Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 56-2 (2023) 1820–1826

Optimal Detector Placement in Networked Control Systems under Cyber-attacks with Applications to Power Networks ⋆

Anh Tung Nguyen *, **Sribalaji C. Anand** **,
André M. H. Teixeira *, **Alexander Medvedev** *

* *Department of Information Technology, Uppsala University, PO Box 337, SE-75105, Uppsala, Sweden (e-mail: {anh.tung.nguyen, andre.teixeira, alexander.medvedev}@it.uu.se)*

** *Department of Electrical Engineering, Uppsala University, PO Box 65, SE-75103, Uppsala, Sweden (e-mail: sribalaji.anand@angstrom.uu.se)*

Abstract: This paper proposes a game-theoretic method to address the problem of optimal detector placement in a networked control system under cyber-attacks. The networked control system is composed of interconnected agents where each agent is regulated by its local controller over unprotected communication, which leaves the system vulnerable to malicious cyber-attacks. To guarantee a given local performance, the defender optimally selects a single agent on which to place a detector at its local controller with the purpose of detecting cyber-attacks. On the other hand, an adversary optimally chooses a single agent on which to conduct a cyber-attack on its input with the aim of maximally worsening the local performance while remaining stealthy to the defender. First, we present a necessary and sufficient condition to ensure that the maximal attack impact on the local performance is bounded, which restricts the possible actions of the defender to a subset of available agents. Then, by considering the maximal attack impact on the local performance as a game payoff, we cast the problem of finding optimal actions of the defender and the adversary as a zero-sum game. Finally, with the possible action sets of the defender and the adversary, an algorithm is devoted to determining the Nash equilibria of the zero-sum game that yield the optimal detector placement. The proposed method is illustrated on an IEEE benchmark for power systems.

Keywords: Networked systems, multi-agent systems, secure networked control systems, game theories, power systems.

1. INTRODUCTION

Society's rising demands require the development of complex and networked systems such as power grids, transportation networks, and water distribution networks. To enhance the performance and the efficiency of such systems, they might be divided into interconnected subsystems which are managed remotely through insecure communication channels. This insecure protocol possibly leaves the networked control systems vulnerable to cyber-attacks such as false data injection, covert, and replay attacks (Teixeira et al., 2015b), inflicting serious civil damages and financial loss. In the last decade, an Iranian industrial control system and a Ukrainian power grid have witnessed the catastrophic consequences of malware such as Stuxnet (Falliere et al., 2011) and Industroyer (Kshetri and Voas, 2017), respectively. Motivated by the above observation, defense strategies are needed to deal with such cyber-attacks with the purpose of protecting the networked control systems.

In this paper, we deal with the problem of optimal detector placement against a cyber-adversary in a networked control system which is represented by interconnected linear second-order agents. Every agent is regulated by its local controller through unprotected communication, which leaves the system vulnerable to malicious cyber-attacks. To guarantee a given local performance, the defender selects an agent on which to place a detector at its controller with the purpose of detecting malicious cyber-attacks. Meanwhile, the malicious adversary chooses an agent on which to inject attack signals with the purpose of maximally worsening the local performance while remaining stealthy to the defender. The contributions of this paper are the following:

(1) The boundedness of the worst-case attack impact is guaranteed by a necessary and sufficient condition based on the suitable choices of control parameters and the system-theoretic property of the underlying dynamical system, namely relative degree. This condition restricts the possible choices of the defender to a subset of available agents.
(2) The bounded worst-case attack impact is employed as a game payoff that enables us to translate the

⋆ This work is supported by the Swedish Research Council under the grants 2018-04396 and 2021-06316 and by the Swedish Foundation for Strategic Research.

10.1016/j.ifacol.2023.10.1896

purposes of the defender and the adversary into a zero-sum game.

(3) Based on the notions of the Nash equilibria (Zhu and Basar, 2015), an algorithm is devoted to determining Nash equilibria of the zero-sum game that yield the best strategies of the defender and the adversary.

To illustrate the obtained results, we apply our proposed method to the IEEE 14-bus system which represents a portion of the American Power Network. We conclude this section by providing the notation used in this paper.

Notation: the sets of real positive (negative) numbers are denoted as $\mathbb{R}_+$ ($\mathbb{R}_-$); $\mathbb{R}^n$ ($\mathbb{C}^n$) stands for sets of real (complex) n-dimensional vectors; every vector v and matrix A can be denoted $v = [v_i]$ where v_i is i-th element and $A = [a_{ij}]$ where a_{ij} is (i, j) entry, respectively; I stands for an identity matrix with an appropriate dimension. Let us define $e_i \in \mathbb{R}^n$ with all zero elements except the i-th element that is set as 1. Consider the norm $\|x\|^2_{\mathcal{L}_2[0,T]} \triangleq \frac{1}{T}\int_0^T \|x(t)\|_2^2 \, dt$, where we simplify the notation to $\|x\|^2_{\mathcal{L}_2}$ if the time horizon $[0, T]$ is clear from the context. The space of square-integrable functions is defined as $\mathcal{L}_2 \triangleq \big\{f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|^2_{\mathcal{L}_2[0,\infty]} < \infty\big\}$ and the extended space be defined as $\mathcal{L}_{2e} \triangleq \big\{f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|^2_{\mathcal{L}_2[0,T]} < \infty, \ \forall\, 0 < T < \infty\big\}$. Let $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$ be a graph with the set of N vertices $\mathcal{V} = \{1, 2, \ldots, N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, and the adjacency matrix $\mathcal{A} = [a_{ij}]$. For every $(i, j \neq i) \in \mathcal{E}$, $a_{ij} > 0$ and with $(i, j) \notin \mathcal{E}$ or $i = j$, $a_{ij} = 0$. The degree of vertex i is denoted as $\Delta_i = \sum_{j=1}^n a_{ij}$ and the degree matrix of graph $\mathcal{G}$ is defined as $\Delta = \mathbf{diag}\big([\Delta_i]\big)$, where **diag** stands for a diagonal matrix. The Laplacian matrix is defined as $L = [\ell_{ij}] = \Delta - \mathcal{A}$. Further, $\mathcal{G}$ is called an undirected connected graph if and only if matrix $\mathcal{A}$ is symmetric and the algebraic multiplicity of zero as an eigenvalue of L is one. The set of all neighbours of vertex i is denoted as $\mathcal{N}_i = \{j \in \mathcal{V} | (i, j) \in \mathcal{E}\}$. We denote a set $\mathcal{V}_{-i} \triangleq \mathcal{V} \setminus \{i\}$.

2. PROBLEM FORMULATION

This section first describes a networked control system under cyber-attacks. Then, we introduce the resources and the strategies of the defender and the adversary. Finally, the worst-case attack impact on the local performance is analyzed.

2.1 Networked control system under cyber-attacks

Consider an undirected connected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$ consisting of N agents where each agent i has a second-order state-space model:

$$\dot{p}_i(t) = v_i(t), \tag{1}$$

$$m_i\dot{v}_i(t) = \sum_{j\in\mathcal{N}_i} \ell_{ij}\Big(p_i(t) - p_j(t)\Big) - h_i v_i(t) + \tilde{u}_i(t), \tag{2}$$

$$y_i(t) = p_i(t), \tag{3}$$

where $p_i(t)$, $v_i(t) \in \mathbb{R}$ are the states, $\tilde{u}_i(t) \in \mathbb{R}$ is the healthy/attacked input, and $y_i(t) \in \mathbb{R}$ is the output of agent i. The local performance of the entire network is evaluated via the output energy over a given, possibly infinite, time horizon of a given agent $\rho \in \mathcal{V}$ denoted as $\|y_\rho\|^2_{\mathcal{L}_2}$. Parameters $m_i, h_i \in \mathbb{R}_+$ and $\forall (i, j) \in \mathcal{E}$, $\ell_{ij} \in \mathbb{R}_-$ are given. We utilize the following healthy local control law, which is adapted from Tegling (2018, Ch. 4), for each agent $i \in \mathcal{V}$

$$u_i(t) = -\theta_i y_i(t) + \phi_i \xi_i(t), \tag{4}$$
$$\dot{\xi}_i(t) = -\frac{1}{\tau}\xi_i(t) - \frac{\kappa_D}{\tau}\dot{y}_i(t),$$

where $\xi_i(t)$ is a virtual control input of agent i and $\theta_i, \phi_i, \kappa_D,$ and $\tau \in \mathbb{R}_+$ are control parameters. If the communication channel to agent i from its local controller is attacked by an adversary, $\tilde{u}_i(t) \neq u_i(t)$ which will be described in the following subsection; otherwise $\tilde{u}_i(t) = u_i(t)$. Let us employ the following assumption.

Assumption 1. The communication between the controller and the system of the given performance agent $\rho \in \mathcal{V}$ is protected from any cyber-attacks. Further, its controller is unavailable for the defender to place a detector. ◁

For convenience, let us use the following notation in the remainder of the paper: $p(t) \triangleq [p_i(t)]$, $v(t) \triangleq [v_i(t)]$, $\xi(t) \triangleq [\xi_i(t)]$, $x(t) \triangleq [x_1(t)^\top, x_2(t)^\top, \ldots, x_N(t)^\top]^\top$ where $x_i(t) \triangleq [p_i(t), v_i(t), \xi_i(t)]^\top$, $M \triangleq \mathbf{diag}\big([m_i]\big)$, $H \triangleq \mathbf{diag}\big([h_i]\big)$, $\Theta \triangleq \mathbf{diag}\big([\theta_i]\big)$, and $\Phi \triangleq \mathbf{diag}\big([\phi_i]\big)$.

Remark 1. The control law (4) will drive the system dynamics (1)-(2) to a closed-loop system that is different from the one in Tegling (2018, Ch. 4), due to no interaction of states v_i among agents. Thus, we will need to show how this control law stabilizes the system (1)-(2) in Section 2.3. Further, this control law plays an important role in the strategy of the defender which will be introduced in Section 3.

Remark 2. In this study, we determine the local performance of the entire network through the energy of the output measurement of the agent ρ over a possibly infinite time horizon. On the other hand, other local performances can be utilized based on different applications. We leave the comparison among local performances for future work.

2.2 Resources of the adversary and the defender

System knowledge: The malicious adversary and the defender know the location of the given protected performance agent ρ, the appearance of their competitors, the agent set $\mathcal{V}$, and the edge set $\mathcal{E}$. They also know all the system parameters M, H, Θ, Φ, κ_D, and τ as well as the detection mechanism which the defender will utilize.

Players' possible actions: According to *Assumption 1*, each player is able to choose a single agent in $\mathcal{V}_{-\rho}$ to implement their strategies. The adversary selects the attack agent $a \in \mathcal{V}_{-\rho}$ on which to conduct a malicious attack signal $\zeta(t) \in \mathbb{R}$ on its input with the aim of maximally disrupting the output of the performance agent ρ as follows:

$$\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & i \in \mathcal{V}_{-a}, \\ \zeta(t), & i \equiv a. \end{cases} \tag{5}$$

Meanwhile, the defender chooses the detection agent $d \in \mathcal{V}_{-\rho}$ on which to place a detector that generates a residual signal with the purpose of detecting the cyber-attack. These strategies of the two players are illustrated in Fig. 1 and described in detail below.

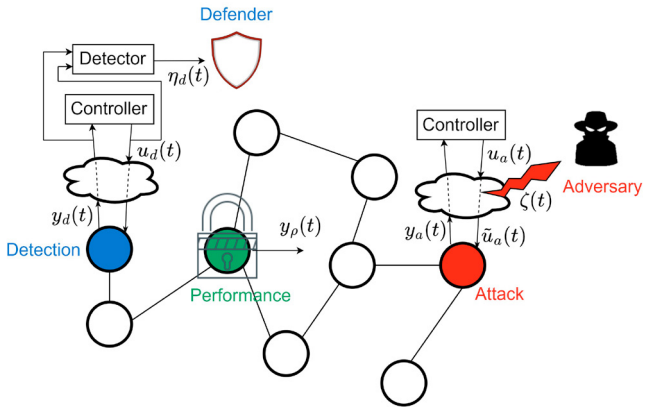

Fig. 1. Illustration of a networked control system with the (green) protected performance agent under cyber-attack. While the defender selects the (blue) detection agent on which to place a detector, the adversary chooses the (red) attack agent on which to conduct a cyber-attack.

Remark 3. In the scope of this study, we assume that the location of the performance agent ρ is revealed to both the defender and the malicious adversary to simplify the security problem. The problem of an unknown performance agent is left for future work.

2.3 Strategies of the adversary and the defender

Before going into those strategies, let us rewrite the closed-loop networked control system with its dynamics (1)-(3) under the control law (4)-(5) as follows

$$\dot{x}(t) = Ax(t) + E_a\zeta(t), \tag{6}$$
$$y_i(t) = C_i x(t), \quad \forall i \in \mathcal{V}, \tag{7}$$
$$y_\rho(t) = C_\rho x(t), \tag{8}$$

where

$$A = \begin{bmatrix} 0 & I & 0 \\ -M^{-1}(L+\Theta) & -M^{-1}H & M^{-1}\Phi \\ 0 & -\frac{\kappa_D}{\tau}I & -\frac{1}{\tau}I \end{bmatrix},$$

$$E_a = \left[0^\top,\ e_a^\top,\ 0^\top\right]^\top,\ C_i = \left[e_i^\top,\ 0^\top,\ 0^\top\right].$$

Lemma 1. Consider the healthy system (6) where $\zeta(t) = 0$ and assume that $\mathcal{G}$ is an undirected connected graph. Then, the matrix A in (6) is Hurwitz. ◁

Proof. Consider the candidate Lyapunov function

$$V\big(x(t)\big) = x(t)^\top \bar{P} x(t), \tag{9}$$

where

$$\bar{P} = \begin{bmatrix} M^{-1}\big(L+\Theta+\sigma H\big) & \sigma I & 0 \\ \sigma I & I & 0 \\ 0 & 0 & \kappa_D^{-1}\tau M^{-1}\Phi \end{bmatrix},$$

$$0 < \sigma < \min\left\{\min_{i\in\mathcal{V}} \frac{h_i}{m_i},\ \frac{4\ \min_{i\in\mathcal{V}}\theta_i}{\kappa_D\ \max_{i\in\mathcal{V}}\phi_i}\right\}. \tag{10}$$

The constraint (10) ensures that the Lyapunov function (9) is positive definite. Next, let us take the time-derivative of the Lyapunov function (9) along the trajectories of dynamics (6) with $\zeta(t) = 0$:

$$\dot{V}\big(x(t)\big) = x(t)^\top\big(A^\top\bar{P} + \bar{P}A\big)x(t) = -x(t)^\top\bar{Q}x(t), \tag{11}$$

where

$$\bar{Q} = \begin{bmatrix} 2\sigma M^{-1}\big(L+\Theta\big) & 0 & -\sigma M^{-1}\Phi \\ 0 & 2\big(M^{-1}H - \sigma I\big) & 0 \\ -\sigma M^{-1}\Phi & 0 & 2\kappa_D^{-1}M^{-1}\Phi \end{bmatrix}.$$

The constraint (10) also ensures that matrix $\bar{Q}$ is positive definite. This implies that $\dot{V}\big(x(t)\big)$ in (11) is negative definite and the matrix A in (6) is Hurwitz. ■

Lemma 1 enables us to have the following assumption.

Assumption 2. The networked control system (6) is at its equilibrium $x_e = 0$ before being attacked. ◁

Defender strategy: At the chosen detection agent $d \in \mathcal{V}_{-\rho}$, the defender employs a detector as follow:

$$\dot{\hat{x}}_d(t) = A\hat{x}_d(t) + K_d\eta_d(t), \quad \hat{x}_d(0) = 0, \tag{12}$$
$$\eta_d(t) = y_d(t) - C_d\hat{x}_d(t), \tag{13}$$

where $\hat{x}_d(t) \in \mathbb{R}^N$ is the estimated state of the networked system observed at agent d and $\eta_d(t) \in \mathbb{R}$ is the residual signal which will be used to detect cyber-attacks. Since the result in *Lemma 1* implies that (A, C_d) is detectable, matrix K_d can be suitably designed such that the matrix $\big(A - K_dC_d\big)$ is Hurwitz. Let us denote $\tilde{x}_d(t) \triangleq x(t) - \hat{x}_d(t)$ and $z_d(t) \triangleq \left[x(t)^\top,\ \tilde{x}_d(t)^\top\right]^\top$. From (6)-(8) and (12)-(13), the augmented model can be rewritten as follows:

$$\dot{z}_d(t) = A_d z_d(t) + \bar{E}_a\zeta(t), \tag{14}$$
$$y_\rho(t) = \bar{C}_\rho z_d(t), \tag{15}$$
$$\eta_d(t) = \bar{C}_d z_d(t), \tag{16}$$

where $y_\rho(t)$ and $\eta_d(t)$ are the outputs of the protected performance agent ρ and the residual signal generated by the detector placed at agent $d \in \mathcal{V}_{-\rho}$, respectively; and

$$A_d = \begin{bmatrix} A & 0 \\ 0 & A - K_dC_d \end{bmatrix},\ \bar{E}_a = \begin{bmatrix} E_a \\ E_a \end{bmatrix},$$
$$\bar{C}_\rho = \begin{bmatrix} C_\rho & 0^\top \end{bmatrix},\ \bar{C}_d = \begin{bmatrix} 0^\top & C_d \end{bmatrix}. \tag{17}$$

We suppose that the defender detects cyber-attacks if the energy of the residual signal over a given time horizon $[0, T]$ exceeds a given threshold δ, i.e., $\|\eta_d\|^2_{\mathcal{L}_2[0,T]} > \delta^2$.

Adversary strategy: The goal of the adversary is to maximally disrupt the output of the protected performance agent ρ while remaining stealthy to the detector placed at agent d. To this end, the adversary conducts the stealthy data injection attack, which is defined as follows. Consider the continuous-time system (14), (16), the attack input signal $\zeta(t)$ is called the stealthy data injection attack if the residual signal satisfies $\|\eta_d\|^2_{\mathcal{L}_2} \leq \delta^2$ where $\delta > 0$ is given and called an alarm threshold.

2.4 Worst-case attack impact on the local performance

Consider the continuous-time system (14)-(16) denoted as $\Sigma_{\rho d} \triangleq (A_d, \bar{E}_a, [\bar{C}_\rho^\top, \bar{C}_d^\top]^\top, 0)$. The malicious adversary attacks the input of the attack agent a with the purpose of maliciously maximizing impact on the output of the given performance agent ρ while remaining undetected by the defender. This adversary purpose is translated into the following non-convex optimal control problem (Teixeira, 2021, Sec. 4):

$$\gamma_\rho^\star(a,d) \triangleq \sup_{\zeta\in\mathcal{L}_{2e}, z_d(0)=0} \|y_\rho\|_{\mathcal{L}_2}^2 \quad \text{s.t.} \quad \|\eta_d\|_{\mathcal{L}_2}^2 \le \delta^2, \tag{18}$$

which has the dual problem as follows:

$$\inf_{\gamma_\rho\in\mathbb{R}_+} \Big[\sup_{\zeta\in\mathcal{L}_{2e}, z_d(0)=0} \big(\|y_\rho\|_{\mathcal{L}_2}^2 - \gamma_\rho\delta^{-2} \|\eta_d\|_{\mathcal{L}_2}^2 \big) + \gamma_\rho \Big]. \tag{19}$$

The dual problem (19) is feasible if $\|y_\rho\|_{\mathcal{L}_2}^2 - \gamma_\rho\delta^{-2} \|\eta_d\|_{\mathcal{L}_2}^2 \le 0,\ \forall\zeta \in \mathcal{L}_{2e}$ and $z_d(0) = 0$, which results in the following optimization problem:

$$\gamma_\rho^\star(a,d) \triangleq \min_{\gamma_\rho\in\mathbb{R}_+} \gamma_\rho \quad \text{s.t.} \quad \|y_\rho\|_{\mathcal{L}_2}^2 \le \gamma_\rho\delta^{-2} \|\eta_d\|_{\mathcal{L}_2}^2,\ \forall\zeta \in \mathcal{L}_{2e},\ z_d(0) = 0. \tag{20}$$

The strong duality can be proven by utilizing S-Procedure (Petersen et al., 2000, Ch .4). Recalling the key results in dissipative system theory for linear systems with quadratic supply rates (Trentelman and Willems, 1991), the constraint of (20) can be translated into a linear matrix inequality (Teixeira, 2021, Prop. 1) as follows:

$$\gamma_\rho^\star(a,d) \triangleq \min_{\gamma_\rho\in\mathbb{R}_+, F=F^\top\ge 0} \gamma_\rho \quad \text{s.t.} \quad R\big(\Sigma_{\rho d}, F, \gamma_\rho\big) \le 0, \tag{21}$$

where

$$R\big(\Sigma_{\rho d}, F, \gamma_\rho\big) \triangleq \begin{bmatrix} A_d^\top F - F A_d & F\bar{E}_a \\ \bar{E}_a^\top F & 0 \end{bmatrix} - \begin{bmatrix} \gamma_\rho\delta^{-2}\bar{C}_d\bar{C}_d^\top - \bar{C}_\rho\bar{C}_\rho^\top & 0 \\ 0 & 0 \end{bmatrix}.$$

The convex optimization problem (21) can be solved numerically efficiently to obtain the worst-case attack impact on the local performance measured at the performance agent ρ. With this worst-case attack impact, we are ready to state the following problem that will be addressed in the remainder of the paper.

Problem 1. Given a protected performance agent ρ and an arbitrary attack agent $a \in \mathcal{V}_{-\rho}$, select a detection agent $d \in \mathcal{V}_{-\rho}$ on which to place a detector that minimizes the worst-case attack impact on the performance agent ρ.

Remark 4. The two strategic players, which are the adversary and the defender, have symmetric information as described in Section 2.1. They know the action space of their competitors instead of actual actions. Therefore, we assume that the two players perform their actions based on such available information at the same time, resulting in a non-cooperative game (Başar and Olsder, 1998) which will be presented in the following section.

3. OPTIMAL DETECTOR PLACEMENT

We first present a necessary and sufficient condition for the defender to ensure that the worst-case attack impact on the local performance is bounded. This condition restricts the possible choices of the defender to a subset of available agents. Then, we translate *Problem 1* into a zero-sum game between two strategic players, namely the malicious adversary and the defender. Finally, within the framework of zero-sum games, an algorithm is proposed to find Nash equilibria that yield the best strategies for the two players.

3.1 Boundedness of the worst-case attack impact on the local performance

Let us evaluate the attack impact of the adversary through the optimization problem (18). The feasibility of the optimization problem (18) is related to invariant zeros of $\Sigma_\rho = \big(A_d, \bar{E}_a, \bar{C}_\rho, 0\big)$ and $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$, which are defined as follows.

Definition 1. (Invariant zeros) Consider the strictly proper system $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$ with $\bar{A}$, $\bar{B}$, and $\bar{C}$ are real matrices with appropriate dimensions. A tuple $(\bar{\lambda}, \bar{x}, \bar{g}) \in \mathbb{C}\times\mathbb{C}^N \times \mathbb{C}$ is a zero dynamics of Σ if it satisfies

$$\begin{bmatrix} \lambda I - \bar{A} & -\bar{B} \\ \bar{C} & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ \bar{g} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \ne 0. \tag{22}$$

In this case, a finite $\bar{\lambda}$ is called a finite invariant zero of $\bar{\Sigma}$. Further, the strictly proper system $\bar{\Sigma}$ always has at least one invariant zero at infinity (Franklin et al., 2002). ◁

More specifically, let us state the following lemma.

Lemma 2. (Teixeira et al., 2015a, Th. 2) Consider the two following continuous time systems $\Sigma_\rho = \big(A_d, \bar{E}_a, \bar{C}_\rho, 0\big)$ and $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$. The optimization problem (18) is feasible if and only if the unstable invariant zeros of Σ_d are also invariant zeros of Σ_ρ. ◁

Inspired by the result in *Lemma 2* and the definition of invariant zeros in *Definition 1*, we will investigate both finite and infinite invariant zeros of the two systems Σ_d and Σ_ρ.

Finite invariant zeros: Let us state the following lemma that considers the finite invariant zeros.

Lemma 3. Consider the system $\Sigma_m = (A, E_a, C_d, 0)$ defined in (6), (7) and, for $\lambda_d \in \mathbb{C}$, define

$$\mathcal{Q}(\lambda_d) = L + \Theta + \lambda_d^2 M + \lambda_d H + \frac{\lambda_d\kappa_D}{\tau\lambda_d + 1}\Phi. \tag{23}$$

The system Σ_m has a finite zero at $\lambda_d \in \mathbb{C}$ if, and only if, $\mathcal{Q}(\lambda_d)$ is non-singular and $e_d^\top \mathcal{Q}(\lambda_d)^{-1} e_a = 0$ ◁

Proof. The proof is postponed to Appendix A. ■

The above result establishes the equivalence between the existence of an invariant zero of Σ_m at $\lambda_d \in \mathbb{C}$ and the matrix $\mathcal{Q}(\lambda_d)^{-1}$ having a zero at the entry $\big[\mathcal{Q}(\lambda_d)^{-1}\big]_{da}$. Next, we leverage this result to show that the detector $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$ has no unstable zero on the real line.

Lemma 4. Consider system dynamics (14),(16) represented by $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$ and assume that $\mathcal{G}$ is an undirected connected graph. Then, for any choice of attack agent $a \in \mathcal{V}_{-\rho}$ and detection agent $d \in \mathcal{V}_{-\rho}$, the corresponding system Σ_d has no finite invariant zero on the positive real line. ◁

Proof. The proof is postponed to Appendix B. ■

Unfortunately, the result in *Lemma 4* cannot be directly extended to consider complex invariant zeros on the right half-plane. The extension on how to deal with complex invariant zeros is left for future work. In the remainder of the paper, we assume that the system Σ_d has no finite, complex unstable zeros.

Infinite invariant zeros: We now investigate the infinite invariant zeros of the systems Σ_ρ and Σ_d. In the investigation, we make use of known results connecting infinite invariant zeros and the relative degree (see Khalil (2002, Ch. 13)) of a linear system. Let us denote $r_{(\rho,a)}$ and $r_{(d,a)}$ as the relative degrees of Σ_ρ and Σ_d, respectively. By following our existing result related to those infinite zeros (Nguyen et al., 2022, Th. 7), the infinite zeros of Σ_d are also the infinite zeros of Σ_ρ if and only if the following condition holds

$$r_{(d,a)} \leq r_{(\rho,a)}. \tag{24}$$

The following theorem presents the necessary and sufficient condition which ensures that the optimization problem (18) admits a finite solution.

Theorem 3.1. Consider a networked control system associated with an undirected connected graph $\mathcal{G} = \big(\mathcal{V}, \mathcal{E}, \mathcal{A}\big)$ and two continuous-time systems $\Sigma_\rho = \big(A_d, \bar{E}_a, \bar{C}_\rho, 0\big)$ and $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$. Suppose Σ_ρ and Σ_d have relative degrees $r_{(\rho,a)}$ and $r_{(d,a)}$, respectively. The optimization problem (18) admits a finite solution if, and only if, the condition (24) holds and the parameters $\theta_i,\ \phi_i,\ \kappa_D,$ and $\tau \in \mathbb{R}_+$ are such that, for every $\lambda_d \in \mathbb{C}$ on the right half plane, the matrix $\mathcal{Q}(\lambda_d)^{-1}$ has no zero entries. ◁

Proof. Following from *Lemma 3*, a suitable choice of parameters $\theta_i,\ \phi_i,\ \kappa_D,$ and $\tau \in \mathbb{R}_+$ ensures that the system Σ_d has no finite unstable zero for any choice of a and d if, and only if, the matrix $\mathcal{Q}(\lambda_d)^{-1}$ has no zero entries for every $\lambda_d \in \mathbb{C}$ on the right half plane. This result and the condition (24) fulfill the necessary and sufficient condition in *Lemma 2* which guarantees that the optimization problem (18) admits a finite solution. ■

For every arbitrary attack agent $a \in \mathcal{V}_{-\rho}$, let us define the detection set $\mathcal{D} \subseteq \mathcal{V}_{-\rho}$ containing agents which satisfy the necessary and sufficient condition in *Theorem 3.1*. The possible action set of the defender will be restricted to the detection set $\mathcal{D}$.

Assumption 3. The detection set $\mathcal{D}$ is not empty, i.e., $\mathcal{D} = \{d_1, d_2, \ldots, d_{|\mathcal{D}|}\}$ where $|\mathcal{D}| \geq 1$. ◁

Assumption 3 enables the defender to optimally select an agent on which to place the observer (12)-(13) with the purpose of detecting the cyber-attack conducted by the adversary. How the defender selects the optimal detector placement will be addressed by a game-theoretic approach, which has been widely used in Pirani et al. (2021); Van Nguyen and Ahn (2018), in the next subsection.

Remark 5. To compute a detection set $\mathcal{D}$ for a given undirected connected graph $\mathcal{G}$, we can utilize an undirected unweighted graph $\mathcal{G}'$ such that $\mathcal{G}$ and $\mathcal{G}'$ have the same topology. Through the graph $\mathcal{G}'$, we adopt the result in Nguyen et al. (2022, Lem. 8) to characterize candidate detection agents that fulfill the condition (24) for every attack agent $a \in \mathcal{V}_{-\rho}$. Such found agents also satisfy the condition (24) for every attack agent $a \in \mathcal{V}_{-\rho}$ in case we consider $\mathcal{G}$.

3.2 Game-theoretic approach to optimal detector placement

According to *Theorem 3.1*, since the optimization problem (18) is feasible for all the possible choices of the attack agent $a \in \mathcal{V}_{-\rho}$ and the detection agent $d \in \mathcal{D}$, we employ the worst-case attack impact (18) as a game payoff that enables us to translate *Problem 1* into a zero-sum game between the malicious adversary and the defender. While the adversary wants to maximize the game payoff, the defender desires to minimize the same game payoff, i.e., *Problem 1* is represented as follows

$$\max_{a \in \mathcal{V}_{-\rho}} \ \min_{d \in \mathcal{D}} \ \gamma_\rho^\star(a,d) < \infty. \tag{25}$$

For every pair of an attack agent $a \in \mathcal{V}_{-\rho}$ and a detection agent $d \in \mathcal{D}$, we find the corresponding game payoff $\gamma_\rho^\star(a,d)$ by solving the convex optimization problem (21). Then, the existence of a pure Nash equilibrium $(a^\star, d^\star)$ is equivalent to concluding that the following equality holds

$$\min_{d_i \in \mathcal{D}} \big[\alpha_i\big] = \max_{a_i \in \mathcal{V}_{-\rho}} \big[\beta_i\big], \tag{26}$$

where $\alpha_i = \max_{a_j \in \mathcal{V}_{-\rho}} \gamma_\rho^\star(a_j, d_i)$; $\beta_i = \min_{d_j \in \mathcal{D}} \gamma_\rho^\star(a_i, d_j)$. The pure optimal detector placement at the detection agent $d_i^\star$ has the same index i with $\alpha_i^\star$ where

$$\alpha_i^\star = \arg\min_{d_i \in \mathcal{D}} \ \big[\alpha_i\big]. \tag{27}$$

The failure of the condition (26) implies that no pure Nash equilibrium exists (Zhu and Basar, 2015). However, the game always admits a mixed-strategy Nash equilibrium which will be computed in the remainder of this section.

Let us denote the probability of an agent $a \in \mathcal{V}_{-\rho}$ that is attacked by the adversary as $\mathfrak{p}_a \in \mathbb{R}_{[0;1]}$; the probability of an agent $d \in \mathcal{D}$ that is employed to implement the detector (12)-(13) by the defender as $\mathfrak{q}_d \in \mathbb{R}_{[0;1]}$; vectors $P = [\mathfrak{p}_i]$ and $Q = [\mathfrak{q}_i]$. According to Zhu and Basar (2015), the optimal mixed-strategy $(P^\star, Q^\star)$ of the adversary and the defender can be found as follows:

$$J_\rho^\star(P^\star, Q^\star) = \min_P \ \max_Q \ \sum_{a \in \mathcal{V}_{-\rho}} \ \sum_{d \in \mathcal{D}} \mathfrak{p}_a \gamma_p^\star(a,d) \mathfrak{q}_d, \tag{28}$$
$$\text{s.t.} \sum_{a \in \mathcal{V}_{-\rho}} \mathfrak{p}_a = 1, \quad \sum_{d \in \mathcal{D}} \mathfrak{q}_d = 1,$$

Inspired by Boyd et al. (2004, Ch. 5), the min-max optimization problem (28) can be efficiently solved by linear programming. Let us summarize the procedure how to determine the optimal detector placement in *Algorithm 1*. In the following section, we will demonstrate our proposed *Algorithm 1* in a case study of power systems.

Algorithm 1 Optimal detector placement

Input: possible detection set $\mathcal{D}$ and attack set $\mathcal{V}_{-\rho}$.
Output: optimal detector placement
1: For every pair of $a \in \mathcal{V}_{-\rho}$ and $d \in \mathcal{D}$, solve (21) to obtain the corresponding game payoff $\gamma_\rho^\star(a,d)$.
2: **if** condition (26) is fulfilled **then**
return a pure detector placement at $d_i^\star$ where its index i is determined by (27).
3: **else** solve (28) to obtain $P^\star$ and $Q^\star$
return a mixed-strategy optimal detector placement represented by $Q^\star$.
4: **end if**

4. A CASE STUDY

In this section, we demonstrate our obtained results via the IEEE 14-bus system (Fig. 2). The system includes 14

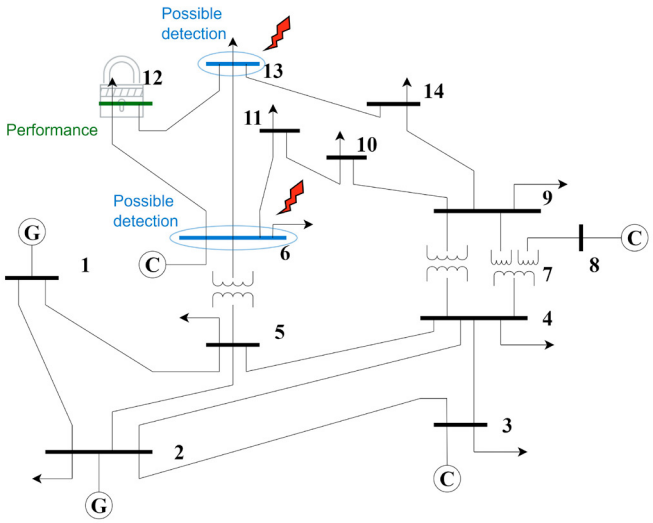

Fig. 2. IEEE 14-bus system where bus 12 (green) is the protected performance bus, buses 6 and 13 (blue) are possible detection buses. Buses 6 (56.2%) and 13 (43.8%) are possibly attacked.

buses and 20 transmission lines. The behavior of a bus $i \in \{1, 2, \ldots, 14\}$ can be described by the so-called swing equation (Tegling, 2018):

$$m_i\ddot{p}_i + h_i\dot{p}_i - \tilde{u}_i(t) = -\sum_{j\in\mathcal{N}_i} Po_{ij}, \tag{29}$$

where m_i and h_i are the inertia and damping coefficients, respectively, $\tilde{u}_i(t)$ is the healthy/attacked mechanical input power and Po_{ij} is the active power flow from bus j to bus i. Considering that there are no power losses and $V_i = |V_i|e^{jp_i}$ ($j^2 = -1$) and p_i be the complex voltage and the phase angle of the bus i, respectively. The active power flow Po_{ij} from bus j to bus i is given by

$$Po_{ij} = -\ell_{ij}\sin(p_i - p_j), \tag{30}$$

where $-\ell_{ij} \in \mathbb{R}_+$ is the susceptance of the power transmission line connecting bus i with bus j. Those parameters consisting of line susceptance $-\ell_{ij}$, inertia m_i, and damping h_i can be found at UW-EE (1993). Since the phase angles usually are close, we can linearize (30) and rewrite the dynamics (29) of bus i as follows

$$m_i\ddot{p}_i + h_i\dot{p}_i = \sum_{j\in\mathcal{N}_i} \ell_{ij}\Big(p_i(t) - p_j(t)\Big) + \tilde{u}_i(t), \tag{31}$$

which is equivalent to the ones in (1)-(3) we investigated in the previous sections. Suppose that the mechanic power input $\tilde{u}_i(t)$ coincides with the one in (4)-(5).

Next, we present numerical results by using *Algorithm 1*. Suppose that bus 12 (coded green) is the protected performance bus. The certain alarm threshold is selected as $\delta^2 = 2.6$. Recalling *Remark 5*, we characterize the possible detection set $\mathcal{D} = \{6, 13\}$ containing buses that fulfill the condition (24). The control parameters are selected as follows: $\theta_i = 1.5$, $\phi_i = 2.2$, $\kappa_d = 2$, and $\tau = 0.4$ $\forall i \in \mathcal{V}$. Those control parameters fulfill the necessary and sufficient condition in *Theorem 3.1* to ensure that the game payoff is bounded. At the *step 1* of *Algorithm 1*, for every pair of $a \in \mathcal{V}_{-\rho}$ and $d \in \mathcal{D}$, we solve (21) by using CVX (Grant and Boyd, 2014) to obtain the following result: $\alpha = \big[4.7449,\ 4.3917\big]$ and $\beta = \big[2.4494,\ 2.5561,\ 2.6185,\ 2.5585,\ 2.4198,\ 2.3087,\ 2.5199,\ 2.5257,\ 2.4695,\ 2.4673,\ 2.3705,\ 2.0717,\ 2.2119\big]$. At the *step 2* of *Algorithm 1*, since $4.3917 = \min[\alpha_i] \neq \max[\beta_i] = 2.6185$, the condition (26) fails, implying that the zero-sum game does not admit a pure Nash equilibrium. Then, we move to the *step 3* to find a mixed-strategy $J_\rho^\star(P^\star, Q^\star) = 3.3757$ at $\mathfrak{p}_6^\star = 0.562$, $\mathfrak{p}_{13}^\star = 0.438$, $\mathfrak{p}_{i\in\mathcal{V}\setminus\{6,\ 12,\ 13\}}^\star = 0$, $\mathfrak{q}_6^\star = 0.4878$, and $\mathfrak{q}_{13}^\star = 0.5122$.

Let us assume that the defender places a detector at the local controller of bus 13 and the adversary conducts the stealthy data injection attack on the input of bus 6. By observing the output energy of the detection bus 13 in Fig. 3a which is under the certain threshold δ^2, the attack signal in Fig. 3b is stealthy to the detector placed at bus 13. However, the adversary only causes a bounded malicious attack impact on the output energy of the local performance bus 12 (see Fig. 3a). The adversary cannot increase the amplitude of the attack signal to gain its attack impact on the output energy of the performance bus 12 since the energy output of the detection bus 13 crosses the certain threshold $\delta^2 = 2.6$, which enables the defender to detect the cyber-attack.

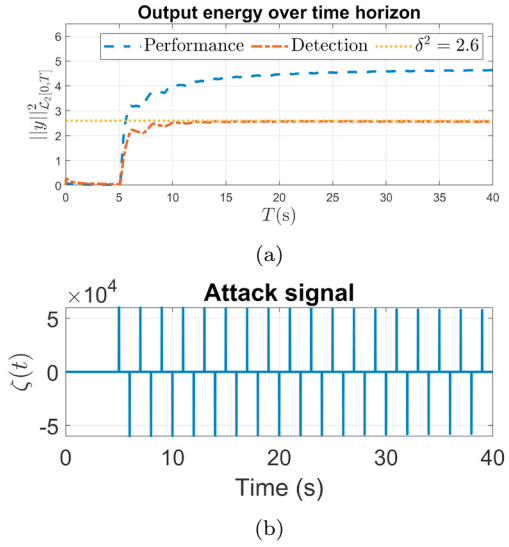

Fig. 3. (a) Output energy of the performance bus 12 and the detection bus 13; (b) Attack signal $\zeta(t)$ conducted on the input of bus 6.

5. CONCLUSIONS

In this paper, we addressed the problem of optimal detector placement in a networked control system under cyber-attacks. First, we presented the necessary and sufficient condition, which is related to the suitable choice of control parameters and the relative degree of dynamic systems, to ensure that the worst-case attack impact on the local performance is bounded. This condition restricts possible detection agents to a subset of available agents. Then, the problem of optimal detector placement was formulated as a zero-sum game between the defender and the adversary where the game payoff was represented by the bounded worst-case attack impact on the local performance. Finally,

an algorithm was devoted to finding the optimal detector placement. The obtained results were illustrated by an actual case study of power systems, namely the IEEE 14-bus system.

APPENDIX A: PROOF OF LEMMA 3

Let us denote a tuple $\big(\lambda_d, \bar{x}_d, g_d\big) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}$ as a zero dynamics of Σ_m where λ_d is a finite invariant zero of Σ_m and $\bar{x}_d = \big[\nu_1^\top, \nu_2^\top, \nu_3^\top\big]^\top$ where $\nu_1, \nu_2, \nu_3 \in \mathbb{C}^N$. From the condition (22) in *Definition 1*, $\big(\lambda_d, \bar{x}_d, g_d\big)$ of Σ_m satisfies

$$\left[\begin{array}{c|c|c|c} \lambda_d I & -I & 0 & 0 \\ M^{-1}\big(L+\Theta\big) & \lambda I + M^{-1}H & -M^{-1}\Phi & e_a \\ 0 & \frac{\kappa_D}{\tau} I & \Big(\lambda + \frac{1}{\tau}\Big) I & 0 \\ e_d^\top & 0 & 0 & 0 \end{array}\right] \left[\begin{array}{c} \nu_1 \\ \nu_2 \\ \nu_3 \\ \bar{g} \end{array}\right] = 0.$$

Solving the above system of equations partially for ν_3 and ν_2, as functions of ν_1, and then for ν_1 as a function of $\bar{g}$ gives us the remaining equation

$$e_d^\top M \mathcal{Q}(\lambda_d)^{-1} \frac{\lambda_d \kappa_D}{\tau \lambda_d + 1} e_a \bar{g} = 0, \tag{32}$$

$$\mathcal{Q}(\lambda_d) = L + \Theta + \lambda_d^2 M + \lambda_d H + \frac{\lambda_d \kappa_D}{\tau \lambda_d + 1} \Phi.$$

From (32), given the positivity of the parameters θ_i, ϕ_i, κ_D, and $\tau \in \mathbb{R}_+$, it follows that $\big(\lambda_d, \bar{x}_d, g_d\big) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}$ is a zero dynamics of Σ_m with $\bar{g} \neq 0$ if, and only if, $e_d^\top M \mathcal{Q}(\lambda_d)^{-1} e_a = \big[\mathcal{Q}(\lambda_d)^{-1}\big]_{da} = 0$ where matrix M is a diagonal positive definite matrix.

APPENDIX B: PROOF OF LEMMA 4

Let us consider the continuous-time systems $\Sigma_{mo} = \big(A - K_d C_d, E_a, C_d, 0\big)$, $\Sigma_m = \big(A, E_a, C_d, 0\big)$, and $\Sigma_o = \big(A - K_d C_d, K_d, -C_d, 1\big)$. From the condition (22) and the structure of matrices (17), the set of invariant zeros of the system Σ_d is the union of the set of eigenvalues of matrix A and the set of invariant zeros of the system Σ_{mo}. Thanks to *Lemma 1*, all the eigenvalues of matrix A is stable. It remains to investigate invariant zeros of the system Σ_{mo}. On the other hand, we have the set of invariant zeros of the Σ_{mo} is contained by the union of the set of invariant zeros of Σ_o and the set of invariant zeros of Σ_m. By following *Definition 1*, the condition (22) gives us that the invariant zeros of the system Σ_o coincides with eigenvalues of matrix A in (6), which are stable, no matter how the matrix K_d in the observer (12) is designed. In the end, we only need to investigate invariant zeros of Σ_m. The proof follows from a contradiction argument. Let us denote a tuple $\big(\lambda_d, \bar{x}_d, g_d\big) \in \mathbb{C} \times \mathbb{C}^{3N} \times \mathbb{C}$ as a zero dynamics of Σ_m where λ_d is assumed to be real and positive.

For every real positive value λ_d, the matrix $\mathcal{Q}(\lambda_d)$ in (23) is positive definite, yielding that $\mathcal{Q}(\lambda_d)$ is non-singular and $-\mathcal{Q}(\lambda_d)$ is Hurwitz. Further, since matrix $\mathcal{Q}(\lambda_d)$ represents a strongly connected graph $\mathcal{G}$ with added self-loops, it is irreducible (Horn and Johnson, 2012, Ch. 6). Obviously, $-\mathcal{Q}(\lambda_d)$ is also a Metzler matrix. According to Bullo (2019, Th. 10.3), $\mathcal{Q}(\lambda_d)^{-1}$ is a positive matrix whose all entries are real positive, that is, $\big[\mathcal{Q}(\lambda_d)^{-1}\big]_{da} > 0$ for all vertices d and a. Following the result of *Lemma 3*, we conclude that a real positive value λ_d cannot be a zero of the system Σ_m, thus concluding the proof.

REFERENCES

Başar, T. and Olsder, G.J. (1998). *Dynamic noncooperative game theory*. SIAM.

Boyd, S., Boyd, S.P., and Vandenberghe, L. (2004). *Convex optimization*. Cambridge University Press.

Bullo, F. (2019). *Lectures on network systems*, volume 1. Kindle Direct Publishing Santa Barbara, CA.

Falliere, N., Murchu, L.O., and Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6), 29.

Franklin, G.F., Powell, J.D., Emami-Naeini, A., and Powell, J.D. (2002). *Feedback control of dynamic systems*, volume 4. Prentice hall Upper Saddle River, NJ.

Grant, M. and Boyd, S. (2014). Cvx: Matlab software for disciplined convex programming, version 2.1.

Horn, R.A. and Johnson, C.R. (2012). *Matrix analysis*. Cambridge University Press.

Khalil, H.K. (2002). *Nonlinear systems third edition*, volume 115. Patience Hall.

Kshetri, N. and Voas, J. (2017). Hacking power grids: A current problem. *Computer*, 50(12), 91–95.

Nguyen, A.T., Teixeira, A.M.H., and Medvedev, A. (2022). A single-adversary-single-detector zero-sum game in networked control systems. *IFAC-PapersOnLine*, 55(13), 49–54.

Petersen, I.R., Ugrinovskii, V.A., and Savkin, A.V. (2000). *Robust control design using H-8 methods*. Springer Science & Business Media.

Pirani, M., Nekouei, E., Sandberg, H., and Johansson, K.H. (2021). A game-theoretic framework for security-aware sensor placement problem in networked control systems. *IEEE Transactions on Automatic Control*, 67(7), 3699–3706.

Tegling, E. (2018). *Fundamental limitations of distributed feedback control in large-scale networks*. Ph.D. thesis, KTH Royal Institute of Technology.

Teixeira, A., Sandberg, H., and Johansson, K.H. (2015a). Strategic stealthy attacks: the output-to-output ℓ_2-gain. In *2015 54th IEEE Conference on Decision and Control (CDC)*, 2582–2587. IEEE.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K.H. (2015b). A secure control framework for resource-limited adversaries. *Automatica*, 51, 135–148.

Teixeira, A.M.H. (2021). Security metrics for control systems. In *Safety, Security and Privacy for Cyber-Physical Systems*, 99–121. Springer.

Trentelman, H.L. and Willems, J.C. (1991). *The dissipation inequality and the algebraic Riccati equation*. Springer.

UW-EE (1993). Ieee 14-bus test case. URL `labs.ece.uw.edu/pstca/pf14/ieee14cdf.txt`.

Van Nguyen, C. and Ahn, H.S. (2018). Distributed solving exact potential games via differential inclusions and consensus algorithms. In *2018 IEEE Conference on Decision and Control (CDC)*, 4212–4217. IEEE.

Zhu, Q. and Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, 35(1), 46–65.