2021 American Control Conference (ACC)
New Orleans, USA, May 25-28, 2021

Bilinear Dynamical Networks Under Malicious Attack: An Efficient Edge Protection Method

Arthur Castello B. de Oliveira[1], Milad Siami[1], and Eduardo D. Sontag [1,2]

***Abstract*— In large-scale networks, agents and links are often vulnerable to attacks. In this paper, we focus on continuous-time bilinear networks, where additive disturbances model attacks or uncertainties on agents/states (node disturbances), and multiplicative disturbances model attacks or uncertainties on couplings between agents/states (link disturbances). We then investigate network robustness notion in terms of the underlying digraph of a network, and the structure of exogenous uncertainties and attacks. Specifically, we define the robustness measure using the $\mathcal{H}_2$-norm of the network and calculate it in terms of the reachability Gramian of the bilinear system. The main result is that under certain conditions, the measure is supermodular over the set of all possible attacked links. The supermodularity property facilitates the efficient solution of the optimization problem. We conclude with a few examples illustrating how different structures can make the system more or less vulnerable to malicious attacks on links.**

I. Introduction

The robust design of control systems against adversarial attacks is crucial for sustainability, from engineering infrastructures to living cells. For linear systems and networks, robustness to external attack is a topic that has been much studied [1]–[4], mainly by investigating how exogenous additive disturbances can affect overall performance. However, for nonlinear systems, the problem is harder to solve. In this paper, we study questions of robustness against attacks in the framework of a subclass of continuous-time nonlinear systems: *bilinear systems*. They constitute an interesting class of nonlinear systems [5], [6], since they have universal approximation properties and have been used to model problems in a wide variety of areas ranging from electrical networks to surface vehicles to immunology.

The performance and robustness analysis of linear consensus networks subject to external stochastic disturbances has been studied in the literature, as in [7]–[9], where the $\mathcal{H}_2$-norm of the system was employed as a scalar performance metric. Supermodularity of a number of control objectives for linear time-invariant (LTI) systems was studied in [10], [11]. Specifically, one of the control objectives is the trace of the inverse of the controllability Gramian, which can be interpreted as the average control energy for steering the system to a unit state. In [12], it was proved that the average control energy is not always supermodular for LTI systems, contrary to claims in [10], [11], [13]. The work in [14] demonstrates a subclass of differentiable systemic performance measures that are supermodular. Gramian-based reachability metrics for discrete-time bilinear systems were considered in [15], where it was shown that the minimum input energy to steer the state from the origin to any reachable target state can be lower bounded by a Gramian-based reachability metric.

To solve model order reduction problems for bilinear systems, in [16] the authors show the existence of a relationship between the $\mathcal{H}_2$-error of two bilinear systems, and their output error. These findings explain the previous results where $\mathcal{H}_2$-based model order reduction algorithms provided good approximation. Also related to the subject of this paper, in [17], [18] both the reachability and observatility Gramians of bilinear systems are related to lower and upper bounds for the controllability and observability energy functionals respectively. These results further indicate the usefulness of the $\mathcal{H}_2$ norm as a performance metric for bilinear systems, since it is directly related to the reachability Gramian.

In this paper, we formulate the problem of attacking a network through multiplicative disturbances on its edges as an optimization problem for a bilinear system. Specifically, the attacker tries to maximize the $\mathcal{H}_2$ norm of the system, while the system designer tries to find the set of edges that minimizes this norm. We find conditions that make the $\mathcal{H}_2$ norm of a bilinear system supermodular on the power set of the vulnerable edges, which allows us to use greedy algorithms to find an approximate solution for the minimization problem. The supermodularity translates the intuitive notion that attacks act in synergy and that they are more effective when applied together rather than individually.

II. Preliminary Definitions

A. Notations and Assumptions

Throughout this paper, the sets of real numbers, nonnegative real numbers, and strictly positive real numbers are represented as $\mathbb{R}$, $\mathbb{R}_+$, and $\mathbb{R}_{++}$, respectively. Similarly, the set of the strictly positive integers is denoted by $\mathbb{N}$, and the set of strictly positive integers up to $m \in \mathbb{N}$ by $\mathbb{N}_{\leq m}$. Matrices are represented by uppercase letters, and for a given matrix N_k, its element in row i and column j is represented as n_k^{ij}. Furthermore, we use the notation $N_k = (n_k(i,j))_{ij}$ to bring attention to the expression of the individual elements of the matrix N_k instead of the matrix itself. For any square matrix $M \in \mathbb{R}^{n\times n}$ the operator $\mathrm{trace}(\cdot) : \mathbb{R}^{n\times n} \to \mathbb{R}$ is $trace(M) = \sum_{k=1}^{n} m^{kk}$, that is, the sum of the elements of the main diagonal of M. For any finite set of elements $\mathcal{V}$, $|\mathcal{V}| \in \mathbb{N} \cup \{0\}$ is the number of elements in the set with $|\mathcal{V}| = 0 \iff \mathcal{V} = \emptyset$, and $2^{\mathcal{V}}$ is the power set of $\mathcal{V}$.

[1]Department of Electrical & Computer Engineering, Northeastern University, Boston, MA 02115 USA (e-mails: {castello.a, m.siami, e.sontag}@northeastern.edu).

[2]Departments of Bioengineering, Northeastern University, Boston, MA 02115 USA.

Furthermore, for any function f with domain in $\mathcal{V}$, for each subset $\overline{\mathcal{V}} \subset \mathcal{V}$ define $f(\overline{\mathcal{V}}) = \{f(v) \mid v \in \overline{\mathcal{V}}\}$.

Finally, the definition below formalizes the concept of underlying digraphs for bilinear systems with distinguished attacked nodes and links:

Definition 1 (Bilinear Digraph)**.** *A* bilinear digraph *is a quintet $\mathcal{G} := (\mathcal{V}, \mathcal{E}, w, \mathcal{E}_a, \mathcal{V}_a)$ where $\mathcal{V} = \mathbb{N}_{\leq n}$, for some $n \in \mathbb{N}$, and is called a node set, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is called an edge set, $\mathcal{V}_a \subseteq \mathcal{V}$ is called an attacked node set, $\mathcal{E}_a \subseteq \mathcal{V} \times \mathcal{V}$ is called an attacked edge set, and $w : \mathcal{E} \to \mathbb{R}$ is a weight function.*

B. Bilinear Systems and Digraphs

We consider a class of nonlinear systems associated with bilinear digraphs that consist of multiple agents with scalar state variables x_i, node disturbances v_i, and link disturbances η_k. We assume that the dynamics of the network can be written in the following compact form

$$\Sigma : \begin{cases} \dot{x}(t) = \left(N_0 + \sum_{k=1}^{m} \eta_k(t) N_k\right) x(t) + Bv(t) \\ y(t) = Cx(t) \end{cases} \tag{1}$$

where the total number of nodes/agents ($|\mathcal{V}|$) is n, $x \in \mathbb{R}^n$ is the state vector, y is the output, $\overline{m}$ is the number of nodes/agents under attack ($|\mathcal{V}_a|$), m is the number of edges/couplings under attack ($\mathcal{V}_a$), vector $v = [v_1, v_2, \cdots, v_{\overline{m}}]^\top$ is the node disturbance/input, and vector $\eta = [\eta_1, \eta_2, \cdots, \eta_m]^\top$ is the link disturbance/input. [1] Matrix $N_0 \in \mathbb{R}^{n \times n}$ is called the drift matrix and captures the autonomous dynamics of the network. Depending on the application, N_0 can be a function of the adjacency matrix or of the Laplacian of the network, the important assumption is that it somehow describes the autonomous evolution of the states of the agents based on their internal dynamics and interconnections. The input matrix B is the column composition of the elementary vectors e_j for every $j \in \mathcal{V}_a$. Each of the coupling matrices N_k are defined as $N_k = E_{i_k, j_k}$ (being E_{ij} the elementary matrix with a nonzero element in the position of row i and column j and zero everywhere else) for all $(i_k, j_k) \in \mathcal{E}_a$. We assume that the attacked edges and nodes are independently disturbed.

We note that the system described above is a particular realization of the general bilinear system

$$\Sigma : \begin{cases} \dot{x}(t) = \left(N_0 + \sum_{k=1}^{m+\overline{m}} \overline{u}_k(t) N_k\right) x(t) + \overline{B}\overline{u}(t) \\ y(t) = Cx(t) \end{cases} \tag{2}$$

where $\overline{u}_i$ is the i-th element of $\overline{u} := [\eta^\top,\ v^\top]^\top$, $\overline{B} := [0_{n \times m},\ B]$ and $N_k = 0_{n \times n}$ for all $k > m$.

Moreover, in the context of network analysis, a bilinear system models a network whose edges can be attacked/actuated directly, without changing the state of its out node. When studying attacking options it is often useful to define the set of attacked edges as a subset of a bigger set of vulnerable ones, defined as:

Definition 2. *For a bilinear network, a set of* vulnerable edges *$\mathcal{E}_v \subseteq \mathcal{E}$ is the subset of the edges of the graph that are vulnerable to attacks.*

This means that for a given bilinear network, the set of its edges that are under attack are always a subset of the set of vulnerable edges (i.e. $\mathcal{E}_a \subseteq \mathcal{E}_v$). Considering this new definition, it is often better to rewrite dynamics (1), through a slight abuse of notation, in a more general form as

$$\Sigma : \begin{cases} \dot{x}(t) = \left(N_0 + \sum_{k \in \mathcal{E}_a} \eta_k(t) N_k\right) x(t) + Bv(t) \\ y(t) = Cx(t) \end{cases} \tag{3}$$

where $\mathcal{E}_a$ is the set of attacked edges, $\eta = \{\eta_k \mid k \in \mathcal{E}_a\}$, and the set $k \in \mathcal{E}_a$ is an abuse of notation for $\{k \in \mathbb{N} \mid (i_k, j_k) \in \mathcal{E}_a\}$. The only difference between this way of describing system and equation (1) is that here we do not require the attacked edges to be numbered consecutively. However, it is possible to change from one to the other by simply changing the edge labels. Finally, if C is not specified, we assume $C = I_n$, where I_n is the $n \times n$ identity matrix.

C. The Volterra Series and the Solution of Bilinear Systems

To study the behaviour of bilinear system (1) we first look at its solution. Formally, this system can be thought of as an infinite sum of interconnected linear systems as follows:

$$\begin{cases} \dot{x}_1(t) = N_0 x_1(t) + Bv(t) \\ \dot{x}_2(t) = N_0 x_2(t) + \sum_{k=1}^{m} N_k x_1(t) \eta_k(t) \\ \qquad \vdots \\ \dot{x}_i(t) = N_0 x_i(t) + \sum_{k=1}^{m} N_k x_{i-1}(t) \eta_k(t) \\ \qquad \vdots \end{cases} \tag{4}$$

where $x(t) = \sum_{i=1}^{\infty} x_i(t)$. Figure 1 shows a graphical representation of this. If this infinite series is uniformly convergent, formally we have:

$$\sum_{i=1}^{\infty} \dot{x}_i = N_0 \sum_{i=1}^{\infty} x_i + \sum_{k=1}^{m} N_k \eta_k \sum_{i=1}^{\infty} x_i + Bv. \tag{5}$$

Defining $\overline{N} = [N_1, \ldots, N_m]$ and $u_i(t) = [\eta_1 x_{i-1}\ ;\ \ldots\ ;\ \eta_m x_{i-1}]$, we can rewrite the systems as the $\mathcal{C}_i$s below

$$\begin{aligned} \mathcal{C}_1 :&\quad \dot{x}_1(t) = N_0 x_1(t) + Bv(t) \\ \mathcal{C}_2 :&\quad \dot{x}_2(t) = N_0 x_2(t) + \overline{N} u_2(t) \\ &\quad \cdots \\ \mathcal{C}_i :&\quad \dot{x}_i(t) = N_0 x_i(t) + \overline{N} u_i(t). \end{aligned} \tag{6}$$

Assuming zero initial conditions, the systems $\mathcal{C}_i$s have solutions as below

$$\begin{aligned} x_1(t) &= \int_0^t \mathrm{e}^{N_0(t-\tau_1)} B v(\tau_1) d\tau_1 \\ x_2(t) &= \int_0^t \mathrm{e}^{N_0(t-\tau_2)} \overline{N} u_2(\tau_2) d\tau_2 \\ &\cdots \\ x_i(t) &= \int_0^t \mathrm{e}^{N_0(t-\tau_i)} \overline{N} u_i(\tau_i) d\tau_i. \end{aligned} \tag{7}$$

[1] In this paper, we consider independent disturbances on each attacked node and edge; however, the results from Theorems 3 and 4 hold for a more general case where the same input vector affects nodes and links (i.e.,$m = \overline{m}$ and $\eta = v$) as long as the coupling matrices are still elementary matrices.

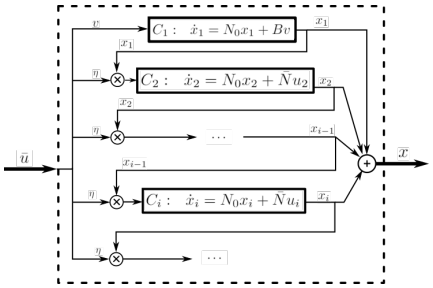

Fig. 1. Graphical representation the bilinear system written as the sum of interconnected linear systems.

After substituting the expression for $\overline{N}$ and $u_i(t)$, equation (7) becomes

$$
\begin{aligned}
&x_1(t) = \textstyle\int_0^t \mathrm{e}^{N_0(t-\tau_1)} B u(\tau_1) d\tau_1 \\
&x_2(t) = \textstyle\int_0^t \int_0^{\tau_2} \mathrm{e}^{N_0(t-\tau_2)} \sum_{k_2=1}^m N_{k_2} \eta_{k_2} \mathrm{e}^{N_0(\tau_2-\tau_1)} B v d\tau_1 d\tau_2 \\
&\cdots \\
&x_i(t) = \textstyle\int_0^t \int_0^{\tau_i} \cdots \int_0^{\tau_2} \mathrm{e}^{N_0(t-\tau_i)} \sum_{k_i=1}^m N_{k_i} \eta_{k_i} \mathrm{e}^{N_0(\tau_i-\tau_{i-1})} \\
&\times \textstyle\sum_{k_i=1}^m N_{k_{i-1}} \eta_{k_{i-1}} \cdots \mathrm{e}^{N_0(t-\tau_2)} \sum_{k_2=1}^m N_{k_2} \eta_{k_2} \mathrm{e}^{N_0(\tau_2-\tau_1)} \\
&\times B v d\tau_1 d\tau_2 \ldots d\tau_i.
\end{aligned}
$$

Finally, adding all terms $x_i(t)$ together results in the Volterra series of the system presented below

$$
\begin{aligned}
x = &\sum_{i=1}^{\infty} \int_0^t \int_0^{\tau_i} \cdots \int_0^{\tau_2} \sum_{k_2,\ldots,k_i=1}^{m} \mathrm{e}^{N_0(t-\tau_i)} N_{k_i} \mathrm{e}^{N_0(\tau_i-\tau_{i-1})} \\
&\times N_{k_{i-1}} \mathrm{e}^{N_0(\tau_{i-1}-\tau_{i-2})} \cdots N_{k_2} \mathrm{e}^{N_0(\tau_2-\tau_1)} B \\
&\times \eta_{k_i}(\tau_i) \eta_{k_{i-1}}(\tau_{i-1}) \cdots \eta_{k_2}(\tau_2) v(\tau_1) d\tau_1 d\tau_2 \cdots d\tau_i.
\end{aligned} \tag{8}
$$

In equation (8) and whenever necessary in the rest of the paper we represent the iterated sums $\sum_{k_1} \sum_{k_2} \cdots \sum_{k_n}$ as $\sum_{k_1,k_2,\ldots k_n}$ for brevity. With the result above we can define the Volterra kernels as below.

Definition 3. *The Volterra kernels of the bilinear systems can be defined as*

$$
\begin{aligned}
h_i(t,\tau_1,\ldots\tau_i) = &\sum_{k_2,\ldots,k_i=1}^{m} e^{N_0(t-\tau_i)} N_{k_i} e^{N_0(\tau_i-\tau_{i-1})} \\
&\times N_{k_{i-1}} e^{N_0(\tau_{i-1}-\tau_{i-2})} \cdots N_{k_2} e^{N_0(\tau_2-\tau_1)} B
\end{aligned} \tag{9}
$$

and their multivariable Laplace transforms are $H_i(s_1,\ldots,s_i) = \mathcal{L}(h_i(t_1,\ldots,t_i))$, also called the i-th order transfer functions of the bilinear system.

Since we use an infinite sum of dynamical systems, special care is needed when analysing its convergence. The study of Volterra series for general nonlinear systems is well explored in the literature, from which we can draw the following regarding its convergence:

Definition 4. *For a Volterra series with kernels h_i, we define its* gain bound function *for $x \geq 0$ as $f(x) := \sum_{i=1}^{\infty} \|h_i\|_\infty x^i$, and its* radius of convergence *as $\rho := (\limsup_{n\to\infty} \|h_i\|_\infty^{1/n})^{-1}$.*

Theorem 1 (Gain Bound Theorem [19])**.** *A Volterra series with kernels h_i, gain bound function f and radius of convergence ρ converges absolutely for inputs with $\|\overline{u}\|_\infty < \rho$*

From Theorem 1, we can conclude that for sufficiently bounded inputs, for any finite $T > 0$ and a stable N_0, the bilinear system in equation (1) has a well defined solution given by (8).

While the previous theorem assures the existence of a solution, we can also check its stability. Consider the definition below:

Definition 5 ([20])**.** *A dynamical system is* integral input to state stable *(iISS) if there exist $\alpha,\ \gamma \in \mathcal{K}_\infty$ and $\beta \in \mathcal{KL}$ so that for all initial states ξ and inputs $u(\cdot)$, its solution $x(t)$ respects*

$$
\alpha(|x(t)|) \leq \beta(|\xi|, t) + \int_0^t \gamma(|u(s)|) ds
$$

for all $t \geq 0$.

Then we can state the following theorem:

Theorem 2 ([20])**.** *The bilinear system* (2) *is iISS if and only if N_0 is Hurwitz.*

Notice that iISS, while not as strong as ISS, still means that any input with "finite energy" (as measured by γ) cannot make the system unstable.

III. $\mathcal{H}_2$ NORM BASED PERFORMANCE METRIC

In this section, we first define a robustness measure to quantify the vulnerability of a system given by equation (3) against attacks on its links. For linear systems, it is shown that the $\mathcal{H}_2$ norm is an effective robustness metric [7]–[9], which makes it appropriate for measuring the vulnerability to external attacks. We then investigate some properties of the $\mathcal{H}_2$ norm for a class of bilinear systems.

A. $\mathcal{H}_2$-norm of bilinear systems

We start this section by making the following assumption for all bilinear systems under analysis:

Assumption 1. *The matrix N_0 is stable and for two numbers α and β, which satisfy the inequality $\|e^{N_0 t}\| \leq \beta e^{-\alpha t}$ for all $t > 0$, we have $\sqrt{\sum_{k\in\mathcal{E}_a} \|N_k N_k^\top\|} < \sqrt{2\alpha}/\beta$.*

This assumption is sufficient for the proper definition of the reachability grammian, and consequently of the $\mathcal{H}_2$ norm, as it will be shown in this section. Consider, now, the following definition for the $\mathcal{H}_2$ norm of bilinear systems:

Definition 6. *Assuming zero initial condition and that assumption 1 holds, and letting the i-th order transfer function $H_i(s_1, s_2, \ldots, s_i)$ be the multivariable Laplace transform of the i-th kernel $h_i(t_1, t_2, \ldots, t_i)$, the $\mathcal{H}_2$ norm of a bilinear system Σ is defined as*

$$
\begin{aligned}
\|\Sigma\|_{\mathcal{H}_2} = \Bigg(&\sum_{i=1}^{\infty} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \mathrm{trace}(H_i^\top(jw_1,\ldots,jw_i) \\
&\times H_i(jw_1,\ldots,jw_i)) dw_1 \ldots dw_i \Bigg)^{1/2}
\end{aligned}
$$

Remark 1. *Notice that* $\|\Sigma\|_{\mathcal{H}_2}^2 = \sum_{i=1}^{\infty} \|\mathcal{C}_i\|_{\mathcal{H}_2}^2$*, that is, the squared* $\mathcal{H}_2$ *norm of the bilinear system* Σ *is the infinite sum of the squared* $\mathcal{H}_2$ *norms of the interconnected linear system. Furthermore, from the Plancherel Theorem we can verify that such definition of* $\mathcal{H}_2$ *for the bilinear system is directly related to*

$$\|\Sigma\|_{\mathcal{L}_2} = \left(\sum_{i=1}^{\infty} \int_0^{\infty} \cdots \int_0^{\infty} \operatorname{trace} \left(h_i^{\top}(t_1, \ldots, t_i) \times h_i^{\top}(t_1, \ldots, t_i) \right) dt_1 \ldots dt_i \right)^{1/2}, \tag{10}$$

the $\mathcal{L}_2$ *norm of the bilinear system, defined as the squared sum of the squared* $\mathcal{L}_2$ *norms of all interconnected subsystems* $\mathcal{C}_i$*'s.*

With this definition, we can state the following theorem from [21] to quantify the value of the $\mathcal{H}_2$ norm of bilinear system (3).

Theorem 3 ([21])**.** *Suppose Assumption 1 holds. Then the Volterra series uniformly converges on the interval* $[0, \infty)$ *and the input-state* $\mathcal{H}_2$ *norm of bilinear system* (3) *can be computed by*

$$\|\Sigma\|_2 = \sqrt{\operatorname{trace}(P)}, \tag{11}$$

where P *is the reachability Gramian of the bilinear system defined as the solution of the generalized lyapunov equation*

$$N_0 P + P N_0^{\top} + \sum_{k \in \mathcal{E}_a} N_k P N_k^{\top} + B B^{\top} = 0, \tag{12}$$

and can be written as

$$P = \sum_{q=1}^{\infty} \int_0^{\infty} \cdots \int_0^{\infty} P_q P_q^{\top} \, dt_1 \cdots dt_q, \tag{13}$$

where $P_q P_q^{\top} = e^{N_0 t_q} \sum_{k \in \mathcal{E}_a} N_k P_{q-1} P_{q-1}^{\top} N_k^{\top} e^{N_0^{\top} t_q}$*, for* $q > 1$*, and* $P_1 P_1^{\top} = e^{N_0 t_1} B B^{\top} e^{N_0^{\top} t_1}$*.*

The results from this theorem allow for the efficient computation of the $\mathcal{H}_2$ norm, enabling its use in optimization problems.

Remark 2. *If all inputs of system* (1) *are Gaussian noises with mean zero and unitary standart deviation, then the reachability grammian is equal to the steady state covariance of the system (see [22]). This means, consequently, that the* $\mathcal{H}_2$ *norm measures how much a gaussian signal disturbs the states of the system. Furthermore even for more general inputs we can see from Definition 6 that the* $\mathcal{H}_2$ *norm measure the energy of the generalized impulse response of the system (see [23]). So we can say that the* $\mathcal{H}_2$ *norm as defined in this paper measures the relationship between the input and the output of the system.*

B. A Simple Example

To illustrate the meaning of Assumption 1, we explore a simple bilinear system subject to white noise inputs. Consider the following system:

$$\dot{x} = -ax + kx\eta + bv, \tag{14}$$

where η and v are independently sampled white noise inputs and a, b and k are positive constants.

The generalized Lyapunov equation (12) simplifies for system (14) to

$$(-2a + k^2)P = -b^2, \tag{15}$$

which results in a reachability Gramian of the form

$$P = \frac{b^2}{2a - k^2}. \tag{16}$$

Assumption 1 can be written as $a > 0$ and $2a - k^2 > 0$. Using (13), we can calculate P as follows:

$$P = \sum_{i=1}^{\infty} \overline{P}_i = \sum_{i=1}^{\infty} \frac{b^2}{2a} \left(\frac{k^2}{2a} \right)^{i-1}, \tag{17}$$

where $\overline{P}_1 = \int_0^{\infty} e^{-a\tau} b b e^{-a\tau} d\tau = \frac{b^2}{2a}$, and

$$\overline{P}_i = \int_0^{\infty} e^{-a\tau} k \overline{P}_{i-1} k e^{-a\tau} d\tau = \frac{b^2}{2a} \left(\frac{k^2}{2a} \right)^{i-1}.$$

Based on equation (17), the reachability Gramian for this system is the infinite sum of a geometric progression with quotient $q = k^2/2a$ and initial value $a_0 = b^2/2a$. The necessary and sufficient convergence condition for the sum is $2a - k^2 > 0$ which coincides with Assumption 1. This means that for this SISO bilinear system, Assumption 1 is necessary and sufficient for any positive values of k, a and b. This simple example also indicates that Assumption 1 is related to the stability of the system (through N_0) and to the existence of the reachability Gramian (through the summation of the N_k's).

C. Supermodularity of the $\mathcal{H}_2$ *Norm*

Our objective is to characterize the $\mathcal{H}_2$ norm of the bilinear system as a function of edges under attack $\mathcal{E}_a$ (a.k.a. attacked edge set). For the main theoretical result of this paper, we consider a family of bilinear digraphs $\mathcal{F}$ generated by the ground set of vulnerable edges $\mathcal{E}_v \subseteq \mathcal{V} \times \mathcal{V}$ as follows:

$$\mathcal{F}(\mathcal{E}_v) := \left\{ \mathcal{G} = (\mathcal{V}, \mathcal{E}, w, \mathcal{E}_a, \mathcal{V}_a) \middle| \; \forall \mathcal{E}_a \in 2^{\mathcal{E}_v} \right\},$$

for given node set $\mathcal{V}$, edge set $\mathcal{E}$, weight function w, and attacked node set $\mathcal{V}_a$. We assume $\Sigma(\mathcal{E}_a)$ is bilinear system (3) induced by the corresponding bilinear digraph $(\mathcal{V}, \mathcal{E}, w, \mathcal{E}_a, \mathcal{V}_a) \in \mathcal{F}(\mathcal{E}_v)$. We can, then, define the square of the $\mathcal{H}_2$ norm as a set function $\rho_{\Sigma}(.) : 2^{\mathcal{E}_v} \to \mathbb{R}_+$ as

$$\rho_{\Sigma}(\mathcal{E}_a) \;:=\; \|\Sigma(\mathcal{E}_a)\|_2^2, \quad \forall \mathcal{E}_a \in 2^{\mathcal{E}_v}. \tag{18}$$

In the following theorem, we characterize some functional properties of set function $\rho_{\Sigma}(.) : 2^{\mathcal{E}_v} \to \mathbb{R}_+$.

Theorem 4. *Suppose that for a family of bilinear digraphs* $\mathcal{F}$ *Assumption 1 holds for everyone of its elements, then the square of the* $\mathcal{H}_2$ *norm function* $\rho_{\Sigma}(\mathcal{E}_a) : 2^{\mathcal{E}_v} \to \mathbb{R}_+$ *is properly defined, monotone, and supermodular.*

The proof is omitted due to the space limitation [24].

Algorithm 1: A greedy heuristic for a given bilinear system Σ which sequentially picks attacked edges.

Input : Σ, $\mathcal{E}_v$, and k
Output: $\mathcal{E}_*$

$\mathcal{E}_a \leftarrow \{\}$
for $k = 1$ *to* k **do**
  $\{e\} \leftarrow$ find an edge in $\mathcal{E}_v$ that returns the minimum value for

$$\rho_\Sigma\left(\mathcal{E}_a \cup \{e\}\right) - \rho_\Sigma(\mathcal{E}_a)$$

  $\mathcal{E}_a \leftarrow \mathcal{E}_a \cup \{e\}$
  $\mathcal{E}_v \leftarrow \mathcal{E}_v \backslash \{e\}$
end
$\mathcal{E}_* \leftarrow \mathcal{E}_a$
return $\mathcal{E}_*$

IV. Optimal Strategy

The network synthesis problem of interest is to improve the performance of bilinear network (3) by protecting and removing $k \geq 1$ edges from the vulnerable edge set $\mathcal{E}_v$. Specifically, we explore how to find the best set of edges to protect that minimizes the $\mathcal{H}_2$ norm of the system for a given cardinality constraint on the attack edge set $\mathcal{E}_a$.

A. Edge Protection Problem Formulation

To formulate the optimization problem, notice that i the coupling matrices are elementary matrices, Assumptio 1 imposes an upper bound on the number of acceptabl attacked edges. This means that if enough edges are attacke the results of this paper become invalid, and the system coul diverge in finite time.

From an attacker's perspective, it is always interesting t target enough edges to break the conditions in Assumptio 1, therefore we assume enough (k) edges are protected t make sure it holds. The edge protection problem can be cas as the following combinatorial optimization problem

$$\begin{aligned} \mathcal{E}_* = \arg\min_{\mathcal{E}_a \subset \mathcal{E}_v} \quad & \rho_\Sigma(\mathcal{E}_a) \\ \text{s.t.} \quad & |\mathcal{E}_a| = |\mathcal{E}_v| - k, \end{aligned} \tag{19}$$

where $\mathcal{E}_v$ is the vulnerable edge set, and budget k is the number of protected edges. The optimal protected edge set can be obtained by $\mathcal{E}_p = \mathcal{E}_v \backslash \mathcal{E}_*$ from (19).

We should note that for $k = 1$ one only needs to compute the value of $\rho_\Sigma(\mathcal{E}_a)$ for all the n sets of attacked edges with $n-1$ elements to find the solution. In general, however, the number of sets with $n-k$ elements grows almost exponentially for values of k close to $n/2$, i.e., $\binom{n}{\lceil n/2 \rceil} \sim \frac{2^n}{\sqrt{n}}$. Therefore such a straightforward strategy could be computationally expensive.

The next intuitive approach is to use a greedy algorithm by leveraging the fact that we can solve the problem for $k = 1$ and turning our problem into the greedy minimization of supermodular functions subject to cardinality constraints. It is known that for the maximization of submodular functions

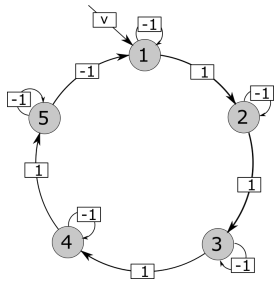

Fig. 2. Ring digraph with five nodes. Each node has a negative self loop and the edge from node five to node one is also negative, both conditions are necessary to enforce stability of the drift matrix for this structure.

(equivalent to our problem) is NP-hard and the greedy algorithm does not deliver the optimal solution in general but optimality gaps are given in the literature. In the following, we present a key result from the theoretical computer science literature to efficiently obtain an approximate solution of this combinatorial optimization.

Theorem 5 ([25]). *There exists an efficient algorithm with time complexity $\mathcal{O}(nk)$ that, given a non-negative submodular function f and a cardinality parameter k, achieves an approximation greater than 0.356 for the problem: $\max\{f(\mathcal{S}) : |\mathcal{S}| = k\}$, where $f(\cdot)$ is a submodular function.*

In [25], the authors present a greedy-based algorithm to prove Theorem 5 and to guarantee that the resulted solution is at least 35.6% of the maximum value of the function.

$\mathcal{E}_a = []$	$\mathcal{E}_a = [1]$	$\mathcal{E}_a = [1\ 5]$	$\mathcal{E}_a = [1\ 2\ 5]$	$\mathcal{E}_a = [1\ 2\ 4\ 5]$
	$\rho_\Sigma = 2.2004$	$\rho_\Sigma = 3.7198$	$\rho_\Sigma = 8.3827$	$\rho_\Sigma = 200.473$
		$\mathcal{E}_a = [1\ 2]$	$\mathcal{E}_a = [1\ 4\ 5]$	
		$\rho_\Sigma = 3.597$	$\rho_\Sigma = 7.7775$	
	$\mathcal{E}_a = [5]$	$\mathcal{E}_a = [1\ 4]$	$\mathcal{E}_a = [1\ 2\ 3]$	$\mathcal{E}_a = [1\ 2\ 3\ 5]$
	$\rho_\Sigma = 1.7109$	$\rho_\Sigma = 2.7771$	$\rho_\Sigma = 7.4422$	$\rho_\Sigma = 200.2365$
		$\mathcal{E}_a = [1\ 3]$	$\mathcal{E}_a = [3\ 4\ 5]$	
		$\rho_\Sigma = 2.6524$	$\rho_\Sigma = 5.2185$	
	$\mathcal{E}_a = [4]$	$\mathcal{E}_a = [4\ 5]$	$\mathcal{E}_a = [1\ 2\ 4]$	$\mathcal{E}_a = [1\ 2\ 3\ 4]$
	$\rho_\Sigma = 1.563$	$\rho_\Sigma = 2.6422$	$\rho_\Sigma = 4.848$	$\rho_\Sigma = 177.8885$
		$\mathcal{E}_a = [3\ 4]$	$\mathcal{E}_a = [1\ 3\ 5]$	
		$\rho_\Sigma = 2.2392$	$\rho_\Sigma = 4.8333$	
$\rho_\Sigma = 1.25$	$\mathcal{E}_a = [3]$	$\mathcal{E}_a = [3\ 5]$	$\mathcal{E}_a = [1\ 3\ 4]$	$\mathcal{E}_a = [1\ 3\ 4\ 5]$
	$\rho_\Sigma = 1.4827$	$\rho_\Sigma = 2.0857$	$\rho_\Sigma = 4.2108$	$\rho_\Sigma = 174.1216$
		$\mathcal{E}_a = [2\ 5]$	$\mathcal{E}_a = [2\ 3\ 4]$	
		$\rho_\Sigma = 2.014$	$\rho_\Sigma = 4.1524$	
	$\mathcal{E}_a = [2]$	$\mathcal{E}_a = [2\ 3]$	$\mathcal{E}_a = [2\ 4\ 5]$	$\mathcal{E}_a = [2\ 3\ 4\ 5]$
	$\rho_\Sigma = 1.4317$	$\rho_\Sigma = 2.0043$	$\rho_\Sigma = 3.3627$	$\rho_\Sigma = 111.723$
		$\mathcal{E}_a = [2\ 4]$	$\mathcal{E}_a = [2\ 3\ 5]$	
		$\rho_\Sigma = 1.8454$	$\rho_\Sigma = 3.0392$	

Fig. 3. Values of $\rho_\Sigma(\cdot)$ for all possible subsets of attacked edges.

To illustrate the effect of disturbances on bilinear systems, we consider a ring digraph with five nodes and negative self loops on each node as presented in Fig. 2. There, we label the nodes from 1 to 5, where node 1 is the only one that suffers an additive attack v (i.e., $B = [1, 0, 0, 0, 0]^\top$). We also label the edges that are not self loops according to their tail ends (e.g. edge 1 is from node 1 to node 2, edge 2 from node 2 to node 3, etc.).

We simulate system (3) for N_0 being the adjacency matrix of the graph and $|\mathcal{E}_v| = |\mathcal{E}| - 1$. With this setup we can easily compute the ρ_Σ function of the system for any set of attacked edges and represent them in Fig. 3. Notice that the case for all five edges being attacked is not included because it breaks the conditions of Assumption 1. Thus, we assume that the

system always has at least one protected edge (i.e., $\mathcal{E}_a \neq \mathcal{E}$). Notice also from Fig. 2 that, in this graph structure, some edges have a greater effect on the norm than others. This happens because of the additive disturbance acting on node one and does not change when the negative edge on the drift matrix is changed with respect to the additive disturbance.

By solving problem (19) for the system given by Fig. 2 and comparing the solutions of Algorithm 1 with the solutions of the brute force method for $k \in \mathbb{N}_{\leq 5}$, we can see from Table I that for two and three attacked edges, the greedy solution is not the actual minimum. In this case, the optimality gap is well within the theoretical gap of 10%, showing that using a greedy method to decide which edges to protect still yields good results.

TABLE I

MINIMUM AND GREEDY SOLUTION OF ρ_Σ - 5-NODE RING GRAPH

$\lvert\mathcal{E}_a\rvert$	Greedy Solution	Actual Minimum
1	1.4317	1.4317
2	1.8454	1.8454
× 3	3.3627	3.0392
4	111.723	111.723

Notice that by protecting the two most vulnerable edges, we significantly decrease the value of the $\mathcal{H}_2$ norm of the system from 111.7 to 3.0, or 3.6 if we consider the greedy solution.

TABLE II

MINIMUM AND GREEDY SOLUTION OF ρ_Σ - 20-NODE RING GRAPH

$\lvert\mathcal{E}_a\rvert$	Greedy Solution	Actual Minimum
1	0.5084	0.5084
2	0.5177	0.5177
3	0.5279	0.5279
4	0.5390	0.5390
5	0.5510	0.5510
× 6	0.5641	0.5640
7	0.5780	0.5780
8	0.5933	0.5933
9	0.6099	0.6099
10	0.6280	0.6280

We next consider a bigger ring graph with twenty nodes and up to ten randomly selected vulnerable edges. For this simulation, we multiply the drift matrix by a constant c to increase its convergence rate and assure Assumption 1 for up to ten attacked edges. From Table II, we can see that the simple greedy algorithm fails to deliver the optimum solution for the case of six attacked edges; however, the difference between the optimal and greedy solution is even smaller for this case than for the previous one.

V. CONCLUSIONS AND FUTURE WORKS

Multiplicative disturbances are a natural extension to the analysis of networks under attack. In this paper we provide a formal framework to evaluate their influence through bilinear system theory. Particularly, the bilinear equivalent of the $\mathcal{H}_2$ norm presents, under appropriate stability conditions, useful properties for evaluating the effects of each disturbances in the network. Particularly, the main result of this paper shows its supermodularity under addition of multiplicative disturbances. While the main result is useful in the context of bilinear networks, since the assumption of independence of the attacks on each edge makes sense in this context, it is also valid for other applications of bilinear systems that could support such hypothesis. We showed how to use this property to find the best set of edges to protect, and the optimization problem formulated in this paper gives useful insights to the design of bilinear networks and can help to build a structure that disperses the sensitivity of the system among the vulnerable edges. This makes the network more robust not only to attacks but to disturbances in general.

REFERENCES

[1] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada, "Smt-based observer design for cyber-physical systems under sensor attacks," *ACM Transactions on Cyber-Physical Systems*, vol. 2, no. 1, pp. 1–27, 2018.

[2] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *2015 American Control Conference (ACC)*. IEEE, 2015, pp. 2439–2444.

[3] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[4] Z. Tang, M. Kuijper, M. Chong, I. Mareels, and C. Leckie, "Sensor attack correction for linear systems with known inputs," *IFAC-PapersOnLine*, vol. 51, no. 23, pp. 206–211, 2018.

[5] R. R. Mohler, "Natural bilinear control processes," *IEEE Transactions on Systems Science and Cybernetics*, vol. 6, no. 3, pp. 192–197, 1970.

[6] D. Elliot, "Bilinear control systems," *Applied Mathematical Science*, vol. 169, 2009.

[7] B. Bamieh, M. Jovanović, P. Mitra, and S. Patterson, "Coherence in large-scale networks: Dimension-dependent limitations of local feedback," *Automatic Control, IEEE Transactions on*, vol. 57, no. 9, pp. 2235 –2249, Sept. 2012.

[8] M. Siami and N. Motee, "Fundamental limits and tradeoffs on disturbance propagation in linear dynamical networks," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 4055–4062, 2016.

[9] A. Jadbabaie and A. Olshevsky., "Combinatorial bounds and scaling laws for noise amplification in networks," in *European Control Conference (ECC)*, July 2013, pp. 596–601.

[10] T. H. Summers, F. L. Cortesi, and J. Lygeros, "On submodularity and controllability in complex dynamical networks," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 1, pp. 91–101, 2015.

[11] T. Summers, I. Shames, J. Lygeros, and F. Dörfler, "Topology design for optimal network coherence," in *2015 European Control Conference (ECC)*. IEEE, 2015, pp. 575–580.

[12] A. Olshevsky, "On (non) supermodularity of average control energy," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1177–1181, 2017.

[13] T. Summers and I. Shames, "Correction to "rigid network design via submodular set function optimization"," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, 2019.

[14] M. Siami and N. Motee, "Growing linear dynamical networks endowed by spectral systemic performance measures," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2091–2106, 2017.

[15] Y. Zhao and J. Cortés, "Gramian-based reachability metrics for bilinear networks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 3, pp. 620–631, 2016.

[16] M. Redmann, "Bilinear systems–a new link to H_2-norms, relations to stochastic systems and further properties," *arXiv preprint arXiv:1910.14427*, 2019.

[17] P. Benner and P. Goyal, "Balanced truncation model order reduction for quadratic-bilinear control systems," *arXiv preprint arXiv:1705.00160*, 2017.

[18] Y. Zhao and J. Cortés, "Reachability metrics for bilinear complex networks," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 4788–4793.

[19] S. Boyd, L. O. Chua, and C. A. Desoer, "Analytical foundations of volterra series," *IMA Journal of Mathematical Control and Information*, vol. 1, no. 3, pp. 243–282, 1984.

[20] E. D. Sontag, "Comments on integral variants of iss," *Systems & Control Letters*, vol. 34, no. 1-2, pp. 93–100, 1998.

[21] L. Zhang and J. Lam, "On H_2 model reduction of bilinear systems," *Automatica*, vol. 38, no. 2, pp. 205–216, 2002.

[22] T. Damm, "Rational matrix equations in stochastic control," *Lecture Notes in Control and Information Sciences*, vol. 297, 01 2004.

[23] M. C. Varona and R. Gebhart, "Impulse response of bilinear systems based on volterra series representation," *arXiv preprint arXiv:1812.05360*, 2018.

[24] A. C. B. de Oliveira, M. Siami, and E. D. Sontag, "Edge selection in bilinear dynamical networks," 2020.

[25] N. Buchbinder, M. Feldman, J. Naor, and R. Schwartz, "Submodular maximization with cardinality constraints," in *Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*. SIAM, 2014, pp. 1433–1452.