2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Toward a Stability Monitoring System of an Asset-Communications Network Exposed to Malicious Attacks

N. Léchevin, C.A. Rabbath, and P. Maupin

Abstract — **This paper proposes stability conditions for a network of assets. The assets are connected to a communications network, thus constituting a two-layered (or two-tier) network. The effectiveness of the network, and even its stability, can be indirectly affected by malicious attacks targeting the communications. The particular case of virus propagation on the assets is considered. The network of assets is modeled as a discrete-time, jump, linear system whose transitions are governed by nonlinear discrete-time dynamics representing a class of virus diffusion. The state-space variables of the latter represent the probabilities of each node receiving the virus and being infected. The stability analysis is obtained by means of a stochastic Lyapunov function argument and yields a sufficient condition expressed as a linear matrix inequality (LMI). This LMI involves the asset state-space matrices and the positive limit set of the probabilistic model of the virus propagation dynamics, which exhibits the attraction property provided a sufficient condition is satisfied. The proposed condition involves the adjacency matrix of the communications network and the parameters characterizing virus propagation. An approximation to the sufficient condition is proposed so that convergence of the system trajectories could be monitored online. The analysis is extended to a class of jump systems, which are affinely excited by some disturbance, yielding an almost-sure boundedness of the trajectories.**

I. Introduction

Despite local and global failure detection and recovery mechanisms, networks are prone to large, although infrequent, outages. The robust-yet-fragile paradigm [1] about network, which is thoroughly documented by the multidimensional description of networked infrastructures proposed in [15], can be illustrated by the following two facts that may help grasp the vulnerabilities: (*i*) the likelihood of uncontrolled and unexpected propagation of an isolated problem tends to increase as the network operates close to its safety margin; (*ii*) coordinated attacks, whether physical or cybernetical, may successfully leverage vulnerabilities of a network, particularly under stressed operating conditions.

Malicious cyberattacks on the supervisory control and data acquisition systems managing critical public infrastructures can indeed bring about disruption of service. Instances of reported cyberattacks towards power electric utilities include, (*i*) the SQL Slammer worm that infected and disabled internal systems at a nuclear plant in Ohio in 2003 [16], (*ii*) hackers who attacked the California Independent System Operator which manages the electricity supply of California [16], and (*iii*) the Aurora vulnerability, illustrated by a Homeland Security video showing a small electric generator being disabled remotely from the internet [11]. Further examples of cyberattacks targeting water supply and waste water system can also be found in [11], where it is reported that a disgruntled employee hacked a sewage treatment system from a laptop, causing significant environmental damages. In a military context, network-centric assets, whether it be weapons or unmanned vehicles, are prone to attacks at the physical layer, data-link layer, and network layer through enemy actions including jamming, deception, destruction, and information overloading [14]. Other critical applications that necessitate accounting for potential mishaps of the communications networks include vehicle networked control pertaining to the automated highway [18] and cooperative mobile sensor coverage [19].

We propose, in this paper, to derive stability and boundedness conditions that are expected to be implemented online for the health monitoring of a network of assets (NA). By asset we mean a stable dynamic system (infrastructure, vehicles, weapons, etc). A healthy asset indicates operation under nominal conditions. The network of assets is subject to disturbances resulting from the prevalence and propagation of viruses through a communications network (CN), which is connected to the assets. The problem considered in this paper is related to the stability analysis of networked control systems whose operating conditions are subject to imperfect communications. Such imperfections may be caused by packet dropouts. However, our model does not explicitly take packet dropouts into account. The closed-loop systems that are typically dealt with, when analyzing the effect of packet dropouts, include asynchronous dynamic systems, switching systems, and jump linear systems with Markov chain. Typically, the dropouts occur in the sensor-to-controller or the controller-to-actuator path. See [8], [20], and references therein for further details. The state of the communications network, which is potentially affected by the propagation of viruses, could be modeled with a Markov chain. This approach, when applied to the two-layered network at hand (NA and CN) is characterized by a jump system whose switching mechanism would be a function of the state of the Markov chain. In that case, convergence in the mean square sense of the jump system can be verified by direct application of the sufficient condition derived in [2]. However, such an approach is likely to be intractable since a communications network with m nodes leads to a Markov chain with 2^m states, with each node being either infective or susceptible. The nonlinear, discrete-time, state-space model proposed in [1] is thus preferred. Each component of the state-space vector represents either the probability that a node of the communication network is infected or the probability that a node will not receive the infection between

N. Léchevin, C.A. Rabbath, and P. Maupin are with Defence R&D Canada Valcartier, 2459 Pie XI North, Québec, Qc, G3J 1X5, Canada. {nicolas.lechevin, camille-alain.rabbath, patrick.maupin}@drdc-rddc.gc.ca

978-1-4577-0079-8/11/$26.00 ©2011 AACC

two successive time instants. The network of assets considered here includes, but is not restricted to, a class of networked control systems. The possible application pertains to the infrastructures that are physically connected and that require remote information obtained from communications network in order to perform inter-area oscillation stabilization. For example, large-scale power grids are likely to behave abnormally or even to be part of cascading failures, should the operation condition deviate from its nominal value and approach safety limits. Similarly, the networked control system could pertain to the control of a network of mobile assets (e.g., drone aircraft) with its stability under cyberattacks.

The article is structured as follows. The model of the two-layered network and the analysis objectives are presented in Section II. The stability conditions used by such system are derived in Section III. Boundedness of the trajectories is analyzed in Section IV, in case the jump system is excited by some exogenous disturbance.

II. Two-Layered Network Model and Problem Formulation

We consider a two-layered (or two-tier) networks (Fig. 1(a)) composed of (*i*) assets such as infrastructures and unmanned vehicles equipped with protection, local self-healing, and control systems and of (*ii*) a communications network (CN). The types of interconnections linking the assets include physical interconnections and information exchanges by means of remote sensors such as cameras, sonar, and lasers. Other types of information are communicated through CN. Regarding possible impact of faults and failures, unidirectional dependency between the networks is considered; i.e., malfunctioning of the communications network may adversely affect the network of assets (NA), whereas the reverse situation is not considered. The unidirectional constraint characterizing the fault tree does not prevent the communications network to interact bidirectionally. This issue is left for future investigations. No particular assumptions are made about the topology of NA. CN is assumed connected and undirected. Its topology is reflected in the contraction analysis of its dynamics through the use of its adjacency matrix.

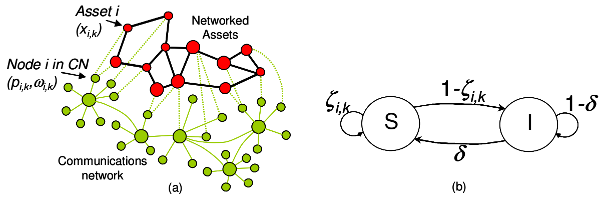

Fig. 1. Two-layered networks. (a) The network of assets (red) is connected to the information network (green). (b) Transition diagram of a node of CN [3]. A susceptible (S) node is healthy at t_k but can receive the virus from a neighbor with probability 1-$\zeta_{i,k}$. An infected (I) node can be cured over $[t_k, t_{k+1})$ with probability δ.

Definition 1 (CN model): Let $p_{i,k}$, $\zeta_{i,k}$, β, and δ denote the probability that node i is infected at time instant $t_k \in \mathbb{R}$, $k \in \mathbb{N}$, the probability that node i will not receive infections from its neighbors over $[t_k, t_{k+1})$, the probability that a node tries to infect its neighbors, and the probability that i gets rid of the virus over $[t_{k-1}, t_k)$, respectively. The virus propagation is represented by a stochastic susceptible-infected-susceptible model that integrates the topology of CN. Its transition diagram for a single node of CN is shown in Fig. 1(b).

The probability $\zeta_{i,k}$ depends on the virus birth rate β, CN topology, and on the fact that every neighbor is either uninfected or infected but fails with probability 1-β to spread the virus, leading to [3]

$$\varsigma_{i,k} = \prod\nolimits_{j \in N_i^c} (p_{j,k-1}(1-\beta) + (1-p_{j,k-1})).$$

The probability 1-$p_{i,k}$ that node i is healthy at t_k depends on the following two facts: (*i*) node i was not infected by its neighbor at t_k and was healthy at t_{k-1}, or (*ii*) was infected at t_{k-1} and has been cured over $[t_{k-1}, t_k)$, yielding

$$1 - p_{i,k} = \varsigma_{i,k}(1-p_{i,k-1}) + \delta\varsigma_{i,k} p_{i,k-1}.$$

The virus propagation through the communications networks is thus given, for i=1,…,m, by the following discrete-time model,

$$\varsigma_{i,k} = \prod\nolimits_{j \in N_i^c} (1-\beta p_{j,k-1}),$$

$$p_{i,k} = 1 - \varsigma_{i,k}(1-p_{i,k-1}) - \delta\varsigma_{i,k} p_{i,k-1}, \tag{1}$$

where m and N_i^c stand for the number of nodes of CN, and the neighboring set of node i, respectively. ⋈

From the knowledge of $p_{i,k}$, the infected population size at time instant t_k is given by $\Sigma_{i=1}^{m} p_{i,k}$. Let $p_k = [p_{1,k},\ldots, p_{n,k}, p_{n+1,k},\ldots, p_{m,k}]^T$, where the first n entries correspond to the nodes of CN that are connected to that of NA.

Definition 2 (NA model): NA is comprised of n nodes, where $n \leq m$, each of which is an asset equipped with its control system and modeled by the following discrete-time, jump, linear system

$$x_{i,k+1} = \mathbf{A}_{i,k}(\omega_{i,k}) x_{i,k} + \sum\nolimits_{j \in N_i^a} \mathbf{B}_{ij,k}(\omega_{i,k}) x_{j,k}, \tag{2}$$

where N_i^a, $x_{i,k} \in \mathbb{R}^{n_i}$, and $\omega_{i,k}$ are the set of neighbors of node i, the state-space vector of asset i at t_k, and the random variable that expresses the asset i's health status at t_k, respectively.

The health state of a node depends on its possible infection by the virus, which may affect the asset through its control system as further explained in *Remarks 2* and *3*.

The random matrix $\mathcal{A}_{i,k}(\omega_{i,k})$ is defined as follows. $\mathcal{A}_{i,k}(\omega_{i,k}=0)=\bar{A}_i$ when the corresponding node i in CN is infected, which occurs with probability $p_{i,k}$ (=P($\omega_{i,k}$=0)), and $\mathcal{A}_{i,k}(\omega_{i,k}=1)=A_i$ with probability $1-p_{i,k}$ (=P($\omega_{i,k}$=1)), when node i is healthy. Similarly, $\mathcal{B}_{ij,k}(\omega_{i,k}=0)=\overline{B}_{ij}$ with probability $p_{i,k}$ and $\mathcal{B}_{ij,k}(\omega_{i,k}=0)=B_{ij}$ with probability $1-p_{i,k}$. ⋈

Remark 1: The interconnection matrix $\mathcal{B}_{ij,k}(\omega_{i,k})$ in (2) represents the dependency of i on j. Bidirectional dependency (not at the fault-tree level) between i and j is thus characterized by the matrix pair ($\mathcal{B}_{ij,k}(\omega_{i,k})$, $\mathcal{B}_{ji,k}(\omega_{j,k})) \in \{B_{ij}, \overline{B}_{ij}\} \times \{B_{ji}, \overline{B}_{ji}\}$, which is determined as a function of the state (infective or susceptible) of corresponding nodes, i on j, in CN.

Remark 2: As already mentioned, stressed operating conditions tend to make the time trajectories of NA approach its safety limits, defined for instance by the boundary of the attraction basin of NA. Being characterized with reduced stability margin, the assets are sensitive to malfunctioning of CN, causing NA's node i to transit from the nominal stable system (A_i, B_{ij}), $j \in N_i^a$, to the potentially unstable system $(\overline{A}_i, \overline{B}_{ij})$, $j \in N_i^a$. Improvement in such tradeoff as performance versus robustness of large interconnected power systems, which are operated in deregulated contexts, can be obtained with advanced Supervisory Control and Data Acquisition Systems (SCADA) and possibly coupled with satellite technologies [5] by leveraging wide-area measurements, rapid communications, advanced stabilizer and optimal power flow systems, and monitoring and energy management systems. However, the overall system is vulnerable to cyberattacks targeting key components of the feedback system shown in Fig. 2. In particular, the SCADA system is connected to local area networks in command-and-control (CC) centers, which can be accessed by malicious intruders, taking actions that have detrimental effects on the power systems. Such actions include injecting undesirable control signals by corrupting or disabling stabilizers of the Automatic Generation Control (AGC) and deceptive effects entailed by false data injection that are undetectable by the monitoring system, thus preventing operators from making appropriate decisions in a timely manner [6].

Matrix $\mathcal{A}_{i,k}(\omega_{i,k})$ in (2) thus arises when asset i of the network switches from a feedback-stabilized dynamics, with state-space matrix $A_i = A_i^* + B_{ij} K_i^* C_i$, to a possible unstable dynamics with matrix $\bar{A}_i = A_i^* + \overline{B}_{ij} \overline{K}_i \overline{C}_i$ and vice versa. Matrices $\overline{B}_{ij}$ and $\overline{C}_i$ may result from the corruption of elements of the data acquisition system and RTUs, whereas $\overline{K}_i$ represents the impacts of cyberattacks on the AGC. It should be noted, however, that this interpretation stands for the linearization of node i's dynamics, $dx_i/dt = f_i(x_i, x_{ij}, u_i)$, $j \in N_i^a$, and that, contrary to the implementation of the AGC, the control signal u_i corrupted by cyberattacker's actions may no longer be expressed as a function of the state x_i.

From (2), the overall dynamics of the network of assets is given by the jump linear system

$$x_{k+1} = \boldsymbol{\mathcal{A}}_k(\omega_k) x_k, \tag{3}$$

where $x_{k+1} = [x_{1,k}^T, \ldots, x_{n,k}^T]^T$ and $\omega_k = [\omega_{1,k}, \ldots, \omega_{n,k}]^T \in \{0,1\}^n$. $x_{i,k}$, and $\omega_{i,k}$ are given in (2). Matrix $\mathcal{A}_k(\omega_k)$ is straightforwardly obtained from $\mathcal{A}_{i,k}(\omega_{i,k})$ and $\mathcal{B}_{ij,k}(\omega_{i,k})$ in (2) for all $i \in \{1, \ldots, n\}$ and $j \in N_i^a$, and is characterized by a graph-Laplacian-like structure [4].

Problem Objective: In case where NA is operating under stressed condition (e.g. shrunk basin of attraction, reduced capacity limits), the disturbed system $(\overline{A}_i, \overline{B}_{ij})$, $1 \le i \le n$, $j \in N_i^a$, which occurs with probability $p_{i,k}$, is potentially unstable. We aim to derive conditions under which the trajectories of system (1), (3) converge to zero with probability 1. Approximations should be derived to conduct online monitoring of the convergence condition of NA. ⋈

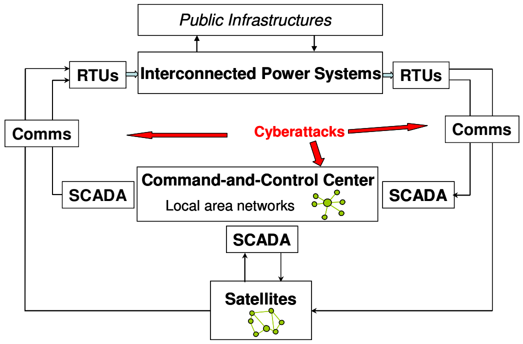

Fig. 2. Power systems in closed loop with information acquisition and CC systems. Remote terminal units (RTUs) transmit (*i*) telemetry data to the SCADA systems or (*ii*) commands to control effectors such as protective relays or automatic generation control by means of various communications links (radio, optic fiber, microwave, etc).

III. Stability Conditions

A. *Preliminaries*

In section III.C, a stability condition is provided in the form of a LMI expressed as a function of the positive limit set of the virus propagation model in (1).

To see this, select the following positive definite function

$$V(x_k) = x_x^T x_k \,. \tag{4}$$

V is instrumental in the definition of the stochastic Lyapunov function candidate used for the stability analysis. Then

$$\begin{aligned} E[V(x_{k+1}) \mid \mathbf{F}_n] &= E[x_x^T \mathbf{A}_k^T(\omega_k) \mathbf{A}_k(\omega_k) x_k] \\ &= x_x^T \overline{p}_k A^T A x_k + \textstyle\sum_{\omega_k \in I_k \setminus\ _n} \displaystyle\prod_{i=1}^{n} \rho_{i,k} x_x^T \mathbf{A}_k^T(\omega_k) \mathbf{A}_k(\omega_k) x_k, \end{aligned} \tag{5}$$

where $\mathcal{F}$ stands for a sequence of nonincreasing σ-algebras measuring $\{x_i, \; i \le n\}$, $A = \mathcal{A}_k(\omega_k = \mathbf{1}_n)$, $\rho_{i,k} \in \{p_{i,k}, 1 - p_{i,k}\}$, $I_{i,k} = \{0,1\}$, $I_i = I_{1,k} \times \ldots \times I_{n,k}$, $\mathbf{1}_n$ is the 1×n unitary vector, and $\overline{p}_k = \Pi_{i=1}^n (1 - p_{i,k})$. Letting $\rho_{i,k} = \rho_{i,k}^* + \tilde{\rho}_{i,k}$, where $\rho_{i,k}^*$ and $\tilde{\rho}_{i,k}$ correspond to some trajectory (equilibrium, periodic orbit) in the limit set of (1) and to the deviation signal of the actual trajectory of (1) with respect to $\rho_{i,k}{}^*$, respectively, and $\overline{p}_k = \overline{p}_k^* + \tilde{\overline{p}}_k$, where the definition of $\overline{p}_k^*$ and $\tilde{\overline{p}}_k$ is similar to that of $\rho_{i,k}^*$ and $\tilde{\rho}_{i,k}$, (5) can be expressed as

$$\begin{aligned} E[V(x_{k+1}) \mid \mathbf{F}_n] &= x_x^T (\overline{p}_k^* A^T A \\ &+ \textstyle\sum_{\omega_k \in I_k \setminus\ _n} \displaystyle\prod_{i=1}^{n} \rho^*_{i,k} \mathbf{A}_k^T(\omega_k) \mathbf{A}_k(\omega_k)) x_k + \tilde{V}_k. \end{aligned} \tag{6}$$

In (6), $\tilde{V}_k$ is defined as follows

$$\begin{aligned} \tilde{V}_k &= x_x^T (\textstyle\sum_{\omega_k \in I_k} M_k(\rho^*_{i,k}, \tilde{\rho}_{j,k}, i \in I, j \in J) \\ &\times \mathbf{A}_k^T(\omega_k) \mathbf{A}_k(\omega_k)) x_k, \end{aligned} \tag{7}$$

where $\mathrm{I} \subset \{1, \ldots, n\}$ and $\mathrm{J} \subset \{1, \ldots, n\} \setminus \mathrm{I}$.

M_k in (7) is the sum of all products expressed as $\prod_{i \in I} \rho_{i,k}^* \prod_{j \in J} \tilde{\rho}_{j,k}$, therefore $\lim_{\tilde{\rho}_k \to 0} M_k = 0$, implying that

$$\lim_{\tilde{\rho}_k \to 0} \tilde{V}_k = 0 \,. \tag{8}$$

As depicted in Fig. 3, the stability analysis will thus consist in deriving a stochastic Lyapunov function candidate V_k, to be determined in Section III.*C*. V_k is based on V and on a perturbation term, δV_k, that compensates for $\tilde{V}_k$ in (7) and that approaches zero as k goes to infinity by exploiting the fact that the trajectory of system (1) approaches the limit set of (1), if any.

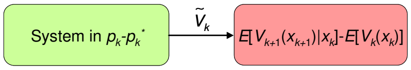

Fig. 3. Cascade structure of the system arising in the stability analysis. V_k is the Lyapunov function candidate expressed as a function of V in (4) and δV_k. δV_k aims to compensate for $\tilde{V}_k$, whereby (1) and (3) are linked.

B. Contraction of virus propagation dynamics

Computing the limit set of (1) for general values of β and δ is intricate. It is shown in [3] that the epidemic threshold τ is equal to $1/\lambda_{1,A}$, where $\lambda_{1,A}$ stands for the largest eigenvalue of the adjacency matrix A of the communications network. Therefore, the virus outbreak dies out, i.e., $\forall\, i,k$, $p_{i,k}\equiv 0$, when $\beta/\delta<\tau$, and survives otherwise. However, when $\beta/\delta>\tau$, the trajectories of (1) exponentially converge to some trajectory of its limit set, defined by a positive probability of infection, $p_{i,k}$. This means that the virus remains prevalent throughout the network, causing system (2) to switch from $(\bar{A}_i, \bar{B}_{ij})$ to (A_i,B_{ij}), $1\le i\le n$, $j\in N_i^a$, and vice versa.

The sufficient condition of convergence to the limit set is derived by applying results from contraction theory [9], whose discrete-time version provides a sufficient condition

$$(v_k^T)'_{p_k}(v_k)'_{p_k} - I \le -\beta I,\ \beta>0, \tag{9}$$

for $p_{k+1}=v_k(p_k)$ to converge exponentially to a single trajectory, which is an element of the limit set of the dynamics. I stands for the identity matrix. The Jacobian matrix in (9) is valued at p_k for all $k\in\mathbb{N}$.

Substituting (1) for $\zeta_{i,k}$ in (2) yields the following ith component of $f_k(p_k)$

$$p_{i,k} = 1-((1-\delta)p_{i,k-1}-1)\prod_{j\in N_i^c}(1-\beta p_{i,k-1}), \tag{10}$$

from which the Jacobian matrix is derived

$$\begin{aligned}(v_k)'_{p_k} &= \beta(I+(\delta-1)diag(p_k))A \\ &+(1-\delta)\prod_{j\in N_i^c}(1-\beta p_{i,k-1})I.\end{aligned} \tag{11}$$

A and diag(p_k) denote the adjacency matrix of CN and the matrix diagonal whose ith entry is $p_{i,k}$, respectively.

Inequality (9) with the Jacobian matrix valued at $p_k\equiv 0$ is consistent with the condition

$$\beta/\delta < 1/\lambda_{1,A}, \tag{12}$$

corresponding to the case where the virus outbreak dies out [3]; i.e., the equilibrium $p_k\equiv 0$ is locally asymptotically stable. Should this inequality not be satisfied, system in (10) approaches other trajectories lying in its limit set, also called an endemic state, provided (9) is satisfied. In that case, viruses remain prevalent throughout the network. The endemic state usually corresponds to a steady state or to a periodic orbit [17].

Monitoring of the contraction property of (9). The way online monitoring is carried out depends on the type of information that is available to the CC center.

Case 1: When the number of infected hosts, $\Sigma_{i=1}^{m} p_{i,k}$, is known, exploiting regression techniques allow to estimate parameters β and δ in (1); see [12], [13], and references therein. The local stability condition in (12) can thus be used to infer that $p_k\equiv 0$ is locally asymptotically stable whenever (12) is satisfied. It should be noted that approaches based on statistical inference techniques could also be used to predict virus propagation. Such approaches make use of specific classes of stochastic processes such as the nonhomogeneous Poisson process [13].

Case 2: When the identity of infected hosts is known over a period of time [t_k-T, t_k), the empirical frequency f_k is computed at t_k to approximate the state p_k in (1). Online monitoring of the sufficient condition (9) for contraction of (1) to its positive limit set, whether endemic or not, is then carried out by verifying whether

$$\bar{\lambda}((v_k^T)'_{p_k}(v_k)'_{p_k})<1, \tag{13}$$

where $\bar{\lambda}(P)$ denotes the largest eigenvalue of P, v_k is given in (11), and parameters β and δ are computed as in *Case 1*.

T should not be too large so that p_k could be considered as a quasi-stationary process. Assume, in doing so, that T is such that the l realizations {$\omega_{i,k,1}$,…, $\omega_{i,k,l}$} of the health status of node $i\in\{1,\ldots,m\}$ of CN are independent and identically distributed over [t_k-T, t_k). First, statistical learning techniques based on Monte Carlo simulations and Chernoff inequality allow to estimate with accuracy $\varepsilon>0$ and confidence $1-\gamma$, $\gamma>0$, the interval $I_k(\varepsilon,\gamma)$=[$f_{1,k,\mathrm{m}}$, $f_{1,k,M}$]×… ×[$f_{m,k,m}$, $f_{m,k,M}$]∋($f_{l,k}$,…,$f_{m,k}$), if any, over which inequality (13) obtained by replacing p_k with f_k is satisfied. Then, applying the central limit theorem allows to compute the probability that p_k, which is approximated by f_k, lies within $I_k(\varepsilon,\gamma)$; i.e., the probability that the virus dynamics is contracting at t_k with confidence 1-γ.

C. Stability analysis of NA

We assume that (10) is contracting toward its limit set. Letting

$$\begin{aligned}&\bar{\lambda}(\tilde{\rho}_k)=\sup_j \lambda_j(\Sigma_{\omega_k\in I_k} M_k(\rho^*_{i,k},\tilde{\rho}_{j,k},i\in I, j\in J) \\ &\times \mathcal{A}_k^T(\omega_k)\mathcal{A}_k(\omega_k))\,|,\end{aligned} \tag{14}$$

where $\lambda_j(P)$ denotes the jth eigenvalue of matrix P, $\tilde{V}_k$ in (7) can be bounded as

$$\tilde{V}_k \le \bar{\lambda}(\tilde{\rho}_k)\,\|\,x_k\,\|^2. \tag{15}$$

$\|x\|$ stands for the Euclidean norm of vector x. It should be noted that $\lim_{\tilde{\rho}_k\to 0}\bar{\lambda}(\tilde{\rho}_k)=0$ since $\lim_{\tilde{\rho}_k\to 0}M_k=0$.

The stochastic Lyapunov function candidate is now selected as follows

$$V_k(x_k) = V(x_k)+\delta V_k, \tag{16}$$

where $V(x_k)$ is defined in (4) and

$$\delta V_k = \bar{\lambda}(\tilde{\rho}_k)\sum_{i=k}^{+\infty} \| x_i \|^2 \; I(\| x_i \|^2 < \| x_k \|^2 + K)\,, \tag{17}$$

for some K>0.

δV_k is positive and can be bounded by

$$\delta V_k \leq \sup_{i \geq k}(\bar{\lambda}(\tilde{\rho}_i)) \underbrace{\sum_{i=k}^{+\infty}(\| x_k \|^2 + K)}_{S_k}\,. \tag{18}$$

The supremum in (18) exits from the definition of $\bar{\lambda}(\tilde{\rho}_k)$ in (14) and from the fact that (10) is contracting.

Since $S_{k+1}-S_k = -K-\|x_k\|^2 < 0$ and S_k is positive, S_k is convergent which, in turn, implies that δV_k is convergent. Owing to the convergence of $\bar{\lambda}(\tilde{\rho}_k)$ to zero as $\tilde{\rho}_k$ approaches zero, i.e., as k goes to infinity (the contraction condition in (12) is satisfied.), we can conclude that

$$\lim_{k \to +\infty} \delta V_k = 0\,. \tag{19}$$

Employing (5), (15), (16), and the fact that

$$\delta V_{k+1} - \delta V_k = -\bar{\lambda}(\tilde{\rho}_k) \| x_k \|^2 \tag{20}$$

yields the difference

$$\begin{aligned} E[V_{k+1}(x_{k+1}) \mid \mathbf{F}_n] - V_k(x_k) = x_x^T \Big(\bar{p}_k^* A^T A \\ + \sum_{\omega_k \in I_k \setminus {}_n} \prod_{i=1}^{n} \rho^*_{i,k} \mathbf{A}_k^T(\omega_k)\mathbf{A}_k(\omega_k) - I \Big) x_k + \tilde{V}_k \\ - \bar{\lambda}(\tilde{\rho}_k) \| x_k \|^2\,. \end{aligned} \tag{21}$$

Provided that there exists a symmetric, positive definite matrix L such that

$$\bar{p}_k^* A^T A + \sum_{\omega_k \in I_k \setminus {}_n} \prod_{i=1}^{n} \rho^*_{i,k} \mathbf{A}_k^T(\omega_k)\mathbf{A}_k(\omega_k) + L < I\,, \tag{22}$$

equation (21) is simplified as

$$E[V_{k+1}(x_{k+1}) \mid \mathcal{F}_n] - V_k(x_k) \leq -\kappa \| x_k \|^2, \tag{23}$$

where κ>0 is the smallest eigenvalue of L.

We now state the main result of this section.

Proposition 1: Assuming a contracting virus propagation dynamics, obtained when (12) is satisfied and monitored by following *Case 1* or *2* in Section III.B, and assuming that the limit set p_k^* is such that LMI in (22) is satisfied for all $k \in \mathbb{N}$, then the state x_k of CN in (3) converges to zero with probability one. ⋈

Proof: The result follows by applying Th. 4.2 in [7] (p. 81) to (16), whose time difference is expressed in (23), and from the convergence property of δV_k established in (19). ⋈

Monitoring the convergence condition of (3): Similar to CN, the following two cases arise for stability monitoring.

Case 1: When the identity of infected hosts is known, empirical frequency f_k^* is substituted for p_k^* in (22), recalling that $\rho_{i,k}^* \in \{p_{i,k}^*, 1-p_{i,k}^*\}$. The stability condition is monitored by direct inspection of the eigenvalues of the left-hand side of LMI in (3).

Case 2: Should the estimate of the limit set p_k^* of (1) be unavailable, the left-hand side of (3) can be approximated by leveraging the state x_k of (3), which is assumed known either from measurement or from state estimation. Noting that

$$\begin{aligned} E[\boldsymbol{\mathcal{A}}_k^T(\omega_k)\boldsymbol{\mathcal{A}}_k(\omega_k)] = \bar{p}_k^* A^T A \\ + \textstyle\sum_{\omega_k \in I_k \setminus {}_n} \prod_{i=1}^{n} \rho^*_{i,k} \mathbf{A}_k^T(\omega_k)\mathbf{A}_k(\omega_k), \end{aligned} \tag{24}$$

and selecting $N \in \mathbb{N}$ sufficiently large, the following approximation is used

$$E[\mathbf{A}_k^T(\omega_k)\mathbf{A}_k(\omega_k)] \cong \frac{1}{N}\sum_{j=k-N}^{N} A_{(j)}^T A_{(j)}\,, \tag{25}$$

where $A_{(j)}$ denotes the realization of $\boldsymbol{\mathcal{A}}_j(\omega_j)$ at t_j.

A least-square estimate of the average of $A_{(j)}^T A_{(j)}$ in (25) can be computed by concatenating $x_{j+1}^T x_{j+1} = x_j^T A_{(j)}^T A_{(j)} x_j$, for all $j \in [k, k+N-1]$, $N \gg \text{size}(x_k)$, which yields

$$X_{k,N} = Y_{k,N-1}\text{vec}_2(\mathrm{E}_{k,N}) + \varepsilon_k\,, \tag{26}$$

where

$$\begin{aligned} & X_{k,N-1}^T = [x_k^T x_k, \ldots, x_{k+N-1}^T x_{k+N-1}], \\ & Y_{k,N-1}^T = [\text{vec}_1(x_k x_k^T) \ldots \text{vec}_1(x_{k+N-1} x_{k+N-1}^T)] \\ & \mathrm{E}_{k,N} = \frac{1}{N}\sum_{j=k}^{k+N-1} A_{(j)}^T A_{(j)}, \tilde{E}_j = A_{(j)}^T A_{(j)} - \mathrm{E}_{k,N} \\ & \varepsilon_k^T = [\varepsilon_{k,1}, \ldots, \varepsilon_{k,j}, \ldots, \varepsilon_{k,N}], \varepsilon_{k,j} = x_j^T \tilde{E}_j x_j\,. \end{aligned} \tag{27}$$

vec$_1$(E) denotes the column vector formed by concatenating the rows of the upper triangular block of matrix E. vec$_2$(E)= vec$_1$(F), where entries f_{ii} and e_{ii} of F and E, respectively, are such that $f_{ii}=e_{ii}$ for all i and $f_{ij}=2e_{ij}$ for all $i \neq j$. N is such that $E(\mathcal{A}^T(\omega_i)\ \mathcal{A}(\omega_i)) \cong E_{k,N}$. The least-square estimate of $E_{k,N}$, which is a symmetric matrix, is given by

$$\text{vec}_2(\hat{\mathrm{E}}_{k,N}) = (Y_{k,N-1}^T Y_{k,N-1})^{-1} Y_{k,N-1}^T X_{k,N}\,, \tag{28}$$

The approximate in (27) can thus be expressed as follows

$$E[\boldsymbol{\mathcal{A}}_k^T(\omega_k)\boldsymbol{\mathcal{A}}_k(\omega_k)] \cong \hat{\mathrm{E}}_{k,N}^T\,. \tag{29}$$

The online monitoring thus consists in verifying that

$$\sup_i \lambda_i(\hat{\mathrm{E}}_{k,N}) < 1\,, \tag{30}$$

where $\hat{\mathrm{E}}_{k,N}$ is obtained from $\text{vec}(\hat{\mathrm{E}}_{k,N})$ in (28).

IV. EXTENSION TO JUMP SYSTEMS WITH DISTURBANCE

The convergence of trajectories is now analyzed by replacing model (3) with the following jump affine system

$$x_{k+1} = \boldsymbol{\mathcal{A}}_k(\omega_k)x_k + G_k(\omega_k), \tag{31}$$

where $G_k(\omega_k) \in \{0, G_k\}$ and $G_k \in \mathbb{R}^n$. In this model the ith component of vector G_k is zero with probability $p_{i,k}$, and nonzero with probability $1-p_{i,k}$. The class of system (31) is justified as follows. Considering the system

$$x_{k+1} = \boldsymbol{\mathcal{A}}_k(\omega_k)x_k + b_k \tag{32}$$

which corresponds to (3) disturbed by some deterministic bias b_k, one can select a new operating condition, $x_{o,k}=(I-A)^{-1} \times b_k$, and adopt the change of variable, $\tilde{x}_k = x_k - x_{o,k}$, such that (32) can be expressed as

$$\tilde{x}_{k+1} = A\tilde{x}_k + \underbrace{(I - (\boldsymbol{\mathcal{A}}_k(\omega_k) - I)(I - A_k)^{-1})b_k}_{G_k(\omega_k)}, \tag{33}$$

yielding $\tilde{x}_{k+1} = A\tilde{x}_k$ when system (32) is deterministic; i.e., when $\mathcal{A}_k \equiv A$. However, when $\mathcal{A}_k$ switches from the nominal matrix A, assumed stable, to one of its potentially unstable realization $A_{(k)}$, one obtains system (31) where $G_k(\omega_k)$ is given in (32). System (32) is interesting when analyzing the robustness of a linear system or a linearized system subject to parameter uncertainty; e.g., a feedback controller in closed loop with a parameter-varying model may give rise to an error system excited with a time-varying bias.

Proposition 2: Assuming a contracting virus propagation dynamics obtained when (12) is satisfied and monitored by following *Case 1* or *2* in Section III.B, and assuming that the limit set p_k^* is such that LMI (22) is satisfied for all $k \in \mathbb{N}$, then the state x_k of CN in (31) is almost-surely bounded. ⋈

Proof: Letting

$$W(x_k) = x_x^T x_k, \tag{34}$$

the time difference of W along the trajectories of (31) is given by

$$\begin{aligned} &E[W(x_{k+1}) \mid \mathcal{F}_n] - W(x_k) = h(x_k) \\ &+ E[2G_k^T(\omega_k)\mathcal{A}_k(\omega_k)]x_k + E[G_k^T(\omega_k)G_k(\omega_k)], \end{aligned} \tag{35}$$

where $h(x_k)$ corresponds to the right-hand side of (5), which is now expressed as a function of the trajectory of (31).

Selecting $W_k(x_k)=W(x_k)+\delta W_k$, where δW_k is defined similarly to δV_k in (17), and following the stability analysis in III.*C* yields, by application of Cauchy's inequality,

$$\begin{aligned} &E[W_{k+1}(x_{k+1}) \mid \mathcal{F}_n] - W_{k+1}(x_k) \le -\kappa \| x_k \|^2 + \rho \| x_k \| \\ &+ E[G_k^T(\omega_k)G_k(\omega_k)]. \end{aligned} \tag{36}$$

κ is defined in (23) and

$$\rho = \left\| E[2G_k^T(\omega_k)\mathcal{A}_k(\omega_k)] \right\|, \tag{37}$$

where $\|P\|$ stands for the spectral norm of matrix P.

Inequality (36) is expressed as

$$\begin{aligned} &E[W_{k+1}(x_{k+1}) \mid \mathcal{F}_n] - W_{k+1}(x_k) \le -\kappa(\| x_k \| - \rho / 2\kappa)^2 \\ &\underbrace{+\frac{\rho^2}{4\kappa} + E[G_k^T(\omega_k)G_k(\omega_k)]}_{>0}. \end{aligned} \tag{38}$$

Following the results on boundedness properties in [10], inequality (38) implies that the trajectory of (31) is both mean square and almost-surely bounded. ⋈

V. Simulation Results

Simulations are performed with the system in Fig. 4, where two out of four assets, whose physical dependences are expressed through matrices B_{12}, B_{24}, B_{31}, and B_{43}, are connected to CN; namely, Asset 1 and Asset 4. Two classes of virus dynamics' parameters are considered, leading to limit sets characterized by $p_k^*=0.1$ and $p_k^*=0.4$, and, in turn, to stable and unstable NA equilibrium, respectively (Fig. 5). The initial condition is $\mathbf{1}_{8\times1}$. The stability condition (30) is monitored in Fig. 6, where the number of samples used at step k to compute $\hat{\mathrm{E}}_{k,N}$ is 500(=N). The condition is no longer met after k=1020 leading to growing oscillations in the state of NA after k=1090 (close-up in Fig. 5).

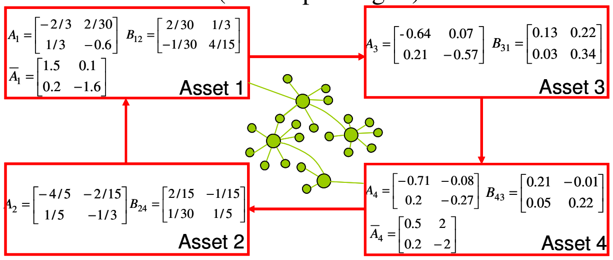
$A_1 = \begin{bmatrix} -2/3 & 2/30 \\ 1/3 & -0.6 \end{bmatrix}$ $B_{12} = \begin{bmatrix} 2/30 & 1/3 \\ -1/30 & 4/15 \end{bmatrix}$
$\bar{A}_1 = \begin{bmatrix} 1.5 & 0.1 \\ 0.2 & -1.6 \end{bmatrix}$
Asset 1
$A_3 = \begin{bmatrix} -0.64 & 0.07 \\ 0.21 & -0.57 \end{bmatrix}$ $B_{31} = \begin{bmatrix} 0.13 & 0.22 \\ 0.03 & 0.34 \end{bmatrix}$
Asset 3
$A_2 = \begin{bmatrix} -4/5 & -2/15 \\ 1/5 & -1/3 \end{bmatrix}$ $B_{24} = \begin{bmatrix} 2/15 & -1/15 \\ 1/30 & 1/5 \end{bmatrix}$
Asset 2
$A_4 = \begin{bmatrix} -0.71 & -0.08 \\ 0.2 & -0.27 \end{bmatrix}$ $B_{43} = \begin{bmatrix} 0.21 & -0.01 \\ 0.05 & 0.22 \end{bmatrix}$
$\bar{A}_4 = \begin{bmatrix} 0.5 & 2 \\ 0.2 & -2 \end{bmatrix}$
Asset 4

Fig. 4. The network of assets used in simulations.

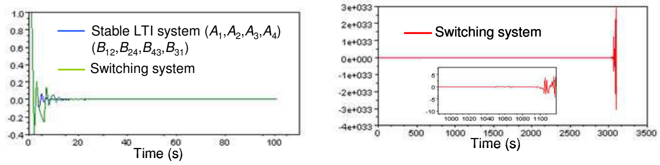

Fig. 5. Time trajectory of one of the states of NA. LTI and switching system obtained when p_k^*=0.1 (left). Switching system with p_k^*=0.4 (right).

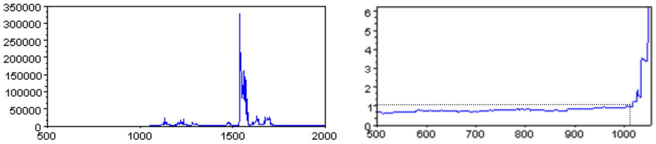

Fig. 6. Largest eigenvalues of $\hat{\mathrm{E}}_{k,N}$ when p_k^*=0.4, with close-up (right).

References

[1] D.L. Alderson and J.C. Doyle, "Can complexity support the engineering of critical network infrastructures?," in *Proc. of the IEEE International Conference on Systems, Man and Cybernetics*, Montréal, QC, Canada, 2007.

[2] B.H. Bharucha, *On the Stability of Randomly Varying Systems*, PhD thesis, University of California, Berkeley, California, 1961, http://www.dtic.mil/dtic/

[3] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Transactions on Information and System Security*, Vol. 10, No. 4, Article 13, 2008.

[4] C. Godsile and G. Royle, *Algebraic Graph Theory,* Springer-Verlag, 2001.

[5] K.E. Holbert, G.T. Heydt, and H. NI, "Use of satellite technologies for power system measurements, Command, and Control," *Proceedings of the IEEE*, Vol. 93, No. 5, pp. 947-955, May 2005.

[6] D. Kirschen and F. Bouffard, "Keep the lights on and the information flowing," *IEEE Power and Energy Magazine*, Vol. 7, No. 1, pp. 55-58, 2009..

[7] H.J. Kushner and G.G. Yin, *Stochastic Approximation Algorithms and Applications*, Springer, 1997.

[8] Q. Ling and M. Lemmon, "Soft real-time scheduling of networked control systems with dropouts governed by a Markov chain," in *Proc. of the American Control Conference*, Denver, CO, 2003.

[9] W. Lohmiller and J.-J.E. Slotine, "On contraction analysis for nonlinear systems," *Automatica*, Vol.34, No. 6, pp. 683-696, 1998.

[10] T. Morozan, "Boundedness properties for stochastic systems," *Stability of Stochastic Systems, Lecture Notes in Mathematics Vol. 294*, R. F. Curtain, Ed. Berlin, Germany: Springer-Verlag, 1972, pp. 21–34.

[11] North American Electric Reliability Corporation, *Annual Report 2008*, Princeton, NJ, USA, May 2009.

[12] H. Okamura, H. Kobayashi, and T. Dohi, "Markovian modeling and analysis of internet worn propagation," in *Proc. of the 16th IEEE International Symposium on Software Reliability Engineering*, Chicago, IL, 2005.

[13] H. Okamura, H. Kobayashi, and T. Dohi, "Statistical inference of computer virus propagation using non-homogeneous Poisson processes," in *Proc. of the 18th IEEE Int. Symposium on Software Reliability Eng.*, Trollhätten, Sweden, 2007.

[14] C.A. Rabbath and N. Léchevin, *Safety and Reliability in Cooperating Unmanned Aerial Systems*, World Scientific, 2010.

[15] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, Vol. 21, No. 6, pp. 11-25, 2001.

[16] R. Schainker, J. Douglas, and T. Kropp, "Electric utility responses to grid security issues," *IEEE Power & Systems Mag.*, Vol. 4, No. 2, pp.30-37, 2006.

[17] I.B. Schwartz, L. Billings, and E.M. Bollt, "Dynamical epidemic suppression using stochastic prediction and control," *Phys. Rev. E*, 046220, 2004.

[18] P. Seiler and R. Sengupta, "Analysis of communication losses in vehicle control problems," in *Proc. of the American Control Conference*, Arlington, VA, 2001.

[19] Y. Wang and I.I. Hussein, "Awareness coverage control over large-scale domains with intermittent communications," in *Proc. of the American Control Conference*, Seattle, WA, 2008.

[20] J. Wu and T. Chen, "Design of networked control systems with packet dropouts," *IEEE Transactions on Automatic Control*, Vol. 52, No. 7, pp. 1314-1319, 2007.