Safety-Critical Control Synthesis for Network Systems with Control Barrier Functions and Assume-Guarantee Contracts

Yuxiao Chen, James Anderson, Karan Kalsi, Aaron D. Ames, and Steven H. Low

***Abstract*—This paper aims at the safety-critical control synthesis of network systems such that the satisfaction of the safety constraints can be guaranteed. To handle the large state dimension of such systems, an assume-guarantee contract is used to break the large synthesis problem into smaller subproblems. Parameterized signal temporal logic (pSTL) is used to formally describe the behaviors of the subsystems, which we use as the template for the contract. We show that robust control invariant sets (RCIs) for the subsystems can be composed to form a robust control invariant set for the whole network system under a valid assume-guarantee contract. An epigraph algorithm is proposed to solve for a contract that is valid, —an approach that has linear complexity for sparse networks, which leads to a robust control invariant set for the whole network system. Implemented with control barrier function (CBF), the state of each subsystem is guaranteed to stay within the safe set. Furthermore, we propose a contingency tube Model Predictive Control approach based on the RCI, which is capable of handling severe contingencies, including topology changes of the network. A power grid example is used to demonstrate the proposed method. The simulation result includes both set point control and contingency recovery, and the safety constraint is always satisfied.**

I. Introduction

Network control systems are sometimes subject to safety constraints that should be satisfied the entire time a system is a running. In the event that the network experiences a “sudden or dramatic change”, either through subsystem failure, malicious attack, or unforeseen disturbance, it is imperative that the perturbed system not only maintains stability, but also still satisfies its safety constraints.

An example of such a network is the power grid. It is well known that if not controlled properly, cascading failures may lead to large-scale blackouts. The consequences of which can have a huge impact on infrastructure and economy, and in the worst case, lead to loss of life.

Traditional control techniques usually cannot guarantee the satisfaction of such constraints. One promising solution is “correct-by-construction synthesis”, which has seen recent success in safety-critical applications such as vehicle control [1], [2] and robot navigation [3]. Correct-by-construction synthesis refers to a collection of methods (including but not limited to; barrier functions, density functions, and model checking). They are based on concepts such as reachable sets and robust control invariant sets [4] that ensure controllers are capable of enforcing safety constraints. Informally, a *robust control invariant set* $\mathcal{S}$ is a subset of the state space, such that given a dynamical system initiated from within $\mathcal{S}$, there exists a control policy such that the system state can be kept within $\mathcal{S}$ for all future time, in the presence of disturbances. Typically, correct-by-construction control synthesis relies on computational tools such as the Hamilton Jacobi PDE [5], Linear Matrix Inequalities (LMIs) [6], and sum-of-squares (SOS) programming [7]. Unfortunately, these methods do not scale well with the state dimension of the system. This curse of dimensionality has limited the applications of correct-by-construction control synthesis to systems with low state dimension. There has been efforts to break “the curse of dimensionality,” which, at the system level, typically utilize either compositional analysis [8] or symmetry [9].

To the best of the authors’ knowledge, the synthesis of robust invariant sets for network systems with heterogeneous subsystems and strong coupling between them remains an open problem. Power grids are prominent examples of systems that exhibit the problematic phenomena just described. Typically, they consist of various types of generation buses e.g., hydroelectric, solar, and wind plants, and load buses, all coupled via transmission lines and the need to balance supply and demand whilst attaining frequency synchronization.

The approach we propose to break the curse of dimensionality is to use assume-guarantee contracts [10] to decompose the overall performance guarantee of the network into individual contracts that each subsystem in the network agree to. Every subsystem in the network can take the performance guarantee from other subsystems as assumptions, and in turn provide its own performance guarantee, which then becomes part of the assumptions for other subsystems in the network. In this way, the big synthesis problem is decomposed into small subproblems. One related work is [11], where the authors use decentralized Lyapunov functions to quantify the coupling between subsystems, yet the computation of the Lyapunov functions was not discussed for general nonlinear systems.

The contributions of this paper are:

(i) We propose the formulation of an assume-guarantee contract approach to compute *robust control invariant sets* (RCIs) for networked systems by combining subsystem RCIs with a network assume-guarantee contract.

(ii) We propose an epigraph algorithm that searches for valid assume-guarantee contracts, which has a computational complexity that scales linearly with system size (assuming the system graph is sparse or the coupling signals from multiple neighbors are summable). Moreover, the epigraph algorithm is general-purpose and can be combined with any RCI computation method to compute RCIs for network systems.

(iii) We propose a contingency tube MPC algorithm based on

Yuxiao Chen, Aaron D. Ames, and Steven Low are with the Division of Engineering and Applied Science and Engineering, Caltech, Pasadena, CA, 91106, USA. Emails: {chenyx,ames,slow}@caltech.edu

James Anderson is with the Department of Electrical Engineering and the Data Science Institute at Columbia University, New York, NY 10027, USA. james.andreson@columbia.edu

Karan Kalsi is with Pacific Northwest National Laboratory, Richland, WA, 99352, USA. Email: Karanjit.Kalsi@pnnl.gov

This work is supported by the Battelle Memorial Institute, Pacific Northwest Division, Grant #424858.

assume-guarantee contracts for set invariance, which is real-time implementable and is able to handle severe contingencies such as a change in the network topology.

Nomenclature: $\mathbb{B}$, $\mathbb{N}$, and $\mathbb{R}$ denote the sets of binary variables, natural numbers, and real numbers, respectively. The n-dimensional Euclidean space is denoted by $\mathbb{R}^n$ and $\mathbb{R}^n_+$ denotes the non-negative orthant. Bold characters denote continuous or discrete-time signals, depending on the context, i.e., $\mathbf{x} = \{x(t)\}_{t=0}^{\infty} \in \mathcal{X}^{\mathbb{N}}$ when it is a discrete-time signal; $\mathbf{x} = \{x(t)\}_{t\in[0,\infty)} \in \mathcal{X}^{\mathbb{R}_+}$ when it is a continuous-time signal. $x(t) \in \mathcal{X}$ is a vector denoting the value(s) of $\mathbf{x}$ at time t, $\mathcal{X}^{\mathbb{N}}$ and $\mathcal{X}^{\mathbb{R}_+}$ denote the space of discrete/continuous-time signals of x. Given the set $\mathcal{X} := \mathcal{X}_1 \times, \mathcal{X}_2 \times \ldots \times \mathcal{X}_n$, $x \downarrow \mathcal{X}_i$ denotes the projection of x onto $\mathcal{X}_i$, i.e., $x \downarrow \mathcal{X}_i = x_i$ where $x_i \in \mathcal{X}_i$. To avoid confusion between temporal signals and value iterations, we use $p[i]$ to denote the value of a parameter p after the i^{th} iteration. $\mathbf{Poly}(P, q) = \{x \mid Px \leq q\}$ denotes a polytope defined with matrix P, q.

II. Problem Setup

In this section, we present the problem setup and show how the power grid control synthesis can be handled with the proposed method.

A. Network System Dynamics

We consider a network dynamic system consisting of subsystems with coupling dynamics. The couplings between neighboring subsystems are treated bounded disturbances. Therefore, the following product of subsystems is considered:[1]

$$\Sigma = \Sigma_1 \times \Sigma_2 \times \ldots \times \Sigma_N. \tag{1}$$

It is assumed that each subsystem can be written in the form

$$\Sigma_i := \begin{cases} x_i^+ = f_i\left(x_i, y_{\mathcal{N}_i}, u_i, d_i\right), \\ y_i = c_i\left(x_i\right), \end{cases} \tag{2}$$

where $x_i \in \mathcal{X}_i \subseteq \mathbb{R}^{n_i}$ is the i^{th} current state and x_i^+ denotes the successor state. The control input is $u_i \in \mathcal{U}_i \subseteq \mathbb{R}^{m_i}$, the exogenous disturbance is $d_i \in \mathcal{D}_i \subseteq \mathbb{R}^{l_i}$, and $y_{\mathcal{N}_i}$ denotes the vector of signals consisting of the outputs of all of the neighboring subsystems connected to subsystem Σ_i. The vector $y_{\mathcal{N}_i}$ can be further decomposed as

$$y_{\mathcal{N}_i} = \begin{bmatrix} y_{j_1} & \ldots & y_{j_{N_i}} \end{bmatrix}^\intercal, \forall\ j_1, \ldots, j_{N_i} \in \mathcal{N}_i, \tag{3}$$

where $\mathcal{N}_i$ is the neighbor set of the i^{th} node with cardinality $|\mathcal{N}_i| = N_i$. The full networked system dynamics is then:

$$\begin{aligned} x^+ = f(x, u, d) &= \begin{bmatrix} f_1(x_1, y_{\mathcal{N}_1}, u_1, d_1) & \ldots & f_N(x_N, y_{\mathcal{N}_N}, u_N, d_N) \end{bmatrix}^\intercal, \\ c(x) &= \begin{bmatrix} c_1(x_1) & \ldots & c_N(x_N) \end{bmatrix}^\intercal. \end{aligned} \tag{4}$$

The overall state space and output space are denoted as $\mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_N$ and $\mathcal{Y} = \mathcal{Y}_1 \times \ldots \times \mathcal{Y}_N$, respectively. Since the method was first proposed for fixed point control, it is assumed w.l.o.g. that the equilibrium point is at the origin, i.e. $f(0, 0, 0) = 0$ and that $c(0) = 0$.

Given the dynamics, the behavior of the i^{th} subsystem is uniquely determined by $x_i(0)$, $\mathbf{y}_{\mathcal{N}_i}$, $\mathbf{u}_i$ and $\mathbf{d}_i$, let $\mathcal{I}_i = \mathcal{X}_i \times \mathcal{Y}_{\mathcal{N}_i}^{\mathbb{N}} \times \mathcal{U}_i^{\mathbb{N}} \times \mathcal{D}_i^{\mathbb{N}}$ denote the space of input signals and initial conditions of the system Σ_i and $\mathcal{X}_i^{\mathbb{N}}$ is the space of all possible state signals of Σ_i. A dynamical system $\Sigma_i \subseteq 2^{\mathcal{I}_i} \times 2^{\mathcal{X}_i^{\mathbb{N}}}$ is understood as a subset of possible input and state signal pairs.

Remark 1. The results in this paper can easily be extended to the case of continuous-time dynamical systems. However, the methods we use to compute robust control invariant sets are most naturally presented in discrete-time, hence our choice.

III. Review of Major Tools

In this section, we review the major tools necessary to our approach, including control barrier functions and parameterized assume-guarantee contracts.

A. Control Barrier Functions

The computed robust control invariant set will be enforced with a control barrier function (CBF). CBFs allow safety constraints which are enforced through barrier functions to be integrated with performance objectives encoded through control Lyapunov functions. Given a set of allowable initial conditions $\mathcal{X}_0$, and an unsafe set $\mathcal{X}_d$, a CBF ensures that all trajectories of a dynamical system initiated from $\mathcal{X}_0$ never enter $\mathcal{X}_d$. Typically the computation of a CBF acquired through convex programming requires an existing stabilizing control law termed the "legacy controller". The controller produced by the CBF is referred to as the "supervisory controller".

To accommodate for the discrete-time dynamics used in this paper, we adopt the result in [13], [14] and utilize a discrete-time zeroing control barrier function. Specifically, given a discrete-time dynamic system:

$$x^+ = f(x, u, d),\ x \in \mathbb{R}^n,\ u \in \mathcal{U},\ d \in \mathcal{D},$$

a discrete-time CBF is a function $h : \mathbb{R}^n \to \mathbb{R}$ that satisfies

$$\begin{aligned} &\forall\ x \in \mathcal{X}_0, && h(x) \geq 0 \\ &\forall\ x \in \mathcal{X}_d, && h(x) < 0 \\ &\forall\ x \in \{x \mid h(x) \geq 0\}, && \forall\ d \in \mathcal{D}, \exists\ u \in \mathcal{U} \\ & && \text{s.t. } h(f(x, u, d)) \geq \gamma(h(x)), \end{aligned} \tag{5}$$

where $\gamma : \mathbb{R} \to \mathbb{R}$ satisfies $s^2 \geq \gamma(s) \cdot s \geq 0$, i.e. $\gamma(s)$ has the same sign as s and $|\gamma(s)| \leq |s|$. The supervisory controller is then implemented with the CBF QP:

$$\begin{aligned} u^\star = \underset{u \in \mathcal{U}}{\arg\min} & \left\| u - u^0(x) \right\|^2 \\ \text{s.t. } & h(f(x, u, d)) \geq \gamma(h(x)), \end{aligned} \tag{6}$$

where u^0 is the legacy controller's policy. The constraint set (5) is not always convex. We will show later that it is convex for the special case discussed in this paper.

Remark 2. For the case when the disturbance set $\mathcal{D}$ is known, (5) is realizable. When the disturbance set is unknown, it is straightforward to extend (5) to a robust CBF which can be solved using quadratic programming, see [15] as an example.

It can be shown that under mild conditions, a CBF ($h(\cdot)$ in (5)) can be constructed with a properly chosen $\gamma(\cdot)$ ($\gamma(x) \equiv$

[1] In general, a networked dynamical system model would be defined over a graph structure [12].However, because we view the coupling between systems as bounded disturbances, we can consider a network of dynamical systems as the more simple the product system.

0 is always a valid choice) from a robust control invariant set (RCI) that contains $\mathcal{X}_0$ and does not intersect $\mathcal{X}_d$.

We use robust linear programming to compute a minimal robust control invariant set for each subsystem in the network [16]. The algorithm is described in Appendix A. Note that the contract-based framework we propose and the epigraph algorithm introduced in Section V, are both compatible with *any* algorithm that constructs and RCI.

The robust linear programming algorithm generates a polytopic RCI $\mathbf{Poly}(P, q)$, where P is a constant $m \times n$ matrix and $q \in \mathbb{R}^m_{>0}$. Note that the origin is always contained in the interior of the RCI. The CBF is defined as

$$h(x) = \min_k \frac{q_k - P_k x}{q_k}, \tag{7}$$

where P_k is the k^{th} row of P and q_k is the k^{th} entry of q.

B. Parameterized Signal Temporal Logic

To break the "curse of dimensionality" for large network systems, we use assume-guarantee contracts to decompose the synthesis problem for the whole network into smaller subproblems for the subsystems [10], [17]. The language of the specifications is Signal Temporal Logic (STL), which is an extension of Linear Temporal Logic (LTL) that allows for real time and predicates over real-valued signals[18], [19]. We note that LTL deals with discrete-time signals, whereas STL uses continuous-time signals. Since the dynamics we consider in this paper are in discrete-time, we extend an STL formula to discrete-time signals by considering sample instances, as discussed in [20]. This is necessary since STL's ability to allow for parameterized propositions is needed. A Signal Temporal Logic formula $\phi : \mathcal{X}^{\mathbb{R}_+} \to \mathbb{B}$ uses the following grammar:

$$\phi = \top \mid \mu \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \mathbf{U}_I \phi_2,$$

where $\top$ is the logical tautology, $\mu : \mathcal{X} \to \mathbb{B}$ is the space of all continuous time signal of x. is a logic proposition, $\neg$ is Boolean negation, $\wedge$ is the Boolean **AND**. Finally, the "until" operator $\mathbf{U}$ which takes ϕ_1 and ϕ_2 as arguments, is true if given the interval I, there exists a time $t \in I$ that ϕ_2 is true, and before t, ϕ_1 is always true. When I is not specified, it is assumed that by default $I = [0, \infty)$. The validity of a formula μ with respect to the signal $\mathbf{x}$ at time t can be determined as

$$\begin{array}{lll}
(\mathbf{x}, t) \models \mu & \text{iff} & x(t) \text{ satisfies } \mu \\
(\mathbf{x}, t) \models \neg\phi & \text{iff} & x(t) \not\models \phi \\
(\mathbf{x}, t) \models \phi_1 \wedge \phi_2 & \text{iff} & x(t) \models \phi_1 \text{ and } x(t) \models \phi_2 \\
(\mathbf{x}, t) \models \phi_1 \mathbf{U}_{[a,b]} \phi_2 & \text{iff} & \begin{array}{l} \exists\ t' \in t + [a, b] \text{ s.t. } x(t) \models \phi_2 \\ \text{and } \forall\ t'' \in [t, t'], x(t) \models \phi_1 \end{array}
\end{array}$$

where $\models$ and $\not\models$ stands for "satisfies" and "does not satisfy" respectively. A signal $\mathbf{x} \models \mu$ if $(\mathbf{x}, 0) \models \mu$. From the above basic grammar, one can derive additional temporal operators such as $\Diamond_I \phi \doteq \top \mathbf{U}_I \phi$, meaning "$\phi$ is eventually true during I," and $\Box_I \phi \doteq \neg(\Diamond_I \neg\phi)$, meaning "$\phi$ is always true in I".

Given an STL formula ϕ, $L(\phi) = \left\{\mathbf{x} \in \mathcal{X}^{\mathbb{R}_+} \mid \mathbf{x} \models \phi\right\}$ is the language of the formula. A partial order is defined among STL formulas as $\phi_1 \preceq \phi_2$ if $\forall\ \mathbf{x} \in \mathcal{X}^{\mathbb{R}_+}, (\mathbf{x} \models \phi_1) \Rightarrow (\mathbf{x} \models \phi_2)$, or equivalently, $L(\phi_1) \subseteq L(\phi_2)$.

A Parameterized Signal Temporal Logic (pSTL) formula is an STL formula with parameters. For example, $\phi = \Box_{[a,b]}(x \geq c)$ can be represented as the following pSTL: $\varphi(a, b, c) = \Box_{[a,b]}(x \geq c)$, where a, b and c are the parameters and $\varphi : \mathbb{R}^3 \to (\mathcal{X}^{\mathbb{R}_+} \to \mathbb{B})$ is the pSTL template. For the rest of the paper, it is assumed that all the pSTL formulas are defined on partially ordered parameter domains. Given a parameter domain $\mathcal{P}$, the partial order is denoted as $\leq_{\mathcal{P}}$. For a pSTL φ with domain $\mathcal{P}_1$, if $\mathcal{P}_1$ is a subspace of $\mathcal{P}_2$, then $\forall\ p \in \mathcal{P}_2$, $\varphi(p) = \varphi(p_{\downarrow}\mathcal{P}_1)$, where $\downarrow$ denotes the projection onto $\mathcal{P}_1$.

C. Assume-Guarantee Contract for Network Systems

Finally, we present a framework that builds a large assume-guarantee contract from small subcontracts, which is then used for the RCI computation whole network. We adopt the definition of assume-guarantee contract from [21]:

Definition 1 (Assume-Guarantee Contract)**.** An assume-guarantee contract $\mathcal{C}$ for the dynamic system Σ is a pair of STL formulae $[\phi_a, \phi_g]$ consisting of an assumption ϕ_a and a guarantee ϕ_g that enforces the logical implication $\phi_a \to \phi_g$.

An assume-guarantee contract $\mathcal{C} = [\phi_a, \phi_g]$ is true for a dynamic system Σ if $\Sigma \cap L(\phi_a) \subseteq L(\phi_g)$, or written compactly as $\phi_a \wedge \Sigma \to \phi_g$ with a slight abuse of notation. Note that Σ here is understood as a proposition, interpreted as "a trace satisfies the system dynamics".

Definition 2 (Parameterized Assume-Guarantee Contract)**.** An assume-guarantee contract $\mathcal{C} = [\phi_a, \phi_g]$ is in parameterized form if there exists pSTLs $\phi_a = \varphi_a(p_a)$, $\phi_g = \varphi_g(p_g)$ and a mapping $\lambda : \mathcal{P}_a \to \mathcal{P}_g$ such that $\mathcal{C}(p_a) = [\varphi_a(p_a), \varphi_g(\lambda(p_a))]$.

In particular, ϕ_a consists of two parts: $\phi_a = \phi_{ae} \wedge \phi_{af} = \varphi_{ae}(p_{ae}) \wedge \varphi_{af}(p_{af})$, where ϕ_{ae} is the specification for exogenous environment behavior and ϕ_{af} is the feedback specification, which is understood as the specification that changes with other contracts.

Definition 3 (Parameterized Network Assume-Guarantee Contract)**.** For a network defined in (1), a parameterized network assume-guarantee contract consists of individual parameterized assume-guarantee contracts $\mathcal{C}_i$ for each subsystem Σ_i. Let $p_{ae} \in \mathcal{P}_{ae}$, $p_{af} \in \mathcal{P}_{af}$ and $p_g \in \mathcal{P}_g$ be the parameters for φ_{ae}, φ_{af} and φ_g. Each subcontract $\mathcal{C}_i$ consists of $\phi^i_a = \varphi^i_{ae}(p^i_{ae}) \wedge \varphi^i_{af}(p^i_{af})$ and $\phi^i_g = \varphi^i_g(p^i_g)$. where $p^i_{ae} = p_{ae} \downarrow \mathcal{P}^i_{ae}$, $p^i_{af} = p_{af} \downarrow \mathcal{P}^i_{af}$ and $p^i_g = p_g \downarrow \mathcal{P}^i_g$. Then the network assume-guarantee contract is defined as $\mathcal{C} = [\phi_{ae} \wedge \phi_{af}, \phi_g]$ with the parameter mapping $\Lambda : \mathcal{P}_{ae} \times \mathcal{P}_{af} \to \mathcal{P}_g$ and

$$\begin{aligned}
\phi_{ae} = \quad \varphi_{ae}(p_{ae}) &= \bigwedge_{i=1}^{N} \phi^i_{ae} = \bigwedge_{i=1}^{N} \varphi^i_{ae}(p^i_{ae}), \\
\phi_{af} = \quad \varphi_{af}(p_{af}) &= \bigwedge_{i=1}^{N} \phi^i_{af} = \bigwedge_{i=1}^{N} \varphi^i_{af}(p^i_{af}), \\
\phi_g = \quad \varphi_g(p_g) &= \bigwedge_{i=1}^{N} \phi^i_g = \bigwedge_{i=1}^{N} \varphi^i_g(p^i_g).
\end{aligned} \tag{8}$$

IV. Set Invariance with Assume-Guarantee Contracts

We now present one of the main results of this paper, which utilizes a network assume-guarantee contract to prove

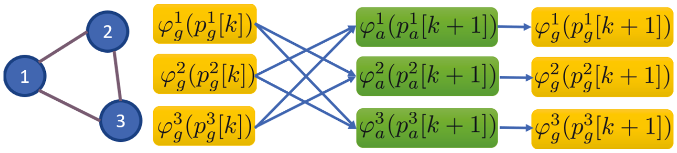

1
2
3
$\varphi_g^1(p_g^1[k])$
$\varphi_g^2(p_g^2[k])$
$\varphi_g^3(p_g^3[k])$
$\varphi_a^1(p_a^1[k+1])$
$\varphi_a^2(p_a^2[k+1])$
$\varphi_a^3(p_a^3[k+1])$
$\varphi_g^1(p_g^1[k+1])$
$\varphi_g^2(p_g^2[k+1])$
$\varphi_g^3(p_g^3[k+1])$

Fig. 1: Network assume-guarantee contract for a 3-node network

set invariance for network systems.

Theorem 1 (Assume-guarantee reasoning)**.** *Consider the network system in* (2) *associated with a parameterized network assume-guarantee contract defined in Definition 3 with parameter mapping* Λ*. Suppose the following are satisfied:*
1. Under the local mapping $\lambda_i : \mathcal{P}^i_{ae} \times \mathcal{P}^i_{af} \to \mathcal{P}^i_g$ *for each subsystem, the following subcontract* $\mathcal{C}_i : \Sigma_i \wedge \varphi^i_{ae}(p^i_{ae}) \wedge \varphi^i_{af}(p^i_{af}) \to \varphi^i_g(\lambda_i(p^i_{ae}, p^i_{af}))$ *is satisfied for all* $p^i_a \in \mathcal{P}^i_a \doteq \mathcal{P}^i_{ae} \times \mathcal{P}^i_{af}$*,*
2. There exists a mapping $\Gamma : \mathcal{P}_g \to \mathcal{P}_{af}$ *such that* $\varphi_g(p_g) \preceq \varphi^i_{af}(\gamma_i(p_g))$*, where* $\gamma_i(p_g) = \Gamma(p_g) \downarrow \mathcal{P}^i_{af}$*.*
3. There exists $p_{ae} \in \mathcal{P}_{ae}$ *such that* $\varphi_{ae}(p_{ae})$ *is true.*
4. There exists an initial feedback parameter $p_{af}[0] \in \mathcal{P}_{af}$ *such that* $\varphi_{af}(p_{af}[0])$ *is true.*

Given p^i_{ae}*, define* $\hat{\lambda}_i(\cdot) = \lambda_i(p^i_{ae}, \cdot)$*. Let* $\hat{\Lambda}(p_{af}) = [\hat{\lambda}_1(p^1_{af})^\intercal,\ \hat{\lambda}_2(p^2_{af})^\intercal,\ \ldots\ \hat{\lambda}_N(p^N_{af})^\intercal]^\intercal$*, then define recursively* $p_g[k] = \hat{\Lambda}(p_{af}[k])$*,* $p_{af}[k+1] = \Gamma(p_g[k])$*. Under these conditions, the network system satisfies*

$$\hat{\phi}_g = \bigwedge_{k=0}^{\infty} \varphi_g(p_g[k]). \tag{9}$$

See the Appendix B for the proof.

Fig. 1 shows an example on a 3-node network. The guarantee of each node constitutes the assumption for the next iteration, and each node takes the assumption about its neighbors as an assumption from which a guarantee is obtained.

Theorem 1 can be viewed as the logical analogy of set invariance. If we have the recursive reasoning that propagates forward (ϕ_{af}), and the initial logic proposition is satisfied (ϕ_{ae}), then all the subsequent propositions are satisfied. Note that the guarantees on subsystems' behavior are shared across the network as assumptions for the next iteration.

Next, we apply Theorem 1 to show set invariance of a network system. Consider a network system described by (2). Suppose that all subsystem outputs, y_i, are scalars[2], and for each subsystem Σ_i, $y_{\mathcal{N}_i}$ is treated as a disturbance. Then given a bound on $y_{\mathcal{N}_i}$: $|y_{\mathcal{N}_i}| \le y^{\max}_{\mathcal{N}_i}$, a bound $\mathcal{D}_i$ on d_i and a bound $\mathcal{U}_i$ on u_i, any RCI algorithm can be applied to compute $\mathcal{S}_i$ for Σ_i that satisfies

$$\begin{aligned} &\forall\ x_i \in \mathcal{S}_i, \quad \forall\ d_i \in \mathcal{D}_i, \quad \forall\ |y_{\mathcal{N}_i}| \le y^{\max}_{\mathcal{N}_i}, \\ &\exists\ u_i \in \mathcal{U}_i\ s.t. \quad x_i^+ = f_i\left(x_i, y_{\mathcal{N}_i}, u_i, d_i\right) \in \mathcal{S}_i. \end{aligned}$$

Assume that $\mathcal{D}_i$ and $\mathcal{U}_i$ are given as part of the problem specification for all subsystems, the only information needed for the RCI computation is $y^{\max}_{\mathcal{N}_i}$. Let $\mathscr{F}$ be such a procedure that takes $y^{\max}$ as input, and computes an RCI. For clarity, we let $\mathscr{F}_i(y^{\max}_{\mathcal{N}_i}) \subseteq \mathcal{X}_i$ be an RCI computed by $\mathscr{F}$ for the i^{th} subsystem Σ_i, and let $\mathscr{F}(y^{\max}) \doteq \mathscr{F}_1(y^{\max}_{\mathcal{N}_1}) \times \ldots \times \mathscr{F}_N(y^{\max}_{\mathcal{N}_N})$ be the products of all the individual RCIs.

Remark 3*.* Given a fixed procedure $\mathscr{F}$, it can be thought of as a mapping from the parameter $y^{\max}$ to the RCIs for the subsystems, which is then used to enforce constraints on the state. Note that $\mathscr{F}(y^{\max})$ is simply the product of RCIs for all the subsystems, and is not necessarily an RCI for the network system. It has to satisfy the validity condition defined later to be an RCI for the network system.

Definition 4. $\mathscr{F}$ is *monotonic* w.r.t. $y^{\max}$ if given $y^{\max,1} \ge y^{\max,2} \ge 0$, $\mathscr{F}(y^{\max,2}) \subseteq \mathscr{F}(y^{\max,1})$. The inequality is defined element-wise.

Lemma 1. *There always exists an* $\mathscr{F}$ *which is monotonic w.r.t.* $y^{\max}$*.*

Proof. $y^{\max,1} \ge y^{\max,2}$ implies that the uncertainty set for $\mathscr{F}(y^{\max,1})$ is a superset of the uncertainty set for $\mathscr{F}(y^{\max,2})$, so $\mathscr{F}(y^{\max,1})$ is also an RCI under $|y| \le y^{\max,2}$. □

The lemma above is intuitive since the size of the RCI should monotonically grow with the size of the disturbance bound. Under lemma 1, we make the following assumption.

Assumption 1. The RCI computation procedure $\mathscr{F}$ considered in this paper is monotonic. Lemma 1 shows that this assumption can be made without loss of generality.

Given a procedure $\mathscr{F}$ that computes RCIs for subsystems given $y^{\max}$ as described above, define the local mapping λ_i:

$$\begin{aligned} \lambda_i(y^{\max}_{\mathcal{N}_i}) &\doteq \max_{x_i \in \mathscr{F}_i(y^{\max}_{\mathcal{N}_i})} \left| h_i(x_i) \right|, \\ \Lambda(y^{\max}) &\doteq [\lambda_1(y^{\max}_{\mathcal{N}_1}); \lambda_2(y^{\max}_{\mathcal{N}_2}); \ldots; \lambda_N(y^{\max}_{\mathcal{N}_N})]. \end{aligned} \tag{10}$$

Note that $\Lambda(y^{\max})$ has the same dimension as $y^{\max}$. Then we have our main theorem:

Theorem 2 (Set invariance of a network system with assume-guarantee contract)**.** *Given an RCI computation procedure* $\mathscr{F}$ *and let* Λ *be defined in* (10)*. If there exists a* $y^{\max} \in \mathbb{R}^N_+$ *such that*

$$\Lambda(y^{\max}) \le y^{\max}, \tag{11}$$

then $\mathscr{F}(y^{\max})$ *is an RCI for the network system.*

See the Appendix C for the proof.

The condition in (11) is the critical condition to show invariance, from hereon we refer to it as the "*validity condition*". It can be interpreted as the condition *that each subsystem can satisfy what other nodes assume of it*. In the next section we will describe an algorithm that searches for a $y^{\max}$ that satisfies the validity condition when feasible.

V. Epigraph Method for Valid Contracts

In this section, we present an *epigraph algorithm* that searches for an assume-guarantee contract that meets the validity condition (11) if one exists. In particular, we show that the epigraph algorithm can be viewed as an extension of the classic *small gain* theorem to network systems with nonlinear "gains" and multiple interconnected systems.

[2] Scalar outputs are required for the epigraph algorithm (described on the next page) to work. Future work will relax this assumption.

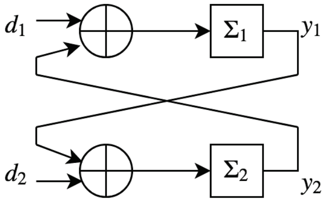


Fig. 2: Two systems interconnection network

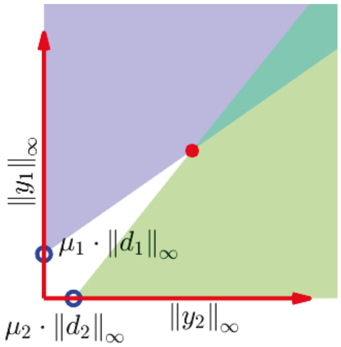


Fig. 3: Epigraph view of the small gain theorem

A. Epigraph Representation of the Validity Condition

Recall that given a function $g : \mathbb{R}^m \to \mathbb{R}$, the epigraph of g is defined as

$$\mathbf{epi}(g) := \{(x, t) \mid x \in \mathbf{dom}\, g,\ g(x) \le t\},$$

where $\mathbf{dom}\, g$ denotes the domain of g.

The idea behind our algorithm is to view each local $\lambda_i : \mathbb{R}_+^{N_i} \to \mathbb{R}_+$ as a function and consider its epigraph. Recall that λ_i defined in (10) denotes the mapping from the bounds on the outputs of the neighbors to the bound on the output of subsystem i. The condition in (11) is equivalent to the following condition:

$$[y_{\mathcal{N}_i}^{\max}; y_i^{\max}] \in \mathbf{epi}(\lambda_i).$$

Note that this is a condition of only $y^{\max}$. Suppose the epigraph of each λ_i is known, the search for a valid contract can be formulated as the following optimization:

$$\begin{aligned} \min_{y^{\max} \ge \mathbf{0}} \ & \sum_{i=1}^{N} y_i^{\max} \\ \text{s.t.}\ & \forall\ i = 1, ..., N,\ [y_{\mathcal{N}_i}^{\max}; y_i^{\max}] \in \mathbf{epi}(\lambda_i). \end{aligned} \tag{12}$$

Example 1. Consider the two systems Σ_1 and Σ_2 interconnected as shown in Fig. 2. Suppose that there exist constants $\mu_1, \mu_2, \nu_1, \nu_2 \ge 0$ such that

$$\begin{aligned} \|y_1\|_\infty &\le \mu_1 \|d_1\|_\infty + \nu_1 \|y_2\|_\infty, \\ \|y_2\|_\infty &\le \mu_2 \|d_2\|_\infty + \nu_2 \|y_1\|_\infty. \end{aligned} \tag{13}$$

If, in addition, the small gain condition is satisfied, i.e., $\nu_1 \nu_2 < 1$, then the small gain theorem tells us that the interconnection is stable and

$$\begin{aligned} \|y_1\|_\infty &\le \frac{\mu_1}{1 - \nu_1\nu_2} \|d_1\|_\infty + \frac{\mu_2 \nu_1}{1 - \nu_1\nu_2} \|d_2\|_\infty, \\ \|y_2\|_\infty &\le \frac{\mu_1 \nu_2}{1 - \nu_1\nu_2} \|d_1\|_\infty + \frac{\mu_2}{1 - \nu_1\nu_2} \|d_2\|_\infty. \end{aligned} \tag{14}$$

The proof can be found in [22]. The same result can be obtained by considering the epigraph.

Proposition 1. *Given* (13) *and bounded* $\|d_i\|_\infty > 0, i = 1, 2,$ *there exists an assume-guarantee contract that guarantees* (14) *if* $\nu_1 \cdot \nu_2 < 1$.

Due to space limitations, the proof is omitted. It can be found in [23].

Remark 4. This example shows that the small gain theorem can be viewed as a special case of the epigraph method, which is still applicable when λ_i are nonlinear functions and when there are more than 2 interconnected subsystems.

In practice, $\mathbf{epi}(\lambda_i)$ usually does not have a simple explicit form. Fortunately, we can replace $\mathbf{epi}(\lambda_i)$ in (12) with a tractable inner approximation and the optimization would still generate a valid contract if feasible. The inner approximation of $\mathbf{epi}(\lambda_i)$ can be obtained by a grid sampling approach. To be specific; evaluate λ_i at all the grid points (fixing $y_{\mathcal{N}_i}^{\max}$) by computing an RCI and evaluating (10). The approximation of $\mathbf{epi}(\lambda_i)$ is the area above the grid points in $[y_{\mathcal{N}_i}^{\max}; \lambda_i(y_{\mathcal{N}_i}^{\max})]$ space. The sampling complexity grows exponentially with the number of neighbors N_i. To reduce the sampling complexity, we introduce the notion of *summable signals.*

Definition 5. Two or more disturbance signals are *summable* if they have the same input dynamics. To be specific, consider $x^+ = f(x, u, d)$, where $d = [d_1, ..., d_l]^\intercal \in \mathbb{R}^l$ is the disturbance. The individual disturbances $\{d_i\}$ are summable if $\exists\ \bar{f}$ such that $f(x, u, d) \equiv \bar{f}(x, u, \sum_i d_i)$.

Summable disturbance inputs can be combined and viewed as one disturbance since they invoke the same disturbance dynamics and their bounds are summable, i.e.,

$$(|d_1| \le \alpha) \wedge (|d_2| \le \beta) \Rightarrow |d_1 + d_2| = |d| \le \alpha + \beta,$$

where the equality follows by definition. Since the number of samples grows exponentially with the number of disturbance inputs, combining summable disturbance inputs reduces the complexity of the epigraph algorithm.

VI. Power Grid Case Study

We now apply our assume guarantee framework (and epigraph algorithm) to a power network case study. We consider the problem of load-side primary frequency control [24]. The safety constraint considered is that the frequency deviation should never exceed a predefined bound. Frequency regulation is critical in power network. Modest deviations can damage electrical equipment and infrastructure (at the point of load, generation and/or distribution), overload transmission lines leading to market inefficiency, degrade the power quality delivered to consumers, and cause a network collapse if protective systems kick in to protect equipment. In the US, the nominal frequency is 60Hz and we further impose that the frequency deviation is below $0.05 rad/s$. Broadly speaking, if power demand exactly matched supply, then frequency would not deviate from its set-point. However, demand and supply can never be exactly matched; excess supply results in an increased frequency while a deficit causes frequency to decrease. Large deviations for extended periods of time will result in load shedding and potentially islanding.

There has been a lot of effort focusing on the stability, optimality, and safety of power networks, see for example the survey paper [25]. Specifically, the Optimal Load Control (OLC) algorithms in [26], [24] provide control laws that can asymptotically track an optimal load-control problem i.e., control policy that achieves good asymptotic performance and maximizes economic benefit. To be more specific, the virtual flow method proposed in [24] formulates an OLC problem and derives a control policy based on a primal-dual update of the Lagrangian. However, despite good asymptotic performance, it lacks a performance guarantee in the transient phase. In particular, under contingencies such as large perturbation or topology change, the frequency deviation may exceed the $\pm 0.05 rad/s$ bound.

We shall use the OLC controller as the legacy controller to demonstrate the capability of the CBF controller proposed in Section III-A. We will later show that robust control invariant sets with control barrier functions are a good complement to the OLC controller since it guarantees set invariance with minimum intervention and preserves the performance of the OLC controller when the violation of safety constraints is not imminent.

A. Power Grid Dynamics

We consider a transmission model of the power grid consisting of two types of buses; generators and loads. Take the IEEE 9-bus network depicted in Fig. 8 as an example. The set of generator buses are $\mathcal{G} = \{1, 2, 3\}$, the remainder are pure load buses, the set of which is denoted by $\mathcal{L}$. The dynamics of the grid can be described by the following model [24]:

$$\begin{aligned} \dot{\theta}_i &= \omega_i, \qquad (15)\\ M_i \dot{\omega}_i &= P_i^{in} - D_i \omega_i - r_i - u_i - \sum_{j \in \mathcal{N}_i} \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), i \in \mathcal{G}\\ 0 &= P_i^{in} - D_i \omega_i - r_i - u_i - \sum_{j \in \mathcal{N}_i} \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), i \in \mathcal{L}, \end{aligned}$$

where θ_i and ω_i are the phase angle and frequency respectively of the voltage at bus i, P_i^{in} and r_i are the input power and uncontrollable load at bus i. A sudden change to either P_i^{in} or r_i is the main source of disturbance to the system, and the controllable load u_i is used to regulate the power network. Each generator bus is modelled as a second order system with state $x_i = [\theta_i, \omega_i]^\intercal$, and M_i and D_i are the generator inertia and damping coefficient respectively; each load bus is modelled as a first order system with $x_i = \theta_i$ and zero inertia. X_{ij} is the reactance of the circuit between bus i and bus j. We choose the output to be $y_i = \theta_i$ since the coupling between buses occurs through the phase angles θ_i. The model in (15) can be linearized and for each node, the subsystem dynamics Σ_i are given by

$$\begin{bmatrix} \delta\dot{\theta}_i \\ \dot{\omega}_i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ \frac{-\sum\limits_{j \in \mathcal{N}_i} B_{ij}}{M_i} & \frac{-D_i}{M_i} \end{bmatrix} \begin{bmatrix} \delta\theta_i \\ \omega_i \end{bmatrix} + \begin{bmatrix} 0 \\ -M_i^{-1} \end{bmatrix} u_i \qquad (16)$$

$$+ \begin{bmatrix} 0 & \cdots & 0 \\ \frac{B_{ij_1}}{M_i} & \cdots & \frac{B_{ij_{N_i}}}{M_i} \end{bmatrix} \begin{bmatrix} \delta\theta_{j_1} \\ \vdots \\ \delta\theta_{j_{N_i}} \end{bmatrix} + e_i, \qquad i \in \mathcal{G},$$

$$\delta\dot{\theta}_i = \frac{-\sum\limits_{j \in N_i} B_{ij}}{D_i} \delta\theta_i + \frac{-1}{D_i} u_i + \frac{\sum\limits_{j \in \mathcal{N}_i} B_{ij} \delta\theta_j}{D_i} + e_i, \quad i \in \mathcal{L}$$

with output $y_i = \delta\theta_i$. $B_{ij} = \frac{V_i V_j}{X_{ij}} \cos(\theta_i^0 - \theta_j^0)$ is the sensitivity of power flow to phase variations and θ_i^0 is the steady-state phase angle at bus i. $B_{ij} \neq 0$ when bus i and j are neighbors.

As mentioned before, the **control objective** is to prevent large frequency deviation from a set value. However, since the coupling is via the phase angle differences, in order to bound the frequency deviation, one needs to bound phase angle deviations as well. We will thus construct a robust control invariant set for both the phase angle and the frequency. The RCI should provide robustness to sudden changes of the input power P_i^{in}, uncontrollable load r_i and the coupling between neighboring buses. We will treat the frequency deviation bound as the **safety constraint**, i.e., the danger set $\mathcal{X}_i^d$ for a generator bus Σ_i is defined as

$$\mathcal{X}_i^d = \{[\delta\theta_i, \omega_i]^\intercal \mid |\omega_i| \geq \omega^{\max}\}, \qquad (17)$$

where $\omega^{\max}$ is the bound for frequency deviation. Note that the coupling between neighboring nodes happens via the phase angle, which is a scalar output. If we can use assume-guarantee contract to put bound on the phase angle deviations, we can compute an RCI for each node, which in turn constitute an RCI for the whole power grid network.

Let $\mathcal{X}_0$ be the set of allowed initial states, $\mathcal{X}_d$ be defined in (17) for the generator buses (there is no $\mathcal{X}_d$ for pure load buses), we enforce additional constraint in the RCI computation such that the RCI does not contain $\mathcal{X}_d$, see Appendix A for further details. With the polytopic RCI computed, the CBF is defined in (7) and it can be verified that it satisfies (5). Then, the RCI can be enforced with the quadratic program (6).

B. Epigraph Method for the search of valid Contracts

To make sure that the CBF QP is always feasible, a robust control invariant set for the power network is needed. Since the goal is fixed point tracking, we use the linearized dynamics presented in (16) for each node, and include the linearization error in the disturbance term. The assume-guarantee contract in this example follows the form introduced in Section III-C. Each bus takes the bound on the phase angle deviation of its neighbors as the assumption, and guarantees that its own phase angle deviation stays bounded. The contract parameters are the bounds on phase angle deviation for each bus $\theta^{\max}$.

The computation of the RCI follows the robust linear programming algorithm [16]. For each bus, the RCI is computed with the linearized model in (16) after time discretization. The inputs to the RCI computation of the i^{th} bus are the input sets $\mathcal{U}_i$ and exogenous disturbance bounds $\mathcal{D}_i$, given as the environment assumptions ϕ_{ae}^i (fixed), and bounds on the phase angle deviations of neighboring buses $\theta_{\mathcal{N}_i}^{\max}$, given as the feedback assumption ϕ_{af}^i. Let $\mathscr{F}$ be the RCI computation procedure, and define

$$\lambda_i(\theta_{\mathcal{N}_i}^{\max}) = \max_{x_i \in \mathscr{F}(\theta_{\mathcal{N}_i}^{\max})} |\theta_i|. \qquad (18)$$

In the IEEE 9 bus example (as shown in Fig. 8), we add an additional constraint to $\mathscr{F}$ such that for each RCI, $\mathcal{S}_i$,

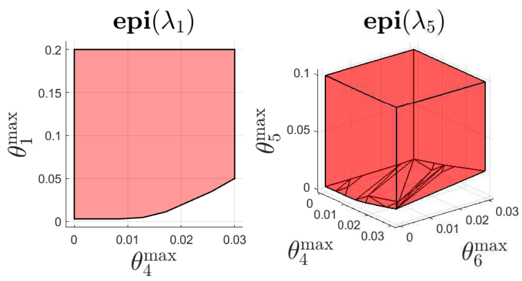


Fig. 4: Inner approximations of $\mathbf{epi}(\lambda_1)$ and $\mathbf{epi}(\lambda_5)$

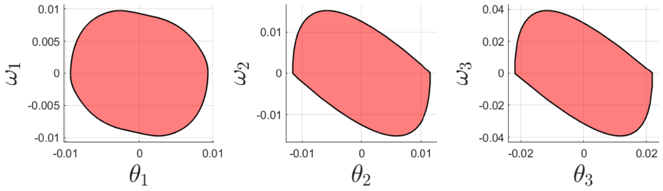


Fig. 5: Robust control invariant sets for the generator buses

computed for the generator buses, $\max_{x_i\in\mathcal{S}_i} |\omega_i| \le \omega^{\max}$, so that $x_i \in \mathcal{S}_i$ implies that the safety constraint is satisfied.

By Assumption 1, λ_i is clearly monotonic. The evaluation of λ_i is done in two steps. First, with $\theta_{\mathcal{N}_i}^{\max}$ fixed, $\mathscr{F}$ is called to compute an RCI $\mathcal{S}_i$, then $\theta_i^{\max}$ is obtained through (18). Next, the inner approximation of $\mathbf{epi}(\lambda_i)$ is computed for each bus with the grid sampling algorithm, shown in Fig. 4.

Remark 5. Clearly, the power flow from neighboring buses are summable, we treat them as separate disturbances in Fig. 4 to visualize the epigraph method with multiple non-summable disturbance inputs.

As shown in Fig. 8, bus 1 has one neighbor (bus 4) and bus 5 has two neighbors (bus 4 and 6), therefore $\mathbf{epi}(\lambda_1)$ is 2-dimensional whereas $\mathbf{epi}(\lambda_5)$ is 3-dimensional. Once a value for $\theta^{\max}$ that satisfies the validity condition is found, it leads to a valid network assume-guarantee contract, and an RCI can be obtained via $\mathscr{F}$.

Fig. 5 shows the robust invariant sets for the generator buses under the assume-guarantee contract, which satisfies the **safety constraint** that $|\omega_i| \le \omega^{\max} = 0.05rad/s$.

C. Simulation Result

For each bus, the computed robust control invariant set is then enforced with a control barrier function as described in Section III-A with the OLC controller introduced in [24] used as the legacy controller providing the policy u^0. In Fig 6 we show a simulation trace of the 9-bus system with the CBF controller as the supervisory controller, and the **safety constraint** with $\omega^{\max} = 0.05rad/s$ is never breached.

Fig. 7 shows the phase angles with and without the CBF supervisor. Under the CBF supervisory controller (magenta plots), all phase anngles are within their respective bound determined by the contract; on the other hand, without CBF control (blue plots), there is no guarantee that the phase angles stay within bounds under the OLC policy u^0.

VII. Model Predictive Control for Contingency Recovery

We have shown how to compute an RCI for the network system with an assume-guarantee contract. We have shown this

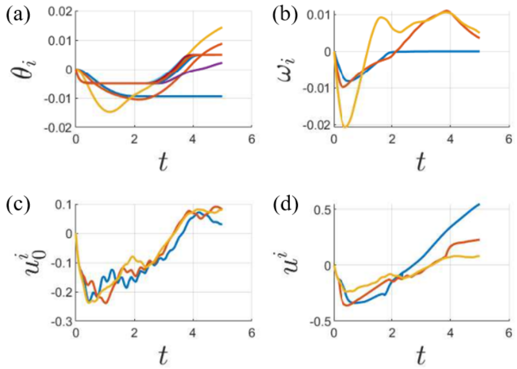


Fig. 6: CBF control: Phase angle deviations of all 9 buses (a); generator frequency deviation (b); OLC legacy control (c); CBF supervisory control (d)

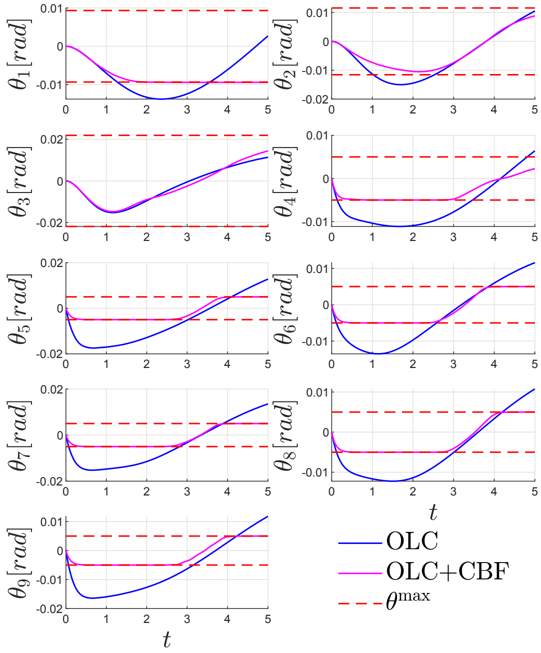


Fig. 7: Phase angle plot with and without the CBF supervisor

strategy is sufficient to guarantee the satisfaction of the safety constraint if the network operates around a fixed operating point θ^0 (around which the dynamics are linearized). However, when a severe contingency occurs such as a change in the network topology, a bus disconnects, or a line shorted, the RCI around the original operating point can no longer be maintained with the available control input, and the operating point has to change. This calls for an alternative controller that deals with the transient.

We propose a contingency tube model predictive controller that can handle the transient caused by contingency cases based on the mechanism developed for fixed point control.

A. Model Predictive Control for Reference Trajectory

Our MPC scheme is slightly different from the classic MPC (see for example [27]), here we briefly review some concepts from the MPC literature and introduce our contingency tube MPC scheme.

There are two important horizons for MPC, the prediction horizon T_p and the control horizon T_c. An MPC controller

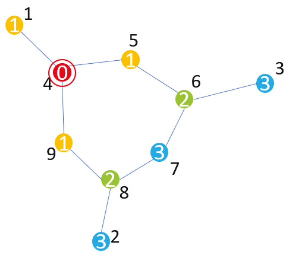


Fig. 8: Contingency positions. Colors determined by delays: yellow (1-step delay), green (2-step delay), blue (3-step).

looks ahead T_p steps and represents the future state trajectory as a function of the input sequence, then solves for the optimal control sequence w.r.t. a cost function and some state and input constraints. The control sequence will be executed for T_c steps, at which point another MPC iteration is executed, and a new control law computed. Traditional MPC schemes typically have $T_c \ll T_p$, often choosing $T_c = 1$, which requires the controller to have access to the state information without delay.

In the network setting, distributed MPC schemes have been proposed [28] that depend on fast communication and distributed optimization techniques. However, when the communication delay is not negligible, the receding horizon scheme is likely to be infeasible. Instead, we consider a contingency tube MPC scheme that is triggered only when a contingency occurs, and the MPC nominal trajectory do not update until the end of the prediction horizon or another contingency occurs. Obviously, such an MPC scheme is equivalent to feedforward control once the MPC input is solved, and would not work without feedback. We use CBF at each node of the network as the feedback controller to guarantee the tracking performance of the reference trajectory generated by the MPC. The contingency tube MPC is designed to guarantee the safe transition of the network to the new operating point after the contingency. Three requirements for the MPC should be considered:

- Computation of the MPC solution should be fast enough to allow real-time implementation.
- Safety constraints should be satisfied.
- Communication limitations should be respected.

Computation limitations differ with applications. In our power grid case study, in order to speed up the computation, we use the linearized model (16) and treat the nonlinearity as a bounded disturbance. With a linear discrete-time model, quadratic costs and linear state and input constraints, the MPC can be solved by convex quadratic programming over the input sequence $\hat{u}(0:T_p-1)$. The MPC controller is triggered when any bus detects a contingency that exceeds the capability of the fixed point controller, such as connecting or disconnecting a bus or a line loss. To obtain the reference trajectory, the following optimization problem is solved:

$$\begin{aligned}
&\min_{\hat{u}} \mathcal{J}(\hat{u},\hat{x},x^\star)\\
&\text{s.t. } \hat{x}(t+1)=\hat{f}(\hat{x}(t),\hat{u}(t),\hat{d}(t)),\\
&\quad \forall\ i\in\mathcal{G}, t=0,1,...,T_p-1, |\omega_i|\le\omega^{\max,ff},\\
&\quad \mathcal{C}\left(\hat{u}(0:T_p-1)\right)=0,
\end{aligned} \tag{19}$$

where $x^\star$ is the new operating point, $\mathcal{J}$ is the cost function, which penalizes $\hat{u}$ and the distance between $\hat{x}$ and $x^\star$. $\omega^{\max,ff}$ is the bound on the bus frequencies for the MPC. Later we show that with CBF, the frequency tracking error is bounded by $\omega^{\max,fb}$. Let $\omega^{\max}=\omega^{\max,ff}+\omega^{\max,fb}$, then the total frequency deviation is bounded by $\omega^{\max}$. $\hat{x}$ and $\hat{u}$ are the reference state and input trajectories and $\hat{d}$ is the predicted disturbance sequence, which depends on the knowledge of the contingency. In the general case $\hat{f}(x,u,d)$ is a linearization of (4), for this case study, the dynamics are given by (16). The set $\mathcal{C}$ is the constraint on the input caused by communication delay, which will be discussed later. The proposed scheme is based on the assumption that the network is close to a steady state when the contingency happens, therefore we can compute the reference trajectory for the whole network assuming that the system is at steady state without real-time state information. Once the MPC controller obtains a solution, the solution is sent to each node as the reference trajectory. Each node then uses a local feedback controller to track the reference trajectory.

Since the transmission of the reference trajectory is also subject to communication delay, we need the additional input constraint $\mathcal{C}$. Take the 9 bus test case as an example, suppose a contingency is detected at bus 4 and the MPC is computed at node 4. Assuming that the signal travels one edge per time-step, then the delay at each node is shown in Fig. 8, and $\mathcal{C}$ would enforce the following input structure:

$$\begin{bmatrix}\hat{u}_1(0:T_p-1)\\ \hat{u}_2(0:T_p-1)\\ \hat{u}_3(0:T_p-1)\\ \hat{u}_4(0:T_p-1)\\ \hat{u}_5(0:T_p-1)\\ \hat{u}_6(0:T_p-1)\\ \hat{u}_7(0:T_p-1)\\ \hat{u}_8(0:T_p-1)\\ \hat{u}_9(0:T_p-1)\end{bmatrix}=\begin{bmatrix}0&*&*&*&*\\0&0&0&*&*\\0&0&0&*&*\\ *&*&*&*&*\\0&*&*&*&*\\0&0&*&*&*\\0&0&0&*&*\\0&0&*&*&*\\0&*&*&*&*\end{bmatrix}, \tag{20}$$

which restricts the input to be zero before the reference trajectory signal arrives.

B. Contingency Tube MPC with CBFs

A local feedback controller is needed to track the reference trajectory generated by the MPC algorithm. The idea of centralized tube MPC was discussed in [29], [30], and was extended to distributed tube MPC for multiple subsystems without coupling in the dynamics [31]. There exist, however, strong coupling between nodes in the model of the grid dynamics (15). We use the assume-guarantee contract method proposed previously to handle the trajectory tracking problem for networks with strong coupling.

We assume that there exists a nominal dynamic model $\hat{f}_i$ for each subsystem in the network, and the difference between the model and the actual dynamics as described by (2) is bounded:

$$f_i\left(x_i,y_{\mathcal{N}_i},u_i,d_i\right)-\hat{f}_i\left(x_i,y_{\mathcal{N}_i},u_i,d_i\right)\in\mathcal{W}_{f_i}, \tag{21}$$

where $\mathcal{W}_{f_i}$ is the bound for model mismatch. The goal is to track a reference trajectory $\hat{x}(1:T_p)$ that satisfies

$$\begin{aligned}
\hat{x}_i(t+1)&=\hat{f}_i\left(\hat{x}_i(t),\hat{y}_{\mathcal{N}_i}(t),\hat{u}_i(t),\hat{d}_i\right),\\
\hat{y}_i(t)&=h(\hat{x}_i(t)), i=1,...,N,t=0,...,T_p-1
\end{aligned} \tag{22}$$

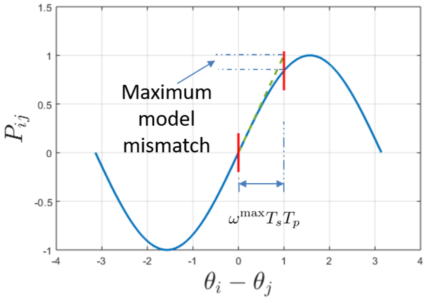


Fig. 9: Linearization error

and keep the tracking error bounded. For the grid dynamics, $\hat{f}_i$ is linear, therefore we can write it as

$$\hat{f}_i(x_i, y_{\mathcal{N}_i}, u_i, d_i) = A_i x_i + B_i u_i + E_i^1 y_{\mathcal{N}_i} + E_i^2 d_i,$$

where (A_i, B_i, E_i^1, E_i^2) are easily obtained from (16). Define the error $e_i = x_i - \hat{x}_i$, then the error evolves as

$$e_i^+ = A_i e_i + B_i \Delta u_i + E_i^1 (y_{\mathcal{N}_i} - \hat{y}_{\mathcal{N}_i}) + E_i^2 (d_i - \hat{d}_i) + \Delta f_i(t)$$

where $\Delta u \doteq u_i - \hat{u}_i$ denotes the feedback part of the input, and $\Delta f_i(t)$ defined by

$$f_i\left(\hat{x}_i(t), \hat{y}_{\mathcal{N}_i}(t), \hat{u}_i(t), \hat{d}_i\right) - \hat{f}_i\left(\hat{x}_i(t), \hat{y}_{\mathcal{N}_i}(t), \hat{u}_i(t), \hat{d}_i\right)$$

is the modeling error from linearization. We assume it is bounded and belongs to the set $\mathcal{W}_{f_i}$. For the power grid case study, the error is caused by linearization of the sinusoidal functions. Since the reference trajectory has a finite duration $T_s T_p$ and ω_i is bounded by $\omega^{\max}$ for every bus, the bound on the modeling error can be obtained, c.f. Fig. 9. We now have everything in place to state the main result of this section.

Theorem 3. *Consider the power system dynamics in* (15)*, denoted as* f*, and the linearized model in* (16)*, denoted as* $\hat{f}$*. For a reference trajectory* $[\hat{x}(1:T_p), \hat{u}(0:T_p-1)]$ *satisfying* (22)*, if for each bus, there exists a feedback controller* $\Delta u_i = k_i(x_i - \hat{x}_i, y_{\mathcal{N}_{\hat{i}}} - \hat{y}_{\mathcal{N}_i}, d_i - \hat{d}_i)$ *such that for a given bound* $\Delta\mathcal{D}_i$ *of* $d_i - \hat{d}_i$*, a given set* $\mathcal{S}_i \subseteq \mathcal{X}_i$ *and a given bound on* $|y - \hat{y}| \leq \Delta y^{\max}$*, the following is true:*

$$\begin{gathered}\forall\ x_i(t) \in \hat{x}_i(t) + \mathcal{S}_i, d_i(t) \in \hat{d}_i(t) + \Delta\mathcal{D}_i \\ \forall\ |y_{\mathcal{N}_i}(t) - \hat{y}_{\mathcal{N}_i}(t)| \leq \Delta y_{\mathcal{N}_i}^{\max}, \\ x_i(t+1) = f_i(x_i, y_{\mathcal{N}_i}, u_i, d_i) \in \hat{x}_i(t+1) + \mathcal{S}_i \\ \max_{x_i(t) \in \hat{x}_i(t) + \mathcal{S}_i} |h_i(x_i) - \hat{y}_i| \leq \Delta y_i^{\max}, t = 0, ..., T_p - 1,\end{gathered}$$

where $\Delta y_{\mathcal{N}_i}^{\max}$ *is a projection of* $\Delta y^{\max}$ *onto* $\mathcal{Y}_{\mathcal{N}_i}$ *and the "+" signs between vectors and sets denote direct sums. Then let* $u_i = \hat{u}_i + k_i(x_i - \hat{x}_i, y_{\mathcal{N}_i} - \hat{y}_{\mathcal{N}_i}, d_i - \hat{d}_i)$*, for any* $x(0)$ *satisfying* $x_i - \hat{x}_i \in \mathcal{S}_i$*, disturbance satisfying* $d_i(t) \in \hat{d}_i(t) + \Delta\mathcal{D}_i$*, the closed loop trajectory stays inside the tube defined as* $\{x(1:T_p) \mid x(t) \in \hat{x}(t) + \mathcal{S}_1 \times ... \times \mathcal{S}_N\}$*.*

Proof. The proof can be obtained by directly applying Theorem 2 on the error dynamics. □

To implement the contingency tube MPC, we first compute an RCI for the error dynamics taking the bound on disturbance and model mismatch into account. When a contingency occurs, the MPC scheme (19) is solved to obtain a reference trajectory $\hat{x}$, then at each node, the following CBF supervisory control is implemented:

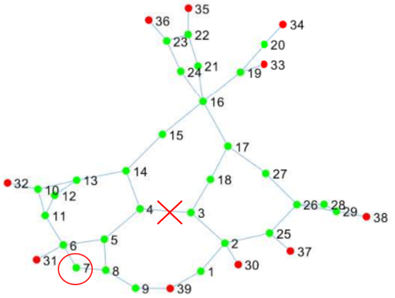


Fig. 10: New England grid structure and failure locations

$$\begin{aligned}u_i(t) = \underset{u \in \mathcal{U}_i}{\arg\min}\ & \left\| u - u_i^0(t) \right\|^2 \\ s.t.\quad & \dot{b}_i(x_i - \hat{x}_i, u) + \kappa b_i(x_i - \hat{x}_i) \geq 0,\end{aligned} \tag{23}$$

where b_i is the CBF for the i^{th} node defined based on the RCI $\mathcal{S}_i$, u_i^0 is the nominal control signal for the i^{th} node, which can be simply chosen as $\hat{u}_i$, or alternatively chosen as $\hat{u}_i$ plus a local feedback part. In the next section, the legacy control u_i^0 is picked as $\hat{u}_i$ plus an LQR feedback component.

C. Simulation of the Contingency Tube MPC

To validate the proposed contingency tube MPC scheme, we use the high-fidelity power grid simulator PST [32] as the simulation environment. PST allows several types of contingency cases, such as the 3-phase error, loss of line and loss of load. The New England network from PST is picked for demonstration, which contains 39 buses with 10 of them generator buses, as shown in Fig. 10. The red nodes are the generator buses and the green nodes are the pure load buses. The two tested contingencies are:

- **Case 1:** Load bus loss at bus 7
- **Case 2:** Line between bus 3 and 4 trips

When bus 7 disconnects, the network is able to find a new set point without changing the generation. When the line between bus 3 and 4 disconnects, the network cannot balance itself with the original generation. So an optimal power flow (OPF) routine (AC OPF routine in Matpower toolbox [33]) is performed to get the new generation together with the new operating point, and the contingency tube MPC is used to complete the transition to the new operating point. The sampling time and horizon for the contingency tube MPC is set at 50ms and 2.5s ($T_p = 50$).

We insert sinusoidal load fluctuation with the maximum magnitude allowed by the RCI at every bus to simulate the effect of uncontrolled load disturbance. Once the contingencies (bus loss in case 1 and line loss in case 2) are detected, the contingency tube MPC kicks in at the nearest node to the contingency (bus 6 in case 1 and bus 4 in case 2) to compute the reference trajectory for the transition to the new operating points. Then the plan is then communicated across the network; the signal is assumed to travel two edges per sampling interval.

Fig. 11 shows the PST simulation of case 1, the load failure occurs at $t = 4s$. The blue line is the state, the magenta

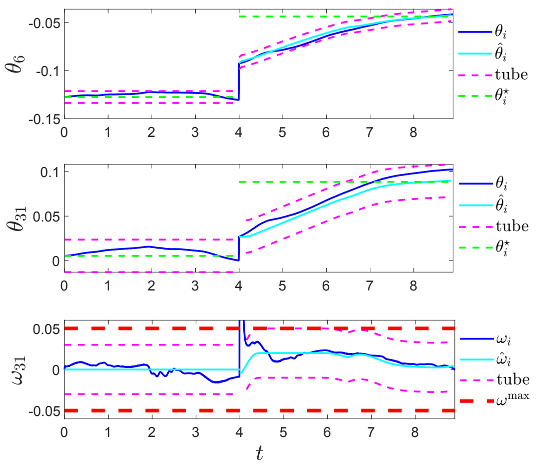


Fig. 11: Case 1: Bus failure contingency

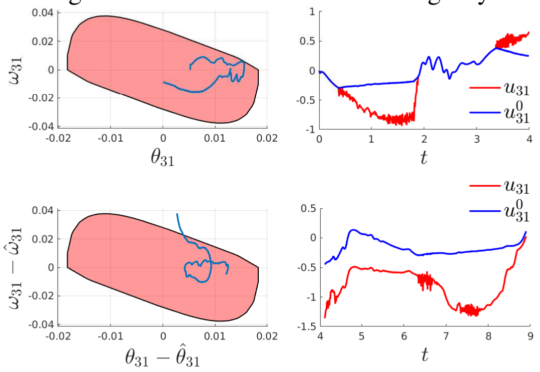


Fig. 12: Robust Control Invariant set with state and input trajectories at bus 31

line represents the tube (i.e. the region the state is confined to lie in), the green line represents the new set point for the phase angle and the red line represents the bound for frequency. We show the state trajectory of bus 6, the bus closest to the contingency, and bus 31, the closest generator bus to the contingency. When the contingency happens, the frequency breached the constraint for a slight moment, the reason for this violation of the safety constraint are (i) the dynamics under the contingency are not modeled accurately (ii) the violation happened instantly after the loss of bus 7, before the contingency tube MPC is able to kick in and react. Once the contingency tube MPC scheme kicks in, the state trajectory was kept within the tube and the network eventually reaches the new operating point without violating the safety constraint. In practice, infrequent small violations over very small time periods are tolerated. In Fig. 12 we plot the state trajectory w.r.t. the RCI and the inputs to the system at bus 31 (generator bus). The two figures on top show the state and input trajectories before the contingency at $t = 4s$. Due to the sinusoidal fluctuation of the load, the phase angle also fluctuates, but it never left the RCI; Fig. 12(a). In Fig. 12(b), the blue curve shows the legacy controller input, and the red curve shows the CBF controller input. The timing of the interventions coincide with the timing when the state is close to the boundary of the RCI. Fig. 12(c) and (d) show the state and input trajectories after the contingency. Note that in the contingency tube MPC scheme, we require the error state $x - \hat{x}$ instead of the state x to stay inside the RCI. After the temporary deviation right after the contingency, $x - \hat{x}$ stays inside the RCI due to the CBF controller.

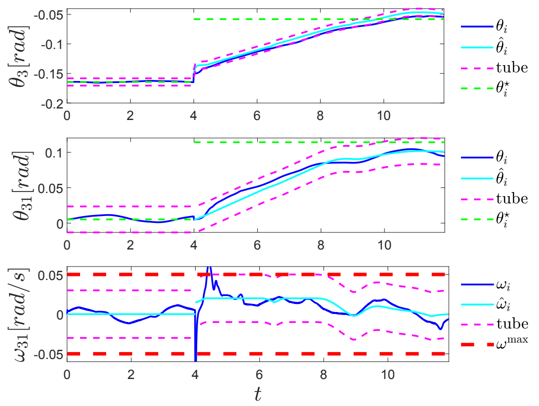


Fig. 13: Case 2: Line failure contingency

Fig. 13 shows the simulation for the line loss case. Similarly, the contingency tube MPC together with the CBF controller is able to keep the system trajectory within the tube and take the whole network to the new operating point.

VIII. Conclusion

We consider the application of robust control invariant set and control barrier functions on network systems to prevent large deviations from the desired working condition. The key idea is to use assume-guarantee contracts to break the large network into small subsystems. The coupling between subsystems are treated as bounded disturbances which are handled with a network assume-guarantee contract. We show that a network assume-guarantee contract satisfying the validity condition guarantees robust set invariance for the whole network system. Furthermore, we propose an epigraph algorithm that searches for a valid contract, and enjoys linear complexity when the network is sparse or the coupling terms are summable. Based on the network assume-guarantee contract idea, we further propose a contingency tube MPC scheme that is capable of handling contingencies with changing operating points while respecting communication limitations.

Appendix A
Robust Linear Programming for RCI Computation

We briefly review the robust linear programming algorithm for minimal robust control invariant set (mRCI) computation proposed in [16]. A set is robust control invariant if there exists a controller that keeps any trajectory starting within the set inside the set under all possible disturbances.

Definition 6. Given a discrete-time dynamical system:

$$x^+ = f(x,u,w), \quad x \in \mathbb{R}^n, u \in \mathcal{U}, w \in \mathcal{W} \tag{24}$$

where x, u, and w are the state, control input, and disturbance. A set $\mathcal{S} \subseteq \mathbb{R}^n$ is *robust control invariant* if $\forall x \in \mathcal{S}$, $\forall w \in \mathcal{W}$, $\exists\, u \in \mathcal{U} \quad \text{s.t.} \quad x^+ = f(x,u,w) \in \mathcal{S}$.

In addition, we assume $w = [w^m; w^u]$, where w^m and w^u are the measured and unmeasured disturbances, respectively. The control policy can depend on w^m, but not on w^u.

The mRCI algorithm assumes a discrete-time linear model:

$$x^+ = Ax + Bu + Ew. \tag{25}$$

The RCI takes a polytopic form $\mathbf{Poly}(P, q)$ with the hyperplane orientation fixed to P. A one-step propagation computes a new polytope $\mathbf{Poly}(P, q^+)$ that contains all possible x^+ with $x \in \mathbf{Poly}(P, q)$, and $w \in \mathcal{W}$ under the dynamics in (25). We assume the control law takes the form $u = K_{ff}w^m + K_{fb}x$, but note that once the mRCI is computed, it is enforced by control barrier functions, as reviewed in Section III-A. The linear control law here is simply used to show that there exists a control strategy that renders the set robustly control invariant, it does not have to be implemented.

The one-step propagation is formulated as a robust linear programming problem by assuming a linear form of the control law $u = K_{ff}d + K_{fb}x$. Robust linear programming (with polytopic uncertainty) is then solved via linear programming using dualization. Thus, it enjoys order constant complexity.

In the power grid case study, with dynamics Σ_i described by (16), we assume that phase angles of the neighboring nodes and the local generation and uncontrolled load are measured disturbances. The unmeasured disturbance is due to the communication delay between the neighboring nodes. Suppose node i and j are neigbors, the bound on frequency is $\omega^{\max}$, and the time delay of communication is τ. Then the maximum difference between the actual value of θ_j and the value used for feedback is $\omega^{\max}\tau$. The bound of the unmeasured disturbance for the i^{th} node w_i^u is then given as $|w_i^u| \leq \left|B_i K_{ff}^i\right| \omega^{\max}\tau$ where B_i and K_{ff}^i are the input matrix and feedforward gain of the i^{th} node. The following one-step propagation solves for a polytopic set $\mathbf{Poly}(P, q^+)$ that contains all possible x^+ with $x \in \mathbf{Poly}(P, q)$ and $w \in \mathcal{W}$:

$$\begin{aligned} \min_{K_{ff}, K_{fb}, q^+} \quad & c^\intercal q^+ \\ \text{s.t.} \quad & \forall\, x \in \mathbf{Poly}(P, q), \forall\, w \in \mathcal{W}, \\ & P\left(Ax + B\left(K_{ff}^\intercal w^m + K_{fb}^\intercal x\right) + Ew\right) \leq q^+, \\ & K_{ff}^\intercal w^m + K_{fb}^\intercal x \in \mathcal{U}, \end{aligned} \tag{26}$$

which is solvable with robust linear programming [34].

Remark 6. We enforce an additional constraint that for the generator buses, the frequency stays bounded $|\omega_i| \leq \omega^{\max}$, which is easily enforced as a constraint on q^+.

Optimization (26) solves the one-step propagation problem, which is embedded in an iterative algorithm to find a minimal robust control invariant set. The algorithm is initiated from a small q and iteratively updates q with q^+. If $q^+ \leq q$, then $\mathcal{P}(P, q)$ is robustly control invariant, and the algorithm terminates, as shown in Algorithm 1.

Algorithm 1 Robust LP algorithm for mRCI

```
procedure RCI-IO($\Sigma$, $P$, $q^0$, $\mathcal{W}$, $\mathcal{U}$, $\epsilon$)
    $q \leftarrow q^0$
    do
        Find $[q^+, K_{ff}, K_{fb}]$ s.t.
        $\forall\, x \in \mathbf{Poly}(P, q), \forall\, w \in \mathcal{W}, K_{ff}w^m + K_{fb}x \in \mathcal{U}$,
        $x^+ \in \mathbf{Poly}(P, q^+ - \epsilon\mathbf{1}_L)$
        $q \leftarrow q^+$
    while $q^+ \leq q + \epsilon\mathbf{1}_L$
    return $[q, K_{ff}, K_{fb}]$
end procedure
```

Appendix B
Proof of Theorem 1

By assumption 3 and 4, p_{ae}^i and $p_{af}^i[0]$ exists so that ϕ_{ae}^i and $\phi_{af}^i[0]$ are satisfied. By assumption 1, define the following recursion:

$$\begin{aligned} p_g[k] &= \hat{\Lambda}(p_{af}[k]) \\ p_{af}[k+1] &= \Gamma(p_g[k]). \end{aligned} \tag{27}$$

Then, we can build an infinite sequence of STLs that the network system satisfies from assumption 1, 2, and (27):

$$\begin{aligned} & \bigwedge_{i=1}^{N} \varphi_{ae}^i(p_{ae}^i) \wedge \bigwedge_{i=1}^{N} \varphi_{af}^i(p_{af}^i[0]) \wedge \\ & \left(\bigwedge_{i=1}^{N} \varphi_{ae}^i(p_{ae}^i) \wedge \bigwedge_{i=1}^{N} \varphi_{af}^i(p_{af}^i[0]) \Rightarrow \bigwedge_{i=1}^{N} \varphi_{g}^i(p_{g}^i[0]) \right) \wedge \\ & \left(\bigwedge_{i=1}^{N} \varphi_{g}^i(p_{g}^i[0]) \Rightarrow \bigwedge_{i=1}^{N} \varphi_{af}^i(p_{af}^i[1]) \right) \wedge \\ & \ldots \end{aligned}$$

which implies (9).

Appendix C
Proof of Theorem 2

Let $\mathcal{S}_i = \mathscr{F}_i(y_{\mathcal{N}_i}^{\max})$, and define a network assume-guarantee contract with

$$\begin{aligned} \phi_{ae}^i =& (x_i(0) \in \mathcal{S}_i) \wedge \Box\left(d_i \in \mathcal{D}_i\right) \\ & \wedge \Box\left(u_i = k_i(x_i, y_{\mathcal{N}_i}, d_i)\right), \end{aligned} \tag{28a}$$

$$\phi_{af}^i = \varphi_{af}^i(T) = \Box_{[0,T]} \left|y_{\mathcal{N}_i}\right| \leq y_{\mathcal{N}_i}^{\max}, \tag{28b}$$

$$\phi_{g}^i = \varphi_{g}^i(\hat{T}) = \Box_{[0,\hat{T}]} x_i \in \mathcal{S}_i; \tag{28c}$$

where k_i is the feedback law that keeps x_i within $\mathcal{S}_i$. By the definition of an RCI, the existence of k_i is guaranteed. Let $\hat{\Lambda}(T) = T + T_s$, $\Gamma(\hat{T}) = \hat{T}$, where T_s is the time step of the discrete dynamics in (2).

Among the 4 assumptions of Theorem 1, Assumption 1 is satisfied by the definition of an RCI. With (11), Assumption 2 is satisfied with Γ defined above. Assumption 3 is satisfied by (28a) and Assumption 4 is satisfied by setting $T = 0$ in (28b). Then, by Theorem 1, the guarantee for the network system is $\hat{\phi}_g^i = \bigwedge_{k=0}^{\infty} \Box_{[0,k \cdot T_s]} x_i \in \mathcal{S}_i$, which is simplified to $\forall\, i = 1, ..., N, \Box_{[0,\infty)} x_i \in \mathcal{S}_i$.

References

[1] P. Nilsson, O. Hussien, Y. Chen, A. Balkan, M. Rungger, A. Ames, J. Grizzle, N. Ozay, H. Peng, and P. Tabuada, "Preliminary results on correct-by-construction control software synthesis for adaptive cruise control," in *2014 IEEE 53rd Annual Conference on Decision and Control (CDC)*. IEEE, 2014, pp. 816–823.

[2] Y. Chen, H. Peng, and J. W. Grizzle, "Validating noncooperative control designs through a lyapunov approach," *IEEE Transactions on Control Systems Technology*, no. 99, pp. 1–13, 2018.

[3] Y. Chen, H. Peng, and J. Grizzle, "Obstacle avoidance for low-speed autonomous vehicles with barrier function," *IEEE Transactions on Control Systems Technology*, vol. 26, no. 1, pp. 194–206, 2018.

[4] F. Blanchini, "Set invariance in control," *Automatica*, vol. 35, no. 11, pp. 1747–1767, 1999.

[5] I. M. Mitchell, A. M. Bayen, and C. J. Tomlin, "A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games," *IEEE Transactions on automatic control*, vol. 50, no. 7, pp. 947–957, 2005.

[6] M. V. Khlebnikov, B. T. Polyak, and V. M. Kuntsevich, "Optimization of linear systems subject to bounded exogenous disturbances: The invariant ellipsoid technique," *Automation and Remote Control*, vol. 72, no. 11, pp. 2227–2275, 2011.

[7] S. Prajna, P. A. Parrilo, and A. Rantzer, "Nonlinear control synthesis by convex optimization," *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 310–314, 2004.

[8] J. Anderson and A. Papachristodoulou, "A decomposition technique for nonlinear dynamical system analysis," *IEEE Transactions on Automatic Control*, vol. 57, no. 6, pp. 1516–1521, 2011.

[9] P. Nilsson and N. Ozay, "Control synthesis for large collections of systems with mode-counting constraints," in *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*. ACM, 2016, pp. 205–214.

[10] R. Alur and T. A. Henzinger, "Reactive modules," *Formal methods in system design*, vol. 15, no. 1, pp. 7–48, 1999.

[11] J. S. Shamma and G. Arslan, "A decomposition approach to distributed control of spatially invariant systems," *IEEE transactions on automatic control*, vol. 51, no. 4, pp. 701–707, 2006.

[12] N. Sandell, P. Varaiya, M. Athans, and M. Safonov, "Survey of decentralized control methods for large scale systems," *IEEE Transactions on automatic Control*, vol. 23, no. 2, pp. 108–128, 1978.

[13] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2017.

[14] A. Agrawal and K. Sreenath, "Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation." in *Robotics: Science and Systems*, 2017.

[15] Q. Nguyen and K. Sreenath, "Optimal robust control for constrained nonlinear hybrid systems with application to bipedal locomotion," in *2016 American Control Conference (ACC)*. IEEE, 2016, pp. 4807–4813.

[16] Y. Chen, H. Peng, J. Grizzle, and N. Ozay, "Data-driven computation of minimal robust control invariant set," in *2018 IEEE 57th Annual Conference on Decision and Control (CDC)*. IEEE, 2018.

[17] C. S. Păsăreanu, D. Giannakopoulou, M. G. Bobaru, J. M. Cobleigh, and H. Barringer, "Learning to divide and conquer: applying the l* algorithm to automate assume-guarantee reasoning," *Formal Methods in System Design*, vol. 32, no. 3, pp. 175–205, 2008.

[18] E. Asarin, A. Donzé, O. Maler, and D. Nickovic, "Parametric identification of temporal properties," in *International Conference on Runtime Verification*. Springer, 2011, pp. 147–160.

[19] V. Raman, A. Donzé, M. Maasoumy, R. M. Murray, A. Sangiovanni-Vincentelli, and S. A. Seshia, "Model predictive control with signal temporal logic specifications," in *53rd IEEE Conference on Decision and Control*. IEEE, 2014, pp. 81–87.

[20] G. E. Fainekos and G. J. Pappas, "Robustness of temporal logic specifications for continuous-time signals," *Theoretical Computer Science*, vol. 410, no. 42, pp. 4262–4291, 2009.

[21] E. S. Kim, M. Arcak, and S. A. Seshia, "A small gain theorem for parametric assume-guarantee contracts," in *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control*. ACM, 2017, pp. 207–216.

[22] C. A. Desoer and M. Vidyasagar, *Feedback systems: input-output properties*. Siam, 1975, vol. 55.

[23] Y. Chen, J. Anderson, K. Kalsi, S. H. Low, and A. D. Ames, "Compositional set invariance in network systems with assume-guarantee contracts," *arXiv preprint arXiv:1810.10636*, 2018.

[24] E. Mallada, C. Zhao, and S. Low, "Optimal load-side control for frequency regulation in smart grids," *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6294–6309, 2017.

[25] D. K. Molzahn, F. Dörfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, 2017.

[26] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 5, pp. 1177–1189, 2014.

[27] B. Kouvaritakis and M. Cannon, "Model predictive control," *Switzerland: Springer International Publishing*, 2016.

[28] A. N. Venkat, I. A. Hiskens, J. B. Rawlings, and S. J. Wright, "Distributed mpc strategies with application to power system automatic generation control," *IEEE transactions on control systems technology*, vol. 16, no. 6, pp. 1192–1206, 2008.

[29] S. V. Raković, B. Kouvaritakis, M. Cannon, C. Panos, and R. Findeisen, "Fully parameterized tube mpc," *IFAC Proceedings Volumes*, vol. 44, no. 1, pp. 197–202, 2011.

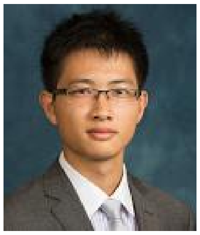
[30] S. Yu, C. Maier, H. Chen, and F. Allgöwer, "Tube mpc scheme based on robust control invariant set with application to lipschitz nonlinear systems," *Systems & Control Letters*, vol. 62, no. 2, pp. 194–200, 2013.

[31] P. Trodden and A. Richards, "Robust distributed model predictive control using tubes," in *2006 American Control Conference*. IEEE, 2006, pp. 6–pp.

[32] J. H. Chow and K. W. Cheung, "A toolbox for power system dynamics and control engineering education and research," *IEEE transactions on Power Systems*, vol. 7, no. 4, pp. 1559–1564, 1992.

[33] R. D. Zimmerman, C. E. Murillo-Sánchez, and D. Gan, "Matpower: A matlab power system simulation package," *Manual, Power Systems Engineering Research Center, Ithaca NY*, vol. 1, 1997.

[34] D. Bertsimas, D. B. Brown, and C. Caramanis, "Theory and applications of robust optimization," *SIAM review*, vol. 53, no. 3, pp. 464–501, 2011.

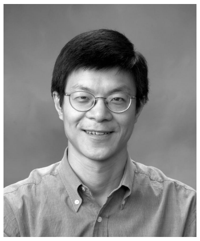


Yuxiao Chen is a Postdoc researcher at Dept. of Mechanical and Civil Engineering, California Institute of Technology. He received his B.S. from Tsinghua University in 2013, and his Ph.D. from the University of Michigan in 2018, both in ME. His research interest is on control and robotics, especially on safety-critical control synthesis and multiagent systems.

James Anderson is an assistant professor of electrical engineering at Columbia University, NY, where he is also a member of the Data Science Institute. Prior to joining Columba he was a senior research scientist at Caltech and junior research fellow at St John's College, University of Oxford. He received his DPhil in Engineering Science from Oxford and MSc and BSc degrees from the University of Reading.

Karanjit Kalsi is the Principal Engineer and Group Leader for the Optimization and Controls Group at the Pacific Northwest National Laboratory (PNNL). He is also currently a visiting faculty member at the California Institute of Technology, where he partners with faculty on the topic of safety-critical controls for complex infrastructure systems. Dr. Kalsi received his Ph.D. from Purdue University in Electrical and Computer Engineering in 2010 and his M.Eng in Electronic Engineering from the University of Sheffield in 2006.

Aaron D. Ames is the Bren Professor of Mechanical and Civil Engineering and Control and Dynamical Systems at Caltech. He received a B.S. in Mechanical Engineering and a B.A. in Mathematics from the University of St. Thomas in 2001, and he received a M.A. in Mathematics and a Ph.D. in EECS from UC Berkeley in 2006. His research interests span the areas of robotics, nonlinear, safety-critical control and hybrid systems, with a special focus on applications to bipedal robotic walking—both formally and through experimental validation.



Steven Low (F'2008) is the Gilloon Professor of Computing & Mathematical Sciences as well as Electrical Engineering at Caltech and an honorary professor of the University of Melbourne, Australia. His research has made a practical impact on the Internet and on large-scale electric vehicle charging. He received his B.S. from Cornell and PhD from Berkeley, both in EE.