Preprints of the 20th World Congress
The International Federation of Automatic Control
Toulouse, France, July 9-14, 2017

Protecting Positive and Second-Order Systems against Undetectable Attacks ⋆

Jianqi Chen * **Jieqiang Wei** ** **Wei Chen** **,*** **Henrik Sandberg** ** **Karl H. Johansson** ** **Jie Chen** *

* *Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China (e-mail: jianqchen2-c@my.cityu.edu.hk, jichen@cityu.edu.hk).*
** *ACCESS Linnaeus Centre, School of Electrical Engineering, KTH Royal Institute of Technology, Sweden (e-mail: jieqiang, hsan, kallej@kth.se).*
*** *University of California at Berkeley, Berkeley, CA 94720, USA (e-mail: wchenust@gmail.com)*

Abstract: Undetectable attacks in security studies of cyber-physical systems render the measurements of the system equal to a possible physical response. In this paper, we investigate defense strategies against the undetectable single-attack for positive systems and second-order systems, which both can be reinterpreted in terms of graphs with nodes and edges, while the undetectable attack is added through one of the nodes. We show that an arbitrary placement of a sensor prevents undetectable single-attack for these classes of systems. It is worth emphasising that we do not need to measure at the corrupted node to prevent the undetectable single-attack, but can measure at any node. The defense strategy is of a low complexity and can be readily implemented.

Keywords: Undetectable attacks, defense strategy, sensor placement, positive systems, second-order systems

1. INTRODUCTION

Cyber-physical systems (CPS), enabled by today's ubiquitous information technology (IT) infrastructure, have been widely regarded as new-generation engineered systems that seek to integrate computational units, communication networks, and physical plants to enable large-scale, coordinated real-time monitoring, control, information processing, and operation. In these systems, different components interact through a set of networked agents, such as sensors, actuators, control processing units and communication devices. While seemingly of an unlimited potential interconnecting network and computing devices however, exposes the vulnerability of CPS and opens the door to potential cyber threats. Through the IT components, malicious attackers can gain access to sensing and actuating devices to launch attacks, which is likely to compromise the safe and reliable operation of a CPS and in an extreme scenario, lead to catastrophic consequences [Cárdenas et al. (2008)].

In light of the ever-expanding scope of CPS, there has been growing concern over security issues of CPS, and the needs to address the challenges in detecting threats, dissecting the impact of attacks, and designing effective defense strategies. Among a variety of issues, of particular interest is the problem concerning undetectable attacks and the protection against such attacks. In [Liu et al. (2011)], undetectable *false data injection attacks* were considered for static systems with limited resources. *Stealthy deception attacks* were studied in [Teixeira et al. (2010)]. *Replay attacks* [Mo and Sinopoli (2009)] act as one special undetectable attack by stealing, recording, and repeating the past signal as the malicious injection into the system. *Zero dynamics attacks* target the invariant zeros of the system and hide in the output [Pasqualetti et al. (2013)]. *Covert attacks* exploit decoupling structures to deceive the controller by interrupting the input and the output simultaneously [Smith (2011)].

The protection of a system is referred to the attribute that attacks on the system can be either detected or prevented. Adding a Gaussian signal unknown to the attacker into communication channels can make *Replay attacks* detectable [Mo and Sinopoli (2009)]. Undetectable attacks can also be detected by changing system dynamics [Teixeira et al. (2012)]. Furthermore, defense mechanism was proposed in [Shames et al. (2011)] against all attacks for general second-order systems by placing sensors on all neighbors of the potential attacked nodes. While effective, this strategy appears excessive. One should note that adding more sensors may neither be effective nor feasible in many situations, especially in a distributed setting, because of environment constraints and cost-effectiveness considerations.

⋆ This research is supported in part by the Hong Kong RGC under the grant number CityU 11260016, in part by Knut and Alice Wallenberg Foundation, Swedish Research Council, and Swedish Foundation for Strategic Research and in part by the Research Grants Council of Hong Kong Special Administrative Region, China, under the Theme-Based Research Scheme T23-701/14-N.

In this paper we first study undetectable attacks and the protection of positive systems. Positive systems are known [Berman and Plemmons (1979); Shafai et al. (1997); Colombino and Smith (2015)] to have applications in modeling growth behaviors of economics, ecological systems, population dynamics, and generally, dynamic systems involving positivity constraints. More recently, positive systems have also been used to model power grids, traffic flow, communication/computation networks, and production planning and logistics [Rantzer (2015)]. One key property of a positive system is its states and outputs all lie in the first orthant under non-negative disturbances. Of particular interest in our present paper is to investigate efficient strategies for the detection of undetectable attacks; in other words, we are interested in using a small and fewest number of sensors to detect attacks on a given number of actuators.

In particular, we are interested in the protection of multi-agent systems connected via a network graph. Intuitively, the protection of interconnected systems to undetectable attacks can be considerably more complex. That actuators and sensors are distributed across an interconnected network exposes the system to attacks of a higher cardinality, and hence potentially makes the system more vulnerable. We study second-order multi-agent systems and design accordingly defense strategies.

The remainder of this paper is organized as follows. In Section 2, we provide a concise background on invariant zeros and non-negative matrix theory, where the relevance to undetectable attacks is discussed. In Section 3, we develop defense strategies against undetectable attacks to stable and semi-stable positive systems. In Section 4, we study second-order systems defined on strongly connected digraphs and show that similar defense strategies can be devised. Illustrative examples are given in Section 5, with concluding remarks followed in Section 6.

Notation. Let $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$ and $\mathbb{R}^{m\times n}$ be the space of real numbers, complex numbers, real vectors and real matrices. For any $A \in \mathbb{R}^{m\times n}$, we denote by $A_{i,j}$, $\rho(A)$, $\Lambda(A)$, $A^\top$, A^{-1}, and $\mathrm{Im}(A)$, the (i,j)th entry, the spectral radius, the spectrum, the transpose, the inverse, and the column space respectively. A matrix A is said to be non-negative (positive), denoted by $A \succcurlyeq 0$ ($A \succ 0$), if all the entries of matrix A are non-negative (positive). For $s \in \mathbb{C}$, denote $\mathrm{Re}(s)$ as the real part. We use e_i to represent the ith Euclidean coordinate and E to represent the canonical basis.

2. PROBLEM FORMULATION AND PRELIMINARIES

In this paper, we investigate the protection of two widely used systems, namely positive systems and second-order systems, with respect to undetectable attacks.

Consider the systems whose measurements $y(t)$ are excited by the initial states $x(0)$ and the attacks $d(t)$ consistently, one interpretation of the undetectable attacks is that the measurements due to the attacks coincide with a possible physical response.

Definition 1. ([Pasqualetti et al. (2013)]) The non-zero attack $d(t)$ is undetectable if the system outputs satisfy

$$y(x(0), d(t), t) = y(\bar{x}(0), 0, t),\ \forall t, \tag{1}$$

where $x(0)$ and $\bar{x}(0)$ are the actual and possible initial states.

For linear systems, the condition (1) is equivalent to $y(x(0) - \bar{x}(0), d(t), t) = 0, \forall t$. Hence the design of undetectable attacks amounts to finding eligible inputs $d(t)$ which yield zero output coordinated with the initial state $x(0) - \bar{x}(0)$. Let us study the following continuous-time linear time-invariant (LTI) systems

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bd(t), \\ y(t) &= Cx(t), \end{aligned} \tag{2}$$

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$, $x(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}^p$, and the attack signal $d(t) \in \mathbb{R}^m$ [1]. It can be recognized that finding a feasible control $d(t)$ and the initial state $x(0) - \bar{x}(0)$ such that $y(t) = 0, \forall t \geq 0$ is the classical zero dynamics problem, which we elaborate below.

Let the LTI system (2) be left-invertible, i.e., $p \geq m$ and the transfer function $G(s) = C(sI - A)^{-1}B$ is column full normal rank, and so is to the associated Rosenbrock system matrix defined below.

Lemma 1. ([Pasqualetti et al. (2013)]) An attack signal $d(t) = -e^{st}d_0$ is undetectable if and only if there exists an invariant zero $s \in \mathbb{C}$, zero state $x(0) - \bar{x}(0) \neq 0$, and zero input d_0 such that

$$\begin{bmatrix} sI - A & B \\ C & 0 \end{bmatrix} \begin{bmatrix} x(0) - \bar{x}(0) \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{3}$$

where $\begin{bmatrix} sI - A & B \\ C & 0 \end{bmatrix}$ is named the Rosenbrock system matrix.

In the rest of this paper, we shall seek effective defense approaches by designing C to prevent undetectable attacks. Generally speaking, adding more sensors such that C is full column rank implies a conspicuous defensive policy [(Shames et al., 2011)]. More precisely, by the Hautus test, the system's observability implies that $x(0) = \bar{x}(0)$. Hence $Bd(t) = 0, \forall t \geq 0$, i.e., undetectable attacks are non-existent. Nevertheless, this approach may not be feasible since the consequent high-cost. This motivates us to investigate defense strategies using the fewest number of sensors possible.

An attack signal $d(t) = -e^{st}d_0$ will vanish, remain a constant d_0, oscillate persistently, or increase exponentially if $\mathrm{Re}(s) < 0$, $s = 0$, $s = j\omega\,(\omega \neq 0)$, or $\mathrm{Re}(s) > 0$, respectively. The vanishing attack, corresponding to a minimum phase zero s, i.e. $\mathrm{Re}(s) < 0$, cannot bring in the significant influences on the dynamics of the system, especial for the stable system, in many applications, which is acceptable for us. This will be illustrated in our later examples. On the other hand, when s is a non-minimum phase zero of the system, then there are two feasible approaches to prevent the corresponding undetectable attacks.

Definition 2. We say that a defense strategy, namely a design of C, successful if one of the following conditions holds:

[1] The undetectable attacks stated in this paper are only through the actuators, while the predominant results addressed later are also referential to attacks through the sensors only, or both.

(i) $\text{rank}\left(\begin{bmatrix} sI-A & B \\ C & 0 \end{bmatrix}\right) = n+m,$

(ii) $\text{rank}\left(\begin{bmatrix} sI-A & B \\ C & 0 \end{bmatrix}\right) < n+m$, while $d_0 = 0$ in (3),

for each s with $\text{Re}(s) \geq 0$.

In the sequel, we focus on the undetectable single-attack scenario, namely the undetectable attacks enter the system only through one channel or one node. In other words, the attack $d(t) \in \mathbb{R}$ and $B = e_i$. Note that $B = e_i$ represents the accessibility of the adversary to the system, which is not like the typical encoder matrix, where the element "1" marks the attacked position.

Like commonly assumed [Dibaji and Ishii (2015)], the number of attacked targets is known, which is one in this paper, while the exact target is unknown.

Next, we introduce some key definitions and preliminary lemmas concerning non-negative matrices and beyond from [Berman and Plemmons (1979)] and [Brualdi and Ryser (1991)].

Definition 3. A matrix A of the form

$$A = \lambda I - \bar{A}, \tag{4}$$

where $\lambda \geq \rho(\bar{A})$ and $\bar{A} \succcurlyeq 0$, is called an M-matrix.

This matrix A of the form (4) for which $\lambda > \rho(\bar{A})$ is a non-singular M-matrix, and a singular M-matrix strictly takes the equality, i.e., $\lambda = \rho(\bar{A})$.

Definition 4. A matrix in which all the off-diagonal elements are non-negative is named a Metzler matrix, i.e., $\forall_{i \neq j}\, A_{i,j} \geq 0$.

The next two lemmas introduce the connections between M-matrix and Metzler matrix.

Lemma 2. Matrix A is a non-singular M-matrix if and only if $-A$ is a Hurwitz stable Metzler matrix.

Lemma 3. Matrix A is a M-matrix defined in (4) if and only if $-A$ is a Metzler matrix and the real part of each non-zero eigenvalue of $-A$ is negative.

Definition 5. Laplacian matrix L is an M-matrix with row sums equal to zero.

Laplacian matrix is a typical example of singular M-matrices. It is customary to define a graph, and so to associate a communication network with a Laplacian matrix, in which connectivity is an important notion.

We use $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ to show a directed graph, where $\mathcal{V} \triangleq \{i\}_1^n$ represents the vertex set, with $i \in \mathcal{V}$ corresponding to node i, and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the directed edge set.

Definition 6. A directed graph is strongly connected if it contains a directed path for every pair of vertices.

Given a matrix A, the corresponding graph can be defined as follows: there is an edge from i to j if and only if $A_{j,i} \neq 0$. Next we introduce the irreducibility of a matrix in the notion of graphs.

Definition 7. A matrix is irreducible if the corresponding graph is strongly connected.

One key lemma of this paper is introduced herein.

Lemma 4. For any irreducible and non-singular M-matrix A, we have $A^{-1} \succ 0$.

3. PROTECTION IN POSITIVE SYSTEMS

We shall first attempt to design the defensive mechanism against the undetectable single-attack for positive systems.

Positive systems can guarantee that states and outputs all lie in the first orthant under non-negative disturbance.

Lemma 5. ([Farina and Rinaldi (2011)]) A linear system (A, B, C) (2) is called positive if and only if
(i) A is Metzler, and
(ii) $B \succcurlyeq 0$ and $C \succcurlyeq 0$.

Theorem 8. Consider a Hurwitz stable positive system with irreducible matrix A, for an arbitrary undetectable single-attack, any defense strategy with arbitrary single measurement is successful, i.e., if $B = e_i, \forall e_i \in E$, any defense strategy with $C = e_j^\top, \forall e_j \in E$ is successful.

Proof. Through Lemma 1, we have

$$\begin{bmatrix} sI-A & e_i \\ e_j^\top & 0 \end{bmatrix} \begin{bmatrix} \tilde{x}(0) \\ d_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{5}$$

where $x(0) - \bar{x}(0)$ in (3) is replaced by $\tilde{x}(0)$. Denote $s = a + j\omega$.

First, we study the case $s = j\omega \neq 0$. Since $[\tilde{x}^\top(0), d_0]^\top \in \mathbb{R}^{n+1}$, and $j\omega I - A$ is column full rank to $\mathbb{R}^n$, i.e., there $\nexists v \in \mathbb{R}^n$ satisfying $v \neq 0$ such that $(j\omega I - A)v = 0$, we have that $\text{rank}\left(\begin{bmatrix} j\omega I - A \\ e_j^\top \end{bmatrix}\right)$ is full column rank to $\mathbb{R}^n$. Similarly, the matrix $\begin{bmatrix} j\omega I - A & e_i \\ e_j^\top & 0 \end{bmatrix}$ is column full rank to $\mathbb{R}^{n+1}$. Furthermore, it is same to the matrix $\begin{bmatrix} aI + j\omega I - A & e_i \\ e_j^\top & 0 \end{bmatrix}$ for $\forall a \in \mathbb{R}$. The discussions above demonstrate that all points with non-zero imaginary parts on the closed right-half complex plane can be blocked successfully with $B = e_i, C = e_j^\top, \forall e_i,\, e_j \in E$.

The next step is to analyze the rank condition for $s = a \geq 0$, where possible unstable zeros lie in the non-negative real axis. Because A is a stable matrix, $aI - A$ is invertible, then we have

$$\begin{aligned} \text{rank}\left(\begin{bmatrix} aI-A & e_i \\ e_j^\top & 0 \end{bmatrix}\right) &= \text{rank}\left(\begin{bmatrix} aI-A & 0 \\ 0 & -e_j^\top (aI-A)^{-1} e_i \end{bmatrix}\right) \\ &= n+1 \end{aligned}$$

if and only if $-e_j^\top (aI - A)^{-1} e_i \neq 0$, $\forall e_i,\, e_j \in E$. This is equivalent to all entries of $(aI - A)^{-1}$ are non-zero. Indeed, since $-A$ is an irreducible and non-singular M-matrix, so is to $aI - A$ for $a \geq 0$, we have $(aI - A)^{-1} \succ 0$ according to Lemma 4.

In conclusion, an arbitrary placement of single measurement, i.e., $C = e_j^\top, \forall e_j \in E$, is a successful defense. □

Next we shall investigate the same problem for a semi-stable positive system with irreducible matrix A. Before that, some definitions and lemmas need to be introduced.

Lemma 6. (Perron-Frobenius [Horn and Johnson (2012)]) Let a matrix A be irreducible and non-negative, then

(a) $\rho(A) > 0$,

(b) $\rho(A) > 0$ is an algebraically simple eigenvalue of A,
(c) there exists uniquely determined and positive left and right eigenvectors to $\rho(A)$.

Lemma 7. To a matrix A with the positive ν_l satisfying $\nu_l^\top A = 0$, we have $e_i \notin \mathrm{Im}(A)$, $\forall e_i \in E$.

Theorem 9. Consider a Hurwitz semi-stable positive system with irreducible matrix A, for an arbitrary undetectable single-attack, any defense strategy with arbitrary single measurement is successful.

Proof. When consider the case $s = j\omega \neq 0$, it is same to the corresponding proof of Theorem 8, and all points with non-zero imaginary parts on the closed right-half complex plane can be blocked in this spirit.

Turn to the case $s = a \geq 0$, through Lemma 6, it is shown that a semi-stable Metzler matrix has no eigenvalue on the imaginary axis except for the origin. Thus recalling Lemma 3, matrix $-A$ herein is a singular M-matrix, which can be also expressed as $-A = \rho(\bar{A})I - \bar{A}$. Then for $a > 0$, $aI - A$ is a non-singular M-matrix and is irreducible like $-A$. Hence we obtain $(aI - A)^{-1} \succ 0$ through Lemma 4.

Nevertheless, when $a = 0$, $aI - A = -A$ is not invertible and we will refer to another approach. From Lemma 6, the irreducible and semi-stable Metzler matrix A above satisfies the condition of Lemma 7, then we have $e_i \notin \mathrm{Im}(A)$, $e_j \notin \mathrm{Im}(A^\top)$, $\forall e_i$, $e_j \in E$. Thus the Rosenbrock system matrix satisfies $\mathrm{rank}\left(\begin{bmatrix} -A & e_i \\ e_j^\top & 0 \end{bmatrix}\right) = n + 1$ herein. □

4. PROTECTION IN SECOND-ORDER SYSTEMS

In this section, we shall consider the design of defense strategies against the undetectable single-attack for a type of second-order systems. In such systems, we investigate a network of n interconnected nodes. The communication topology is given by a weighted digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. In this network, node i receives information from node j if and only if there exists an edge from node j to node i in the graph $\mathcal{G}$. Moreover, denote $N_i = \{j \in \mathcal{V} : i, j \in \mathcal{E}\}$ as the negiborhood set of node i. We assume the following double integrator dynamics for node i

$$\begin{aligned} \dot{\xi}_i(t) &= \zeta_i(t) \\ \dot{\zeta}_i(t) &= u_i(t), \end{aligned} \tag{6}$$

where ξ_i and ζ_i are the corresponding scalar states. In this paper, we consider one general type of distributed control law given as

$$u_i = -k_i\zeta_i(t) + \sum_{j\in N_i} \upsilon_{i,j}(\xi_j(t) - \xi_i(t)), \tag{7}$$

where $k_i, \upsilon_{i,j} > 0$, $\forall i, j = 1, \cdots, N$. It is shown in [Shames et al. (2011)] that the controller (7) can guarantee the asymptotically convergence to consensus. The closed-loop of system (6) and (7) can be used to formulate many physical systems in reality. One example is power networks, where $\xi_i(t)$ and $\zeta_i(t)$ represent the phase angle and frequency of bus i. The coefficients k_i and $\upsilon_{i,j}$ are the damping coefficient of bus i and the susceptance of the power line connecting buses i and j normalized by the inertia of bus i [Kundur et al. (1994)]. Another example is the mass-damper systems with friction and linear dampers, see e.g., [Van der Schaft and Maschke (2013)].

When the attacks are implemented and the sensors are placed, the closed-loop of system (6) and (7) can be rewritten in the following compact form:

$$\begin{aligned} \begin{bmatrix} \dot{\xi}(t) \\ \dot{\zeta}(t) \end{bmatrix} &= \begin{bmatrix} 0 & I \\ -L & -K \end{bmatrix} \begin{bmatrix} \xi(t) \\ \zeta(t) \end{bmatrix} + Bd(t), \\ y(t) &= C \begin{bmatrix} \xi(t) \\ \zeta(t) \end{bmatrix}, \end{aligned} \tag{8}$$

where $\xi(t) = [\xi_1(t), \cdots, \xi_n(t)]^\top$, $\zeta(t) = [\zeta_1(t), \cdots, \zeta_n(t)]^\top$, $B \in \mathbb{R}^{2n}$, $C^\top \in \mathbb{R}^{2n}$, L is the Laplacian matrix associated with a strongly connected graph, and $K = \mathrm{diag}\{k_1, \cdots, k_n\}$.

Theorem 10. Consider a second-order system defined on a strongly connected graph, for an arbitrary undetectable single-attack, any defense strategy with arbitrary single measurement is successful.

Proof. The possible entrances of the single-attack can be expresses as $B = \begin{bmatrix} e_i^\top & 0^\top \end{bmatrix}^\top$ or $B = \begin{bmatrix} 0^\top & e_i^\top \end{bmatrix}^\top$, and the available placement of single measurement is $C = \begin{bmatrix} e_j^\top & 0^\top \end{bmatrix}$ or $C = \begin{bmatrix} 0^\top & e_j^\top \end{bmatrix}$. Here we shall investigate these four combinations.

For all four cases, the Rosenbrock system matrices are column full rank when $s = j\omega \neq 0$ in a similar spirit of the proof of Theorem 8. The rest of the proof is devoted to the case $s = a \geq 0$. We shall consider all the four possible combinations of B and C. We start with $a > 0$.

(i) If $B = \begin{bmatrix} e_i^\top & 0^\top \end{bmatrix}^\top$ and $C = \begin{bmatrix} e_j^\top & 0^\top \end{bmatrix}$, we have that

$$\begin{aligned} &\mathrm{rank}\left(\begin{bmatrix} aI - A & B \\ C & 0 \end{bmatrix}\right) = \mathrm{rank}\left(\begin{bmatrix} aI & -I & e_i \\ L & aI + K & 0 \\ e_j^\top & 0 & 0 \end{bmatrix}\right) \\ &= \mathrm{rank}\left(\begin{bmatrix} 0 & -I & e_i \\ I & 0 & (aI + K)e_i \\ 0 & 0 & -e_j^\top(a^2I + aK + L)^{-1}(aI + K)e_i \end{bmatrix}\right). \end{aligned} \tag{9}$$

The invertibility of matrix $a^2I + aK + L$ is apparent since $a > 0$ and $K = \mathrm{diag}(k_1, \cdots, k_n) \succcurlyeq 0$. Hence

$$\mathrm{rank}\left(\begin{bmatrix} aI - A & B \\ C & 0 \end{bmatrix}\right) = 2n + 1 \tag{10}$$

if and only if
$e_j^\top(a^2I + aK + L)^{-1}(aI + K)e_i \neq 0$, $\forall e_i, e_j \in E$.

(ii) If $B = \begin{bmatrix} 0^\top & e_i^\top \end{bmatrix}^\top$ and $C = \begin{bmatrix} e_j^\top & 0^\top \end{bmatrix}$, we have that (10) holds if and only if
$e_j^\top(a^2I + aK + L)^{-1}e_i \neq 0$, $\forall e_i, e_j \in E$

(iii) If $B = \begin{bmatrix} 0^\top & e_i^\top \end{bmatrix}^\top$ and $C = \begin{bmatrix} 0^\top & e_j^\top \end{bmatrix}$, we have that (10) holds if and only if
$e_j^\top a(a^2I + aK + L)^{-1}e_i \neq 0$, $\forall e_i, e_j \in E$,

(iv) If $B = \begin{bmatrix} e_i^\top & 0^\top \end{bmatrix}^\top$ and $C = \begin{bmatrix} 0^\top & e_j^\top \end{bmatrix}$, we have that (10) holds if and only if
$e_j^\top \left(I - a(a^2I + aK + L)^{-1}(aI + K)\right) e_i \neq 0$, $\forall e_i, e_j \in E$.

Therefore, the case (i), (ii), (iii) require us to prove that all entries of matrix $(a^2I + aK + L)^{-1}$ are non-zero, whilst we need to clarify the matrix $\left(I - a(a^2I + aK + L)^{-1}(aI + K)\right)$ holds no zero entry for the case (iv).

We first prove that all entries of $(a^2I + aK + L)^{-1}$ are non-zero. Since the Laplacian matrix L is a singular M-matrix, then we have $L = \rho(\bar{L}) - \bar{L}$ and $\bar{L} \geq 0$. Choosing k_i to be the largest entry of K, the matrix K can be decomposed into $K = k_iI - \bar{K}$, where $\bar{K} = \text{diag}\,(k_i - k_1, \cdots, k_i - k_{i-1}, 0, k_i - k_{i+1}, \cdots, k_i - k_n) \geq 0$. This implies that

$$\begin{aligned} a^2I + aK + L &= a^2I + ak_iI + \rho(\bar{L}) - a\bar{K} - \bar{L} \\ &= (a^2 + ak_i + \rho(\bar{L}))I - (a\bar{K} + \bar{L}). \end{aligned}$$

Since the row sums of the Laplacian matrix L are equal to zero, then the row sums of the matrix $\bar{L}$ are equal to $\rho(\bar{L})$. By Theorem 8. 1. 22 in [Horn and Johnson (2012)] towards the spectral radius inequalities for the non-negative matrix, we can easily show that

$$\rho(a\bar{K} + \bar{L}) \leq \rho(\bar{L}) + \rho(a\bar{K}) = \rho(\bar{L}) + \max_{1\leq j\leq n} a(k_i - k_j).$$

Furthermore, since $a^2 + ak_i + \rho(\bar{L}) > \rho(\bar{L}) + \max_{1\leq j\leq n} a(k_i - k_j)$, then $a^2I + aK + L = (a^2 + ak_i + \rho(\bar{L}))I - (a\bar{K} + \bar{L})$ is a irreducible and singular M-matrix. Hence, we have $(a^2I + aK + L)^{-1} > 0$ from Lemma 4.

Next, we shall show that $\left(I - a(a^2I + aK + L)^{-1}(aI + K)\right)$ holds no zero entry. It is straightforward to see that

$$a(a^2I + aK + L)^{-1}(aI + K) = \left(I + (a^2I + aK)^{-1}L\right)^{-1}.$$

Since $(a^2I + aK)^{-1}$ is a positive diagonal matrix, $(a^2I + aK)^{-1}L$, denoted as $\tilde{L}$ is a Laplacian matrix of a strongly connected digraph. It is straightforward that $(I + \tilde{L})$ is an irreducible and non-singular M-matrix, satisfying that $(I + \tilde{L})^{-1} > 0$. Together with the fact that $(I + \tilde{L})^{-1}$ is a row stochastic matrix, which is implied by $(I + \tilde{L})$ is a row stochastic matrix, we have that $(I + \tilde{L})^{-1}_{i,j} \in (0, 1), \forall i, j$. Thus, we can see that

$$\begin{aligned} &\left(I - a(a^2I + aK + L)^{-1}(aI + K)\right)_{i,i} > 0, \\ &\left(I - a(a^2I + aK + L)^{-1}(aI + K)\right)_{i,j} < 0,\ \forall i \neq j. \end{aligned} \tag{11}$$

The final step of the proof is to investigate the case $a = 0$. Recall what we have mentioned before in Lemma 7, the negative Laplacian matrix $-L$ defined on a strongly connected digraph inherits key properties of the irreducible and semi-stable Metzler matrix, which are $e_i \notin \text{Im}(L)$ and $e_j \notin \text{Im}(L^\top)$, $\forall e_i,\ e_j \in E$. The Rosenbrock system matrices of four cases can be divided into two groups. When $B = \begin{bmatrix} e_i^\top & 0^\top \end{bmatrix}^\top$, $C = \begin{bmatrix} e_j^\top & 0^\top \end{bmatrix}$ or $B = \begin{bmatrix} 0^\top & e_i^\top \end{bmatrix}^\top$, $C = \begin{bmatrix} e_j^\top & 0^\top \end{bmatrix}$, the Rosenbrock system matrices are two full column rank matrices since $e_i \notin \text{Im}(L)$, $e_j \notin \text{Im}(L^\top)$, $\forall e_i,\ e_j \in E$. However, when $B = \begin{bmatrix} e_i^\top & 0^\top \end{bmatrix}^\top$, $C = \begin{bmatrix} 0^\top & e_j^\top \end{bmatrix}$ or $B = \begin{bmatrix} 0^\top & e_i^\top \end{bmatrix}^\top$, $C = \begin{bmatrix} 0^\top & e_j^\top \end{bmatrix}$, the Rosenbrock system matrices are clearly not full column rank. In this occasion, it is straightforward to verify that $d_0 = 0$. □

5. ILLUSTRATIVE EXAMPLES

Example 11. In this example, we shall verify the result in Theorem 8. We consider a positive system given as

$$\begin{aligned} A &= \begin{bmatrix} -4 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -2 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \\ C &= \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}, \end{aligned} \tag{12}$$

where A is irreducible, whilst B and C represent the case with a undetectable single-attack and a single measurement. Since zero of the system is -4, one possible solution of (3) with $s = -4$ is $\tilde{x}(0) = x(0) - \bar{x}(0) = \begin{bmatrix} -10 & 10 & 0 \end{bmatrix}^\top$ and $d_0 = 10$. This implies an attack signal is $d(t) = -10e^{-4t}$.

In Fig. 1, the solid lines indicate the trajectories initiate from $x(0) = \begin{bmatrix} 14.92 & 10.84 & 10.53 \end{bmatrix}^\top$ with attack $d(t)$, while the dot lines are initiated from the possibly fraudulent initial state $\bar{x}(0) = \begin{bmatrix} 24.92 & 0.84 & 10.53 \end{bmatrix}^\top$. Notice that the outputs of these two cases (the red line) coincide always, which reveals the undetectability of the attack $d(t)$. In Fig. 2, there are the trajectories initiated from $x(0)$ with (solid lines) and without (dash lines) the attack $d(t)$. The attack $d(t)$ cannot affect the asymptotic stability of the system. In these figures, $x(t)$, $\bar{x}(t)$, and $\hat{x}(t)$ represent the normal state trajectories, the fraudulent state trajectories, and the attacked state trajectories respectively.

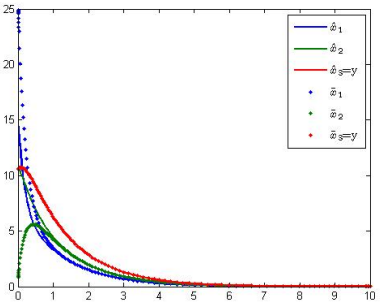

Fig. 1. The undetectability of the attack $d(t)$ on the stable positive system defined in Example 11.

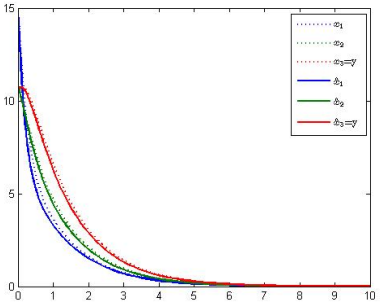

Fig. 2. The influence of the attack $d(t)$ on the stable positive system defined in Example 11.

Example 12. Here we shall present the result in Theorem 10. Without loss of generality, we consider a second-order system given as

$$\begin{aligned} A &= \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -2 & 1 & 1 & -1 & 0 & 0 \\ 1 & -2 & 1 & 0 & -1 & 0 \\ 1 & 1 & -2 & 0 & 0 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \\ C &= \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \end{aligned} \tag{13}$$

Notice that the zeros of the system are 0, -1 and $-0.5 \pm 1.6583j$. For $s = -1$ one solution to the equation (3) is $\bar{x}(0) = x(0) - \tilde{x}(0) = [1\ 1\ 1\ 0\ -1\ -1]^\top$ and $d_0 = 1$ which implies the attack signal $d(t) = -10e^{-t}$. For $s = 0$ and $s = -0.5 \pm 1.6583j$, all the solution to (3) satisfies $d_0 = 0$. Hence the attack does not exist.

For the simulation in Fig. 3, the actual initial state are set to be $x(0) = [0.21\ 0.09\ 0.77\ 0.21\ 0.39\ 0.55]^\top$ and the possibly fraudulent initial state are $\bar{x}(0) = [-0.79\ -0.91\ -0.23\ 0.21\ 1.39\ 1.55]^\top$.

The solid lines in Fig. 3 are the trajectories initiated from $x(0)$ with attack $d(t)$, while the dot lines are initiated from $\bar{x}(0)$. Notice that the outputs of these two cases (the cyan line) are exact the same and the undetectability is confirmed. In Fig. 4, there are the trajectories initiated from $x(0)$ with (solid lines) and without (dash lines) the attack $d(t)$. The second-order system can still achieve consensus with the attack $d(t)$ while the final stable point of $\{x_i(t), i = 1, 2, 3\}$ is deflected.

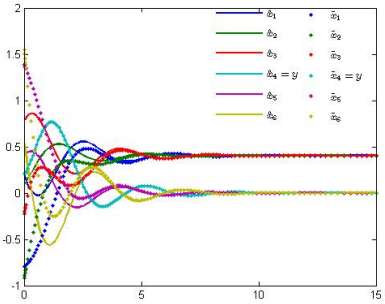

Fig. 3. The undetectability of the attack $d(t)$ on the second-order system defined in Example 12.

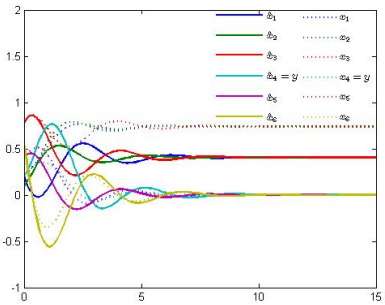

Fig. 4. The influence of the attack $d(t)$ on the second-order system defined in Example 12.

6. CONCLUSION

An explicit and efficient protection of positive systems and second-order systems to undetectable attacks was investigated in this paper. We showed that for any undetectable single-attack, defense with any single measurement is successful. The next step is to extend our analysis to the more general scenario of multiple attacks, in a progressive manner for (1) general high-order distributed positive systems and (2) general linear multi-agent systems.

REFERENCES

Berman, A. and Plemmons, R. J. (1979), 'Nonnegative matrices', *The Mathematical Sciences, Classics in Applied Mathematics* **9**.

Brualdi, R. A. and Ryser, H. J. (1991), *Combinatorial matrix theory*, Vol. 39, Cambridge University Press.

Cárdenas, A. A., Amin, S. and Sastry, S. (2008), Research challenges for the security of control systems., *in* 'HotSec'.

Colombino, M. and Smith, R. (2015), 'A convex characterization of robust stability for positive and positively dominated linear systems', *IEEE transactions on automatic control* **61**(7), 1965 – 1971.

Dibaji, S. M. and Ishii, H. (2015), Resilient consensus of second-order agent networks: Asynchronous update rules over robust graphs, *in* '2015 American Control Conference (ACC)', IEEE, pp. 1451–1456.

Farina, L. and Rinaldi, S. (2011), *Positive linear systems: theory and applications*, Vol. 50, John Wiley & Sons.

Horn, R. A. and Johnson, C. R. (2012), *Matrix analysis*, Cambridge university press.

Kundur, P., Balu, N. J. and Lauby, M. G. (1994), *Power system stability and control*, Vol. 7, McGraw-hill New York.

Liu, Y., Ning, P. and Reiter, M. K. (2011), 'False data injection attacks against state estimation in electric power grids', *ACM Transactions on Information and System Security (TISSEC)* **14**(1), 13.

Mo, Y. and Sinopoli, B. (2009), Secure control against replay attacks, *in* 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on', IEEE, pp. 911–918.

Pasqualetti, F., Dörfler, F. and Bullo, F. (2013), 'Attack detection and identification in cyber-physical systems', *IEEE Transactions on Automatic Control* **58**(11), 2715–2729.

Rantzer, A. (2015), 'Scalable control of positive systems', *European Journal of Control* **24**, 72–80.

Shafai, B., Chen, J. and Kothandaraman, M. (1997), 'Explicit formulas for stability radii of nonnegative and metzlerian matrices', *IEEE transactions on automatic control* **42**(2), 265–270.

Shames, I., Teixeira, A. M., Sandberg, H. and Johansson, K. H. (2011), 'Distributed fault detection for interconnected second-order systems', *Automatica* **47**(12), 2757–2764.

Smith, R. S. (2011), 'A decoupled feedback structure for covertly appropriating networked control systems', *IFAC Proceedings Volumes* **44**(1), 90–95.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H. and Sastry, S. S. (2010), Cyber security analysis of state estimators in electric power systems, *in* '49th IEEE conference on decision and control (CDC)', IEEE, pp. 5991–5998.

Teixeira, A., Shames, I., Sandberg, H. and Johansson, K. H. (2012), Revealing stealthy attacks in control systems, *in* 'Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on', IEEE, pp. 1806–1813.

Van der Schaft, A. and Maschke, B. (2013), 'Port-hamiltonian systems on graphs', *SIAM Journal on Control and Optimization* **51**(2), 906–937.