Resilient Control of Dynamic Flow Networks Subject to Stochastic Cyber-Physical Disruptions

Yu Tang, Graduate Student Member, IEEE, and Li Jin, Member, IEEE

Abstract—Modern network systems, such as transportation and communication systems, are prone to cyber-physical disruptions and thus suffer efficiency loss. This article studies network resiliency, in terms of throughput, and develops resilient control to improve throughput. We consider single-commodity networks that admit congestion propagation. We also apply a Markov process to model disruption switches. For throughput analysis, we first use insights into congestion spillback to propose novel Lyapunov functions and then exploit monotone network dynamics to reduce computational costs of verifying stability conditions. For control design, we show that 1) for a network with infinite link storage space, there exists an open-loop control that attains the min-expected-cut capacity; 2) for a network with observable disruptions that restrict maximum sending and/or receiving flows, there exists a mode-dependent control that attains the expected-min-cut capacity; 3) for general networks, there exists a closed-loop control with throughput guarantees. We also derive lower bounds of resiliency scores for a set of numerical examples and verify resiliency improvement with our method.

Index Terms—Dynamic flow networks, cyber-physical disruptions, piecewise-deterministic Markov processes (PDMP), monotone dynamical systems.

I. INTRODUCTION

A. Motivation

Dynamic flow networks are widely used to model engineering systems including transportation systems [1] and communication networks [2]. These systems are susceptible to disruptions both in physical and cyber parts. In the physical part, link flows can be disrupted by capacity-reducing events, such as traffic incidents [3]. In the cyber part, unreliable state observation or faulty feedback actuation may occur, which degrades the effectiveness of feedback controllers and lead to physical losses [4]. Typically, both types of disruptions are hard to predict and thus need treatment in a stochastic manner. For instance, probabilistic models were used to evaluate freeway capacity, which is supported by field studies [5]. This modeling technique is also applicable to sensing faults [6]. Since network systems involve very large numbers of cyber-physical components, it is neither economically feasible nor technically necessary to prevent all disruptions. Instead, a practical solution is to integrate disruptions into modeling control schemes [7]. However, limited studies have discussed such method for dynamic flow networks subject to stochastic disruptions.

In this article, we first evaluate network throughput as a measure of resiliency against stochastic cyber-physical disruptions, arising from reliability failures, and then design control strategies that mitigate throughput losses. To this end, we consider single-commodity networks that have found applications in real systems, such as freeway systems [1]. Although single-commodity networks could simplify real-world cases, they are worth studying since multicommodity networks require origin-destination demands that are hard to acquire in practice. We use a finite-state Markov process to model the occurrence and clearance of disruptions. Then, we investigate stability condition of networks, which allows for resiliency quantification and resilient control configuration. Particularly, our discussion on control design, inspired by the classical max-flow min-cut theorem [8] for static flow networks, proposes min-expected-cut capacity (MECC) and expected-min-cut capacity (EMCC) and reveals their relation to throughput, network storage space, disruptions and control laws. In case of a general network whose throughput is not guaranteed with these capacities, we present a closed-loop control with lower-bounded throughput.

B. Related Work

Previous work on dynamic flow networks typically considered a nominal or robust setting. In the disruption-free case, in-depth

1In this article, reliability failures refer to temporary malfunction of components of controlled dynamic flow networks, such as node/link breakdown and sensing/actuation faults. They do not include communication delay or malicious cyber attacks. Although this article mainly considers sensing failures for cyber disruptions, our approach can be applied to address actuation faults with minor modifications.
stability analysis was provided for networks characterized by various flow structures including monotone dynamics, nonlinear demand/supply constraints, and congestion spillover [9], [10], [11], [12], [13]. Besides, optimal routing control has been extensively investigated for dynamical flow networks [9], [14]. Robust control strategies, along with resiliency analysis, were developed in the face of physical disruptions [15], [16], [17], [18], [19], [20]. However, the above work assumes perfect sensing and actuation; the resiliency against cyber disruptions remains unclear. Besides, robust control handles disturbances with uncertainty sets [20]; it does not apply to recurrently switching disruptions.

The model we consider belongs to a subclass of piecewise-deterministic Markov processes (PDMP) [21], sometimes known as Markov jump nonlinear systems (MJNSs) [22], where continuous states (traffic densities) evolve according to a set of ordinary differential equations and a discrete state (disruption mode) determines the mode of the continuous dynamics [23]. Such a formulation allows analysis of joint impacts of cyber and physical disruptions on network resiliency. Although the general theories of PDMPs [23], [24], [25] and MJNSs [26], [27] have been extensively investigated, the implementation is still challenging due to nonlinear flow dynamics. Typical Lyapunov functions, such as piecewise quadratic functions [27], fail to capture congestion dynamics and thus only lead to trivial stability analysis; see our discussion in Section III. It is vital to design appropriate Lyapunov functions for analyzing our model.

Our work is also related to stochastic fluid models [28], [29]. These models are applied to performance analysis or admission/priority control for servers subject to demand or service disruptions [30], [31]. Currently, limited results consider congestion spillover over stochastic flow networks, let alone the corresponding control design. Only a few results were developed for networks with special structures, such as parallel links [3], [32] and serial links [33], [34]. To the best of the authors’ knowledge, the general stochastic flow networks are still not well investigated.

C. Our Contributions

This article focuses on the two following questions.

1) How to quantify resiliency against stochastic disruptions, especially for networks with congestion propagation?

2) How to attain resiliency-by-design or improve resiliency?

We define resiliency score as a ratio of disrupted network throughput to its nominal value. Here, the disrupted (respectively, nominal) throughput means the maximal inflow under which the network with (respectively, without) disruptions can be stabilized, i.e., traffic densities in all links being bounded on average. The max-flow min-cut theorem states that the nominal throughput equals min-cut capacity (MCC) [8], but we can hardly resolve the disrupted throughput in an analytical way. It is because our PDMP model allows complicated disruptions, including the physical ones creating new bottlenecks and the cyber ones inducing mismatches between control instructions and actual interlink flows. Thus, we address 1) by deriving and sharpening lower bounds of throughput. The lower bounds are obtained from a set of stability conditions built on the Foster–Lyapunov criterion [35]. To formulate the stability conditions, we use the insights into network-wide congestion propagation to propose a set of novel Lyapunov functions. We also exploit monotone network dynamics to simplify the condition verification from over unbounded sets to over only compact sets, which saves computational costs.

As indicated above, the max-flow min-cut theorem could be compromised. Thus, we consider its variants for resiliency-by-design control. Meanwhile, a more practical concern is that full observation of disruption modes and network states (traffic densities) could not be available to control design. To answer 2), we first show that there exists an open-loop control that attains the EMCC if the disruptions restrict maximum sending/receiving flows. The above results resemble the classical max-flow min-cut theorem. Third, we propose a density-dependent control, that is throughput-guaranteed, for general networks disrupted stochastically. Finally, we use numerical examples to demonstrate that our methods can enhance network resiliency.

The rest of this article is organized as follows. Section II introduces our PDMP model for networks subject to stochastic cyber-physical disruptions. Section III analyzes the resiliency of this network. Section IV presents resilient control design. Finally, Section V concludes this article and discusses future directions.

II. DYNAMIC FLOW NETWORK WITH CYBER-PHYSICAL DISRUPTIONS

Consider a single-origin-single-destination directed network \( \mathcal{G} = (V, E) \), where \( V \) and \( E \) denote the node set and the link set, respectively. Although single-commodity networks may have multiple origins and destinations, we can introduce one artificial origin and destination so that we obtain single-origin-single-destination networks where demands are routed from the artificial origin to real ones by proportions. For ease of presentation, we assume that the network is acyclic. Note that the proposed method can be applied to cyclic networks as well; see our discussion in Appendix B. We denote the starting and ending nodes of link \( e \) by \( \sigma_e \) and \( \tau_e \), respectively. We number the origin node as \( v_0 \) and the destination node as \( v_d \). The origin is subject to a constant inflow of \( \alpha \in \mathbb{R}_{>0} \). Without loss of generality, we assume that the flow enters the network via link \( e_0 \); see Fig. 1. Following the convention [18], we consider traffic density (mass per unit) as the network state and denote by \( X_e(t) \).
the density of link $e$ at time $t$. We also assume that all links have the same unit length for convenience of computing densities. For link $e$ with finite storage space, $X_e(t)$ can only take values from a closed interval $[0, x_e^{\text{max}}]$, where $x_e^{\text{max}} < \infty$ is called the jam density. For link $e$ with infinite storage space, $X_e(t)$ can take values from $\mathbb{R}_{\geq 0}$ and we let $x_e^{\text{max}} = \infty$. In particular, we assume that link $e_0$ has infinite storage space; this ensures that no traffic is rejected into $e_0$. We use $\mathcal{X}_e$ to denote the set of $X_e(t), \mathcal{X} = \prod_{e \in \mathcal{E}} \mathcal{X}_e \subseteq \mathbb{R}_{\geq 0}^{|\mathcal{E}|}$ to denote the set of the state vector $X(t)$, where $\mathcal{R}_e$ stands for a set of nonnegative vectors whose components are indexed by elements of $\mathcal{E}$.

For a node $v \in \mathcal{V}$, we let $\mathcal{E}_v^+ := \{ e \in \mathcal{E} | \tau_e = v \}$ (respectively, $\mathcal{E}_v^- := \{ e \in \mathcal{E} | \sigma_e = v \}$) denote the set of its incoming (respectively, outgoing) links; for a link $e \in \mathcal{E}$, we use $\mathcal{E}_e^+ := \{ i \in \mathcal{E} | \tau_e = i \}$ (respectively, $\mathcal{E}_e^- := \{ j \in \mathcal{E} | \sigma_j = \tau_e \}$) to denote the set of its upstream (respectively, downstream) adjacent links.

Clearly, we have $\mathcal{E}_e^- = \mathcal{E}_e^+_v$ if $v = \sigma_e$ and $\mathcal{E}_e^+ = \mathcal{E}_e^-_v$ if $v = \tau_e$. We also let $\mathcal{P} := \{ (e,j) | e \in \mathcal{E}, j \in \mathcal{E}_e^+ \}$ denote the set of ordered pairs of adjacent links. It follows $|\mathcal{P}| = \sum_{e \in \mathcal{E}} |\mathcal{E}_e^+|$, where $|\cdot|$ denotes the cardinality of a set. We say that link $e$ is accessible from link $i$, denoted by $i \rightarrow e$, if there exists a directed path starts with link $i$ and ends at link $e$. For link $e \in \mathcal{E}$, let $\mathcal{A}_e^- := \{ (i \rightarrow e) | i \in \mathcal{E} \}$ be the set of links from which link $e$ is accessible, and let $\mathcal{A}_e^+ := \{ (j \rightarrow e) | j \in \mathcal{E} \}$ be the set of links that are accessible from link $e$.

In the rest of this section, we first define flow functions, control laws, and disruption modes (see Section II-A), and then specify the network’s dynamics as a piecewise-deterministic Markov process (see Section II-B). Finally, we define network stability and resiliency score (see Section II-C).

### A. Flows, Control Laws and Disruptions

Below we introduce the essential definitions and assumptions for our network model. The illustrative examples are also provided.

1) **Sending/receiving Flows:** The sending flow of link $e$ is specified by $f_e : \mathcal{X}_e \rightarrow \mathbb{R}_{\geq 0}$. It stands for the maximum outflow from link $e$ given a state $x_e$. The receiving flow of link $e$ is specified by $r_e : \mathcal{X}_e \rightarrow \mathbb{R}_{\geq 0}$. It is recognized as the maximum inflow allowed into link $e$ given a state $x_e$. We assume that these flows satisfy as follows.

**Assumption 1** (Sending/receiving flows):

1. **Sending flows:** For every $e \in \mathcal{E}$, $f_e(x_e)$ is Lipschitz continuous and nondecreasing in $x_e$. Furthermore, $f_e(x_e) = 0$ if $x_e = 0$ and $\sup_{x_e} f_e(x_e) < \infty$.

2. **Receiving flows:** For every $e \in \mathcal{E}$, $r_e(x_e)$ is Lipschitz continuous and nonincreasing in $x_e$. Furthermore, for link $e$ with finite storage space, we assume $r_e(x_e) = 0$ if $x_e = x_e^{\text{max}}$; for link $e$ with infinite storage space, we assume a constant receiving flow $r_e$, independent of $x_e$.

Note that receiving flows are not considered in some flow networks. In that case we just let link $e$ have infinite storage space with $r_e = \infty$.

We define link capacity $Q_e$ and critical density $x_e^c$ as

$$Q_e := \sup_{x_e \in \mathcal{X}_e} \min \{ f_e(x_e), r_e(x_e) \}$$

(1a)

$$x_e^c := \inf \{ x_e \in \mathcal{X}_e | f_e(x_e) = Q_e \}.$$  

(1b)

Practically, the capacity $Q_e$ indicates an upper bound of sustainable outflow from link $e$, and the critical density $x_e^c$ denotes a threshold where the capacity flow $Q_e$ can be maintained with a relatively high speed $Q_e/x_e^c$. Link $e$ is considered as “congested” when its density $x_e$ exceeds the critical value $x_e^c$.

Here, are two examples of sending and receiving flows. In road network, as per the cell transmission model [36], the sending and receiving flows are given by

$$f_e(x_e) = \min \{ v_j x_e, Q_e \}$$

(2a)

$$r_e(x_e) = \min \{ Q_e, w_e(x_e^{\text{max}}) - x_e \}$$

(2b)

where $x_e$ represents vehicle density of road section $e$, and traffic parameters $v_j, Q_e, w_e$, and $x_e^{\text{max}}$ are typically assumed to satisfy $Q_e/x_e^{\text{max}} \leq v_j w_e/(v_j + w_e)$ [34]. It follows $x_e^c = Q_e/v_j$. In data networks, the sending flow can be approximated as a fluid model [18] with

$$f_e(x_e) = Q_e (1 - e^{-\rho_c x_e})$$

(3)

where $x_e$ stands for queue length on channel $e$, $\rho_c$ is a positive constant, and $Q_e$ is channel capacity. The receiving flow is not explicitly modeled in data networks and thus we assume $r_e = \infty$, which yields $x_e^c = \infty$.

2) **Control Laws:** We consider a control law $\mu : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}$ to be a concatenation of controllers $\mu_{ej} : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}, (e,j) \in \mathcal{P}$, that regulate flows from link $e$ to link $j$. In this article, we focus on locally responsive control laws defined below.

**Definition 1** (Locally responsive control laws): A control law $\mu$ for a network $G = (\mathcal{V}, \mathcal{E})$ is locally responsive if $\mu_{ej}(x)$, for any $(e,j) \in \mathcal{P}$, can depend on the states of the links in $\mathcal{E}_e^- \cup \mathcal{E}_j^+$ only, where $\mathcal{E}_e^- \cup \mathcal{E}_j^+$ denotes the set of incoming and outgoing links of node $\tau_e$.

In general, actual interlink flows $q^{\text{act}}_{ej}(x) : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}$ may not equal the control inputs $\mu(x)$ if the control law violates sending or receiving flows, e.g., under open-loop control. We define it as follows:

$$q^{\text{act}}_{ej}(x) := \min \{ \mu_{ej}(x), f^{\mu}_{ej}(x), r^{\mu}_{ej}(x) \}$$

(4)

where

$$f^{\mu}_{ej}(x) := \frac{\mu_{ej}(x)}{\sum_{j \in \mathcal{E}_j^+} \mu_{ej}(x)} f_e(x_e)$$

(5a)

$$r^{\mu}_{ej}(x) := \frac{\mu_{ej}(x)}{\sum_{i \in \mathcal{E}_e^-} \mu_{ej}(x)} r_j(x_j).$$

(5b)

This modeling approach enables us to study inappropriate control instructions induced by cyber-physical disruption introduced later. It is necessary since controllers may not have accurate knowledge of sending/receiving flows due to disruptions. The actual controlled flow $q^{\text{act}}_{ej}(x)$ represents how the network responds to the control input $\mu$. The sending and receiving flows are allocated proportionally to $\mu_{ej}(x)$, which is a typical modeling approach; for more discussion on this and alternative models, see [37]. Obviously, these techniques, with minor modifications, can be applied to flow allocations in multicommodity dynamical flow networks [38]. Note that the superscript “$\mu$” in (4) indicates the reliance of interlinks flows on the control law. We typically omit it unless we want to emphasize the dependence on a particular control law.
Assumption 2 (Controlled flows):

2.1 Continuity: The controlled flow \( q(x) \) is Lipschitz continuous in \( x_e \) for any \( e \in \mathcal{E} \).

2.2 Monotonicity: For any two different links \( e, e' \in \mathcal{E} \):
   i) \( \sum_{c \in \mathcal{E}_C^e} q_{ec}(x) \) is nondecreasing in \( x_{e'} \);
   ii) \( \sum_{c' \in \mathcal{E}_C^{e'}} q_{ec'}(x) \) is nonincreasing in \( x_{e'} \).

Assumption 2.1 indicates that our approach is applicable to nonsmooth control laws. Assumption 2.2 implies that the considered dynamic flow network is cooperative, which is a special class of monotone systems [39]. The following elaborates Assumption 2.2(i) to reveal the cooperativity. If link \( e' \) locates upstream of link \( e \) and \( x_{e'} \) increases, Assumption 2.2(ii) implies that the link set \( \mathcal{E}_e^c \) tends to send more flows to link \( e \) in order to avoid density accumulation in the upstream. If \( e' \) does not appear upstream of link \( e \) and \( e' \neq e \), the increase of \( x_{e'} \) implies that somewhere (at least not link \( e \)) becomes congested and Assumption 2.2(ii) indicates that the link set \( \mathcal{E}_e^c \) tends to send more flows to link \( e \), which benefits alleviating congestion somewhere. A similar explanation applies to Assumption 2.2(ii).

Thus, Assumption 2.2 indicates how the links reduce congestion cooperatively.

While dynamic flow networks are, in general, not monotone [10], the rationale behind Assumption 2.2 lies in that the monotonicity applies to a broad class of flow networks [19] and provides a tractable structure that benefits analysis and computation. The assumption of monotonicity can be relaxed in our stability analysis, with a rise of computational costs; see Propositions 1 and 2.

Below are the examples regarding routing and merging strategies satisfying Assumption 2. Consider routing control for a diverging junction with an upstream link \( e \). The classical logit routing policy [18] gives

\[
q_{e_j}(x) = \min \left\{ \frac{e^{-\theta_j x_j}}{\sum_{j' \in \mathcal{E}_e^+} e^{-\theta_j x_{j'}} f_e(x_{j'}), r_j(x_j)} \right\}
\]

where \( \theta_j \) quantifies the sensitivity of route choice to \( x_j \). Now consider a merging junction with a minor upstream link \( e_1 \), a major upstream link \( e_2 \) and a downstream link \( e \). A typical ramp metering policy, namely the occupancy strategy [40], yields

\[
q_{e_1}(x) = \min \{ u - \kappa x_{e_1}, f_{e_1}(x_{e_1}), r_e(x_e) \}
\]

\[
q_{e_2}(x) = \min \{ r_e(x_e) - q_{e_1}(x), f_{e_2}(x_{e_2}) \}
\]

where \( u, \kappa \geq 0 \) are control parameters.

3) Disruption Modes: We consider a set \( S \) of modes that capture cyber and/or physical disruptions. With a slight abuse of notation, we use \( f_e : S \times X_e \rightarrow \mathbb{R}_{\geq 0}, r_e : S \times X_e \rightarrow \mathbb{R}_{\geq 0}, \mu : S \times X \rightarrow \mathbb{R}_{\geq 0} \) and \( q : S \times X \rightarrow \mathbb{R}_{\geq 0} \) to denote the sending flow of link \( e \), the receiving flow of link \( e \), the control law and the actual inter-link flows influenced by disruptions, respectively.

Assumption 3 (Cyber-physical disruptions):

3.1 Nominal mode: There exists a nominal mode, denoted by \( s_0 \in S \), under which the network is free from cyber-physical disruptions and thus stable.

3.2 Disrupted sending/receiving flows: For every \( s \in S \) and \( e \in \mathcal{E} \), \( f_e(s, x_e) \) and \( r_e(s, x_e) \) satisfy Assumption 1. Furthermore, \( f_e(s, x_e) \leq f_e(s_0, x_e) \) and \( r_e(s, x_e) \leq r_e(s_0, x_e) \).

3.3 Disrupted controlled flows: For every \( s \in S \) and \( e \in \mathcal{E} \), \( q(s, x) \) satisfies Assumption 2.

Assumption 3.1 ensures one stable mode. In this article, our primal interest is to study whether the network is destabilized given the switched modes. Assumptions 3.2 and 3.3 imply that disruptions will not fundamentally change the flow dynamics. They hold for typical reliability failures; see the examples later. Then, mode-specific link capacities and critical densities are given by

\[
Q_{se} := \sup_{x_e \in \mathcal{X}_e} \min \{ f_e(s, x_e), r_e(s, x_e) \}
\]

\[
x_{sc} := \inf \{ x_e \in \mathcal{X}_e | f_e(s, x_e) = Q_{se} \}
\]

Note that Assumption 3.2 also indicates \( Q_{se} \leq Q_{s_0e} \) for any \( s \in S \) and \( e \in \mathcal{E} \). We denote by \( x_{sc}^e \) the maximum critical density over disruption modes

\[
x_{sc}^e := \max_{s \in S} x_{sc}^e, e \in \mathcal{E}.
\]

The following are examples of physical and cyber disruptions. Consider logit routing for a diverging junction with an upstream link \( e \), and suppose that the outflow from link \( e \) may decrease by a certain ratio. Thus, we consider \( S = \{ s_0, s_1 \} \) and \( f_e(s_1, x) = \chi f_e(s_0, x) \), where \( \chi \in (0, 1] \). The actual interlink flows are given by

\[
q_{e_1}(s, x) = \min \left\{ \frac{e^{-\theta_j x_j}}{\sum_{j' \in \mathcal{E}_e^+} e^{-\theta_j x_{j'}} f_e(s_{j'}, x_{j'}), r_j(x_j)} \right\}
\]

Now suppose that the observation of link \( j^* \in \mathcal{E}_e^+ \), denoted by \( T_j(s, x) \), may be biased. Without loss of generality, we let \( T_j(s_1, x) = \kappa x_j \). with some \( \kappa \geq 0 \) and \( T_j(s, x) = x_j \) for any \( (s, j^*) \neq (s_1, j^*) \). The controlled flows are given by

\[
q_{e_2}(s, x) = \min \left\{ \frac{e^{-\theta_j x_j}}{\sum_{j' \in \mathcal{E}_e^+} e^{-\theta_j x_{j'}} f_e(s_{j'}, x_{j'}), r_j(x_j)} \right\}
\]

B. PDMP Model

Now we can define the piecewise-deterministic dynamics of the controlled process \( \{ S(t), X(t) \} : t \geq 0 \). The discrete-state process \( \{ S(t); t \geq 0 \} \) of the mode is a homogeneous finite-state Markov process that is independent of the continuous-state process \( \{ X(t); t \geq 0 \} \) of the traffic densities. The state space of the discrete process is \( S := \{ s_0, s_1, \ldots, s_M \} \). The transition rate from mode \( s \) to mode \( s' \) is \( \lambda_{ss'} \). Without loss of generality, we assume that \( \lambda_{ss} = 0 \) for all \( s \in S \). The discrete-state process evolves as follows:

\[
Pr\{ S(t + \delta) = s' | S(t) = s \} = \lambda_{ss'} \delta + o(\delta), \forall s, s' \in S
\]

where \( \delta \) denotes an infinitesimal increment. We assume that the discrete-state process is ergodic, which means that every disruption will be resolved in finite time almost surely. It follows that \( \{ S(t); t \geq 0 \} \) admits a unique steady-state probability vector \( p := [p_{s_0}, p_{s_1}, \ldots, p_{s_M}]^T \in \mathbb{R}_{\geq 0}^S \) satisfying

\[
\Lambda^T p = 0
\]

2Security failures, which are beyond the scope of this article, however, may violate this assumption.
where $0$ denotes the zero vector and $\Lambda$ is the transition matrix given by
\[
\Lambda := \begin{bmatrix}
-\sum_{s' \in S} \lambda_{ss'} & \lambda_{s0s1} & \cdots & \lambda_{s0sm} \\
\lambda_{s1s0} & -\sum_{s' \in S} \lambda_{s1s'} & \cdots & \lambda_{s1sm} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_{sms0} & \lambda_{sms1} & \cdots & -\sum_{s' \in S} \lambda_{sms'}
\end{bmatrix}.
\]
(13)

The continuous-state process $\{X(t); t \geq 0\}$ is defined as follows. We let $G_c(s, x) := (d/dt)X_c(t)$. The conservation law associated with flows implies
\[
G_c(S(t), X(t)) = \begin{cases}
\alpha - \sum_{j \in \mathcal{E}_+} g_{ej}(S(t), X(t)) & \text{if } \tau_e = v_o \\
\sum_{i \in \mathcal{E}_-} g_{ie}(S(t), X(t)) & \text{if } \tau_e \notin \{v_0, v_d\}
\end{cases}
\]
(14a)
\[
\sum_{j \in \mathcal{E}_+} g_{ej}(S(t), X(t)), \quad \text{if } \tau_e = v_d.
\]
(14b)
\[
-f_c(S(t), X(t)),
\]
(14c)

Note $G_c$ is bounded. So is $G(s, x) := (d/dt)X(t)$. The joint evolution of $S(t)$ and $X(t)$ is a PDMP and can be described compactly using an infinitesimal generator [35]
\[
\mathcal{L}V(s, x) = G(s, x)^T \nabla_x V(s, x) + \sum_{s' \in S} \lambda_{ss'} (V(s', x) - V(s, x))
\]
(15)
for any differentiable function $V : \mathcal{S} \times \mathcal{X} \to \mathbb{R}_{\geq 0}$, where $\nabla_x V(s, x)$ is the gradient of $V$ with respect to $x$. The bounded dynamics $G(s, x)$ indicates that $\{(S(t), X(t)); t \geq 0\}$ is a non-explosive Markov process, which is a prerequisite for discussing stability [35].

C. Stability and Resiliency

In this section, we define network stability and resiliency, which are the focus of the subsequent analysis.

1) Stability and Invariant Set: Below we present several concepts regarding stability.

**Definition 2 (Stability and Instability):** The network is stable if there exists a scalar $\bar{Z} < \infty$ such that for any initial condition $(s, x) \in \mathcal{S} \times \mathcal{X}$
\[
\limsup_{t \to \infty} \frac{1}{t} \int_0^t \mathbb{E}[\|X(t)\| | S(0) = s, X(0) = x] dt \leq \bar{Z}
\]
(16)
where $\|X(t)\|$ denotes 1-norm of $X(t)$, namely, $\|X(t)\| = \sum_{e \in \mathcal{E}} |X_e(t)|$. The network is unstable if there does not exist $\bar{Z} < \infty$ such that for any initial condition $(s, x) \in \mathcal{S} \times \mathcal{X}$ such that the inequality (16) holds.

The notion of stability follows a classical definition [28], which is closely related to “first-moment stable” [22]. Practically, if the time-average traffic densities in all links are bounded, the network is stable; otherwise, it is unstable.

Verifying the stability requires to check (16) for all initial conditions $(s, x) \in \mathcal{S} \times \mathcal{X}$. This can be simplified by considering an invariant set $\mathcal{X}^\mu \subseteq \mathcal{X}$ [24], which is defined as follows.

**Definition 3 (Invariant set):** For the PDMP $\{(S(t), X(t)); t \geq 0\}$, a subset $\mathcal{X}^\mu \subseteq \mathcal{X}$ is an invariant set if it is i) globally attracting and ii) positively invariant
\[
\begin{align*}
\text{i)} & \quad \forall (S(0), X(0)) \in \mathcal{S} \times \mathcal{X} \quad \lim_{t \to \infty} \text{Pr}\{X(t) \in \mathcal{X}^\mu | (S(0), X(0))\} = 1; \\
\text{ii)} & \quad \forall (S(0), X(0)) \in \mathcal{S} \times \mathcal{X} \quad \forall t \geq 0, X(t) \in \mathcal{X}^\mu.
\end{align*}
\]
The definition above indicates that i) for any initial condition $X(0) \in \mathcal{X}$, the state $X(t)$ enters $\mathcal{X}^\mu$ almost surely, and that ii) given any initial condition $X(0) \in \mathcal{X}^\mu$, the state $X(t)$ never leaves $\mathcal{X}^\mu$. Note that one trivial candidate set is $\mathcal{X}$ itself, but a tight invariant set depends on the control law $\mu$ and disruption modes $\mathcal{S}$. It is assumed that $\mathcal{X}^\mu$ is unbounded; otherwise, the network is naturally stable. Besides, we define
\[
\bar{\mu} := \inf_{x \in \mathcal{X}^\mu} \{x, \bar{x}_e := \sup_{x \in \mathcal{X}^\mu} x, e \in \mathcal{E} \}
\]
if $x_e$ does not have an invariant upper bound, we let $\bar{x}_e = \infty$. Clearly, we have $\mathcal{X}^\mu \subseteq \bigcap_{e \in \mathcal{E}} [\bar{x}_e, \bar{x}_e']$. The following sets of links are induced by the invariant set $\mathcal{X}^\mu$. Clearly they also depend on the control law $\mu$, but we omit the superscript “$\mu$” for notational convenience without causing confusion. We denote by $\mathcal{E}_{inf} := \{e \in \mathcal{E} | \bar{x}_e = \infty\}$ the set of density-unbounded links. For any $e \in \mathcal{E}_{inf}$, let $\mathcal{A}_{e, inf} := \mathcal{A}_e^- \cap \mathcal{E}_{inf}$ (respectively, $\mathcal{A}_{e, inf}^+ := \mathcal{A}_e^+ \cap \mathcal{E}_{inf}$) denote its upstream (respectively, downstream) density-unbounded links. We also define the set of density-bounded links that are upstream (respectively, downstream) of link $e$ in $\mathcal{E}_{inf}$, denoted by $\mathcal{A}_{e, fin} := \mathcal{A}_e^- \setminus \mathcal{A}_{e, inf}$ (respectively, $\mathcal{A}_{e, fin}^+ := \mathcal{A}_e^+ \setminus \mathcal{A}_{e, inf}$). Particularly, we let
\[
\mathcal{E}_e^+ := \{n \in \mathcal{A}_e^+ | \forall i \in X_e \} = \{n \in \mathcal{A}_e^+ \cap \mathcal{A}_n^- \}
\]
(17)
\[
\begin{align*}
(i) & \quad \ell \in \mathcal{A}_{e, fin}^+ \\
(ii) & \quad \exists (s, x) \in \mathcal{S} \times \mathcal{X}, \exists i \in X_{e, fin}^- \min\{\mu_i(s, x), r_{i, e}^- (s, x)\} > r_{i, e}^- (s, x)
\end{align*}
\]
denote the set of links downstream of link $e \in \mathcal{E}_{inf}$ such that (i) link $n \in \mathcal{E}_e^+$ is density-bounded, (ii) link $n \in \mathcal{E}_e^+$ can block the flows from its upstream link $i$, and (iii) any link $\ell$ between $e$ and $n$, namely, $\ell \in \mathcal{A}_e^+ \cap \mathcal{A}_n^-$ satisfies (i) and (ii), where $r_{i, e}^- (s, x)$ (respectively, $r_{i, e}^- (s, x)$) is defined as in (15a) (respectively, (15b)), denoting allocated sending (respectively, receiving) flow between links $i$ and $\ell$. Intuitively, $\mathcal{E}_e^+$ is the set of connected bottlenecks, between link $e$ and its downstream density-unbounded links, that induce congestion spillback and block the discharging flow of link $e$.

We use the classical Wheatstone bridge [41] to illustrate the definitions above; see Fig. 3. Suppose that only links $e_o$ and $e_5$ have infinite storage and that the flows out of links $e_2$ and $e_5$ are decreased randomly by physical disruptions. Then, the congestion builds up at links $e_2$ and $e_5$. Due to the infinite storage, the traffic density at link $e_5$ may blow up. Meanwhile, link $e_o$ could be blocked as well once the jam at link $e_2$ spills...
back to link $e_0$ via link $e_1$. It indicates $\mathcal{E}_{\text{inf}} = \{e_0, e_5\}$ with $\mathcal{B}_e^+ = \{e_1, e_2\}$ and $\mathcal{B}_e^- = \emptyset$.

2) Resiliency, throughput and Min-Cut Capacities: The throughput $\alpha^\mu$ of a network with control $\mu$ is defined as the maximal demand that the network can accept while maintaining stability, i.e., traffic densities in all links being bounded on average

$$\alpha^\mu := \sup_{\alpha \geq 0, \text{s.t. network is stable}} \alpha.$$  

For a network $\mathcal{G} = (\mathcal{E}, \mathcal{V})$ with link capacities $\mathcal{Q} := \{Q_e | e \in \mathcal{E}\}$, we denote by $C(\mathcal{Q}; \mathcal{G})$ its MCC. The min-cut max-flow theorem states that the nominal throughput equals the MCC [8], which is obtained by solving the maximum flow problem

$$\begin{align*}
\text{(P1)}: \quad \max_{\alpha \geq 0, u \in \mathcal{E}_{\text{inf}}} \alpha \\
\text{s.t.} \quad \alpha = \sum_{j \in \mathcal{E}^+_o} u_{ej}, \quad \tau_e = v_o
\end{align*}$$

where the optimal $\alpha^*$ is equal to $C(\mathcal{Q}; \mathcal{G})$. Then, we define resiliency score as

$$\eta^\mu := \alpha^\mu / C(\mathcal{Q}_{s_0}; \mathcal{G})$$

motivation for the resiliency score lies in that MCC is an important measurement of network capability. Meanwhile, for monotone dynamical flow networks, it is easily attainable with an open-loop control in the nominal case; see Appendix A. Thus, the ratio can capture throughput losses due to disruptions.

III. Resiliency Analysis

In this section, we analyze a network’s stability under a given control law $\mu$. The main results allow quantification of the resiliency score $\eta^\mu$ given by (20).

To state the results, we define

$$I_e(s, x) := \sum_{m \in \mathcal{A}_c} G_m(s, x) + \sum_{i \in \mathcal{E}_c^+} q_{ie}(s, x)$$

$$O_e(s, x) := \sum_{j \in \mathcal{E}_c^-} q_{ej}(s, x) - \sum_{e \in \mathcal{E}_c} \rho_e(x_e) G_e(s, x)$$

where $\rho_e : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is a weight function

$$\rho_e(x_e) = \begin{cases} 
0, & x_e < \bar{x}_e^\mu \\
\frac{x_e - \bar{x}_e^\mu}{\bar{x}_e^\mu - \bar{x}_e}, & \bar{x}_e^\mu \leq x_e < \bar{x}_e^\mu \\
1, & x_e \geq \bar{x}_e^\mu.
\end{cases}$$

The weight function indicates that $G_e$, the dynamics of link $e$, has more impacts on (21b) as the traffic density $x_e$ increases. We interpret (21a) as the inflow from the origin $v_o$ to link $e$, by considering the flow conservation but not the dynamics on the intermediate links. To see that, we first notice by (14a) and (14b) that $G_m(s, x)$ is the net flow only considering neighboring links of link $m$, and then recognize $\sum_{m \in \mathcal{A}_c} G_m(s, x)$ as the net flow of the upstream network whose inflow is the demand $\alpha$ and whose outflows comprise of 1) those passing link $e$ and 2) those never passing link $e$. Since the former outflows are canceled by $\sum_{i \in \mathcal{E}_c} q_{ie}(s, x)$ in (21a), it is easy to understand that (21a) denotes the demand $\alpha$ minus the flows never passing link $e$. In a similar way, we interpret (21b) as a weighted outflow of link $e$ including those traversing the downstream bottlenecks and those not. Aware of the physical meanings of (21a) and (21b), we let

$$N_e(s, x) := I_e(s, x) - O_e(s, x)$$

denote the net flow of link $e$ considered in a larger scope, from the location of demand generation to the sites of bottleneck dissipation. It captures necessary networkwide dynamics and thus helps investigate the network stability conditions.

We use the Wheatstone bridge in Fig. 3 to enhance the understandings of (21a) and (21b). First, we have $I_{e_5}(s, x) = \alpha - q_{e_5 e_3}(s, x)$, where the flow $q_{e_5 e_3}$ never enters link $e_3$. If we plug $\rho_e = 1$ into (21b), we obtain $O_{e_3}(s, x) = q_{e_3 e_4}(s, x) + q_{e_3 e_5}(s, x)$, where $q_{e_3 e_4}$ denotes the outflow of link $e_3$ through the bottleneck and $q_{e_3 e_5}$ represents the flows never entering the bottleneck. Although the physical meaning is clear given $\rho_e = 1$, it leads to trivial stability analysis. This is because congestion spillback is oversimplified. For example, the flows $q_{e_5 e_2}$ and $q_{e_3 e_2}$ are omitted in $O_{e_3}(s, x)$. This will happen if piecewise quadratic Lyapunov functions with $\rho_e = 1$ are used.
A. Main Results

This section presents two main results of stability analysis. The first stability condition emphasizes a physical intuition that any dynamic flow network is stable if the long-term net flow is negative for each density-unbounded link; the second is stronger but more abstract.

The first main result is as follows.

Theorem 1: Consider an acyclic network satisfying Assumptions 3.1–3.3. Suppose that the network admits a demand \( \alpha \) and an invariant set \( \mathcal{X}^\mu \subseteq \prod_{s \in \mathcal{E}} [\underline{x}^\mu_s, \overline{x}^\mu_s] \) under a control law \( \mu : \mathcal{S} \times \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}^m \). Then, the network is stable if

\[
\sum_{s \in \mathcal{S}} p_s \max_{x \in D_c^\mu} N_c(s, x) < 0 \quad \forall \mu \in \mathcal{E}_{\text{inf}} \tag{24}
\]

where \( \{p_s | s \in \mathcal{S}\} \) is the steady-state probability distribution of disruption modes and \( D_c^\mu \) is given by

\[
\begin{align*}
D_c^\mu := \{ & x | x_e = x^\mu_e, \ x_m = x^\mu_m \ \forall m \in A^-_c \\
& x_n = \overline{x}^\mu_n \ \forall n \in \mathcal{E} \setminus (A^-_c \cup \{e\} \cup B^+_e) \\
& x_t \in [\underline{x}^\mu_t, \overline{x}^\mu_t] \ \forall \ell \in B^+_t \}. \tag{25}
\end{align*}
\]

Theorem 1 essentially states that the network is stable if the expectation of the maximum \( N_c(s, x) \) over \( D_c^\mu \) is negative for every link \( e \in \mathcal{E}_{\text{inf}} \), where \( D_c^\mu \) is a refinement of \( \prod_{s \in \mathcal{E}} [\underline{x}^\mu_s, \overline{x}^\mu_s] \) by using monotone network dynamics. Recalling the definition of \( N_c(s, x) \) and the physical meanings of \( I_c(s, x) \) and \( O_c(s, x) \), we see that the lower bounds \( \underline{x}^\mu_n \) and the upper bounds \( \overline{x}^\mu_n \) in \( D_c^\mu \) make our stability verification consider as many flows as possible from the origin into link \( e \) to act as the inflow of link \( e \). Note that \( x_n \) will take the infinite value if \( \overline{x}^\mu_n = \infty \); we conclude the limit exists as \( x_n \rightarrow \infty \) by noting that \( N_c(s, x) \) is nondecreasing in \( x_n \) for \( n \in \mathcal{E} \setminus (A^-_c \cup \{e\} \cup B^+_e) \) (see the proof in Section III-C) and that \( N_c(s, x) \) is bounded.

Another observation on Theorem 1 is that we use a rectangle-like set \( \prod_{s \in \mathcal{E}} [\underline{x}^\mu_s, \overline{x}^\mu_s] \) instead of \( \mathcal{X}^\mu \), to simplify the computation. Although simple, such kind of set suffices to yield interesting results; see Theorems 3 and 4. In general, the invariant set \( \mathcal{X}^\mu \) could be in other shapes; the stability condition can be further refined given a specific invariant set.

One can obtain a lower bound of the resiliency score by finding the supremum of those demands \( \alpha \) that satisfy the criterion (24). It involves solving a set of maximization problems only over compact sets \( \prod_{s \in \mathcal{E}} [\underline{x}^\mu_s, \overline{x}^\mu_s] \). Thus, we are able to find the global optimal solution efficiently with searching algorithms. This is a significant refinement with respect to the general stability criteria, which essentially require search over unbounded sets [24]. Note that though the criterion (24) is a sufficient condition, it is also necessary in particular settings; see Theorems 3 and 4.

Theorem 1 is proved based on a novel Lyapunov function (32) relying on the weight function (22). We enhance it by considering more general weights for links from the sets \( A^-_{e,\text{fin}} \) and \( B^+_e \), which is achieved by a more sophisticated Lyapunov function (41). Weighting link dynamics \( G_{e,\text{fin}}(s, x), \ell \in A^-_{e,\text{fin}} \) can enhance the stability analysis if there are upstream bottlenecks with congestion spillback. Note that by appropriately restricting the weights for \( A^-_{e,\text{fin}} \) and \( B^+_e \), we only need to consider \( x_m = x^\mu_m, \ m \in A^-_{e,\text{fin}} \), when checking the stability, just like Theorem 1. We do not consider weighting \( G_m(s, x), m \in A^-_{e,\text{inf}} \) for two reasons. First, link \( m \in A^-_{e,\text{inf}} \) has infinite storage and does not block its inflow. Second, weighting \( G_m(s, x), m \in A^-_{e,\text{inf}} \), will destroy the monotonicity with respect to \( x_m \), which incurs additional computational costs of the stability verification.

For \( A^-_{e,\text{fin}} \cup B^+_e = \{e_1, e_2, \ldots, e_i \} \), we define its state vector by

\[ x_e^* := [x_{e_1}, x_{e_2}, \ldots, x_{e_i}]^T \in \bigcup_{h=1}^H A^\mu_{e_h}. \]

Along with the advanced Lyapunov function (41), we let

\[ N_e^\mu(s, x) := \sum_{m \in A^-_{e,\text{inf}}(e)} G_m(s, x) + 2x^T \{s, x, \ldots, x_{e_1}, \ldots, x_{e_2}, \ldots, x_{e_i} \} \in \mathbb{R}_{\geq 0}^m \]

denote a generalization of \( N_e^\mu(s, x) \), where \( \xi_k(x_e^*) := [1, x_{e_1}, \ldots, x_{e_i}, \ldots, x_{e_2}, \ldots, x_{e_1}, \ldots, x_{e_i}] \in \mathbb{R}_{\geq 0}^m \) is a monomial basis of degree \( k \) for \( x_e^* \)

\[ \xi_k(x_e^*) := \frac{d^k}{dt^k} \xi_k(x_e^*(t)) \]

is the derivative of \( \xi_k(x_e^*) \) with respect to time \( t \), and \( B_{se} \in S_{k+1}^+ \) is a symmetric positive definite matrix for \( s \in \mathcal{S} \) and \( e \in \mathcal{E}_{\text{inf}} \).

The second main result of this section is as follows:

Theorem 2: Consider an acyclic network satisfying Assumptions 3.1–3.3. Suppose that the network admits a demand \( \alpha \) and an invariant set \( \mathcal{X}^\mu \subseteq \prod_{s \in \mathcal{E}} [\underline{x}^\mu_s, \overline{x}^\mu_s] \) under a control \( \mu : \mathcal{S} \times \mathcal{X} \rightarrow \mathbb{R}_{\neq 0}^m \). Besides, there exist a set of symmetric positive definite matrices \( B_{se} \in S_{k+1}^+ \), \( m \in \mathcal{E}_{\text{inf}} \), \( e \in \mathcal{E} \), \( s \in \mathcal{S} \), such that

\[ 0 \leq 2J_{\xi_k}^T(x_e^*) B_{se} \xi_k(x_e^*) \leq 1 \quad \forall x_e^* \in \bigcup_{h=1}^H A^\mu_{e_h} \tag{27} \]

where

\[ J_{\xi_k}(x_e^*) := \frac{d}{dx_e^*} \xi_k(x_e^*) \in \mathbb{R}^{(k+1) \times H} \]

is a Jacobian matrix. Then, the network is stable if

\[ \max_{x \in D_c^\mu} N_e^\mu(s, x) < 0 \quad \forall \mu \in \mathcal{E}_{\text{inf}}, s \in \mathcal{S} \tag{28} \]

where \( D_c^\mu \) is given by

\[
\begin{align*}
D_c^\mu := \{ & x | x_e = x_e^*, \ x_m = x^\mu_m \ \forall m \in A^-_{e,\text{inf}}, \\
& x_n = \overline{x}^\mu_n \ \forall n \in \mathcal{E} \setminus (A^-_c \cup \{e\} \cup B^+_e), \\
& x_t \in [\underline{x}^\mu_t, \overline{x}^\mu_t] \ \forall \ell \in A^-_{e,\text{fin}} \cup B^+_t \}. \tag{29}
\end{align*}
\]

The weight constraint (27) induces each weight function of the link dynamics \( G_{e,\text{fin}}(s, x) \) to have a range \([0, 1]\). The nonnegativity endows the weighted \( G_{e,\text{fin}}(s, x) \) with the correct physical meaning of net flows, and less than one makes \( x_m, m \in A^-_{e,\text{inf}} \subseteq A^-_e \), attain the minimum value by monotone network dynamics, such as Theorem 1.

The proof of Theorem 2 is based on the generalized Lyapunov function (41). Note that the extension is not unique. For example, we can further adapt the Lyapunov function if the control law is specified; see our proof of Theorem 3 in Section IV-C.
In general, Theorem 2 yields stronger criteria than Theorem 1. The throughput bounds derived from Theorem 2 can be further sharpened by increasing the degree $k$ of the basis $\xi_k(x')$, but it requires more computational costs. We check the stability by solving the following semi-infinite programming (SIP) [42] with finite decision variables but infinite constraints

$$
(P_2) \min_{\gamma, B_{e}} \gamma
$$

s.t. (27)

$$
\gamma \geq N^*_e(s, x) \quad \forall (s, x) \in \mathcal{S} \times \mathcal{D}^*_{e} \quad \forall e \in \mathcal{E}_{\text{inf}}.
$$

The programming problem has infinite constraints because (27) and (30) should hold for infinitely many states $x$. If the optimal $\gamma^* < 0$, we say the network is stable. Since $\ell \in \mathcal{A}_{e \in \mathcal{H} \cup B_{e}}$ is density-bounded, the constraint (27) is required to hold over the compact set $\prod_{i=1}^{H} \mathcal{X}_{e_i}$, as well. Thus, we can solve $P_2$ efficiently with the solution algorithms for SIPs, such as adaptive convexification [42].

The rest of this section is devoted to a numerical example for resiliency analysis based on the above results (see Section III-B) and the proof of Theorem 1 (see Section III-C) and Theorem 2 (see Section III-D).

### B. Numerical Example

Consider the network in Fig. 3. The sending flow function of link $e$ is given by $f_e(s, x_e) = \min \{v_f x_e, Q_{se}\}$, where $v_f > 0$ is a coefficient of free-flow speed [36] and $Q_{se}$ is the mode-specific capacity of link $e$. The receiving flow functions are given by

$$
r_e(x_e) = \begin{cases} 
\min \{w_e(x_e^{\max} - x_e), Q_e\}, & \text{if } x_e^{\max} < \infty \\
\infty, & \text{if } x_e^{\max} = \infty
\end{cases}
$$

where $w_e > 0$ is a coefficient of congestion-wave speed [36] and $Q_e$ is the nominal capacity. In this example, we set $v_f = 1$, $w_e = 1/2$, $Q_{se} = Q_{e_1} = Q_{e_2} = 1$, and $Q_{e_3} = Q_{e_4} = 1.2$. If links $e_1, \ldots, e_5$ have finite storage space, we let $x_e^{\max} = x_e^{\max} = 3$, and $x_e^{\max} = x_e^{\max} = x_e^{\max} = 3/2$.

The network is subject to cyber-physical disruptions as follows. On link $e_5$, the traffic state $x_{e_5}$ may temporarily appear to be zero to the controller. On link $e_5$, the sending capacity can be temporarily reduced to zero. Table I characterizes the fault mapping $T_{e_5}(s, x)$ for cyber disruptions and the mode-specific capacity $Q_{se_5}$ for physical disruptions. The other links are not subject to disruptions; i.e., $T_e(s, x) = x_e$ for all $s$ and all $e \neq e_5$, and $Q_{se_5} = Q_e$ for all $s$ and all $e \neq e_5$. Hence, the network has at most four modes.

| Mode | $s_0$ | $s_1$ | $s_2$ | $s_3$ |
|------|------|------|------|------|
| $T_{e_5}(s, x)$ | $x_{e_5}$ | $x_{e_5}$ | 0 | 0 |
| $Q_{se_5}$ | 1 | 0 | 1 | 0 |

| Infinite space | Cyber disruptions | Physical disruptions | $\gamma_{\text{logit}}^{1/2}$ | $\gamma_{\text{logit}}^{1/4}$ |
|----------------|------------------|---------------------|-----------------|-----------------|
| yes            | no               | yes                | 0.1             | 1.1             |
| yes            | yes              | yes                | 0.783           | 0.984           |
| yes            | no               | yes                | 0.667           | 0.667           |
| yes            | yes              | yes                | 0.602           | 0.623           |
| no             | no               | no                 | 1               | 1               |
| yes            | yes              | yes                | 0.792           | 0.910           |
| yes            | yes              | yes                | 0.741           | 0.848           |
| yes            | yes              | yes                | 0.493           | 0.708           |

The corresponding steady-state probabilities $p_s$ can be computed for the mode $s \in \{s_0, s_1, s_2, s_3\}$: $p_{s_0} = p_{s_1} = p_{s_2} = p_{s_3} = 1/4$.

In the following we specify network dynamics. The traffic flows at the diverges are routed according to the classical logit model

$$
q_{e_i}^{\text{logit}}(s, x) = \min \left\{ \frac{e^{-\nu x_{e_i}}}{e^{-\nu x_{e_1} + e^{-\nu T_{e_i}(s, x)}} f_e(s, x_e), r_{e_1}(x_{e_1})} \right\}
$$

$$
q_{e_i}^{\text{logit}}(s, x) = \min \left\{ e^{-\nu x_{e_i}} f_e(s, x_e), r_{e_4}(x_{e_4}) \right\}
$$

$$
q_{e_i}^{\text{logit}}(s, x) = \min \left\{ e^{-\nu x_{e_i} + e^{-\nu T_{e_i}(s, x)}} f_e(s, x_e), r_{e_4}(x_{e_4}) \right\}
$$

$$
q_{e_i}^{\text{logit}}(s, x) = \min \left\{ e^{-\nu x_{e_i} + e^{-\nu T_{e_i}(s, x)}} f_e(s, x_e), r_{e_4}(x_{e_4}) \right\}
$$

$$
q_{e_i}^{\text{logit}}(s, x) = \min \left\{ e^{-\nu x_{e_i} + e^{-\nu T_{e_i}(s, x)}} f_e(s, x_e), r_{e_4}(x_{e_4}) \right\}
$$

In this example, we select $\nu = 2$ as the sensitivity coefficient. At the merge, we assume that link $e_2$ is prioritized over link $e_4$. Such a priority can be realized by

$$
q_{e_2}^{\text{logit}}(s, x) = \min \{f_{e_2}(s, x_{e_2}), r_{e_4}(x_{e_4})\}
$$

$$
q_{e_4}^{\text{logit}}(s, x) = \min \{f_{e_4}(s, x_{e_4}), r_{e_4}(x_{e_4}) - q_{e_2}^{\text{logit}}(s, x)\}
$$

Table II lists resiliency scores in various scenarios. The column “Infinite space” indicates whether links $e_1, e_2, \ldots, e_5$ have infinite storage space. Clearly, we have the nominal MCC equal to one, i.e., $C(Q_{se_0}; Q) = 1$. The lower bounds $\gamma_{\text{logit}}^{1/2}$ are derived from Theorem 1, while the bounds $\gamma_{\text{logit}}^{1/4}$ are obtained through Theorem 2. The details are available in the supplementary material. We also used numerical simulation to evaluate true resiliency scores, denoted by $\gamma_{\text{sim}}^{\text{logit}}$. Our findings are summarized below, where the finding (iii) is a little surprising at the first glance as follows.

1) It is demonstrated that Theorem 2 yields tighter lower bounds than Theorem 1. More importantly, the bounds $\gamma_{\text{logit}}^{1/4}$ are close to $\gamma_{\text{logit}}^{1/2}$, i.e., the resiliency scores revealed by numerical simulation.

2) Cyber-physical disruptions can significantly decrease the network performance. For instance, the resiliency score decreases to 0.860 when links $e_1, \ldots, e_5$ only have finite...
space and the network suffers the physical disruption. It further declines to 0.722 when the network is also subject to the cyber disruption.

3) Increasing link storage may not help improve resiliency under inappropriate localized controls. As seen in Table II, the disruptions have more significant impacts given infinite link storage space. The reason lies in that the congestion in link $e_5$ does not affect the upstream routing when link $e_5$ has infinite storage.

C. Proof of Theorem 1

The proof consists of two steps. We first prove Proposition 1, and then show that under Assumption 3.3 we only need to check over $\mathcal{D}^\mu_e$ given by (25) instead of the unbounded set $\mathcal{D}^\mu_e$ in Proposition 1.

Proposition 1: Consider an acyclic network satisfying Assumptions 3.1 and 3.2. Suppose that the network admits a demand $\alpha$ and an invariant set $\mathcal{X}^\mu \subseteq \prod_{e \in \mathcal{E}_e} \mathcal{X}^\mu_e \times \mathcal{P}^\mu_e$ under a control law $\mu: \mathcal{S} \times \mathcal{X} \to \mathbb{R}_0^m$. Then, the network is stable if

$$\sum_{s \in \mathcal{S}} p_s \max_{x \in \mathcal{P}^\mu_e} N_e(s, x) < 0 \quad \forall e \in \mathcal{E}_{\text{inf}} \tag{31}$$

where $\mathcal{D}^\mu_e := \{x \in \mathcal{X}^\mu | x \geq x^e_{\text{cs}}\}$.

We prove Proposition 1 by applying the following Foster–Lyapunov criterion adapted from [35, Th. 4.3 (ii)]. Foster–Lyapunov criterion: Consider a nonexplosive piecewise-deterministic Markov process $\{(S(t), X(t); t \geq 0)\}$ with a state space $\mathcal{S} \times \mathcal{X}$, an infinitesimal generator $\mathcal{L}$, and a Lyapunov function $V: \mathcal{S} \times \mathcal{X} \to \mathbb{R}_0$. If there exist constants $c > 0$, $d < \infty$ and a function $f: \mathcal{X} \to \mathbb{R}_0$, with $f(x) \to \infty$ as $|x| \to \infty$, such that

$$\mathcal{L}V(s, x) \leq -c f(x) + d \quad \forall(s, x) \in \mathcal{S} \times \mathcal{X}$$

then, for each initial condition $(s, x) \in \mathcal{S} \times \mathcal{X}$

$$\limsup_{t \to \infty} \frac{1}{t} \int_{\tau=0}^t E[f(X(\tau))|S(0) = s, X(0) = x]d\tau \leq d/c.$$

Consider a novel switched polynomial Lyapunov function

$$V(s, x) := \sum_{e \in \mathcal{E}_{\text{inf}}} a_e x_e \left[ \frac{1}{2} x_e + \sum_{m \in \mathcal{A}^e_s} x_m \right] + \sum_{e \in \mathcal{E}_{\text{inf}}} \int_{\mathbb{R}^+} \rho(t) \mathcal{L}x_e d\tau + b_{\text{se}} \tag{32}$$

where $a_e > 0$ and $b_{\text{se}} \geq 0$ for any $s \in \mathcal{S}$ and $e \in \mathcal{E}_{\text{inf}}$. The design of (32) is motivated by network dynamics as follows.

1) For each $e \in \mathcal{E}_{\text{inf}}$, its upstream links, $\mathcal{A}^e_s$, and downstream bottlenecks, $\mathcal{B}^+_e$, are taken into account.
2) The weight function (22) is introduced to better capture bottleneck dynamics. If $\rho_l \equiv 1$, (32) is reduced to a piecewise quadratic function.
3) The parameters $a_e$ and $b_{\text{se}}$ are used to model the impact of mode $s$ on link $e$. We will show that such a design saves finding explicit values of $a_e$ and $b_{\text{se}}$.

In the following we show that if (31) holds, we must have $a_e > 0$, $b_{\text{se}} \geq 0$, $c > 0$ and $d < \infty$ such that $V(s, x)$ satisfies:

$$\mathcal{L}V(s, x) \leq -c \sum_{e \in \mathcal{E}_{\text{inf}}} x_e + d \quad \forall(s, x) \in \mathcal{S} \times \mathcal{X}^\mu. \tag{33}$$

To proceed, we apply the infinitesimal generator $\mathcal{L}$ to the Lyapunov function $V(s, x)$. By (15), we have

$$\mathcal{L}V(s, x) = \sum_{e \in \mathcal{E}_{\text{inf}}} \left( a_e x_e \left( N_e(s, x) + \lambda^T s (b_e - b_{\text{se}} 1) \right) \right)$$

$$+ a_e G_e(s, x) \left( \sum_{m \in \mathcal{A}^e_s} x_m + \sum_{e \in \mathcal{E}_{\text{inf}}} \int_{\mathbb{R}^+} \rho(t) \mathcal{L}x_e d\tau + b_{\text{se}} \right)$$

where $1$ denotes the all-ones vector, $\lambda_s := [\lambda_{s_0}, \ldots, \lambda_{s_{\text{sf}}}]^T$ and $b_e := [b_{s_0 e}, \ldots, b_{s_{\text{se}} e}]^T$.

Noting

$$\sum_{e \in \mathcal{E}_{\text{inf}}} G_e(s, x) \sum_{m \in \mathcal{A}^e_s} x_m = \sum_{e \in \mathcal{E}_{\text{inf}}} G_e(s, x) x_m \mathcal{I}_{\mathcal{A}^e_s}(m)$$

$$= \sum_{e \in \mathcal{E}_{\text{inf}}} G_e(s, x) x_e \mathcal{I}_{\mathcal{A}^e_s}(e)$$

$$= \sum_{e \in \mathcal{E}_{\text{inf}}} x_e \sum_{n \in \mathcal{A}^e_s \cap \mathcal{E}_{\text{inf}}} G_n(s, x)$$

we obtain

$$\mathcal{L}V(s, x) = \sum_{e \in \mathcal{E}_{\text{inf}}} \left( D_e(s, x) x_e + a_e G_e(s, x) \right) \sum_{m \in \mathcal{A}^e_s \cap \mathcal{E}_{\text{inf}}} x_m$$

$$+ \sum_{e \in \mathcal{E}_{\text{inf}}} \int_{\mathbb{R}^+} \rho(t) \mathcal{L}x_e d\tau + b_{\text{se}}$$

where $\mathcal{I}_{\mathcal{A}}(e)$ is an indicator function such that $\mathcal{I}_{\mathcal{A}}(e) = 1$ if $e \in \mathcal{A}$ and $\mathcal{I}_{\mathcal{A}}(e) = 0$; otherwise, and

$$D_e(s, x) := a_e \left( N_e(s, x) + \lambda^T s (b_e - b_{\text{se}} 1) \right) + \sum_{n \in \mathcal{A}^e_s \cap \mathcal{E}_{\text{inf}}} a_n G_n(s, x).$$

It follows $\mathcal{L}V(s, x) \leq \sum_{e \in \mathcal{E}_{\text{inf}}} D_e(s, x) x_e + d_0$ with $d_0 < \infty$. The existence of $d_0$ is guaranteed by the boundedness of $x_m$ for $m \in \mathcal{A}^e_s \cap \mathcal{E}_{\text{inf}}$ of $x_k$ for $k \in \mathcal{B}^+_e$ and of $G_n(s, x)$ for $x \in \mathcal{E}_{\text{inf}}$.

Next, we show, if (31) holds, there exist $a_e > 0$, $b_{\text{se}} \geq 0$, $c > 0$ and $d < \infty$ such that

$$D_e(s, x) x_e \leq -c_e x_e + d_e \quad \forall(s, x) \in \mathcal{S} \times \mathcal{X}^\mu \quad \forall e \in \mathcal{E}_{\text{inf}} \tag{34}$$

which implies that (33) is satisfied with $c := \min_{e \in \mathcal{E}_{\text{inf}}} c_e$ and $d := \sum_{e \in \mathcal{E}_{\text{inf}}} d_e$.

For any $e \in \mathcal{E}_{\text{inf}}$, we must have $d_{e,1} < \infty$ such that

$$\max_{(s, x) \in \mathcal{S} \times (\mathcal{X}^\mu \cup \mathcal{D}^\mu_e)} D_e(s, x) x_e \leq d_{e,1}. \tag{35}$$
Besides, for any \((s, x) \in \mathcal{S} \times \mathcal{D}_e^\mu\)
\[
D_c(s, x) \leq a_c \left[ \hat{N}_{sc} + \lambda_s^n (b_e - b_{se} 1) \right] + \hat{G} \sum_{n \in \mathcal{A}_{e, \text{inf}}} a_n
\leq a_c \sum_{s' \in \mathcal{S}} p_{s'} \hat{N}_{s'c} + \hat{G} \sum_{n \in \mathcal{A}_{e, \text{inf}}} a_n
\] (36)
where \(\hat{N}_{sc} := \max_{z \in \mathcal{P}} N_e(s, x)\) and \(\hat{G}\) denotes an upper bound of \(G_e(s, x)\) for \(e \in \mathcal{E}\). The last step is derived from the following lemma, which we prove in Appendix C.

Lemma 1: The system of equations
\[
\sum_{s' \in \mathcal{S}} \lambda_s^n (y_{s'} - y_s) = \sum_{s' \in \mathcal{S}} p_{s'} x_{s'}, s \in \mathcal{S}
\] (37)
has a nonnegative solution for \(y = [y_{s_0}, \ldots, y_{s_m}]^T\), where \(\lambda_{s_n}, \lambda_{s_n}'\), and \(x_{s_n}\) are given, and \(p_{s_n}\) and \(\lambda_{s_n}'\) satisfy (12).

Given (31) and (36), Lemma 2 proved in Appendix D tells that there exists \(c_e\) for \(e \in \mathcal{E}_{\text{inf}}\) such that \(D_c(s, x) < 0 \forall (s, x) \in \mathcal{S} \times \mathcal{D}_e^\mu \forall e \in \mathcal{E}_{\text{inf}}\). Thus, we must have \(c_e > 0\) for each \(e \in \mathcal{E}_{\text{inf}}\) such that
\[
D_c(s, x) x_e \leq -c_e x_e \forall (s, x) \in \mathcal{S} \times \mathcal{D}_e^\mu \forall e \in \mathcal{E}_{\text{inf}}.
\] (38)

Lemma 2: The system of equations
\[
\pi_e a_e + \sum_{n \in \mathcal{A}_{e, \text{inf}}} a_n < 0 \forall e \in \mathcal{E}_{\text{inf}}
\] (39)
has a positive solution for \(\{d_e | e \in \mathcal{E}_{\text{inf}}\}\) if \(\pi_e < 0\) for any \(e \in \mathcal{E}_{\text{inf}}\).

Combining (35) and (38) yields (34) with \(d_e = d_{e, 1} + c_e x_e^\circ\).

It indicates that we finish the proof of Proposition 1.

Noting \(\lambda^n \leq \prod_{e \in \mathcal{E}} \lambda^n_{s_e, x_e}^\mu\), we must have
\[
\max_{\lambda^n_{s_e, x_e}} N_e(s, x) \geq \max_{x \in \mathcal{D}_e^\mu} N_e(s, x).
\]
Then, the rest of the proof is devoted to showing that
\[
\max_{x \in \mathcal{D}_e^\mu} N_e(s, x) = \max_{x \in \mathcal{D}_e^\mu} N_e(s, x) \geq \mathcal{N}_e(s, x)
\] (40)
under Assumption 3.3. Using (40), we can derive (31) from (24), which finishes the proof.

The definition of localized control laws indicates
\[
\max_{x \in \mathcal{D}_e^\mu} N_e(s, x) = \max_{x \in \mathcal{D}_e^\mu} G_{e, \tau_{ev}}(s, x) + G_{e, \sigma_{ev}}(s, x) \ \forall e' \in \mathcal{E}
\]
where \(G_{e, \tau_{ev}}(s, x)\) and \(G_{e, \sigma_{ev}}(s, x)\) denote the projections of \(N_e(s, x)\) onto nodes \(\tau_{ev}\) and \(\sigma_{ev}\), respectively. The projection onto an arbitrary node \(v \in \mathcal{V}\) is given by
\[
G_{e, v}(s, x) := \sum_{j \in \mathcal{E}_e} q_{ij}(s, x) + \sum_{j \in \mathcal{E}_e, j \in \mathcal{E}_e^+} x_{ij}(s, x) - \sum_{j \in \mathcal{E}_e, j \in \mathcal{E}_e^-} x_{ij}(s, x)
\]
where \(x_{ij}(s, x)\) and \(q_{ij}(s, x)\) are specified by (22), and the link sets \(\mathcal{E}_e^+, \mathcal{E}_e^+, \mathcal{E}_e^-,\) and \(\mathcal{E}_e^-\), are illustrated in Fig. 4(a). Note that these sets could be empty. We also use the example in Fig. 3 to present two specific cases in Fig. 4(b) and (c), respectively.

The following first shows \(N_e(s, x)\) is nondecreasing in \(x_n\) for \(n \in \mathcal{E} \setminus \{A_e^- \cup \{v \cup B_e^+\}\}\) by proving \(G_{e, \tau_{ev}}(s, x) + G_{e, \sigma_{ev}}(s, x)\) is nondecreasing in \(x_n\). By Assumption 3.3, the incoming flow \(\sum_{i \in \mathcal{E}_e} q_{ij}(s, x)\) into link \(j \in \mathcal{E}_e^+ \cup \mathcal{E}_e^+\) is nondecreasing in \(x_{ij}\), the outgoing flow \(\sum_{i \in \mathcal{E}_e} q_{ij}(s, x)\) from link \(i \in \mathcal{E}_e^+ \cup \mathcal{E}_e^+\) is nonincreasing in \(x_{ij}\). Thus, \(G_{e, v}(s, x)\) is nondecreasing in \(x_{ij}\). Similarly, it is easy to verify that \(G_{e, v}(s, x)\) is nonincreasing in \(x_{ij}\). This implies that both \(G_{e, \tau_{ev}}(s, x)\) and \(G_{e, \sigma_{ev}}(s, x)\) are nonincreasing in any \(n \in \mathcal{E} \setminus \{A_e^- \cup \{v \cup B_e^+\}\}\).

Now we show \(N_e(s, x)\) is nonincreasing in \(x_m\) for \(m \in \mathcal{A}_e^- \cup \{v\}\) by proving \(G_{e, \tau_{ev}}(s, x) + G_{e, \sigma_{ev}}(s, x)\) is nonincreasing in \(x_m\).

Noting \(\mathcal{E}_e^+ \cup \mathcal{E}_e^+ \cup \mathcal{E}_e^- = \mathcal{E}_e^\mu\) and \(\mathcal{E}_e^+ \cup \mathcal{E}_e^+ \cup \mathcal{E}_e^- = \mathcal{E}_e^\mu\) from Fig. 4, we rewrite \(G_{e, v}(s, x)\) as
\[
G_{e, v}(s, x) = \sum_{i \in \mathcal{E}_e^-} x_{ij}(s, x) + \sum_{i \in \mathcal{E}_e^-} (1 - \rho_{ij}(x_{ij})) x_{ij}(s, x) - \sum_{i \in \mathcal{E}_e^-} q_{ij}(s, x) + \sum_{i \in \mathcal{E}_e^-} (1 - \rho_{ij}(x_{ij})) x_{ij}(s, x).
\]
By Assumption 3.3, the incoming flow \(\sum_{i \in \mathcal{E}_e} q_{ij}(s, x)\) into link \(j \in \mathcal{E}_e^+ \cup \mathcal{E}_e^+\) is nondecreasing in \(x_{ij}\), the outgoing flow \(\sum_{i \in \mathcal{E}_e} q_{ij}(s, x)\) from link \(i \in \mathcal{E}_e^-\) is nonincreasing in \(x_{ij}\). Thus, \(G_{e, v}(s, x)\) is nonincreasing in \(x_{ij}\). Similarly, we can show \(G_{e, v}(s, x)\) is nondecreasing in \(x_{ij}\). Thus, we conclude both \(G_{e, \tau_{ev}}(s, x)\) and \(G_{e, \sigma_{ev}}(s, x)\) are nonincreasing in \(x_{ij}\) for any \(m \in \mathcal{A}_e^- \cup \{v\}\).

Thus, we conclude (40) by the monotonicity of \(N_e(s, x)\), which completes the proof.

D. Proof of Theorem 2

The proof is similar to that of Theorem 1. The major difference lies in the following Lyapunov function:
\[
V^*(s, x) := \sum_{e \in \mathcal{E}_{\text{inf}}} a_e x_e \left[ \frac{1}{2} x_e + \sum_{m \in \mathcal{A}_{e, \text{inf}}} x_m \right]
\]
Fig. 5. Classification of incoming links $E_v^-$ and outgoing links $E_v^+ \in E_{\text{int}}$ and $v \in V$ in Theorem 2.

\[ \sum_{e \in E_{\text{int}}} [D_e^+(s, x_e) + d_0] \]

where $D_e^+(s, x_e) := a_e N_e^+(s, x_e) + \sum_{n \in A_{e,\text{out}}} a_n G_n(s, x_e)$. Then, we obtain the following result similar to Proposition 1.

**Proposition 2:** Consider an acyclic network satisfying Assumptions 3.1 and 3.2. Suppose that the network admits a demand $\alpha$ and an invariant set $\mathcal{X}^\alpha \subseteq \prod_{e \in E} [\underline{x}_e, \overline{x}_e]$ under a control law $\mu : \mathcal{S} \times \mathcal{T} \rightarrow \mathbb{R}_{\geq 0}$. Then, the network is stable if

\[ \max_{x \in D_e^+} N_e^+(s, x) < 0 \quad \forall e \in E_{\text{int}} \quad \forall s \in S \]  

where $D_e^+ := \{ x \in \mathcal{X}^\alpha : x_e \geq \overline{x}_e \}$.

Because of $\mathcal{X}^\alpha \subseteq \prod_{e \in E} [\underline{x}_e, \overline{x}_e]$, we must have

\[ \max_{x \in \prod_{e \in E} [\underline{x}_e, \overline{x}_e]} N_e^+(s, x) \geq \max_{x \in D_e^+} N_e^+(s, x). \]

Next, we only need to prove

\[ \max_{x \in D_e^+} N_e^+(s, x) = \max_{x \in \prod_{e \in E} [\underline{x}_e, \overline{x}_e]} N_e^+(s, x). \]  

For $N_e^+(s, x)$ given by (26), we notice

\[ 2\xi^T(x_e^+)B_{\text{res}}\xi_k(x_e^+) = 2\xi^T(x_e^+)B_{\text{res}}J_{\text{res}}(x_e^+) \]

\[ \begin{bmatrix} G_{e,11}(s, x) \\ G_{e,12}(s, x) \\ \vdots \\ G_{e,n}(s, x) \end{bmatrix} \]

Clearly, (27) indicates $\rho_{e,h}(x) \in [0, 1]$ for $h = 1, 2, \ldots, H$. We see $\rho_{e,h}(x)$ as a generalization of $\rho_{e,h}(x_e)$ given by (22). We then consider the link classification as shown in Fig. 5. We can show the monotonicity of $N_e^+(s, x)$ with respect to 1) $x_n$, $n \in E \setminus (A^-_e \cup \{ e \} \cup B^+_e)$, and 2) $x_m$, $m \in A^-_{\text{int}} \cup \{ e \}$, in a similar way to that in Section III-C, and thus prove (43).}

**IV. RESILIENT CONTROL DESIGN**

In this section, we study control design with guaranteed throughput. We will extend the classical notion of MCC to stochastic networks and present a series of results characterizing the resiliency under various classes of control laws.

Two extensions of the MCC, i.e., the MECC and the EMCC, are considered in the stochastic setting. The MECC is the minimum cut capacity evaluated with the expected capacity of each link, and the EMCC is the expected minimum cut capacity over various modes. Noting that $C(\mathcal{Q}; \mathcal{G})$ denotes the MCC of network $\mathcal{G}$ with a set of link capacities $\mathcal{Q}$, we have

\[ \text{MECC} := C(\mathcal{Q}; \mathcal{G}), \quad \text{EMCC} := \sum_{s \in S} p_s C(\mathcal{Q}; \mathcal{G}) \]

where $\mathcal{Q} := \{ \sum_{s \in S} p_s q_{s,e} : e \in E \}$ and $\mathcal{Q}_e := \{ q_{s,e} : e \in E \}$. In general, the MECC and the EMCC are not equal. Noting that the MCC is concave with respect to link capacities [18], one can show that the MECC is never less than the EMCC by Jensen's inequality. For instance, consider the numerical example in Section III-B: it is shown that the EMCC equals 0.75 and MECC equals 1 in Fig. 6.

**A. Main Results**

The following investigates in which case there exist controls that attain the EMCC/MECC. We start from the simplest open-loop control. It is shown that if every link $e \in E$ has infinite storage space without restricted receiving flows, there exists an open-loop control $\mu^{\text{ol}}$ that guarantees the MECC. The control design is inspired by the solution of the maximum flow problem (P1). Before presenting it, we denote by $u^*(\mathcal{Q}) := \{ u^*_{e,j}(\mathcal{Q}) \} (e, j) \in \mathcal{P}$ the solution of (P1) given the set of link capacities $\mathcal{Q}$ and define

\[ \gamma_{e,j} := \frac{u^*_{e,j}(\mathcal{Q})}{\sum_{j' \in \mathcal{E}_{e}^+} u^*_{e,j'}(\mathcal{Q})}, \quad (e, j) \in \mathcal{P}. \]

Clearly, $\gamma_{e,j}$ denotes the proportion of the outflow of link $e$ routed to link $j$ per the solution $u^*(\mathcal{Q})$.

Then, the open-loop control is given by

\[ \mu^{\text{ol}}(e, j) = \gamma_{e,j} Q_{e,j}^{\max}, \quad (e, j) \in \mathcal{P} \]

where $Q_{e,j}^{\max} := \max_{s \in S} q_{e,j}(s)$. The formal result of the open-loop control is stated below.

**Theorem 3 (Max-flow min-expected-cut):** Consider an acyclic dynamic flow network with $x_e^{\max} = \infty$ and $r_e(s, x_e) = \infty$ for any link $e \in E$. There exists an open-loop control $\mu^{\text{ol}}$ given by (45) such that the network throughput equals the MECC.

However, few links in practice have infinite storage, which indicates the MECC is generally unattainable. For networks possibly with finite storage space, we consider mode-dependent control given observable disruption mode $S(t)$. Suppose a network with the following physical disruptions:

\[ f_e(s, x_e) = \min\{f_e(x_e), F_{se}\} \]

\[ r_e(s, x_e) = \min\{r_e(x_e), R_{se}\}. \]

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
These disruptions restrict maximal outflows or inflows, which satisfy Assumption 3.2. For the sake of simplicity of analysis, we also assume the critical density \( x^c_e \) given by (9) is finite for every \( e \in \mathcal{E} \). If any disruption mode \( s \in \mathcal{S} \) can be correctly observed, we design a mode-dependent control as follows:

\[
\mu_{ej}^{md}(s) := u_{ej}^*(Q_s), \quad (e, j) \in \mathcal{P}
\]  

(47)

where \( u_{ej}^*(Q_s) \) is an optimal solution to the maximum flow problem \((P_1)\) with the set of link capacities \( Q_s \). Then, we state the following theorem.

**Theorem 4 (Max-flow expected-min-cut):** Consider an acyclic dynamic flow network with a set of observable disruptions (46a) and (46b). There exists a mode-dependent control \( \mu_{ej}^{md} \) given by (47) such that the network throughput equals the EMCC.

Note that EMCC is less than the MECC in general. Hence, the mode-dependent control above may appear conservative, provided a gap between the EMCC and the MECC. Besides, the mode-dependent control requires quick detection of disruptions and informs local controllers of disruption occurrences. If some of controllers are unaware of changes of disruption modes, Theorem 4 does not hold and the EMCC may not be guaranteed. In that case, we can apply Theorems 1 and 2 to the throughput analysis by modeling actuation faults.

By contrast, it is more practical to measure the network state \( X(t) \). Thus, we consider density-dependent control using the network state feedback. For a general network (with possibly incorrect sensing or with finite link storage spaces), one can apply the results of our resiliency analysis to design closed-loop controls. Suppose the control law is parameterized by \( \theta \). Then, the parameter \( \theta \) is designed by solving the following programming problem:

\[
(P_3) \quad \max_{\alpha \geq 0, \theta \in \Theta} \alpha \ \text{s.t.} \ (24).
\]

Let \( \theta^* \) and \( \alpha^* \) denote optimal solutions of the programming problem \( P_3 \). Then, it follows from Theorem 1 that the throughput under the control law parameterized by \( \theta^* \) is lower bounded by \( \alpha^* \).

**Corollary 1 (Throughput-guaranteed control):** Consider an acyclic dynamic flow network with a density-dependent control \( \mu_{ej}^{dd} \) deriving from \( P_3 \). Then, \( \mu_{ej}^{dd} \) can attain a throughput lower-bounded by the optimal \( \alpha^* \).

To facilitate the control design, we can restrict the control structure \( \theta \in \Theta \) so that \( \mathcal{E}_{inf} \) and \( \{B^+_e | e \in \mathcal{E}_{inf}\} \) are fixed. In practice, the determination of these sets may depend on infrastructure capability or control preferences, e.g., whether link \( e \) has sufficient storage space, or whether link \( e \) is allowed to be a bottleneck.

The rest of this section first illustrates the above results with a numerical example (see Section IV-B) and then proves them, respectively (see Section IV-C and IV-D).

### B. Numerical Example

Again, consider the network in Fig. 3. We use Theorems 3 and 4, and Corollary 1 to design open-loop control \( \mu_{ol} \), mode-dependent control \( \mu_{ej}^{md} \) and density-dependent control \( \mu_{ej}^{dd} \), respectively. Table III lists the resiliency scores in various scenarios. Note the nominal MCC equals one. Our discussions are as follows.

1) It is demonstrated that the open-loop control can attain the MECC when the links have infinite storage space. Besides, the results also show that the MECC is not guaranteed when the link storage space becomes finite.

2) It is verified that the mode-dependent control can attain the EMCC. Although this control seems conservative, it is still able to outperform the logit routing in case of links with infinite storage space; see Table II.

3) Compared with the open-loop control, density-dependent control can achieve higher resiliency scores when dealing with physical disruptions. However, it is vulnerable to cyber disruptions.

4) The results indicate that we can improve network resiliency by designing control laws with higher lower bounds of the resiliency scores.

Next, we present the design of three controls.

1) **Open-Loop Control:** Solving the maximum flow problem \((P_1)\) with the expected link capacities gives \( u_{ej}^{*e} = u_{ej}^{*e,c} = u_{ej}^{*e,c,e} = 0.5 \) and \( u_{ej}^{*e,r} = 0 \). According to (44) and (45), we have \( \mu_{eol} = \mu_{eol}^{md} = \mu_{eol}^{dd} = 0.5 \) and \( \mu_{eol}^{ol} = 0 \).

2) **Mode-Dependent Control:** The control \( \mu_{ej}^{md} \) is derived from solving the maximum flow problem \((P_1)\) for each disruption mode \( s \). Then, we have \( \mu_{ej}^{md} = \mu_{ej}^{md} = 0.5, \mu_{ej}^{md} = 0 \) and

\[
\mu_{eol}^{md}(s) = \mu_{eol}^{md}(s) = \begin{cases} 0.5, & \text{if } s \in \{s_0, s_2\} \\ 0, & \text{if } s \in \{s_1, s_3\}. \end{cases}
\]

3) **Density-Dependent Control:** We consider the density-dependent routing at node \( v_e \), namely, \( \mu_{eol}^{dd}(s, x) = w_e(u_1 - x_1) \) and \( \mu_{eol}^{dd}(s, x) = w_e(u_4 - T_{e,s}(x, s)) \), where the gains are set as the congestion wave speed \( w_e \), the parameters \( u_1 \) and \( u_4 \) are to be designed, and \( T_{e,s}(x, s) \) is the fault mapping given
in Table I. We interpret $u_1$ (respectively, $u_4$) as the maximum density allowed by the control for link $e_1$ (respectively, $e_4$). We also let $\rho_{\text{max}}^{\text{dd}}(s, x) = f_{e_1}(s, x_{e_1})$ and $\rho_{\text{max}}^{\text{dd}}(e_4, x) = 0$.

When all links $e_o, e_1, \ldots, e_5$ have infinite storage space, solving $P_3$ gives $u_1 = u_4 = \infty$. It means that the density-dependent control is reduced to an open-loop control that routes flows into links $e_1$ and $e_4$ with the same proportion. For links $e_1, e_2, e_5$ only with finite storage space, our method yields $u_1 = u_4 = 1.5$ for the network subject to either the cyber or physical disruption and $u_1 = 2.3, u_4 = 1.5$ in case of both the cyber and physical disruptions. More details can be found in the Supplementary Material.

C. Proof of Theorem 3

1) Sufficiency: The proof is similar to that of Theorem 1. Noting $\rho_e(s, x_e) = \infty$ for any $e \in E$, we obtain $B_+ = \emptyset$ for $e \in E_{\text{inf}}$. Consider the following Lyapunov function:

$$V^0(s, x) := \sum_{e \in E} a_e x_e \left(\frac{1}{2} x_e + \sum_{m \in A_e} \tilde{\gamma}_{me} x_m + b_{se}\right)$$

where $\tilde{\gamma}_{me}$ is recursively defined by

$$\tilde{\gamma}_{me} = \sum_{i \in A_e \cap \mathcal{C}_e} \tilde{\gamma}_{mi} \tilde{\gamma}_{ie}$$

with $\tilde{\gamma}_{ie}$ given by (44). Noting the physical meaning of $\tilde{\gamma}_{ie}$, we interpret $\tilde{\gamma}_{me}$ as the proportion of the outflow of link $m$ routed to link $e$ per the solution $u^*(Q)$. Specially, for link $e_o$ with a demand $\alpha = C(Q; G)$, we have

$$\tilde{\gamma}_{e_o} C(Q; G) = \sum_{i \in E^+_e} u^*_i (Q). \quad (49)$$

The above equation holds because, as specified by the solution $u^*(Q)$, the optimal demand $\alpha^*$ equals $C(Q; G)$ and the flow routed from link $e_o$ to link $e$ equals $\sum_{i \in E_e^+} u^*_i (Q)$.

The Lyapunov function indicates that we only need to show

$$\sum_{s \in S} p_s \max_{x \in \mathcal{X}_e} N_e(s, x) < 0 \quad \forall \alpha < C(Q; G) \quad \forall e \in E_{\text{inf}} \quad (50)$$

where $\mathcal{X}_e = \{x \mid x_e \geq x_e^c\}$ and $N_e(s, x) = \sum_{m \in A_e} \tilde{\gamma}_{me} G_m(s, x) + G_e(s, x)$.

The open-loop control yields $q^0_{mj}(s, x) = \tilde{\gamma}_{mj} f_m(s, x_m)$. Thus, for any link $m \in A_e^-$, we have

$$\sum_{j \in E^+_m} \tilde{\gamma}_{mj} q^0_{mj}(s, x) + \sum_{j' \in E^+_m \cap A_e} \tilde{\gamma}_{j'e} q^0_{j'e}(s, x) \leq 0$$

$$= \sum_{j \in E^+_m} \tilde{\gamma}_{mj} f_m(s, x_m) + \sum_{j' \in E^+_m \cap A_e} \tilde{\gamma}_{j'e} \tilde{\gamma}_{mj} f_m(s, x_m) \quad (44)$$

So we obtain

$$N_e(s, x) = \tilde{\gamma}_{e_o} C(Q; G) - f_{e_o}(s, x_{e_o}) \sum_{s \in S} p_s \max_{x \in \mathcal{X}_e} N_e(s, x) = \sum_{s \in S} p_s Q_{se} \quad \forall e \in E_{\text{inf}}. \quad (51)$$

Recalling (49), we arrive at

$$\tilde{\gamma}_{e_o} C(Q; G) = \sum_{i \in E^+_e} u^*_i (Q) \leq \sum_{s \in S} p_s Q_{se} \quad (52)$$

where the last inequality holds because of the constraint in the maximum flow problem. Combining (51) and (52), we complete the proof of (50).

2) Necessity: We prove the necessity by definition. Consider the cut-set $C$ with the MCC $C(Q; G)$, where $C$ is a set of links that divide the network into two disjoint parts containing the origin $v_o$ and the destination $v_d$, respectively. Let $E^-_C$ denote the set of links upstream of the cut-set. By the open-loop control, the outflow from $E^-_C \cup C$ does not exceed $C(Q; G)$. If the inflow $\alpha$ is not less than $C(Q; G)$ and $Z < \infty$ is given, there must exist some initial condition such that (16) fails to hold. It concludes the proof.

D. Proof of Theorem 4

1) Sufficiency: The proof is based on Theorem 1. Noting Lemma 3 proved in Appendix E, we only need to show

$$\sum_{s \in S} p_s \max_{x \in \mathcal{X}_e} \left(\alpha - \sum_{j \in E^+_e} q^\text{md}_{e,j}(s, x)\right) < 0 \quad \forall \alpha < \sum_{s \in S} p_s C(Q; G). \quad (53)$$

**Lemma 3:** The mode-dependent control $\mu^\text{md}$ admits an invariant set

$$\mathcal{X}^\text{md} = \left[\mathcal{X}_{v_o} \cap \infty\right] \times \prod_{e \notin e_o} \left[0, x^*_e\right]$$

which leads to $E_{\text{inf}} = \{e_o\}$ and $B^+_e = \emptyset$.

Then, it follows:

$$\sum_{s \in S} p_s \max_{x \in \mathcal{X}_{v_o}} \left(\alpha - \sum_{j \in E^+_e} q^\text{md}_{e,j}(s, x)\right)$$

$$= \sum_{s \in S} p_s \left(\alpha - \sum_{j \in E^+_e} \mu^\text{md}_{e,j}(s)\right)$$

where the equality is due to (1) $B^+_e = \emptyset$, (2) $f_{e_o}(s, x_{e_o}) \geq Q_{se_o}$ for $x_{e_o} \geq x^*_e$, and (3) the constraint (19a). By the constraint (19a), we obtain $\sum_{j \in E^+_e} \mu^\text{md}_{e,j}(s) = \alpha^*(Q_e; G) = C(Q_e; G)$, which completes the proof of (53).

2) Necessity: We consider the set $\{e_o\}$. Then, the remaining proof is similar to that for the necessity of Theorem 3.

V. CONCLUDING REMARKS

This article investigates resiliency and control design of dynamic flow networks suffering cyber-physical disruptions. First, we apply piecewise-deterministic Markov process to modeling disruptions and their impacts on networks. Then, a set of stability criteria are proposed with the physical insights into flow networks. We also simplify these criteria with the monotone network dynamics. The stability conditions enable the measurement of resiliency in terms of throughput. They also contribute to two specific resiliency-by-design controls. The first one attains the MECC if every link has infinite storage space; the second one attains the EMCC if the disruptions decrease maximum sending and/or receiving flows. In the general case, we propose a density-dependent control with a lower-bounded throughput. Our numerical examples show that the stability condition can
yield tight lower bounds of resiliency scores and enhance resiliency by designing control laws that raise the lower bounds.

This work can serve as a basis for multiple future studies. First, our sufficient stability conditions only yield lower bounds of throughput. It is tempting to derive upper bounds by investigating the necessary conditions. Besides, this article exploits the property of monotone flow networks to reduce the computation costs of verifying our stability conditions. However, monotone dynamics could be unavailable in multicommodity networks [38]. It is worthwhile considering networks with weaker properties, such as mixed monotonicity [19]. Finally, this article formulates the control design problem for the whole network. Solving it for large-scale networks could not be easy. Thus how to design control laws with guaranteed performances but only using a part of links/nodes is worth investigating.

APPENDIX A
OPEN-LOOP CONTROL IN THE NOMINAL CASE

We consider an open-loop control policy as follows:

\[ \bar{\mu}_{e,j}^{\text{ol}} = \bar{\gamma}_{e,j} Q_{e,o} \]  

(54)

where

\[ \bar{\gamma}_{e,j} := \frac{u_{e,j}^*(Q_{e,o})}{\sum_{j' \in \mathcal{E}_e} u_{j'j}^*(Q_{e,o})}, \quad (e, j) \in \mathcal{P}. \]  

(55)

Clearly, it has the same structure as the open-loop control \( \nu_{e,j}^{\text{ol}} \) given by (45).

Before we state the lemma, we define

\[ \bar{\gamma}_{e,c} = \sum_{i \in \mathcal{A}_0^\text{in} \cap \mathcal{E}_e} \gamma_{i \to e}. \]  

(56)

Noting (48) and (52), for any \( \alpha < C(Q_{e,o}; \mathcal{G}) \), we obtain in a similar way

\[ \bar{\gamma}_{e,c} \alpha < \bar{\gamma}_{e,c} C(Q_{e,o}; \mathcal{G}) = \sum_{i \in \mathcal{E}_e} u_{i \to e}^*(Q_{e,o}) \leq Q_{e,o}. \]  

(57)

**Lemma 4:** Consider an acyclic network satisfying Assumption 3 and only admitting the nominal mode \( s_0 \). Given any demand \( \alpha < C(Q_{e,o}; \mathcal{G}) \) and the open-loop control defined by (54), there exists a stable equilibrium such that \( f_e(s_0, \bar{x}_e) = \bar{\gamma}_{e,c}\alpha \) for any \( e \in \mathcal{E} \). Moreover, if there exists a neighborhood \( U(\bar{x}) \) of \( \bar{x} \) such that \( f_e(s_0, \bar{x}_e) \) is strictly increasing in \( \bar{x}_e \) for every \( e \in \mathcal{E} \), the equilibrium \( \bar{x} \) is also globally asymptotically stable.

 Obviously, the global asymptotic stability stated in Lemma 4 implies that the open-loop control (54) can enable the throughput to achieve the nominal MCC. Note that the required condition is really mild. As we will see in the proof, all of the link densities are fewer than their corresponding critical densities. It means that none of the links are congested. In that case, the sending flow \( f_e(s_0, \bar{x}_e) \) is typically sensitive to density changes, i.e., strictly increasing in \( \bar{x}_e \).

Below we give the proof of Lemma 4.

**Proof:** We first show the existence of \( \bar{x} \). For any demand \( \alpha < C(Q_{e,o}; \mathcal{G}) \), we conclude \( \bar{x} \in \prod_{e \in \mathcal{E}} [0, x^c_{\text{net}}] \) by using Assumptions 3.1 and 3.2 and \( f_e(s_0, \bar{x}_e) = \bar{\gamma}_{e,c}\alpha < Q_{e,o} \), where \( x^c_{\text{net}} \) is given by (8b).

Next, we prove that \( \bar{x} \) is a stable equilibrium. Again noting (54) and (57), we conclude that there exists a neighbourhood \( W(\bar{x}) \) of \( \bar{x} \) such that \( q_{e,j}(s_0, x) = \bar{\gamma}_{e,j} f_e(s_0, x_e) \). Then, \( \bar{x} \) is an equilibrium by (56). The stability of \( \bar{x} \) is directly implied by [19, Th. (iii)].

Note that \( \bar{x} \) is globally asymptotically stable if and only if it is locally asymptotically stable; see [19, Th. 6 (iv)]. Below we show that the network is locally asymptotically stable over the neighborhood \( W(\bar{x}) \cap U(\bar{x}) \). We first notice link \( x_e \) converges to \( \bar{x}_e \) by using the monotonicity and Lipschitz continuity of \( f_e(s_0, x_e) \). Then we consider links from the upstream to the downstream. We can show \( x_e \) converges by using the convergence of its upstream links.

**APPENDIX B
EXTENSION FOR CYCLIC NETWORKS**

We present stability analysis for cyclic networks. One major difference between cyclic and acyclic networks is \( \mathcal{A}_e^\text{in} \cap \mathcal{A}_e^\text{out} \neq \emptyset \) for some \( e \in \mathcal{E} \) in a cyclic network. It induces that Lemma 2 may not hold because of \( \mathcal{A}_e^\text{in} \cap \mathcal{A}_e^\text{out} \neq \emptyset \). We address this problem by considering a partition of \( \mathcal{E}_\text{inf} \).

We denote by \( \{ \mathcal{L}_z \}_{z=1}^Z \) a partition of \( \mathcal{E}_\text{inf} \) such that any \( z_1, z_2 \in \{1, 2, \ldots, Z\} \) with \( z_1 \neq z_2 \)

\[ a \leftrightarrow j \quad \forall e, j \in \mathcal{L}_{z_1}, e \neq j \]  

(58a)

\[ e \not\leftrightarrow j \quad \forall e \in \mathcal{L}_{z_1}, j \in \mathcal{L}_{z_2} \]  

(58b)

where \( a \leftrightarrow j \) represents that the two links are reachable from each other, and \( e \not\leftrightarrow j \) denotes that at least one link is unreachable from the other. For a cyclic network, a partition can be obtained by merging the sets above whose elements are accessible from each other, and we can prove by contradiction the uniqueness of the partition.

Then, we show by the partition \( \{ \mathcal{L}_z \}_{z=1}^Z \) that Theorem 1 holds for acyclic networks. It implies that the other stability results in Section III also apply to acyclic networks.

**Proposition 3:** Consider a cyclic network satisfying Assumptions 3.1–3.3. Suppose that the network admits a demand \( \alpha \) and an invariant set \( \mathcal{X}^c \subseteq \prod_{e \in \mathcal{E}} [0, x^c_e] \) under a control law \( \mu : \mathcal{S} \times \mathcal{X} \rightarrow \mathcal{P}_0^\text{c} \). The network is stable if (24) holds.

**Proof:** Consider the following Lyapunov function:

\[ \hat{V}(s, x) := \sum_{e \in \mathcal{E}_{\text{out}}} a_e x_e \left[ \frac{1}{2} \sum_{i \in \mathcal{E}_e} x_i + \sum_{m \in \mathcal{A}_e \cap \mathcal{L}_e} x_m \right. 

\left. + \sum_{e \in \mathcal{G}_e} \int_{\mathcal{L}_e} \rho_e(\zeta) d\zeta + b_{\text{ex}} \right] \]  

(59)

where \( \epsilon_e \) denotes the set index such that \( e \in \mathcal{L}_e \). The rest of the proof is similar to that of Theorem 1, except Lemma 2. We instead use the following lemma.

**Lemma 5:** The system of equations

\[ \pi_e a_{i,e} + \mathcal{G} \sum_{n \in \mathcal{A}_e^\text{in} \cap \mathcal{L}_e} a_{i,n} < 0 \quad \forall e \in \mathcal{E}_\text{inf} \]  

(60)

has a positive solution for \( \{ a_{i,e} | e \in \mathcal{E}_\text{inf} \} \) if \( \pi_e < 0 \) for any \( e \in \mathcal{E}_\text{inf} \).
Note that (58a) and (58b) reveals an acyclic structure of the partition. Thus, we can prove Lemma 5 in a similar way to Lemma 2.

APPENDIX C

PROOF OF LEMMA 1

To show the existence of a solution, note that (37) is equivalent to \( \Delta y = p^T z - z \) where \( z = [z_{s_0}, \ldots, z_{s_M}]^T \). Since the discrete state process is ergodic, the rank of the matrix \( \Lambda = M \). Scaling row \( i + 1 \) with \( p_{s_i} \) for \( i = 0, 1, \ldots, M \) and adding the scaled rows \( 1, 2, \ldots, M \) to row \( M + 1 \), we obtain

\[
\begin{bmatrix}
-p_{s_0} \sum_{i \neq 0} \lambda_{s_0 s_i} & \cdots & p_{s_0} \lambda_{s_0 s_M} \\
\vdots & \ddots & \vdots \\
p_{s_M} \lambda_{s_M s_0} - p_{s_M} \sum_{i \neq M} \lambda_{s_M s_i} & \cdots & -p_{s_M} \sum_{i \neq M} \lambda_{s_M s_i} \\
\end{bmatrix} y = \tilde{z}
\]

(61)

APPENDIX E

PROOF OF LEMMA 3

First, we note that the disruptions (46a) and (46b) imply

\[
\begin{aligned}
Q_{sc} &\leq r_e(s, x_e) \quad \forall s \in S \quad \forall x_e \preceq x_e^s \quad (62a) \\
Q_{sc} &\leq f_e(s, x_e) \quad \forall s \in S \quad \forall x_e \preceq x_e^s \quad (62b)
\end{aligned}
\]

where \( x_e^s \) is given by (9). Besides, for any \( x \in X \) with \( x_j \leq x_j^e \), we obtain

\[
r_{e;j}^* (s, x_j) = \sum_{i \in \mathcal{E}^j} \mu_{e;i}^*(s) r_{e;i} (s, x_j) \geq \mu_{e;j}^*(s) \quad (63)
\]

To show that \( \lambda^m \) is an positively invariant set, we prove that on the boundary of \( \lambda^m \), the vector field \( G(s, x) \) points toward the interior regardless of \( s \in S \). That is, for any \( e \neq e_0 \in E \) and \( (s, x) \in S \times \lambda^m \) with \( x_e = x_e^* \), we have

\[
G_e (s, x) \leq \sum_{i \in \mathcal{E}^e} \mu_{e;i}^m(s) - \min_{j \in \mathcal{E}^e^*} \{ \mu_{e;j}^m(s), Q_{sc} \} \leq 0
\]

(19b),(19d)

To show that \( \lambda^m \) is global attracting, we perform an induction on links. We first consider link \( e \) reaching the destination, i.e., \( \tau_e = d_e \), since it does not have downstream bottlenecks. We see \( G_e (s, x) \leq 0 \) for any \( (s, x) \in \{ (s, x) \in S \times X | x_e > x_e^* \} \). In addition, given \( a < \sum_{e \in S} p_{s_e} c | Q_e; G \), there exists some mode \( s \in S \) under which \( x_e \) converges to a value strictly less than \( x_e^* \). Since the process \( \{ S(t); t \geq 0 \} \) is ergodic, it is concluded that \( x_e \) enters \([0, x_e^*] \) almost surely. Then, as indicated by (63), link \( e \) is not a bottleneck for its upstream links under the mode-dependent control. The similar proof can be iteratively applied to links upstream of link \( e \) until all links are considered.

The invariant set \( \lambda^m \) immediately gives \( \mathcal{E}^m = \{ e_0 \} \); by noting (63), we also obtain \( B_{e_0}^+ = \emptyset \).

REFERENCES

[1] M. Schmitt and J. Lygeros, “An exact convex relaxation of the freeway network control problem with controlled merging junctions,” Transp. Res. Part B, Methodological, vol. 114, pp. 1–25, 2018.
[2] M. Mandjes, D. Mitra, and W. Scheinhardt, “Models of network access control problem with controlled merging junctions,” IEEE Trans. Autom. Control, vol. 63, no. 11, pp. 3948–3955, Nov. 2018.
[3] H. Sandberg, S. Amin, and K. H. Johansson, “Cyberphysical security in networked control systems: An introduction to the issue,” IEEE Control Syst. Mag., vol. 35, no. 1, pp. 20–23, Feb. 2015.
[4] A. Polus and M. A. Pollatschek, “Stochastic nature of freeway capacity and its estimation,” Can. J. Civil Eng., vol. 29, no. 6, pp. 842–852, 2002.
Yu Tang (Graduate Student Member, IEEE) received the B.Eng. and M.S. degrees in transportation engineering from Tongji University, Shanghai, China, in 2016 and 2019, respectively. He is currently working toward the Ph.D. degree in transportation systems with the Tandon School of Engineering, New York University, New York, NY, USA.

His research interests include using ideas from stochastic processes and dynamic control to design resilient intelligent transportation systems.

Li Jin (Member, IEEE) received the B.Eng. degree from Shanghai Jiao Tong University, Shanghai, China, in 2011, the M.S. degree from Purdue University, West Lafayette, IN, USA, in 2012, both in mechanical engineering, and the Ph.D. degree in transportation from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 2018.

From 2018 to 2020, he was an Assistant Professor with the Tandon School of Engineering, New York University, New York, NY, USA. Since 2021, he was John Wu and Jane Sun Associate Professor and is John Wu and Jane Sun Associate Professor of Electrical and Computer Engineering with the UM Joint Institute and the Department of Automation, Shanghai Jiao Tong University. His research interests include from stochastic processes, control, optimization, and machine learning to address key challenges in smart and connected system, which also include connected and autonomous vehicles, and intelligent transportation systems.

[6] H. Dong, Z. Wang, and H. Gao, “Fault detection for Markovian jump systems with sensor saturations and randomly varying nonlinearities,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 10, pp. 2354–2362, Oct. 2012.
[7] A. Cardenas et al., “Challenges for securing cyber physical systems,” in Proc. Workshop Future Directions Cyber-Phys. Syst. Secur., 2009.
[8] G. B. Dantzig and D. R. Fullerksen, “On the max flow min cut theorem of networks,” RAND CORP SANTA MONICA CA. Tech. Rep. P-826, 1955.
[9] G. Como, E. Lovisari, and K. Savla, “Throughput optimality and overload behavior of dynamical flow networks under monotone distributed routing,” IEEE Trans. Control Netw. Syst., vol. 2, no. 1, pp. 57–67, Mar. 2015.
[10] S. Coogan and M. Arcak, “A compartmental model for traffic networks and its dynamical behavior,” IEEE Trans. Autom. Control, vol. 60, no. 10, pp. 2698–2703, Oct. 2015.
[11] G. Nilsson and S. Coogan, “Strong integral input-to-state stability in dynamical flow networks,” in Proc. IEEE Amer. Control Conf., 2021, pp. 4836–4841.
[12] L. Massai, G. Como, and F. Fagnani, “Stability and phase transitions of dynamical flow networks with finite capacities,” IFAC-PapersOnLine, vol. 53, no. 2, pp. 2588–2593, 2020.
[13] S. Coogan and M. Arcak, “Stability of traffic flow networks with a polytree topology,” Automatica, vol. 66, pp. 246–253, 2016.
[14] S. Jafari and K. Savla, “On structural properties of optimal feedback control of traffic flow under the cell transmission model,” in Proc. IEEE Amer. Control Conf., 2019, pp. 3309–3314.
[15] A. Johansson, J. Wei, H. Sandberg, K. H. Johansson, and J. Chen, “Optimization of the H∞-norm of dynamic flow networks,” in Proc. IEEE Amer. Control Conf., 2018, pp. 1280–1285.
[16] X. Fan, M. Arcak, and J. T. Wen, “Robustness of network flow control against disturbances and time-delay,” Syst. Control Lett., vol. 53, no. 1, pp. 13–29, 2004.
[17] T. Alpcan, J. P. Singh, and T. Basar, “Robust rate control for heterogeneous network access in multihomed environments,” IEEE Trans. Mobile Comput., vol. 8, no. 1, pp. 41–51, Jan. 2009.
[18] G. Como, K. Savla, D. Acemoglu, M. A. Dahleh, and E. Frazzoli, “Robust distributed routing in dynamical networks part I: Locally reactive policies and weak resilience,” IEEE Trans. Autom. Control, vol. 58, no. 2, pp. 317–332, Feb. 2013.
[19] G. Como, “On resilient control of dynamical flow networks,” Annu. Rev. Control, vol. 43, pp. 80–90, 2017.
[20] K. Savla, J. S. Shamma, and M. A. Dahleh, “Network effects on the robustness of dynamic systems,” Annu. Rev. Control Robot. Autom. Syst., vol. 3, pp. 115–149, 2020.
[21] A. R. Teel, A. Subbaraman, and A. Sferlazzi, “Stability analysis for stochastic hybrid systems: A survey,” Automatica, vol. 50, no. 10, pp. 2435–2456, 2014.
[22] P. Shi and F. Li, “A survey on markovian jump systems: Modeling and design,” Int. J. Control. Autom. Syst., vol. 13, no. 1, pp. 1–16, 2015.
[23] M. H. A. Davis, “Piecewise-deterministic Markov processes: A general class of non-diffusion stochastic models,” J. Roy. Stat. Soc. Ser. B. Methodological, vol. 46, no. 3, pp. 353–388, 1984.
[24] M. Benaim, S. Le Borgne, F. Malrieu, and P.-A. Zitt, “Qualitative properties of certain piecewise deterministic Markov processes,” Annales de l’Institut Henri Poincaré, Probabilités et Statistiques, vol. 51, pp. 1040–1075, 2015.
[25] A. R. Mesquita and J. P. Hespanha, “Construction of Lyapunov functions for piecewise-deterministic Markov processes,” in Proc. IEEE 49th Conf. Decis. Control, 2010, pp. 2408–2413.
[26] C. E. de Souza and D. F. Coutinho, “Robust stability of a class of uncertain Markov jump nonlinear systems,” IEEE Trans. Autom. Control, vol. 51, no. 11, pp. 1825–1831, Nov. 2006.
[27] D. Chatterjee and D. Liberzon, “On stability of randomly switched nonlinear systems,” IEEE Trans. Autom. Control, vol. 52, no. 12, pp. 2390–2394, Dec. 2007.
[28] J. G. Dai and S. P. Meyn, “Stability and convergence of moments for multiclass queueing networks via fluid limit models,” IEEE Trans. Autom. Control, vol. 40, no. 11, pp. 1889–1904, Nov. 1995.
[29] H. Chen and D. D. Yao, “A fluid model for systems with random disruptions,” Operations Res., vol. 40, no. 3-supplement-2, pp. S239–S247, 1992.
[30] H. Yu and C. G. Cassandras, “Perturbation analysis of feedback-controlled stochastic flow systems,” IEEE Trans. Autom. Control, vol. 49, no. 8, pp. 1317–1332, Aug. 2004.
[31] Y. Wardi, R. Adams, and B. Melamed, “A unified approach to infinitesimal perturbation analysis in stochastic flow models: The single-stage case,” IEEE Trans. Autom. Control, vol. 55, no. 1, pp. 89–103, Jan. 2010.
[32] Q. Xie and L. Jin, “Resilience of dynamic routing in the face of recurrent and random sensing faults,” in Proc. IEEE Amer. Control Conf., 2020, pp. 1173–1178.