2022 IEEE 61st Conference on Decision and Control (CDC)
December 6-9, 2022. Cancún, Mexico

Decentralized Signal Temporal Logic Control for Perturbed Interconnected Systems via Assume-Guarantee Contract Optimization

Kasra Ghasemi, Sadra Sadraddini, and Calin Belta

2022 IEEE 61st Conference on Decision and Control (CDC) | 978-1-6654-6761-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/CDC51059.2022.9992326

Abstract— **We develop a decentralized control method for a network of perturbed linear systems with dynamical couplings subject to Signal Temporal Logic (STL) specifications. We first transform the STL requirements into set containment problems, then we develop controllers to solve these problems. Our approach is based on treating the couplings between subsystems as disturbances, which are bounded sets that the subsystems negotiate in the form of parametric assume-guarantee contracts. The set containment requirements and parameterized contracts are added to the subsystems' constraints. We introduce a centralized optimization problem to derive the contracts, reachability tubes, and decentralized closed-loop control laws. We show that, when the STL formula is separable with respect to the subsystems, the centralized optimization problem can be solved in a distributed way, which scales to large systems. We present formal theoretical guarantees on robustness of STL satisfaction. The effectiveness of the proposed method is demonstrated via a power network case study.**

I. INTRODUCTION

Formal methods provide mathematical guarantees for the behavior of control systems. Formal languages, such as temporal logics [1], can be used to describe system specifications. With particular relevance to this work, Signal Temporal Logic (STL) [16] can describe a broad range of temporally bounded constraints. The use of formal methods in multi-agent systems has also been investigated [20], [14], [13]. But, with only one exception [13], they only studied dynamically decoupled agents, and none of them took into account the presence of additive disturbances. A related approach in formal methods is based on set-valued dynamics. Analyzing such systems enables characterizing all the possible responses in the presence of bounded uncertainties. Reachability analysis and correct-by-design control synthesis, which guarantee correctness without system testing, received a lot of attention in recent years [10], [15], [7].

Formal methods come with a high computational cost, which makes it challenging to apply them to multi agent systems. That is especially true when we are considering systems with disturbances, and want to guarantee the satisfaction of temporal logic specification under all allowed disturbances. Divide and conquer techniques are a natural way to break the problem into smaller pieces. They can be applied to interconnected systems, where the dynamics of the agents are coupled. Assume-guarantee contracts [4] formalize the promises that systems make and provide over dynamical couplings. For instance, assume-guarantee contracts were used to describe vehicular flow between neighborhoods of a traffic network [12], aircraft power distributions, [19], and dynamics of an aerial robot tethered to a ground one [17].

In this paper, we study the problem of decentralized control design for interconnected perturbed linear systems subject to STL constraints. Unlike approaches that assume given a-priori feasible assume-guarantee contracts [18], [5], we parameterize the contracts and search for feasibility. Unlike the search method in [12], our parameterization, which is based on our prior work [8] and [9], has a special convexity property that leads to a tractable solution. The approach in [17] also parameterized contracts and found them using convex optimization, but was limited to polytopic invariant sets. Here we include complex, non-convex STL constraints, and retain the parameterization from [9]. We achieved this goal by fixing the "logical behavior" through solving a MILP. This enabled us to convert the STL specifications into set containment problems. Then, a linear program is proposed to jointly optimize assume-guarantee contracts, set-valued trajectories, and decentralized closed loop control laws. This allows steering the aggregate system in a way that the global STL formulae is satisfied, while disturbances are rejected in a decentralized manner. When the given STL formula is separable with respect to the subsystems, we provide a method to make the contribution above computationally more tractable for large networks by making it compositional. We use the convexity properties in [8] to optimize contracts, reachability sets, and controllers in a distributed way.

II. NOTATIONS AND PRELIMINARIES

$\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{N}$ stand for the sets of real, non-negative real, and non-negative integers, respectively; $\mathbb{N}_h$ represents the set of non-negative numbers up to $h \in \mathbb{N}$.

We use $\mathbb{B}_h$ to denote an h-dimensional box. $\mathbb{S}_1 \oplus \mathbb{S}_2 := \{s_1 + s_2 | s_1 \in \mathbb{S}_1, s_2 \in \mathbb{S}_2\}$ is the Minkowski sum of two sets $\mathbb{S}_1$ and $\mathbb{S}_2$. The *Directed Hausdorff distance* between two sets $\mathbb{S}_1$ and $\mathbb{S}_2$ is denoted by $d_{DH}(\mathbb{S}_1, \mathbb{S}_2)$ For compact sets, $d_{DH}(\mathbb{S}_1, \mathbb{S}_2) = 0$ iff $\mathbb{S}_2 \subseteq \mathbb{S}_1$. The Cartesian product of sets $\mathbb{S}_1$ and $\mathbb{S}_2$ is denoted by $\mathbb{S}_1 \times \mathbb{S}_2$ and the Cartesian product of $\mathbb{S}_1, \cdots, \mathbb{S}_N$ by $\prod_{i=1}^{N} \mathbb{S}_i$. I_n, 0_n, and $[A_1, A_2]$ represent the $n \times n$ identity matrix, the n-dimensional zero vector, and the horizontal concatenation of matrices A_1, A_2 with the same number of rows, respectively.

A zonotope is a symmetric shape set representation defined as $\mathcal{Z}(c, G) := \{c + Gb | \forall b \in \mathbb{B}_q\}$, where $c \in \mathbb{R}^n$ and

This work was partially supported by the NSF under grants IIS-2024606 and IIS-1723995.

K. Ghasemi and C. Belta are with the Division of System Engineering, Boston University, Boston, MA 02215, USA kasra0gh@bu.edu, cbelta@bu.edu

S. Sadraddini is with the Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA 02139, USA sadra@mit.edu

978-1-6654-6761-2/22/$31.00 ©2022 IEEE

$G \in \mathbb{R}^{n\times q}$ $(n, q \in \mathbb{N})$ denote the zonotope's center and generator, respectively. The order of the zonotope is equal to $\frac{q}{n}$. Zonotopes are convenient for set calculations, such as Minkowski sums and linear transformations. Given two sets $\mathbb{S}_1 = \mathcal{Z}(c_1, G_1)$ and $\mathbb{S}_2 = \mathcal{Z}(c_2, G_2)$, a matrix $A \in \mathbb{R}^{m\times n}$, and a vector $b \in \mathbb{R}^n$, where $c_1, c_2 \in \mathbb{R}^n$ and $G_1 \in \mathbb{R}^{n\times q_1}$, $G_2 \in \mathbb{R}^{n\times q_2}$, we have $\mathbb{S}_1 \oplus \mathbb{S}_2 = \mathcal{Z}(c_1 + c_2, [G_1, G_2])$ and $A\mathbb{S}_1 + b = \mathcal{Z}(Ac_1 + b, AG_1)$.

Signal Temporal Logic (STL) was introduced in [16] to specify Boolean and temporal properties of real-valued, time signals. A discrete-time signal is a function $s : \mathbb{N} \to \mathbb{R}^q$. We use $(s, [t_1, t_2])$ to denote the sequence $s(t_1), ..., s(t_2)$ and (s, t) for $(s, [t, \infty])$. An STL formula is defined with the following recursive grammar:

$$\varphi ::= \pi|\neg\varphi|\varphi\wedge\psi|\varphi|\varphi\vee\psi|\mathbf{F}_{[t_1,t_2]}\varphi|\mathbf{G}_{[t_1,t_2]}\varphi|\varphi\mathbf{U}_{[t_1,t_2]}\psi \quad (1)$$

where π is a predicate. All predicates are assumed to be linear in the form $p(s) \leq c$ or $p(s) \geq c$, with c being a scalar and $p : \mathbb{R}^q \to \mathbb{R}$ being a linear function. Symbols $\neg$, $\wedge$, and $\vee$ denote Boolean negation, conjunction, and disjunction, respectively; $\mathbf{F}_{[t_1,t_2]}$, $\mathbf{G}_{[t_1,t_2]}$, and $\mathbf{U}_{[t_1,t_2]}$ are temporal operators for "eventually","always", and "until", respectively. Also, $(s, t) \models \varphi$ denotes that signal s satisfies formula φ at time t, and $(s, t) \not\models \varphi$ if this is not the case. The satisfaction of a formula φ by a signal s at time t is defined in Definition 1 at [2]. For simplicity, $(s, 0) \models \varphi$ is denoted by $s \models \varphi$. The *horizon* of a formula is the shortest amount of time required to determine whether a formula φ is satisfied, and it is denoted by $hrz(\varphi)$ [2]. The *robustness* [6] of formula φ with respect to signal s at time t is denoted by $\rho(s, \varphi, t)$. Without loss of generality, we only consider negation free formulas in this paper. This is not restrictive, as any STL formula can be made negation-free. It is also worth noting that, while predicates with inequalities are used in the semantics definition, strict inequalities and equalities can be formed using the Boolean operators.

III. Problem Definition and Approach

Consider the following network of coupled time-variant linear subsystems:

$$x_{i,t+1} = A_{ii,t}x_{i,t} + B_{ii,t}u_{i,t} + \sum_{j\neq i} A_{ij,t}x_{j,t} + \sum_{j\neq i} B_{ij,t}u_{j,t} + w_{i,t},\ i \in \mathcal{I}, \quad (2)$$

where $\mathcal{I}$ is an index set for the subsystems; $A_{ii,t} \in \mathbb{R}^{n_i\times n_i}$, $A_{ij,t} \in \mathbb{R}^{n_i\times n_j}$, $B_{ii,t} \in \mathbb{R}^{n_i\times m_i}$, and $B_{ij,t} \in \mathbb{R}^{n_i\times m_j}$ are given, time-variant matrices for subsystem i. Let $\eta = |\mathcal{I}|$ denote the number of subsystems in the network. The state, control input, and disturbance for subsystem i at time step t are represented by $x_{i,t} \in \mathbb{R}^{n_i}$, $u_{i,t} \in \mathbb{R}^{m_i}$, and $w_{i,t} \in \mathbb{R}^{n_i}$, which are bounded by given polytopic sets $x_{i,t} \in X_{i,t} \subseteq \mathbb{R}^{n_i}$, $u_{i,t} \in U_{i,t} \subseteq \mathbb{R}^{m_i}$, and $w_{i,t} \in W_{i,t} \subset \mathbb{R}^{n_i}$, respectively. A *decentralized controller* $\mu_{i,t}(.) : X_{i,t} \to U_{i,t}$ is a function that maps the current state of subsystem i into a control input in the control space of the same subsystem. System (2) with no disturbances is called a *nominal system.*

Definition 1 (Decentralized Finite-Time Viable Sets): Given $h \in \mathbb{N}$, the sequences of sets $\Omega_{i,0}, \Omega_{i,1}, ..., \Omega_{i,h}$, $i \in \mathcal{I}$ for the interconnected system in (2) are called decentralized *viable* sets, if for all $t \in \mathbb{N}_h, \forall i \in \mathcal{I}$, $\Omega_{i,t} \subseteq X_{i,t}$ and there exists a set of policies $\mu_{i,t}(.)$ such that $\Theta_{i,t} \subseteq U_{i,t}$ and $\forall t \in \mathbb{N}_{h-1}, \forall x_{i,t} \in \Omega_{i,t}, \forall w_{i,t} \in W_{i,t} \Rightarrow x_{i,t+1} \in \Omega_{i,t+1}$, where $\Theta_{i,t} := \mu_{i,t}(\Omega_{i,t})$ is called *action set*.

A signal $s : \mathbb{N} \to X \times U \subset \mathbb{R}^{n+m}$ is a trajectory where $s(t)$ represents a vector stacking the state and control of the aggregated system at time step t, which is represented by $s(t) = (x_t, u_t)$, where $x_t = [x_{1,t}^T, \cdots, x_{\eta,t}^T]^T \in \mathbb{R}^n$ and $u_t = [u_{1,t}^T, \cdots, u_{\eta,t}^T]^T \in \mathbb{R}^m$ and $n = \sum_{i\in\mathcal{I}} n_i$ and $m = \sum_{i\in\mathcal{I}} m_i$. In this paper, we consider the following problem:

Problem 1: Given a network of perturbed linear systems in the form (2), the initial states $x_i^{initial} \in X_{i,0}, \forall i \in \mathcal{I}$, a bounded STL formula φ with linear predicates in the states and / or controls, and a quadratic cost $J : \mathbb{S} \to \mathbb{R}_+$, find the optimal decentralized controllers $\mu_{i,t}(x_{i,t}), \forall i \in \mathcal{I}$ and their corresponding sequence of viable sets $\Omega_{i,t}$ such that J is minimized, $x_{i,t} \in X_{i,t}$, $u_{i,t} \in U_{i,t}$, and $s \models \varphi$. If such a signal does not exist, find $\Omega_{i,t}$ corresponding to the maximum possible value of the robustness, i.e, find a signal with the least amount of violation.

To solve Problem 1, a two-step optimization-based approach is proposed. We begin by solving a mixed-integer program for the aggregated nominal system, which is constrained by the STL formula φ [2]. It allows us to determine active predicates at each time and convert the STL formula satisfaction into a set containment problems, which is shown to be a convex programming problem [22]. In the second step, we take into account the additive disturbance, along with the set containment constraints, and we find a set of decentralized closed-loop controllers and viable sets.

IV. Converting STL formulas into Set Containment Problems

We borrowed the method explained in [2] to encode an STL formula into a mixed-integer linear program. Then, the set of predicates whose satisfaction corresponds to the maximum robustness for the nominal system is identified and transformed to a set containment problem.

A. Encoding the STL Formulas

Following the predicate-based encoding from [2], a binary variable $z_t^\pi \in \{0, 1\}$ is dedicated to each predicate $\pi = (y \geq 0)$, which must be assigned to 1 if the predicate is true, and to 0 otherwise. The relation between z_t^π, the robustness ρ, and y_t is encoded as

$$y_t + M(1 - z_t^\pi) \geq \rho \quad , \quad y_t - Mz_t^\pi < \rho, \quad (3)$$

where M is a sufficiently large number such that for all time steps, $M \geq \max y_i, i \in \mathbb{N}_{n_y}$. The equations in (3) enforce the binary variable z_t^π to be equal to 1 when $y_t \geq \rho$ and equal to 0 when $y_t < \rho$. Disjunctions and conjunctions are captured by the following constraints:

$$z=\bigwedge_{i=0}^{n_z} z_i \Rightarrow z \leq z_i, i \in \mathbb{N}_{n_z}, z=\bigvee_{i=0}^{n_z} z_i \Rightarrow z \leq \sum_{i=0}^{n_z} z_i, \tag{4}$$

where $n_z \in \mathbb{N}$ and $z \in [0,1]$ is declared as a continuous variable. However, as the above equation shows, it can only take binary values. In [11], [21] upper-bounding constraints are added to create a necessary and sufficient condition:

$$z=\bigwedge_{i=0}^{n_z} z_i \Leftrightarrow z \geq \sum_{i=0}^{n_z} z_i - n_z + 1, z \leq z_i, i \in \mathbb{N}_{n_z} \tag{5a}$$

$$z=\bigvee_{i=0}^{n_z} z_i \Leftrightarrow z \geq z_i, i \in \mathbb{N}_{n_z}, z \leq \sum_{i=0}^{n_z} z_i. \tag{5b}$$

The upper-bound constraints are necessary when the specification does not include negation. $z_t^{\varphi} \in [0,1]$ is the variable that indicates whether $(s,t) \models \varphi$. A recursive translation of an STL formula is as follows:

$$\begin{aligned}
&\varphi=\bigwedge_{i=1}^{n_\varphi} \varphi_i \Rightarrow z_t^{\varphi}=\bigwedge_{i=1}^{n_\varphi} z_k^{\varphi_i}; \varphi=\bigvee_{i=1}^{n_\varphi} \varphi_i \Rightarrow z_t^{\varphi}=\bigvee_{i=1}^{n_\varphi} z_t^{\varphi_i};\\
&\varphi=G_I\psi \Rightarrow z_t^{\varphi}=\bigwedge_{t' \in I} z_{t'}^{\psi}; \varphi=F_I\psi \Rightarrow z_t^{\varphi}=\bigvee_{t' \in I} z_{t'}^{\psi};\\
&\varphi=\psi_1 U_I \psi_2 \Rightarrow z_t^{\varphi}=\bigvee_{t' \in I}(z_{t'}^{\psi_2} \wedge \bigwedge_{t'' \in [t,t']} z_{t''}^{\psi_1}),
\end{aligned} \tag{6}$$

where $n_\varphi \in \mathbb{N}$. Given a formula φ, the set of constraints recursively constructed by equations (3), (5), and (6) is denoted by $\mathcal{C}_\varphi$.

Theorem 1 (Adapted from [2]): The following properties hold for the above mixed-integer linear program encoding:(i) $(s,t) \models \varphi$, if adding $z_t^{\varphi}=1$ and $\rho \geq 0$ to the constraints makes $\mathcal{C}_\varphi$ feasible, (ii) $(s,t) \not\models \varphi$, if adding $z_t^{\varphi}=1$ and $\rho \geq 0$ makes $\mathcal{C}_\varphi$ infeasible, (iii) the largest ρ such that $z_t^{\varphi}=1$ and $\mathcal{C}_\varphi$ is feasible is equal to the robustness.

It is shown in [2] that when the STL formulas are negation free, ρ equals robustness. As a result, it can be used as an objective function to maximize robustness.

B. Set Containment for STL Formula Satisfaction

The objective of this subsection is to get the set of z_t^{π}s equal to 1, which are called active predicates, for the maximum robustness while considering the nominal system. If the disturbance bound is small enough, it can be assumed that the perturbed and nominal systems have the same set of active predicates, and a closed-loop controller can be found to ensure that the system's reachability set still satisfies those predicates. We can do the synthesis for the aggregate nominal system [2] rewritten as $x_{t+1}=A_t x_t + B_t u_t$ from (2), by using the STL satisfaction constraints introduced before:

$$\begin{aligned}
&\max_{x_t,u_t,z_t^{\pi},\rho} \quad -J(s[0,hrz(\varphi)])+\mathcal{M}(|\rho|-\rho)\\
&\text{s.t.} \quad x_{t+1}=A_t x_t + B_t u_t, t \in \mathbb{N}_{hrz(\varphi)-1}\\
&\qquad x_0=[x_1^{initial},...,x_\eta^{initial}],\\
&\qquad \mathcal{C}_\varphi, z_0^{\varphi}=1.
\end{aligned} \tag{7}$$

As long as robustness is positive, the proposed objective function minimizes the user defined cost function $J(.)$, which can be a regular quadratic function in the form of $\sum_{t=0}^{hrz(\varphi)} x_t^T Q x_t + u_t^T R u_t$. Otherwise, it maximizes robustness due to the effect of the large scalar $\mathcal{M}$ and finds the nominal trajectory with the least violation.

Each active predicate is actually a set, $y_t \geq \rho, \forall y_t$, which must hold for all possible signals at time t. By definition, we have $s(t) \in \prod_i \Omega_{i,t} \times \prod_i \Theta_{i,t}$. Assuming the set $\prod_i \Omega_{i,t} \times \prod_i \Theta_{i,t}$ is represented by a zonotopic set $\mathcal{Z}(c,G)$ (notation t is removed for readability), then any possible signal must satisfy $\mathrm{e} \geq \rho, \quad \forall \mathrm{e} \in \mathcal{Z}(p(c),p(G))$. Also, by definition, the zonotope $\mathcal{Z}(c,G)$ has the following upper and lower bounds $c-\sum_i |g_i| \leq \mathcal{Z}(c,G) \leq c+\sum_i |g_i|$, where g_i is the ith column of G. Using these bounds, the satisfaction constraint for an active predicate would be:

$$-p(c)+\sum_i |p(G)_i| \leq -\rho \tag{8}$$

where $p(G)_i$ is the ith element of $p(G)$.

Theorem 2: The constraint in (8) can be written as a set of linear constraints as follows:

$$-p(c)+\sum_i p'_i \leq -\rho, p'_i \geq p(G)_i, p'_i \geq -p(G)_i. \tag{9}$$

Proof: It can be easily seen that if such p'_is exist, the following relation holds:

$$-p(c)+\sum_i |p(G)_i| \leq -p(c)+\sum_i p'_i \leq -\rho, \tag{10}$$

which also satisfies the original constraint (8). Also, because (9) is the relaxed form of the original problem, if such p'_is do not exist, the original problem is also infeasible. ■

Finally, the set of linear constraints that guarantees any possible trajectories in viable and action sets satisfies the STL formula φ is denoted by $\mathcal{G}_\varphi$.

V. Computation of Viable Sets under Additive Disturbance

The original problem has been transformed into a decentralized control synthesis problem with zonotopic set containment constraints. The latter problem was considered in [9], where a compositional approach using assume-guarantee contracts is proposed. In this section, we give a brief overview of [9] and incorporate the linear constraints $\mathcal{G}_\varphi$ into its formulation.

A. Decentralized Synthesis

First, the subsystems are decoupled from each other by considering the effects of other subsystems as disturbances, and by making some assumptions on the operational sets of each subsystem, as follows:

$$x_{i,t+1}=A_{ii,t}x_{i,t}+B_{ii,t}u_{i,t}+w_{i,t}^{aug}, \tag{11}$$

where $w_{i,t}^{aug}$ is the augmented disturbance set on subsystem i, which belongs to:

$$w_{i,t}^{aug} \in \bigoplus_{j \neq i} A_{ij,t}\mathcal{X}_{j,t} \oplus \bigoplus_{j \neq i} B_{ij,t}\mathcal{U}_{j,t} \oplus W_{i,t}, \tag{12}$$

where $\mathcal{X}_{j,t}$ and $\mathcal{U}_{j,t}$ are assumed operational sets for the state and the control input of subsystem $j \in \mathcal{I}$. It can be seen that the performance of each subsystem affects the assumptions of the other subsystems. This give and take contracts are called assume-guarantee contracts.

Definition 2 (Assume-Guarantee Contracts): An assume-guarantee contract for subsystem $i \in \mathcal{I}$ is a pair $\mathcal{C}_i = (\mathcal{A}_i, \mathcal{G}_i)$, where:

- The assumption $\mathcal{A}_i$ is the assumption set over the disturbance $w^{aug}_{i,t} \in \mathcal{W}_{i,t}$,
- The guarantee $\mathcal{G}_i$ is the promise of subsystem i over its state and control input $x_{i,t} \in \mathcal{X}_{i,t}, u_{i,t} \in \mathcal{U}_{i,t}$.

As seen in (12), the following relation holds between the guarantee of other subsystems $\mathcal{X}_j, \mathcal{U}_j, j \neq i$ and the assumption of subsystem i, $\mathcal{A}_i$:

$$\mathcal{W}_{i,t} = \bigoplus_{j \neq i} A_{ij,t}\mathcal{X}_{j,t} \oplus \bigoplus_{j \neq i} B_{ij,t}\mathcal{U}_{j,t} \oplus W_{i,t} \qquad (13)$$

The above zonotopic set is represented by $W_{i,t} = \mathcal{Z}(d^w_{i,t}, G^w_{i,t})$, where $d^w_{i,t} \in \mathbb{R}^{n_i}$ and $G^w_{i,t} \in \mathbb{R}^{n_i \times l_t}$. Next, we define a parametric assume-guarantee contract, which is similar to the regular contract except that the sets $\mathcal{X}_{i,t}$, $\mathcal{U}_{i,t}$ are replaced with the parametric sets below:

$$\mathcal{X}_{i,t}(\alpha^x_{i,t}) := \mathcal{Z}(c^x_{i,t}, G^x_{i,t}\text{Diag}(\alpha^x_{i,t})), \qquad (14a)$$

$$\mathcal{U}_{i,t}(\alpha^u_{i,t}) := \mathcal{Z}(c^u_{i,t}, G^u_{i,t}\text{Diag}(\alpha^u_{i,t})), \qquad (14b)$$

where $G^x_{i,t} \in \mathbb{R}^{n_i \times f_{i,t}}$ and $G^u_{i,t} \in \mathbb{R}^{m_i \times g_{i,t}}$ $(f_{i,t}, g_{i,t} \in \mathbb{N})$ are given matrices defined by the user, and the vectors $c^x_{i,t} \in \mathbb{R}^{n_i}$, $\alpha^x_{i,t} \in \mathbb{R}^{f_{i,t}}$, $c^u_{i,t} \in \mathbb{R}^{m_i}$, and $\alpha^u_{i,t} \in \mathbb{R}^{g_{i,t}}$ are parameters. Also, the parametric assumption set $\mathcal{W}_{i,t}(\alpha^{ext})$ is derived by replacing the above parametric sets into equation (13), where α^{ext} denotes the set of all parameters. To deal with the mismatch between the assumed and real operational disturbance sets, we introduce the notion of correctness:

Definition 3 (Correctness): A set of parametric contracts $\mathcal{C}_i$ is correct if

$$\mathcal{W}_{i,t} \subseteq \bigoplus_{j \neq i} A_{ij,t}\Omega_{j,t} \oplus B_{ij,t}\Theta_{j,t} \oplus W_{i,t}, \forall i, t. \qquad (15)$$

The preceding definition is required to resolve the circularity problem of assumption-guarantee contracts. It was shown in [8] that constraints $\mathcal{X}_{i,t}(\alpha^x_{i,t}) \subseteq \Omega_{i,t}$ and $\mathcal{U}_{i,t}(\alpha^u_{i,t}) \subseteq \Theta_{i,t}$ imply (15). The next step is to design a robust controller for each subsystem. The following decentralized controller structure is proposed for each subsystem:

$$x_{i,t} = \bar{x}^i_t + T^i_t\zeta, u_{i,t} = \bar{u}^i_t + M^i_t\zeta, \zeta \in \mathbb{B}_k, \qquad (16)$$

where $\bar{x}^i_t \in \mathbb{R}^{n_i}$, $\bar{u}^i_t \in \mathbb{R}^{m_i}$, $T^i_t \in \mathbb{R}^{n_i \times q_{i,t}}$, and $M^i_t \in \mathbb{R}^{m_i \times q_{i,t}}$ are unknowns that need to be tuned and $q_{i,t} = k + \sum_{i=0}^{i=t} l_i$, where $k \in \mathbb{N}$ is a hyper-parameter. Then, for subsystem i, it can be shown that the following linear constraints are sufficient for tuning the control parameters:

$$[A_{ii,t}T^i_t + B_{ii,t}M^i_t, G^{aug}_{i,t}] = [T^i_{t+1}], t \in \mathbb{N}_{h-1} \qquad (17a)$$

$$A_{ii,t}\bar{x}^i_t + B_{ii,t}\bar{u}^i_t + d^{aug}_{i,t} = \bar{x}^i_{t+1}, t \in \mathbb{N}_{h-1}. \qquad (17b)$$

If such parameters exist, $\Omega_{i,t} = \mathcal{Z}(\bar{x}^i_t, T^i_t)$ is the viable set, $\Theta_{i,t} = \mathcal{Z}(\bar{u}^i_t, M^i_t)$ is the action set, and (16) is the controller. Intuitively, constraints (17a) and (17b) are set containment constraints; (17b) adjusts the centers of the viable sets and (17a) takes care of the set expansion at each step, such that all the possible trajectories are contained within the tube $\Omega_{i,0}, \Omega_{i,1}, \cdots, \Omega_{i,h}$, where h is the horizon, which is set to $hrz(\varphi)$ in our problem. Additionally, the following constraints are proposed to impose hard constraints:

$$\mathcal{Z}(\bar{x}^i_t, T^i_t) \subseteq X_{i,t}, \mathcal{Z}(\bar{u}^i_t, M^i_t) \subseteq U_{i,t}, t \in \mathbb{N}_h. \qquad (18)$$

It was demonstrated in [22] that zonotope and polytope containment problems can be encoded into linear constraints. Thus, all of the suggested constraints (15), (17), (18), and $\mathcal{G}_\varphi$ for all subsystems and time steps may be merged to build a centralized linear program to solve Problem 1. The objective function is ad-hoc, but we recommend the mean square error between the center line of viable/action sets and the nominal trajectory/controllers generated by (7).

B. Compositional Computation of Decentralized Viable Sets

Despite the fact that the centralized solution presented at the end of the preceding subsection is a linear program, it still suffers from curse of dimensionality in high dimensions. Nevertheless, it is demonstrated in [9] that the suggested parameterization (14) allows for compositional computation of viable sets in a time-efficient manner by transforming a single, large linear program into a group of smaller linear programs. We show that if the STL formula in Problem 1 is separable by subsystems, we can also use the parameterization to solve the same centralized approach in the previous section in a compositional manner. Additionally, convergence is ensured due to the convexity of the problem set.

Assumption 1: The STL formula in Problem 1 is separable by the subsystems, meaning it can take the form $\varphi = \varphi_1 \wedge ... \wedge \varphi_\eta$, where i is the subsystem's index.

In [9], we proposed a parametric potential function that quantifies how far a set of contracts is from correctness. This comes in contrast to the previously introduced correctness property, which was either true or false. The larger the parametric potential function, the farther the set of contracts is from correctness, so the goal is to minimize the proposed potential function. Here, the parametric potential function is modified by including the containment constraints coming from the STL formulas, as well as adding the sum of the directed Hausdorff distances between the hard constraints and the viable/action sets in (18) into the potential function.

Definition 4 (Parametric potential function): The parametric potential function $\mathcal{V}(\alpha^{ext})$ is defined as $\mathcal{V}(\alpha^{ext}) = \sum_{i \in \mathcal{I}} \mathcal{V}_i(\alpha^{ext})$, where

$$\mathcal{V}_i(\alpha^{ext}) := \sum_{t \in \mathbb{N}_{hrz(\varphi)}} [d_{DH}(\mathcal{X}_{i,t}, \Omega_{i,t}) +$$

$$d_{DH}(\mathcal{U}_{i,t}, \Theta_{i,t}) + d_{DH}(X_{i,t}, \Omega_{i,t}) + d_{DH}(U_{i,t}, \Theta_{i,t})] \qquad (19)$$

Using the technique explained in Subsection IV-B, the satisfaction of the STL formula φ_i for subsystem i can be encoded as a set of linear constraints denoted by $\mathcal{G}_{\varphi_i}$. Each component of the parametric potential function $\mathcal{V}_i(\alpha^{ext})$ can be computed using these constraints and (17) by solving the following linear program:

$$\mathcal{V}_i(\alpha) = \min_{\substack{\mathrm{x}^i, T^i, \mathrm{u}^i, M^i \\ , d^x_t, d^u_t, \bar{d}^x_t, \bar{d}^u_t}} \sum_{t \in \mathbb{N}_{hrz(\varphi)}} [d^x_t + \bar{d}^x_t] + \sum_{t \in \mathbb{N}_{hrz(\varphi)-1}} [d^u_t + \bar{d}^u_t]$$

subject to

$$[A_{ii,t}T^i_t + B_{ii,t}M^i_t, G^w_{i,t}] = [T^i_{t+1}], \forall t \in \mathbb{N}_{hrz(\varphi)-1} \tag{20a}$$

$$A_{ii,t}\bar{\mathrm{x}}^i_t + B_{ii,t}\bar{\mathrm{u}}^i_t + d^w_{i,t} = \bar{\mathrm{x}}^i_{t+1}, \forall t \in \mathbb{N}_{hrz(\varphi)-1} \tag{20b}$$

$$\mathcal{Z}(\bar{\mathrm{x}}^i_t, T^i_t) \subseteq \ \mathcal{X}_{i,t}(\alpha^x_{i,t})) \oplus \mathcal{Z}(0, d^x_t I_{n_i}), \forall t \in \mathbb{N}_{hrz(\varphi)} \tag{20c}$$

$$\mathcal{Z}(\bar{\mathrm{u}}^i_t, M^i_t) \subseteq \ \mathcal{U}_{i,t}(\alpha^u_{i,t}) \oplus \mathcal{Z}(0, d^u_t I_{m_i}), \forall t \in \mathbb{N}_{hrz(\varphi)-1} \tag{20d}$$

$$\mathcal{Z}(\bar{\mathrm{x}}^i_t, T^i_t) \subseteq X_{i,t} \oplus \mathcal{Z}(0, \bar{d}^x_t I_{n_i}), \forall t \in \mathbb{N}_{hrz(\varphi)} \tag{20e}$$

$$\mathcal{Z}(\bar{\mathrm{u}}^i_t, M^i_t) \subseteq U_{i,t} \oplus \mathcal{Z}(0, \bar{d}^u_t I_{m_i}), \forall t \in \mathbb{N}_{hrz(\varphi)-1} \tag{20f}$$

$$\mathcal{G}_{\varphi_i}, \bar{\mathrm{x}}^i_0 = x^{initial}_i \tag{20g}$$

$$d^x_t, \bar{d}^x_t \geq 0, \ \ \forall t \in \mathbb{N}_{hrz(\varphi)}, \tag{20h}$$

$$d^u_t, \bar{d}^u_t \geq 0, \ \ \forall t \in \mathbb{N}_{hrz(\varphi)-1}. \tag{20i}$$

Constraints (20a) and (20b) originate from (17). Also, the STL satisfaction constraints and the initial state constraint are added in (20g). The remaining constraints along with the objective function compute an over-approximation for the summation of the directed Hausdorff distance between sets $\Omega_{i,t}$ and $\mathcal{X}_{i,t}/X_{i,t}$ and $\Theta_{i,t}$ and $\mathcal{U}_{i,t}/U_{i,t}$ over all time steps. This approach of computing the Directed Hausdorff distance is inspired from [22].

Theorem 3 (Convexity of the potential function): The potential function proposed above is convex with respect to the parameters. The set of acceptable parameters (correct and valid) is also a convex set.

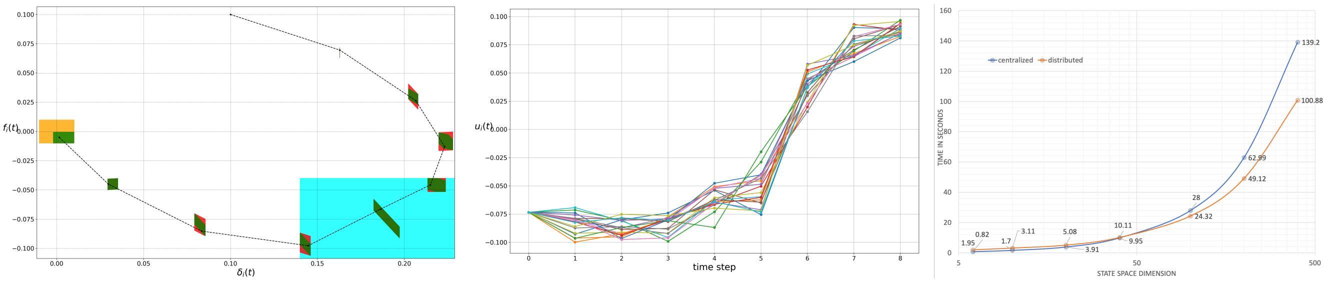
Proof: As seen in (20), each component of the potential function is a linear program, which makes $\mathcal{V}_i(\alpha^{ext})$ a convex and piecewise affine function (a sum of convex functions is convex). Also, it is a well-known fact that the level set of a convex function is a convex set, thus, the set of acceptable parameters, which is equal to the zero level set of the potential function, is also a convex set. ■

The idea is to minimize the potential function using gradient descent and iteratively update the parameters by $\alpha^{ext} \leftarrow \alpha^{ext} - \sum_{i \in \mathcal{I}} \nabla_{\alpha^{ext}} \mathcal{V}_i(\alpha^{ext})$. Convergence to the global minimum is guaranteed because the proposed potential function is convex. Each subsystem can find the direction that is best for it ($\nabla_{\alpha^{ext}} \mathcal{V}_i(\alpha^{ext})$), using its own local information and the common knowledge parameters, breaking the problem down into many smaller linear programs. If the minimum of the potential function is zero (by definition, the potential function is always larger than zero), it indicates that both the set of derived parametric contracts are correct and the viable and actions sets are within hard constraints. Thus, the desired control policies and viable sets are determined. Also, the nominal trajectories and controllers derived from (7) can be used as initial values for the center parameters in our parameterized sets to give the gradient descent a warm start.

VI. Case Study

We apply our method to the load-frequency problem in power networks [3]. A network is made up of several areas, each with its own power generator and demands, and some of them can be connected to each other to interchange power as needed, depending on the network architecture. Each area's state is represented by a 2-dimensional vector $[\delta_{i,t}, f_{i,t}]^T$, where $\delta_{i,t} \in \mathbb{R}$ is the deviation of the phase angle and $f_{i,t} \in \mathbb{R}$ is the deviation of the frequency at time t for area $i \in \mathbb{N}$. Also, $u_{i,t} \in \mathbb{R}$ is the control input, which is the amount of change from its nominal value in the power generated by the generator at the area i and time t. The dynamics for each area is given by $\dot{\delta}_{i,t} = 2\pi f_{i,t}$ and $\dot{f}_{i,t} = -\frac{f_{i,t}}{T_{p_i}} + \frac{K_{p_i} u_{i,t}}{T_{p_i}} - \frac{K_{p_i}}{2\pi T_{p_i}}(\sum_{j \in \mathcal{N}_i} K_{s_{ij}}[\delta_{i,t} - \delta_{j,t}]) - \frac{K_{p_i}\omega_{i,t}}{T_{p_i}}$, where $K_{p_i}, K_{s_{ij}}, T_{p_i}$ are the system gain, synchronizing coefficient between area i and j, and system model time constant. In this case study, they are set to 110, 0.5, and 25, respectively, for all areas. Also, $\omega_{i,t}$ is the load disturbance for area i at time t, which is bounded by $|\omega_{i,t}| \leq 0.001$. In addition, $\mathcal{N}_i$ denotes the neighbours of area i. Here, we consider the ring network architecture consisted of 20 areas. Also, the control input is bounded by $|u_{i,t}| \leq 0.1$. We use the Euler method to discretize the dynamics for every 0.1 unit of time. For all areas, the initial state is $[0.1, 0.1]^T$ and the STL specification is $\varphi_i = \mathbf{F}_{[0,6]}\mathbf{G}_{[0,2]}\psi_1 \wedge \mathbf{F}_{[0,8]}\psi_2$, where $\psi_1 = [\delta_i \leq 0.26] \wedge [\delta_i \geq 0.14] \wedge [f_i \leq -0.04] \wedge [f_i \geq -0.16]$ and $\psi_2 = [\delta_i \leq 0.01] \wedge [\delta_i \geq -0.01] \wedge [f_i \leq 0.01] \wedge [f_i \geq -0.01]$. The goal is to synthesize decentralized controllers for each area subject to the specifications. We set the horizon to nine and synthesize the controllers using our approach. The baseline parametric sets are selected to be the viable and action sets generated from (17) while couplings to other areas are ignored. The initial value of all parameters in the distributed algorithm is one. We used Gurobi on a MacBook Pro with 2.6 GHz 6-Core Intel Core i7 and 16 GB memory to run the algorithm. The results are shown in Fig.1a, and Fig.1b. It can be seen that any possible trajectory that passes through the viable sets satisfies the STL specification and at the same time all the implemented controllers satisfy the hard constraint on the control input.

To demonstrate the approach's scalability, we experimented with various number of areas in the ring network and reported the running time in Fig 1c. The stated time period includes only the time spent on second step, but not on solving the MILP. That is because both distributed and centralized approaches share the first step. Additionally, to ensure that the solution exists for high-dimensional state spaces, we consider a large bound for the controller(i.e. $|u_{i,t}| \leq 10$). As predicted, the distributed approach has a slower growth rate, making it more appropriate for the state spaces larger than 40. Moreover, one of the primary benefits of the distributed technique is that it may be calculated in parallel. While we handled everything sequentially here, if multiprocessing is employed, the stated time could be reduced more depending on the number of cores used.



(a) (b) (c)

Fig. 1: (a) The green sets illustrate the viable sets for one of the areas in the case study. The blue and orange sets are the set of states satisfying ψ_1 and ψ_2, respectively. The red sets show the parameterized sets defined on the state space at different time steps for this specific area (some of them are tightly close to the viable sets and are not visible). The black line represents the trajectory traveled by this area. (b) Controllers for each area as time series. (c) Reported time in seconds for the distributed and centralized approach for different state space dimensions.

VII. CONCLUSIONS

Control synthesis subject to both a STL formula and a bounded disturbance is a computationally challenging problem. To overcome this challenge, we propose a solution which consists of two steps: First, we convert satisfaction of the STL formula into a set containment problem. To handle it, we consider the nominal system and use a centralized MILP. We claim that for small enough disturbances, both systems would have the same set of active predicates, which are seen as bounds. Second, we synthesize controllers subject to these bounds. Since the second step needs a set-based calculation, it has a relatively higher computational cost and thus creates a bottleneck for large scale systems. We show that this step can be achieved in a compositional fashion when the STL formula is separable by subsystems.

REFERENCES

[1] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT press, 2008.

[2] Calin Belta and Sadra Sadraddini. Formal Methods for Control Synthesis: An Optimization Perspective. *Robotics, and Autonomous Systems Annu. Rev. Control Robot. Auton. Syst*, 28:12–13, 2018.

[3] E. Camponogara, D. Jia, B.H. Krogh, and S. Talukdar. Distributed model predictive control. *IEEE Control Systems Magazine*, 22(1):44–52, 2002.

[4] Krishnendu Chatterjee and Thomas A Henzinger. Assume-guarantee synthesis. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 261–275. Springer, 2007.

[5] Yuxiao Chen, James Anderson, Karan Kalsi, Steven H Low, and Aaron D Ames. Compositional set invariance in network systems with assume-guarantee contracts. In *2019 American Control Conference (ACC)*, pages 1027–1034. IEEE, 2019.

[6] Alexandre Donzé and Oded Maler. Robust satisfaction of temporal logic over real-valued signals. In *International Conference on Formal Modeling and Analysis of Timed Systems*, pages 92–106. Springer, 2010.

[7] Souradeep Dutta, Xin Chen, and Sriram Sankaranarayanan. Reachability analysis for neural feedback systems using regressive polynomial rule inference. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, pages 157–168, 2019.

[8] Kasra Ghasemi, Sadra Sadraddini, and Calin Belta. Compositional synthesis via a convex parameterization of assume-guarantee contracts. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, pages 1–10, 2020.

[9] Kasra Ghasemi, Sadra Sadraddini, and Calin Belta. Compositional synthesis for linear systems via convex optimization of assume-guarantee contracts. *arXiv preprint arXiv:2208.01701*, 2022.

[10] Antoine Girard. Reachability of uncertain linear systems using zonotopes. In *International Workshop on Hybrid Systems: Computation and Control*, pages 291–305. Springer, 2005.

[11] Sertac Karaman, Ricardo G Sanfelice, and Emilio Frazzoli. Optimal control of mixed logical dynamical systems with linear temporal logic specifications. In *2008 47th IEEE Conference on Decision and Control*, pages 2117–2122. IEEE, 2008.

[12] Eric S Kim, Murat Arcak, and Sanjit A Seshia. Compositional controller synthesis for vehicular traffic networks. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 6165–6171. IEEE, 2015.

[13] Lars Lindemann and Dimos V Dimarogonas. Control barrier functions for multi-agent systems under conflicting local signal temporal logic tasks. *IEEE control systems letters*, 3(3):757–762, 2019.

[14] Zhiyu Liu, Bo Wu, Jin Dai, and Hai Lin. Distributed communication-aware motion planning for multi-agent systems from stl and spatel specifications. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 4452–4457. IEEE, 2017.

[15] Anirudha Majumdar and Russ Tedrake. Funnel libraries for real-time robust feedback motion planning. *The International Journal of Robotics Research*, 36(8):947–982, 2017.

[16] Oded Maler and Dejan Nickovic. Monitoring temporal properties of continuous signals. In *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, pages 152–166. Springer, 2004.

[17] Petter Nilsson and Necmiye Ozay. Synthesis of separable controlled invariant sets for modular local control design. In *2016 American Control Conference (ACC)*, pages 5656–5663. IEEE, 2016.

[18] Pierluigi Nuzzo, Alberto L Sangiovanni-Vincentelli, Davide Bresolin, Luca Geretti, and Tiziano Villa. A platform-based design methodology with contracts and related tools for the design of cyber-physical systems. *Proceedings of the IEEE*, 103(11):2104–2132, 2015.

[19] Chanwook Oh, Eunsuk Kang, Shinichi Shiraishi, and Pierluigi Nuzzo. Optimizing assume-guarantee contracts for cyber-physical system design. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 246–251. IEEE, 2019.

[20] Yash Vardhan Pant, Houssam Abbas, Rhudii A Quaye, and Rahul Mangharam. Fly-by-logic: Control of multi-drone fleets with temporal logic objectives. In *2018 ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS)*, pages 186–197. IEEE, 2018.

[21] Vasumathi Raman, Alexandre Donzé, Mehdi Maasoumy, Richard M Murray, Alberto Sangiovanni-Vincentelli, and Sanjit A Seshia. Model predictive control with signal temporal logic specifications. In *53rd IEEE Conference on Decision and Control*, pages 81–87. IEEE, 2014.

[22] Sadra Sadraddini and Russ Tedrake. Linear encodings for polytope containment problems. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, pages 4367–4372. IEEE, 2019.