**: For every $i \in [g], m \in [M], f_i^m(\cdot, m)$ is a local contraction, that is, there exists constants $L_m^i \in [0, 1], c_m^i > 0$ such that

$$\|f_i^m(\theta_1, m) - f_i^m(\theta_2, m)\| \leq L_m^i \|\theta_1 - \theta_2\|$$

(10)

for every $\theta_1, \theta_2 \in \Theta_i$ with $\|\theta_1 - \theta_2\| \leq c_m^i$.

This assumption holds for the temperature dynamics in (1).

Now, we construct an abstraction of $S_i^j$ for every $i \in [g]$ by uniformly discretizing $\Theta_i$. For a given grid size $\eta$, the abstraction function $\gamma_\eta : \mathbb{R}^d \rightarrow \mathbb{R}^d$ is defined as

$$\gamma_\eta(\theta) = \eta \left( \frac{\theta}{\eta} \right) + \frac{1}{2}.$$  

(11)

Suppose that the grid size for the abstraction corresponding to group $i$ is $\eta_i^g$, and define the set $\Xi^i := \gamma_\eta_i(\Theta_i^g) = \xi_1^i, \ldots, \xi_{K_i^g}^i$, where $K_i^g$ is the number of elements $\xi_k^i$. Then, an abstraction for $S_i^j$ is

$$S_i^{\eta_i^g} = \left( \Xi^i, [M], \gamma_\eta^i, \text{Id}_{\mathbb{R}^d} \right)$$

(12)

where $\xi \xrightarrow{(\eta_i^g)} \xi'$ if and only if $\gamma_\eta^i(f^i(\xi, \mu)) = \xi'$. This means that the transition relation between the states of $S_i^{\eta_i^g}$ is determined by propagating each grid point $\xi$ with the dynamics and finding the closest grid point $\xi'$ to where it reaches in one time step, as shown in Fig. 3. The abstraction of each subsystem $S_j^i$ is denoted as $S_j^{\eta_i^g}$, and its state is denoted as $\xi_j^i$. For simplicity, we drop the superscript $(i)$ from $\eta_i^g$ when not crucial.

The following lemma, which follows from [28, Prop. 1], states a condition for $S_i^j$ and $S_i^{\eta_i^g}$ to be bisimilar.

**Lemma 1**: If $\epsilon$ and $\eta$ are such that $(1 - L_m^i) \epsilon \geq \eta_i^g/2$ for all $m \in [M]$, then $S_i^j$ and $S_i^{\eta_i^g}$ are $\epsilon$-approximately bisimilar.

If $S_i^j$ and $S_i^{\eta_i^g}$ are $\epsilon$-approximately bisimilar, the states of $S_i^j$ and $S_i^{\eta_i^g}$ remain $\epsilon$-close (i.e., $\|\theta(t) - \xi(t)\| \leq \epsilon$) if the same input sequence is applied to both systems from the initial state $\theta(0)$, which satisfies $|\theta(0) - \xi(0)| \leq \epsilon$.

By Assumption 1, we can show that, for any $0 < \epsilon < \min_{m \in [M]} \frac{\epsilon_m^i}{2}$, there is a small enough $\eta_i^g > 0$ that satisfies the condition in Lemma 1. Moreover, even when small disturbances, parameter variations, or time variations in the state dynamics of subsystems within the same group exist, a single $\epsilon$-approximately bisimilar system for the entire group can be constructed. In particular, for any $m \in [M]$, let $\overline{\eta}_m$ be a constant, which satisfies $1 - L_m^i \epsilon \geq \frac{\eta_i^g}{2} + \overline{\eta}_m$. Then, any time-varying subsystem, whose state evolution function $f_i(\theta, m, t)$ satisfies

$$\|f_i(\theta, m, t) - f_i(\theta, m)\| \leq \overline{\eta}_m \forall \theta \in \Theta_i, m \in [M], t \in [0, t]$$

is also $\epsilon$-approximately bisimilar to $S_i^{\eta_i^g}$. This allows for mild heterogeneity and time variation in the state dynamics of the subsystems within a group as long as the state evolution function of every subsystem in the group satisfies the previous inequality at every time step.

The abstraction of each group $i$ can be represented by the product transition system $S_i^{\eta_i^g} \times X_i$, and the abstraction of the entire system can be represented as the product of those systems, denoted as $S_i^g := S_i^{\eta_i^g} \times X_i$. By Definition 4, it is easy to see that $S_i^g$ and $S_i^{\eta_i^g}$ are $\epsilon$-approximately bisimilar if $S_i^j$ and $S_i^{\eta_i^g}$ are $\epsilon$-approximately bisimilar for all $i \in [g]$. Then, we can show the following theorem.

**Theorem 1**: Assume that $S_i^j$ and $S_i^{\eta_i^g}$ are $\epsilon$-approximately bisimilar and $\delta$ is larger than $\epsilon + \frac{\eta_i^g}{2}$. If the abstracted subsystem $S_j^{\eta_i^g}$ starting at $\xi_0$ stays inside $\gamma_\eta^i(\Theta_i^g \cap B(0, \delta))$ under an input trajectory $\mu_j^i(t)$, then for every $\theta \in \Theta_i$ satisfying $\|\theta(t) - \xi_0\| \leq \epsilon$, the trajectory of $S_j^i$ starting at $\theta(0)$ stays inside the safe set $\Theta_i^{\text{safe}}$ under $\mu_j^i(t)$.

This theorem states that if we can obtain an input sequence for an abstracted subsystem that keeps its state inside a safe set...
shrunken by $\delta > \epsilon + \eta(i)/2$, then the input sequence is also safe for the original subsystem.

Using Theorem 1, we define the safe set for the abstracted subsystem as $\Xi_{\text{safe}}^{(i)} := \gamma_{\text{afe}}(\Theta_{\text{afe}}) \in B(0, \delta)$ and impose the following local constraints on the abstracted subsystems:

$$
\xi_j^{(i)}(t) \in \Xi_{\text{safe}}^{(i)} \quad \forall i \in [g], \quad j \in [N^{(i)}], \quad t \in \mathbb{N}_0. \quad (13)
$$

Fig. 3 illustrates how $S^i_{\text{afe}}$ and its set of safe states $\Xi_{\text{afe}}^{(i)}$ are constructed.

Now our goal is to develop a safe control algorithm for the abstracted subsystems satisfying (13).

C. Aggregate System

We now construct an aggregate system for each group as an alternative representation of $S^i_{\text{afe}} \times N^{(i)}$. An aggregate system is a compact representation that keeps track of the number of subsystems in each possible combination of mode, state, and lockout duration (i.e., the number of time steps it has been locked in its current mode). The input to an aggregate system is the number of subsystems that switch modes, which can be used to determine the modes of the individual subsystems. To construct an aggregate system, we build a graph for each group that captures all possible transitions of the subsystem $S^i_{\text{afe}}$ for all combinations of mode, state, and lockout duration. In particular, we extend the graph construction method from our preliminary work [18] by considering the lockout duration as an additional feature of a node. Then, the graph is used to express how the number of subsystems at each possible combination evolves, which acts as the dynamics of the aggregate system.

We first construct a graph for the state-abstracted subsystem $S^i_{\text{afe}}$, i.e., $G^{(i)} = (V^{(i)}, E^{(i)})$, where $V^{(i)}$ are the vertices and $E^{(i)}$ are the edges. Each node is denoted by $\nu^{(i)}_{m,\tau,k}$ ($m \in [M], \tau \in [T^{(i)}], k \in [K^{(i)}]$); when $S^i_{\text{afe}}$ is at state $\xi^{(i)}_k$ in mode $m$, and with lockout duration $\tau$, we say that $S^i_{\text{afe}}$ “corresponds to” $\nu^{(i)}_{m,\tau,k}$. Edges are defined for any possible autonomous or controlled transition between nodes; specifically, $(\nu^{(i)}_{m_1,\tau_1,k_1}, \nu^{(i)}_{m_2,\tau_2,k_2})$ belongs to $E^{(i)}$ if $\xi^{(i)}_{k_1} \xrightarrow{m_2}{(i),\eta} \xi^{(i)}_{k_2}$ and one of the following holds.

1) $m_1 = m_2$ and $\tau_1 = \tau_2 = 0$ (system is unlocked and its mode remains unchanged).
2) $m_1 = m_2$, $\tau_1 > 0$, and $\tau_2 = \tau_1 + 1$ (system is locked and lockout duration is updated).
3) $m_1 = m_2$, $\tau_1 = \tau^{(i)}_{m_1}$ and $\tau_2 = 0$ (system becomes unlocked).
4) $m_1 \neq m_2$, $\tau_1 = 0$, and $\tau_2 = \min(1, \tau^{(i)}_{m_2})$ (system is unlocked and its mode changes).

Fig. 4 illustrates how $G^{(i)}$ is constructed.

Now, we define the safe nodes of $G^{(i)}$ as the elements of the set

$$
V_{\text{afe}}^{(i)} := \left\{ \nu^{(i)}_{m,\tau,k} : \forall m \in [M], \tau \in [T^{(i)}], k \in \mathbb{T}_{\text{afe}}^{(i)} \right\}
$$

where $\mathbb{T}_{\text{afe}}^{(i)}$ is the set of indices $\{ k \in [K^{(i)}] : \xi^{(i)}_k \in \Xi_{\text{afe}}^{(i)} \}$. To abide by the local constraint for each subsystem (13), every $S^i_{\text{afe}}$ in group $i$ should correspond to an element of $V_{\text{afe}}^{(i)}$.

Then, the aggregate system is constructed with state $x^{(i)} \in \mathbb{N}_0^{D^{(i)}}$ (where $D^{(i)} := K^{(i)} \sum_{m=1}^{M}(T^{(i)}_m + 1)$), whose elements represent the number of subsystems in group $i$ corresponding to the nodes of $G^{(i)}$, and input $u^{(i)} \in \mathbb{N}_0^{D^{(i)}}$ (where $D^{(i)} := K^{(i)}(M - 1)$), whose elements represent the number of subsystems switching mode from each node. Specifically, the element $x^{(i)}_{m,\tau,k}$ of $x^{(i)}$ represents the number of subsystems corresponding to $\nu^{(i)}_{m,\tau,k}$ and the element $u^{(i)}_{m,m',k}$ of $u^{(i)}$ represents the number of unlocked subsystems corresponding to $\nu^{(i)}_{m,0,k}$. Switching mode from $m_1$ to $m_2$. Then, the evolution of each element $x^{(i)}_{m,\tau,k}(t)$ is governed by

$$
x^{(i)}_{m,\tau,k}(t + 1) = \begin{cases} 
\sum_{(\tau',k') \in Z^{(i)}_{m,\tau,k}} x^{(i)}_{m,\tau',k'}(t), & \text{if } \tau \neq 1 \\
\sum_{(m',k') \in Z^{(i)}_{m,0,k}} u^{(i)}_{m,m',k}(t), & \text{if } \tau = 1
\end{cases}
$$

where the set $Z^{(i)}_{m,\tau,k}$ is the set of indices of the predecessors of $\nu^{(i)}_{m,\tau,k}$ defined as $\{ (m',\tau',k') : (m',\tau',k',\nu^{(i)}_{m,\tau,k}) \in E^{(i)} \}$.

Since every element of $x^{(i)}$ evolves as a linear combination of the state and input, the dynamics of $x^{(i)}$ can be written as the linear dynamics

$$
\Gamma^{(i)} : x^{(i)}(t + 1) = A^{(i)}x^{(i)}(t) + B^{(i)}u^{(i)}(t)
$$

where $A^{(i)}$ and $B^{(i)}$ are determined by (14) and depend upon the incidence matrices of $G^{(i)}$. Considering the number of subsystems $N^{(i)}$ in each group and the fact that only unlocked subsystems can switch mode, the state space $X^{(i)}$ and the admissible input space $U^{(i)}(x)$ of $\Gamma^{(i)}$ are as follows:

$$
X^{(i)} = \left\{ x^{(i)} \in \mathbb{N}_0^{D^{(i)}} : \sum_{m=1}^{M} \sum_{\tau=0}^{T^{(i)}_m} \sum_{k=1}^{K^{(i)}} x^{(i)}_{m,\tau,k} = N^{(i)} \right\}
$$

$$
U^{(i)}(x^{(i)}) = \left\{ u^{(i)} \in \mathbb{N}_0^{D^{(i)}} : \right\}
$$
Note that the lockout constraint (8) is never violated if the number of subsystems switching mode at each node is an element in the admissible input set.

The local constraint imposed on $\Gamma^{(i)}_\eta$ is specified by the set $X_{\text{safe}}^{(i)}$, defined as follows:

$$X_{\text{safe}}^{(i)} := \{ x^{(i)} \in X^{(i)} : x_{m, \tau, k}^{(i)} = 0 \}$$

which requires all subsystems to correspond to safe nodes.

We can also construct an alternative representation of $S_\eta$ by combining all $\Gamma^{(i)}_\eta$, defined as $\Gamma_\eta := \bigcap_{i=1}^g \Gamma^{(i)}_\eta$. Accordingly, the state and input of $\Gamma_\eta$ are the concatenation of all $x^{(i)}$ and $u^{(i)}$ respectively, which are written as $x := (x^{(1)})^T, \ldots, (x^{(g)})^T$ and $u := (u^{(1)})^T, \ldots, (u^{(g)})^T$. The state space and the admissible input space are $X := X^{(1)} \times \ldots \times X^{(g)}$ and $U(x) := U^{(i)}(x^{(i)}) \times \ldots \times U^{(g)}(x^{(g)})$, respectively. Then, the system dynamics of $\Gamma_\eta$ can be written as

$$\Gamma_\eta : x(t + 1) = Ax(t) + Bu(t)$$

where the system matrices are $A := \text{diag}(\{ A^{(i)} \}_{i=1}^g)$ and $B := \text{diag}(\{ B^{(i)} \}_{i=1}^g)$. Hence, $\Gamma_\eta$ is a linear system with integer-valued state and admissible input space. Crucially, the dimension of the state or input does not depend on the total number of subsystems $N^{(i)}$. Rather, it increases exponentially with the dimension of the state of each subsystem. Therefore, our method is suitable for systems consisting of a large number of low-dimensional subsystems.

Now, we define the set of safe states of $\Gamma_\eta$ comprising all states satisfying the local and global constraints as follows:

$$X_{\text{safe}} := \{ x \in X : x^{(i)} \in X_{\text{safe}}^{(i)} \forall i \in [g] \},$$

$$P_m \leq \sum_{i=1}^g \sum_{\tau=0}^{t^{(i)}_m} \sum_{k=1}^{K^{(i)}_m} x^{(i)}_{m, \tau, k} \leq P_m \forall m \in [M]$$

where the first line enforces the local constraints on all subsystems, and the second line enforces the global constraint (9); note that $\sum_{\tau=0}^{t^{(i)}_m} \sum_{k=1}^{K^{(i)}_m} x^{(i)}_{m, \tau, k} \leq P_m \forall m \in [M]$.

Our objective is to develop a control algorithm for $\Gamma_\eta$ that keeps the system safe. Our algorithm, which will be introduced in Section V, incorporates a controlled invariant set to guarantee recursive safety and feasibility. However, the large dimension of $\Gamma_\eta$ makes it difficult to use existing invariant set computation tools for linear systems [7], [9], [28]. Therefore, in the next section, we propose a method that obtains an implicit representation of an invariant set of $\Gamma_\eta$, which can be leveraged in the control algorithm.

IV. CONSTRUCTION OF AN INVARIANT SET BY AN IMPLICIT REPRESENTATION

In this section, we show how to construct a controlled invariant set for the aggregate system $\Gamma_\eta$. Leveraging the cycles of the graphs, this method finds an implicit representation of an invariant set of $\Gamma_\eta$ by identifying a set of states that can be kept inside $X_{\text{safe}}$ via periodic inputs. This method is an extension of the method in our preliminary work [18] to accommodate aggregate systems with more than one group.

We first define a safe cycle as a sequence of nodes $\tilde{\nu} = (\tilde{\nu}_1, \ldots, \tilde{\nu}_C) \in (V_{\text{safe}}^{(i)})^C$ with corresponding mode sequence $\tilde{\mu} = (\tilde{\mu}_1, \ldots, \tilde{\mu}_C) \in [M]^C$ that satisfies $\tilde{\nu}_1 \xrightarrow{\tilde{\mu}_{i+1}} \tilde{\nu}_{i+1}$ if $l \neq |C|$ and $\tilde{\nu}_C \xrightarrow{\tilde{\mu}_{i}} \tilde{\nu}_{1}$ if $l = |C|$. Since every node of a safe cycle belongs to $V_{\text{safe}}^{(i)}$, if an abstracted subsystem $S_{j, \eta}^{(i)}$ corresponds to one of these nodes at time $t$, then the subsystem satisfies the local constraint (13) at time $t$. Note that at least one safe cycle should exist in each $G^{(i)}$ for the existence of a controlled invariant set of $\Gamma_\eta$. Fig. 5 shows an example of a safe cycle in $G^{(i)}$.

First, we introduce a strategy that uses a safe cycle to control each abstracted subsystem without the violation of its local constraint (13). Consider an abstracted subsystem $S_{j, \eta}^{(i)}$ that corresponds to a node $\tilde{\nu}_1$ of the safe cycle $C$. If we apply the mode sequence $(\tilde{\mu}_1, \ldots, \tilde{\mu}_C)$ periodically to this subsystem, it visits $(\tilde{\nu}_1, \ldots, \tilde{\nu}_C, \tilde{\nu}_1, \ldots, \tilde{\nu}_1)$ periodically so that it never leaves $V_{\text{safe}}^{(i)}$. This means that if $S_{j, \eta}^{(i)}$ corresponds to a node of a safe cycle, applying the mode sequence of the safe cycle periodically guarantees recursive satisfaction of (13). We call this a circular shift strategy.

Next, we present a condition for recursive satisfaction of the global constraint (9) when every subsystem is controlled by a circular shift strategy. Note that (9) is a linear inequality with respect to the number of subsystems in each mode in each group. Moreover, the total number of subsystems in each mode in each group at each time is periodic since the mode of every subsystem $S_{j, \eta}^{(i)}$ is periodic under a circular shift strategy. This implies that, to ensure global constraint satisfaction, we only need to determine whether the maximum/minimum number of subsystems in each mode in each group within one period satisfies the global constraint. Furthermore, these maximum/minimum values are functions of the nodes each subsystem corresponded to at the initial time step. Therefore, we can characterize an invariant set implicitly by a constraint on the initial number.
of subsystems corresponding to each node that guarantees the recursive satisfaction of the global constraint under a circular shift strategy.

Mathematically, we first select \( n^{(i)} \) safe cycles from \( G^{(i)} \) for all \( i \in \{g\} \); at least one safe cycle should be selected from each group (i.e., \( n^{(i)} > 0 \) for all \( i \in \{g\} \)). The cycles selected from graph \( G^{(i)} \) are denoted as \( C_1^{(i)}, \ldots, C_{n^{(i)}}^{(i)} \) whose nodes are \( \tilde{v}^{(i)}_1 := (\tilde{v}^{(i)}_{1,j}, \ldots, \tilde{v}^{(i)}_{l_{j}^{(i)},j}) \) with corresponding mode sequence \( \tilde{v}^{(i)}_j := (\tilde{v}^{(i)}_{j,1}, \ldots, \tilde{v}^{(i)}_{j,l_{j}^{(i)},j}) \), where \( l_{j}^{(i)} \) is the length of \( C_{n^{(i)}}^{(i)} \).

Next, we define the subsystem assignment of \( C_{n^{(i)}}^{(i)} \) as a vector \( \beta_{j}^{(i)} \in \mathbb{N}_0^{(i)} \) whose \( l \)-th element \( [\beta_{j}^{(i)}]_l \) represents the number of subsystems corresponding to \( v_{j}^{(i)} \). Since the state of every subsystem in group \( i \) corresponds to only one node at a time, the following holds:

\[
\sum_{j=1}^{n^{(i)}} 1^\top \beta_{j}^{(i)} = N^{(i)} \quad \forall i \in \{g\}.
\]  

Next, we consider how the number of subsystems corresponding to each node changes as the subsystems are controlled by a circular shift strategy. We first define the circulant matrix as

\[
\Psi_l := \begin{bmatrix}
0 & 0 & \cdots & 0 & 1 \\
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & 0
\end{bmatrix} \in \mathbb{R}^{l \times l}.
\]

Then, the number of subsystems at each node of \( C_{n^{(i)}}^{(i)} \) after \( q \)-steps of circular shift from \( \beta_{j}^{(i)} \) is \( (\Psi_l^{(i)})^q \beta_{j}^{(i)} \). Also, the number of subsystems in mode \( m \) corresponding to \( C_{n^{(i)}}^{(i)} \) after \( q \)-steps of circular shift from \( \beta_{j}^{(i)} \) is defined as

\[
H_{m,q}(\beta_{j}^{(i)}) := \sum_{l: l_{j}^{(i)}=m} [(\Psi_l^{(i)})^q \beta_{j}^{(i)}]_l.
\]

Note that \( H_{m,q}(\beta_{j}^{(i)}) \) is periodic with respect to \( q \) with period \( l_{j}^{(i)} \) because of the periodicity of \((\Psi_l^{(i)})^q\).

Then, considering all selected cycles \( C_1^{(i)}, \ldots, C_{n^{(i)}}^{(i)} \) for group \( i \), the number of subsystems in mode \( m \) in group \( i \) after \( q \)-steps of circular shift is \( \sum_{j=1}^{n^{(i)}} H_{m,q}(\beta_{j}^{(i)}) \). Hence, the global constraint (9) holds after \( q \)-steps of circular shift if the following holds:

\[
P_m \leq \sum_{i=1}^{g} \sum_{j=1}^{n^{(i)}} H_{m,q}(\beta_{j}^{(i)}) \leq P_m \quad \forall m \in [M].
\]  

For recursive satisfaction of the global constraint under a circular shift strategy, we need (21) to hold for all \( q \in \mathbb{N}_0 \). Considering the periodicity of each \( H_{m,q} \) with respect to \( q \), recursive satisfaction of (9) is achieved if the following two inequalities hold:

\[
\sum_{i=1}^{g} \sum_{j=1}^{n^{(i)}} \min_{q \in [l_{j}^{(i)}]} H_{m,q}(\beta_{j}^{(i)}) \geq P_m \quad \forall m \in [M].
\]  

\[
\sum_{i=1}^{g} \sum_{j=1}^{n^{(i)}} \max_{q \in [l_{j}^{(i)}]} H_{m,q}(\beta_{j}^{(i)}) \leq P_m \quad \forall m \in [M].
\]

Fig. 6 illustrates one example of subsystem assignment for each cycle that satisfies those inequalities for \( m = 1 \).

Now, a set \( \Omega \) of subsystem assignments for which the circular shift strategy never violates the given constraints can be defined as

\[
\Omega := \{ (\beta_{1}^{(1)}\top, \ldots, \beta_{n^{(g)}}^{(g)}\top) \top \in \mathbb{N}_0^{L} : \text{s.t. (19), (22), (23)} \}
\]

where \( L \) is defined as \( \sum_{i=1}^{g} l_{j}^{(i)} \).

This implies that any state \( x \) of \( \Gamma_n \) corresponding to a subsystem assignment in \( \Omega \) will always stay inside \( X \) using a circular shift strategy. To obtain a set \( \mathcal{X}_{\text{inv}} \) of such \( x \), we use a mapping \( \Phi_{j}^{(i)} \) from subsystem assignment vectors \( \beta_{j}^{(i)} \) to the state of \( \Gamma_n^{(i)} \). Specifically, if \( x^{(i)} = \sum_{j=1}^{n^{(i)}} \Phi_{j}^{(i)}(\beta_{j}^{(i)}) \), its element \( x^{(i)}_{m,\tau,k} \) is

\[
x^{(i)}_{m,\tau,k} = \sum_{j=1}^{n^{(i)}} \Phi_{j}^{(i)}(\beta_{j}^{(i)}) \quad \forall i \in \{g\}.
\]

Then, using this mapping, we can define the projection of \( \Omega \) into the state space \( \mathcal{X} \) of \( \Gamma_n \) as

\[
\mathcal{X}_{\text{inv}} := \left\{ x \in \mathcal{X} : \exists (\beta_{1}^{(1)}\top, \ldots, \beta_{n^{(g)}}^{(g)}\top) \top \in \Omega, \text{s.t. } x^{(i)} = \sum_{j=1}^{n^{(i)}} \Phi_{j}^{(i)}(\beta_{j}^{(i)}) \quad \forall i \in \{g\} \right\}.
\]

Therefore, the following theorem holds.

\[1\] These two inequalities are more conservative than the constraints introduced in our preliminary work [18]; yet, the number of inequalities needed is significantly less.
**Theorem 2:** $X_{\text{inv}}$ is a controlled invariant set of the system $\Gamma_\eta$ under the constraint set $X_{\text{safe}}$.

Note that the definition (26) is not an explicit representation of $X_{\text{inv}}$ since we use additional variables $(\beta_1^{(1)}, \ldots, \beta_n^{(g)})$ in its description. To obtain an explicit representation that only depends on constraints in $x^{(i)}$, one needs to project the implicit representation (26) to the state space $X$. However, because of the large dimension of the set, the computational burden is large, and thus, the projection is usually intractable [30]. Fortunately, to check whether a state $x$ belongs to $X_{\text{inv}}$ or to compute an input $u \in U(x)$ that guarantees invariance, an explicit representation is not necessary. Instead, if we introduce integer variables encoding the minimum/maximum in (22)–(23), $X_{\text{inv}}$ can be represented with linear inequalities in $x^{(i)}$, $\beta_j^{(i)}$, and these integer variables, and these inequalities can be used in our formulation. We also remark that given a nonempty maximal controlled invariant set $\overline{X}_{\text{inv}}$ for the aggregate system $\Gamma_\eta$, according to [28, Th. 5], there exists a set of cycles with large enough lengths that leads to a nonempty invariant set $X_{\text{inv}}$. In practice, we observe that a small set of cycles is sufficient to find a nonempty $X_{\text{inv}}$. But when $X_{\text{inv}}$ is empty, longer cycles can be added within the computational budget as per the work in [28].

**V. IMPLICIT INVARIANT-SET-DRIVEN MPC**

In this section, we propose an MPC-based control algorithm with recursive safety and feasibility, referred to as implicit invariant-set-driven MPC. Suppose the state of $\Gamma_\eta$ is $x(t)$ at time step $t$. Then, this algorithm solves the following program at every time step $t \in \mathbb{N}_0$ for a given horizon length $h$:

$$
\min_{x^{(i)}} \sum_{\tau=0}^{h} \hat{c}_\tau + x^{(i)}(t) \tag{27a}
$$

s.t. $x^{(i)}(t+1) = Ax^{(i)} + Bu^{(i)}$ \quad $\forall \tau \in [h-1]_0$

$$
u^{(i)}(t) \in U(x^{(i)}) \quad \forall \tau \in [h-1]_0 \tag{27b}
$$

$$
x^{(i)}(t) = x(t) \tag{27c}
$$

$$(\beta^{(1)}_j, \ldots, \beta^{(g)}_j) \in \Omega \tag{27d}
$$

The decision variables are $x^{(i)}(t) \in \mathbb{N}_0 \sum_{\tau=0}^{h} D^{(i)}_\tau$ for all $\tau$ in $[h]_0$, $u^{(i)}(t) \in \mathbb{N}_0 \sum_{\tau=0}^{h} D^{(i)}_\tau$ for all $\tau$ in $[h-1]_0$, and $\beta_j^{(i)} \in \mathbb{N}_0$ for all $i \in [g]$, $j \in [h^{(i)}]$. The function $\hat{c}_\tau$ is the cost with respect to the state of $\Gamma$ corresponding to $c_\tau$ in Problem 2. In (27d), $(\beta^{(i)}_j)$ is a vector with the entries of $\beta^{(i)}_j$ corresponding to group $i$. After solving this problem, we select the optimal $u^{(i)}$ as the input $u(t)$, which drives the state to $x(t+1) = x^{(i)}(t+1)$.

To guarantee recursive feasibility and safety, this algorithm uses a similar scheme to those introduced in [4], [5], and [6], in which the state trajectory $x^{(i)}(t)$ within the prediction horizon is confined to the maximal controlled invariant set $\overline{X}_{\text{inv}}$ and the terminal state $x^{(i)}(t)$ belongs to invariant set $X_{\text{inv}}$, as illustrated in Fig. 7. However, unlike previous methods that employ an explicit representation, our algorithm uses the obtained implicit representation to formulate the constraint (27d).

**Theorem 3:** Suppose that $X_{\text{inv}}$ is nonempty and the initial state $x(0)$ belongs to the $h$-step backward reachable set of $X_{\text{inv}}$. Then, the program (27) has a feasible solution at any time step $t \in \mathbb{N}_0$. In addition, the trajectory $x(t)$ generated by the algorithm always belongs to the maximal controlled invariant set $\overline{X}_{\text{inv}}$ of $\Gamma_\eta$ and, therefore, belongs to $X_{\text{safe}}$, for every $t \in \mathbb{N}_0$.

Since the proof of this theorem is similar to the one of [5, Th. III.5, and Th. III.7.], we do not provide it here.

Note that the computational complexity of the algorithm (26) depends on the dimension of the state and input of $\Gamma_\eta$, which exponentially increases as the state dimension of the subsystems increases. Thus, the scalability of the algorithm may be limited if the subsystems are high dimensional.

**Remark 1:** The performance of implicit invariant-set-driven MPC in terms of cost minimization becomes better as the size of $X_{\text{inv}}$ and the length of horizon $h$ increases, and the size of $X_{\text{inv}}$ usually increases when the number of cycles $n^{(i)}$ selected from $G^{(i)}$ is larger. However, more cycles and larger $h$ mean more variables and constraints, requiring more computation time. Thus, $h$ and $n^{(i)}$ should be carefully chosen considering this tradeoff.

To implement the control input, we arbitrarily select $u^{(i)}_{m_1,m_2,k}(t)$ out of $x^{(i)}_{m_1,m_2,k}(t)$ unlocked subsystems in mode $m_1$ and state $k$ (i.e., subsystems corresponding to node $\nu^{(i)}_{m_1,m_2,k}$) and switch their mode to $m_2$. This process is repeated for all $m_2 \in [M] \setminus \{m_1\}$. The state of each subsystem at each time step can be determined from the sequence of states $x(t)$ and inputs $u(t)$ obtained by implicit invariant-set-driven MPC.

By Theorems 1 and 3, this switching control approach guarantees that $S$ always satisfies the constraints (7)–(9). First, the lockout constraint (8) is never violated since the controller only switches unlocked subsystems. Second, the global constraint (9) holds by Theorem 3: the obtained state trajectory $x(t)$ always belongs to $X_{\text{safe}}$. Third, and finally, the local constraint (7) holds because every subsystem $S_j^{(i)}$ corresponds to one of the nodes in $V_{\text{safe}}^{(i)}$, i.e., state $\zeta_j^{(i)}(t)$ always belongs to $\gamma^{(i)}_{T_{\text{safe}}^{(i)}}(\Theta_{\text{safe}}^{(i)} \cap B(0, \delta))$.

![Fig. 7. Illustration of an invariant set $X_{\text{inv}}$ (yellow) and maximal controlled invariant set (green) $\overline{X}_{\text{inv}}$. The state trajectory $x^{(i)}$ obtained from implicit invariant-set-driven MPC stays within $\overline{X}_{\text{inv}}$ and terminates within $X_{\text{inv}}$.](image-url)
and so, by Theorem 1, the state trajectory \( \theta_j^{(i)}(t) \) of each \( S_j^{(i)} \) always belongs to \( \Theta_j^{(i)} \).

VI. SIMULATION RESULTS

In this section, we compare the performance of implicit invariant-set-driven MPC to several benchmark algorithms by solving Problem 1. We assume that two groups of homogeneous TCLs (i.e., \( g = 2 \)) are connected to the 56-bus balanced distribution network in [31]. The uncontrollable load at each node is assumed to be constant with the value of 50% of the nominal power consumption at each node; the other 50% is the nominal power consumption of controllable TCLs. We use a time discretization \( \Delta t \) of the TCL dynamics of 40 s.

For the safety of the network, we try to prevent undervoltages, where the lower bound on voltage is set to 0.95 per unit. From this bound on voltage, the safe upper bound on aggregate power \( T_{agg} \) is obtained using the method proposed in [19]. Note that our preliminary work [18] did not explicitly consider a network model, or show the impact of TCL control on the network, like we do here.

The reference signal \( r(t) \) for aggregate TCLs is obtained by shifting and scaling a PI margin frequency regulation signal [25] from 13:00 to 14:30. We both shift and scale it by the nominal power consumption of the controllable TCLs. The cost function to measure the tracking performance is

\[
c_{t}(x) = \left| \sum_{i=1}^{g} p_i(t) \tau_{i}(t) \sum_{\tau=0}^{K} x_{i}(\tau,k) - r(t) \right| . \tag{28}
\]

We select eight random simple cycles from the graphs of each of the two groups. The parameters for the abstraction are \( \epsilon = 0.8, \eta^{(1)} = 0.066, \eta^{(2)} = 0.055, \) and \( \delta = 0.8033 \). Gurobi is used to solve the optimization problems, and the limitation on the solve time of each iteration of MPC is set to 1000 s; if the solver cannot find an optimal solution in 1000 s, a suboptimal solution is used.

A. Benchmark Algorithms

Three benchmark algorithms are compared with implicit invariant-set-driven MPC.

1) Benchmark 1: This MPC algorithm requires the states to be inside \( X_{safe} \) over the optimization horizon. The problem solved at time \( t \) is

\[
\min \sum_{\tau=0}^{h} \tilde{c}(x^{\tau|t}, r(t + \tau)) \tag{27a}
\]

s.t. (27b), (27c)

\[
x^{\tau|t} \in X_{safe} \quad \forall \tau \in [h]_0,
\]

When this problem is feasible, the obtained solution keeps the state inside \( X_{safe} \). However, this algorithm does not ensure recursive feasibility. Therefore, the state may go outside of the maximal controlled invariant set and the problem may become infeasible.

2) Benchmark 2: Instead of imposing a constraint for safety, this MPC algorithm tracks the reference signal truncated between the aggregate power limits (the blue line in Fig. 2). The truncated reference signal is

\[
\tilde{r}(t) = \begin{cases} 
    r(t), & \text{if } P_{agg} \leq r(t) \leq \overline{P}_{agg} \\
    \frac{P_{agg}}{P_{agg}}, & \text{if } r(t) < \frac{P_{agg}}{P_{agg}} \\
    \frac{P_{agg}}{P_{agg}}, & \text{if } r(t) > \frac{P_{agg}}{P_{agg}}.
\end{cases}
\]

Then, the problem solved at time \( t \) is

\[
\min \sum_{\tau=0}^{h} \tilde{c}(x^{\tau|t}, \tilde{r}(t + \tau)) \tag{27c}
\]

s.t. (27a), (27b), (27c).

Since this problem has fewer constraints, the computational burden of this algorithm is less than that of the others. However, solutions from this algorithm may violate the aggregate power limits if \( \tilde{r} \) is not perfectly tracked.

3) Benchmark 3: The third benchmark is a version of invariant-set-driven MPC introduced in our preliminary work [18], which does not consider lockout constraints.

Note that Benchmarks 1 and 2 use the same aggregate system \( \Gamma_{\eta} \) as implicit invariant-set-driven MPC, while Benchmark 3 leverages an aggregate system introduced in [18], whose state does not include locked durations.

B. Numerical Experiments

1) Experiment 1: We first verify the recursive feasibility of implicit invariant-set-driven MPC in contrast to Benchmark 1. Fig. 8 shows the results of Benchmark 1 and implicit invariant-set-driven MPC. Neither algorithm violates the bounds on aggregate power. Benchmark 1 shows better tracking performance at first. However, to achieve this, the temperatures of many of the TCLs in off-mode increase toward the upper bounds of their dead-bands. Eventually, no input exists that satisfies both the temperature and aggregate power constraints at the next time step. Thus, the problem becomes infeasible around 13.25 h. In contrast, even though, initially, implicit invariant-set-driven
Experiment 2: Benchmark 2 violates the network-safe power bounds and the lower voltage limit while Benchmark 3 and implicit invariant-set-driven MPC never do.

| TABLE I | PERFORMANCE COMPARISON |
|---------|------------------------|
|         | Benchmark 2 | Benchmark 3 | Invset MPC |
| RMSE (kW) | 3.95 x 10^4 | 4.40 x 10^4 | 4.37 x 10^4 |
| % of TCLs violating (3) | 0 | 12.42 | 0 |
| Violation of (4) | Yes | None | None |
| Average Time (s) | 2.18 | 131.46 | 73.37 |

MPC has worse tracking performance, it ensures feasibility at any time step by turning on some TCLs in advance.

2) Experiment 2: In this experiment, we compare Benchmarks 2 and 3 with implicit invariant-set-driven MPC in terms of both tracking performance and constraint satisfaction. The results are shown in Fig. 9 and Table I. Benchmark 2 has the best tracking performance, but the aggregate power exceeds the upper bound around 13.8 and 14.1 h. Benchmark 3 never violates the bounds on aggregate power, but it makes an average of 12% of TCLs violate their lockout constraints at each time step. In contrast, implicit invariant-set-driven MPC never violates the aggregate power or lockout constraints.

The plots at the bottom of Fig. 9 show the voltage at every node in the network for each algorithm. We see that Benchmark 2 leads to an undervoltage violation when the bound on aggregate power is violated. In contrast, Benchmark 3 and implicit invariant-set-driven MPC maintain safe voltages across the network. We note that the particular voltage violation seen in Fig. 9 is small and unlikely to cause a real issue in the network, but other combinations of tracking signals, aggregate power bounds, and networks could lead to more severe violations that our approach would guard against.

The average time expended for each iteration of MPC is presented in Table I. Each iteration of implicit invariant-set-driven MPC takes much longer than that of Benchmark 2. Note that the average value exceeds the sampling time Δt = 40 s. This means that the current implementation of the algorithm cannot be leveraged online. Systems with more heterogeneity, and thus more groups, would also require more computational time. Therefore, reducing the computational burden of our approach is an important topic for future work.

VII. CONCLUSION

In this article, we proposed an invariant set construction method that provides an implicit representation of the safe set of a system of heterogeneous switched subsystems with both local and global safety constraints. This representation is incorporated, via a terminal condition, into our proposed MPC-based control algorithm. Since the computational burden of this algorithm is independent of the number of subsystems, it is scalable to large collections of subsystems. Numerical simulation results demonstrated the safety and recursive feasibility of the approach.

Possible future work includes the development of data-driven abstractions to allow for realistic levels of heterogeneity. From an application-domain standpoint, it would also be valuable to 1) develop approaches that handle time-varying power bounds, temperature setpoints, ambient temperatures, and disturbances; 2) explore the impact of the control approach on TCL wear-and-tear/longevity; 3) explore the impact of network model error on the accuracy of the power bounds; and 4) develop approaches to determine power bounds for multiple aggregators operating on the same network.

APPENDIX

Supplements and Proofs for Section III

The following lemma is used to prove Theorem 1.

Lemma 2: If δ > ε + η(i)/2 holds, γ(Θ(i)) ⊄ B(0, δ) is a subset of Θ(i) ⊄ B(0, ε).

Proof: First, the abstraction function γ satisfies γ(Θ(i)) ⊄ (Θ ⊄ B(0, η(i)/2)) ∀Θ ⊂ Rd from which we obtain

γ(Θ(i)) (Θ(i) ⊄ B(0, δ)) ⊄ (Θ(i) ⊄ B(0, δ)) ⊄ B(0, η(i)/2).

Also, by δ > ε + η(i)/2, we have

(Θ(i) ⊄ B(0, δ)) ⊄ B(0, η(i)/2) ⊄ B(0, ε)

⊂ (Θ(i) ⊄ B(0, δ)) ⊄ B(0, δ) = Θ(i).
Since $\Theta_{safe}^{(i)} \subseteq B(0, \epsilon)$ is the largest set in $X$ that satisfies $X \oplus B(0, \epsilon) = \Theta_{safe}^{(i)}$, the following holds:

$$\gamma_{\eta^{(i)}}(\Theta_{safe}^{(i)} \oplus B(0, \delta)) \subseteq \left( \Theta_{safe}^{(i)} \oplus B(0, \delta) \right) \oplus B\left(0, \frac{\eta^{(i)}}{2}\right) \subseteq \Theta_{safe}^{(i)} \oplus B(0, \epsilon)$$

and the statement has been proven. $\blacksquare$

**Proof.** [Theorem 1]: Let $\delta$ be larger than $\epsilon + \eta^{(i)}/2$. From the statement of the theorem, the following holds:

$$\xi_j^{(i)}(t) \in \gamma_{\eta^{(i)}}(\Theta_{safe}^{(i)} \oplus B(0, \delta)) \quad \forall t \in \mathbb{N}_0$$

(29)

Now assume that the initial state of $S_n^{(i)}$ is $\theta^{(i)}(0) = \theta_0$ and the input is $\mu_j^{(i)}(t)$. By the assumption that $S_n^{(i)}$ and $S_{\eta^{(i)}}$ are $\epsilon$-approximately bisimilar, $\|\theta^{(i)}(t) - \xi_j^{(i)}(t)\|$ is always smaller than or equal to $\epsilon$. Moreover, from Lemma 2 and (29), we have $\xi_j^{(i)}(t) \in \Theta_{safe}^{(i)} \oplus B(0, \epsilon)$. Therefore, $\theta_j^{(i)}$ belongs to $\Theta_{safe}^{(i)} \ominus B(0, \epsilon) = \Theta_{safe}$ for any $t \in \mathbb{N}_0$. $\blacksquare$

**Proofs for Section IV:**

**Proof.** [Theorem 2] We first show that $X_{inv}$ is a subset of $X_{safe}$. Let $x := (x^{(1)})^\top, \ldots, (x^{(g)})^\top)$ be an element of $X_{inv}$. By the definition of $X_{inv}$, there exists a vector $(\beta^{(1)}_1, \ldots, \beta^{(g)}_{n^{(g)}})^\top \in \Omega$ such that $x^{(i)} = \sum_{j=1}^{n^{(i)}} \Psi_j^{(i)}(\beta_j^{(i)})$ for all $i \in [g]$. Then, for any $x \in [K] \setminus \mathcal{X}_{safe}^{(i)}$, we can show

$$x_{m,\tau,k} = \sum_{j=1}^{n^{(i)}} \sum_{l \in \mathcal{X}_{safe}} [\beta_j^{(i)}]_l = 0 \quad \forall \tau \in \mathcal{X}_{safe}^{(i)}$$

(30)

since all the nodes $x_{j,k}^{(i)}$ belong to $\mathcal{X}_{safe}^{(i)}$.

Also, the following equation holds by (25):

$$\tau_{m,\tau,k} = \sum_{j=1}^{n^{(i)}} \sum_{l \in \mathcal{X}_{safe}} [\beta_j^{(i)}]_l = \sum_{j=1}^{n^{(i)}} \sum_{l \in \mathcal{X}_{safe}} \beta_j^{(i)}$$

(31)

Therefore, we obtain the following:

$$p_m^{(i)} \tau_{m,\tau,k} = p_m^{(i)} \sum_{j=1}^{n^{(i)}} \sum_{l \in \mathcal{X}_{safe}} \beta_j^{(i)} = H_m,\tau(\beta_j^{(i)})$$

(31)

From (21) and (31), the following holds:

$$P_m \leq \sum_{i=1}^{g} p_m^{(i)} \sum_{\tau=0}^{\tau_{m,\tau,k}} x_{m,\tau,k} \leq \bar{P}_m \quad \forall \tau \in \mathcal{X}_{safe}^{(i)}$$

(32)

Next, we show the recurrence property of $X_{inv}$. Let $\hat{u}$ be the input corresponding to one-step of circular shift from $(\beta^{(1)}_1, \ldots, \beta^{(g)}_{n^{(g)}})^\top$, and $\tilde{x} := (\tilde{x}^{(1)})^\top, \ldots, (\tilde{x}^{(g)})^\top)$ be the corresponding next state from $x$ under $u$ (i.e., $\tilde{x} = Ax + B\hat{u}$). Then, $\tilde{x}$ equals to $\sum_{j=1}^{n^{(i)}} \Psi_j^{(i)}(\beta_j^{(i)})$ for any $i \in [g]$.

Now, it is sufficient to show that $\tilde{x}$ is an element of $X_{inv}$. First, from $I^{\top} \Psi_j^{(i)} = I^{\top}$, the following is easily shown:

$$\sum_{j=1}^{n^{(i)}} I^{\top} \Psi_j^{(i)} \beta_j^{(i)} = \sum_{j=1}^{n^{(i)}} I^{\top} \beta_j^{(i)} = N^{(i)}$$

(33)

Also, using $H_{m,q^{(i)}}(\Psi_j^{(i)} \beta_j^{(i)}) = H_{m,q^{(i)}}(\beta_j^{(i)})$ for $q^{(i)}$ equal to $q^{(i)} + 1$ (mod $I^{\top}$), we obtain

$$\min_{q^{(i)} \in [I^{\top}]} H_{m,q^{(i)}}(\Psi_j^{(i)} \beta_j^{(i)}) = \min_{q^{(i)} \in [I^{\top}]} H_{m,q^{(i)}}(\beta_j^{(i)})$$

(34)

Hence, from (22), the following holds for any $m \in [M]$:

$$\sum_{i=1}^{g} p_m^{(i)} \sum_{j=1}^{n^{(i)}} \min_{q^{(i)} \in [I^{\top}]} H_{m,q^{(i)}}(\Psi_j^{(i)} \beta_j^{(i)}) \geq \bar{P}_m$$

(35)

Similarly, the following holds for any $m \in [M]$:

$$\sum_{i=1}^{g} p_m^{(i)} \sum_{j=1}^{n^{(i)}} \max_{q^{(i)} \in [I^{\top}]} H_{m,q^{(i)}}(\Psi_j^{(i)} \beta_j^{(i)}) \leq \bar{P}_m$$

(35)

By (33), (34), and (35), $((\Psi_j^{(i)} \beta_j^{(i)} \mid i \in [g])^{(1)}, \ldots, (\Psi_j^{(i)} \beta_j^{(i)} \mid i \in [g])^{(g)})^\top$ belongs to $\Omega$. Therefore, $\tilde{x}$ belongs to $X_{inv}$, which shows the recurrence property of $X_{inv}$.

$\blacksquare$

**REFERENCES**

[1] D. Bertsekas, “Infinite time reachability of state-space regions by using feedback control,” IEEE Trans. Autom. Control, vol. AC-17, no. 5, pp. 604–613, Oct. 1972.

[2] J.-P. Aubin, A. Bayen, and P. Saint-Pierre, Viability Theory: New Directions. Berlin, Germany: Springer, 2011.

[3] F. Blanchini, “Set invariance in control,” Automatica, vol. 35, no. 11, pp. 1747–1767, 1999.

[4] T. Koller, F. Berkenkamp, M. Turchetta, and A. Krause, “Learning-based model predictive control for safe exploration,” in Proc. IEEE Conf. Decis. Control, 2018, pp. 6059–6066.

[5] K. P. Wabersich and M. N. Zeilinger, “Linear model predictive safety certification for learning-based control,” in Proc. IEEE Conf. Decis. Control, 2018, pp. 7130–7135.

[6] K. P. Wabersich, L. Hewing, A. Carron, and M. N. Zeilinger, “Probabilistic model predictive safety certification for learning-based control,” IEEE Trans. Autom. Control, vol. 67, no. 1, pp. 176–188, Jan. 2022.

[7] T. Anevlavis and P. Tabuada, “Computing controlled invariant sets in two moves,” in Proc. IEEE Conf. Decis. Control, 2019, pp. 6248–6254.

[8] M. Fiacchini and M. Alamir, “Computing controlled invariant sets in high dimension is easy,” 2018, arXiv:1810.10372.

[9] A. Wintenberg and N. Ozay, “Implicit invariant sets for high-dimensional switched affine systems,” in Proc. IEEE Conf. Decis. Control, 2020, pp. 3291–3297.

[10] S. Bashash and H. K. Fathy, “Modeling and control of aggregate air conditioning loads for robust renewable power management,” IEEE Trans. Control Syst. Technol., vol. 21, no. 4, pp. 1318–1327, Jul. 2013.

[11] W. Zhang, J. Lian, C.-Y. Chang, and K. Kalsi, “Aggregated modeling and control of air conditioning loads for demand response,” IEEE Trans. Power Syst., vol. 28, no. 4, pp. 4655–4664, Nov. 2013.
[12] S. Tindemans, V. Trovato, and G. Strbac, “Decentralized control of thermostatic loads for flexible demand response,” IEEE Trans. Control Syst. Technol., vol. 23, no. 5, pp. 1685–1700, Sep. 2015.

[13] A. Coffman, N. Cammardella, F. Barooah, and S. Meyn, “Aggregate capacity of TCLs with cycling constraints,” IEEE Trans. Power Syst., vol. 38, no. 1, pp. 52–62, Jan. 2023.

[14] C. Ziras, S. You, H. W. Bindner, and E. Vrettos, “A new method for handling lockout constraints on controlled TCL aggregations,” in Proc. Power Syst. Comput. Conf., 2018, pp. 1–7.

[15] E. Dall’Anese, S. Gugliglam, A. Simonetto, Y. C. Chen, and S. Dhople, “Optimal regulation of virtual power plants,” IEEE Trans. Power Syst., vol. 33, no. 2, pp. 1868–1881, Mar. 2018.

[16] A. Bernstein and E. Dall’Anese, “Real-time feedback-based optimization of distribution grids: A unified approach,” IEEE Trans. Control Netw. Syst., vol. 6, no. 3, pp. 1197–1209, Sep. 2019.

[17] E. Vrettos and G. Andersson, “Combined load frequency control and active distribution network management with thermastically controlled loads,” in Proc. IEEE Int. Conf. Smart Grid Commun., 2013, pp. 247–252.

[18] S. Jang, N. Ozay, and J. L. Mathieu, “Large-scale invariant sets for safe coordination of thermostatic loads,” in Proc. Amer. Control Conf., 2021, pp. 4163–4170.

[19] S. C. Ross and J. L. Mathieu, “A method for ensuring a load aggregator’s power deviations are safe for distribution networks,” Elect. Power Syst. Res., vol. 189, 2020, Art. no. 106781.

[20] N. Nazir and M. Almassalkhi, “Convex inner approximation of the feeder hosting capacity limits on dispatchable demand,” in Proc. IEEE Conf. Decis. Control, 2019, pp. 4858–4864.

[21] D. Molzahn and L. Rould, “Grid-aware versus grid-agnostic distribution system control: A method for certifying engineering constraint satisfaction,” in Proc. 52nd Hawaii Int. Conf. Syst. Sci., 2019, pp. 3445–3454.

[22] B. Cui, A. Zamzam, and A. Bernstein, “Network-cognizant time-coupled aggregate flexibility of distribution systems under uncertainties,” in Proc. Amer. Control Conf., 2021, pp. 4178–4183.

[23] PJM, “Implementation and rationale for PJM’s conditional neutrality regulation signals,” 2017. [Online]. Available: https://www.pjm.com/~/media/committees-groups/task-forces/mistf/postings/regulation-market-whitepaper ashesx.

[24] CAISO, “Non-generator resource (NGR) and regulation energy management (REM) overview - phase 1,” 2014. [Online]. Available: https://www.caiso.com/documents/rg-rem-overview.pdf.

[25] PJM, “RTO regulation signal data for 7.19.2019 & 7.20.2019.xls,” 2019. Accessed: Oct. 22, 2019. [Online]. Available: https://www.pjm.com/markets-and-operations/ancillary-services.aspx.

[26] R. C. Sonderegger, “Dynamic models of house heating based on equivalent thermal parameters,” Ph.D. dissertation, Dept. Aerospace Mech. Sci., Princeton Univ., Princeton, NJ, USA, 1978.

[27] S. E. Z. Soudjani and A. Abate, “Aggregation and control of populations of thermostatically controlled loads by formal abstractions,” IEEE Trans. Control Syst. Technol., vol. 23, no. 3, pp. 975–990, May 2015.

[28] P. Nilsson and N. Ozay, “Control synthesis for permutation-symmetric high-dimensional systems with counting constraints,” IEEE Trans. Auton. Control, vol. 65, no. 2, pp. 461–476, Feb. 2020.

[29] P. Tabuada, Verification and Control of Hybrid Systems: A Symbolic Approach. Berlin, Germany: Springer, 2009.

[30] H. Tiwary, “On the hardness of computing intersection, union and Minkowski sum of polytopes,” Discrete Comput. Geometry, vol. 40, no. 3, pp. 469–479, 2008.

[31] S. Bolognani and S. Zampieri, “On the existence and linear approximation of the power flow solution in power distribution networks,” IEEE Trans. Power Syst., vol. 31, no. 1, pp. 163–172, Jan. 2016.

[32] S. Ross, P. Nilsson, N. Ozay, and J. Mathieu, “Managing voltage excursions on the distribution network by limiting the aggregate variability of thermostatic loads,” in Proc. Amer. Control Conf., 2019, pp. 4260–4267.

Sunho Jang (Student Member, IEEE) received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2019. He is currently working toward the Ph.D. degree in electrical and computer engineering with the University of Michigan, Ann Arbor, MI, USA.

His research is focused on developing safe control strategies for cyber-physical systems, with a particular emphasis on network-safe coordination of distributed energy resources.

Necmiye Ozay (Senior Member, IEEE) received the B.S. degree from Bogazici University, Istanbul, Turkey, in 2004, the M.S. degree from Pennsylvania State University, State College, PA, USA, in 2006, and the Ph.D. degree from Northeastern University, Boston, MA, USA, in 2010, all in electrical engineering.

She was a Postdoctoral Scholar with the California Institute of Technology, Pasadena, CA, USA, between 2010 and 2013. She joined the University of Michigan, Ann Arbor, MI, USA, in 2013, where she is currently a Chen-Luan Family Faculty Development Professor of electrical and computer engineering, and an Associate Professor of electrical engineering and computer science, and robotics. Her research interests include hybrid dynamical systems, control, optimization and formal methods with applications in cyber-physical systems, system identification, verification and validation, autonomy, and dynamic data analysis.

Johanna L. Mathieu (Senior Member, IEEE) received the B.S. degree in ocean engineering from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2004, and the M.S. and Ph.D. degrees in mechanical engineering from the University of California, Berkeley, CA, USA, in 2008 and 2012, respectively.

She is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA.