A Single-Adversary-Single-Detector Zero-Sum Game in Networked Control Systems *

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

*Department of Information Technology, Uppsala University,
PO Box 337, SE-751 05, Uppsala, Sweden
(e-mail: {anh.tung.nguyen, andre.teixeira,
alexander.medvedev}@it.uu.se).*

Abstract: This paper proposes a game-theoretic approach to address the problem of optimal sensor placement for detecting cyber-attacks in networked control systems. The problem is formulated as a zero-sum game with two players, namely a malicious adversary and a detector. Given a protected target vertex, the detector places a sensor at a single vertex to monitor the system and detect the presence of the adversary. On the other hand, the adversary selects a single vertex through which to conduct a cyber-attack that maximally disrupts the target vertex while remaining undetected by the detector. As our first contribution, for a given pair of attack and monitor vertices and a known target vertex, the game payoff function is defined as the output-to-output gain of the respective system. Then, the paper characterizes the set of feasible actions by the detector that ensures bounded values of the game payoff. Finally, an algebraic sufficient condition is proposed to examine whether a given vertex belongs to the set of feasible monitor vertices. The optimal sensor placement is then determined by computing the mixed-strategy Nash equilibrium of the zero-sum game through linear programming. The approach is illustrated via a numerical example of a 10-vertex networked control system with a given target vertex.

Keywords: Cyber-physical security, networked control systems, game theory.

1. INTRODUCTION

The notion of networked control systems has gained popularity in modeling and analysis of real-world large-scale interconnected systems such as power systems, transportation networks, and water distribution networks. Networked control systems, generally employing non-proprietary and pervasive communication and information technology, such as the Internet and wireless communications, may leave the systems vulnerable to cyber-attacks (Teixeira et al., 2015b) and inflict significant financial and societal costs. Reports on Stuxnet (Falliere et al., 2011), for example, have shown the devastating consequences of this malicious software attack on the nuclear program of Iran. Motivated by the above observations, cyber-physical security has become an increasingly important aspect of control systems in recent years.

This study considers a continuous-time networked control system under attack with two strategic agents: a malicious adversary and a detector. The system consists of multiple one-dimensional subsystems, so-called vertices, in which there exists a single protected target vertex. The purpose of the adversary is to affect the output of the target vertex without being detected. To this end, the adversary chooses

one vertex to attack and directly injects attack signals into its input. Meanwhile, the detector chooses one monitor vertex and measures its output, with the aim of unmasking the presence of the adversary. Assuming both agents to be strategic, we investigate the optimal selection of the monitor vertex through a game-theoretic approach. Fig. 1 visualizes the above-defined game in a networked control system.

The game-theoretic approach has been successfully applied to tackle the problem of robustness, security, and resilience of cyber-physical systems (Zhu and Basar, 2015). It allows us to deal with the robustness and security of cyber-physical systems within the common well-defined framework of $\mathcal{H}_\infty$ robust control design. Further, many other concepts of games describing networked systems subjected to cyber-attacks such as dynamic games (Gupta et al., 2016) and stochastic games (Miao et al., 2018) have been recently studied.

Although the above games were successful in studying control systems subjected to cyber-attacks such as denial-of-service attacks, changing the locations of detectors to increase the detection of such cyber-attacks was not considered. To address this gap, Pirani et al. (2021) consider a game-theoretic formulation where the defender chooses the location of sensors in a networked system, to protect against an adversary that aims at maximally
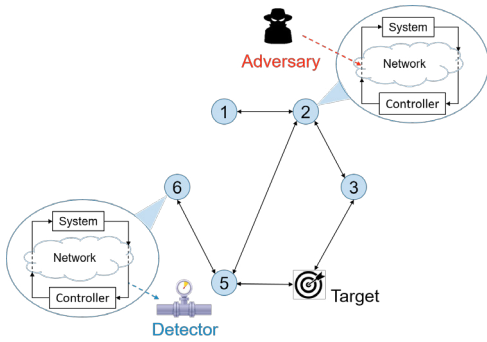
Fig. 1. Visualisation of a single-adversary-single-detection zero-sum game in a networked control system.

disrupting the system while remaining undetected. The game payoff in Pirani et al. (2021) has been formulated by combining the maximum $\mathcal{L}_2$ gains of multiple outputs w.r.t. a single input representing the attack signal. On the one hand, these multiple $\mathcal{L}_2$ gains are evaluated separately and thus may be attained for different optimal input signals, possibly resulting in pessimistic payoffs that cannot be attained by any admissible input signal. On the other hand, the use of a maximum gain for characterizing detectability corresponds to an optimistic perspective, where the adversary attempts to maximize the energy of the detection output, instead of the opposite.

In this paper, we consider a game-theoretic approach that is inspired and related to the one in Pirani et al. (2021). However, to address the above-mentioned limitations, we invoke the output-to-output gain (OOG) proposed in Teixeira et al. (2015a); Teixeira (2021) as the game payoff for the adversary and the detector. This game payoff affords us to fully explore the cyber-attack impact on the monitor and the target outputs simultaneously with a single input signal. As our main contributions, we cast the optimal selection of a monitor vertex as a zero-sum game and investigate the existence of a set of feasible monitor vertices that, if selected, result in a bounded game-payoff. We show that the existence of such a set is related to the system-theoretic properties of the underlying dynamical system, namely its relative degrees. Then, we propose an algebraic condition to characterize the set of feasible monitor vertices that guarantee a bounded game payoff for any attack vertex. Finally, a numerical example is given to demonstrate the effectiveness of the proposed approach. Further, a mixed-strategy Nash equilibrium of the game is also investigated in a simulation example.

We conclude this section by providing the notation to be used throughout this paper. The problem formulation is introduced in Section 2. Thereafter, Section 3 investigates and characterizes the set of feasible monitor vertices through the system-theoretic properties of the system. Section 4 presents a numerical example of the zero-sum game between an adversary and a detector and computes the optimal monitor selection based on a mixed-strategy Nash equilibrium. Section 5 concludes the paper.

Notation: the set of real positive numbers is denoted as $\mathbb{R}_+$; $\mathbb{R}^n$ and $\mathbb{R}^{n\times m}$ stand for sets of real n-dimensional vectors and n-row m-column matrices, respectively. Let us define $e_i \in \mathbb{R}^n$ with all zero elements except the i-th

element is set as 1. A continuous-time system with the state-space model $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$ is denoted as $\Sigma \triangleq (A, B, C, D)$. Consider the norm $\|x\|_{\mathcal{L}_2[0,T]}^2 \triangleq \int_0^T \|x(t)\|_2^2 \, dt$. The space of square-integrable functions is defined as $\mathcal{L}_2 \triangleq \big\{ f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|_{\mathcal{L}_2[0,\infty]} < \infty \big\}$ and the extended space be defined as $\mathcal{L}_{2e} \triangleq \big\{ f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|_{\mathcal{L}_2[0,T]} < \infty, \ \forall \ 0 < T < \infty \big\}$. Let $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$ be a digraph with the set of N vertices $\mathcal{V} = \{v_1, v_2, ..., v_N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, and the adjacency matrix $A = [a_{ij}]$. For any $(v_i, v_j) \in \mathcal{E}$, $i \neq j$, the element of the adjacency matrix a_{ij} is positive, and with $(v_i, v_j) \notin \mathcal{E}$ or $i = j$, $a_{ij} = 0$. The degree of vertex v_i is denoted as $d_i = \sum_{j=1}^n a_{ij}$ and the degree matrix of graph $\mathcal{G}$ is defined as $D = \mathbf{diag}(d_1, d_2, \ldots, d_N)$, where $\mathbf{diag}$ stands for a diagonal matrix. The Laplacian matrix is defined as $L = [\ell_{ij}] = D - A$. Further, $\mathcal{G}$ is called an undirected graph if A is symmetric. An edge of an undirected graph $\mathcal{G}$ is denoted by a pair $(v_i, v_j) \in \mathcal{E}$. An undirected graph is connected if for any pair of vertices there exists at least one path between two vertices. The set of all neighbours of vertex v_i is denoted as $\mathcal{N}_i = \{v_j \in \mathcal{V} : (v_i, v_j) \in \mathcal{E}\}$.

2. PROBLEM FORMULATION

This section consists of three subsections. Firstly, the networked control system in the presence of a cyber-attack is defined. Then, we introduce the optimal stealthy data injection attack which will be studied throughout the paper. The last subsection describes our game-theoretic approach to select feasible monitor vertices.

2.1 Networked control system under attack

Consider a connected undirected network $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with N vertices, the state-space model of a one-dimensional vertex v_i is described:

$$\dot{x}_i(t) = u_i(t), \quad i \in \{1, \, 2, \ldots, \, N\}, \tag{1}$$

where $x_i(t) \in \mathbb{R}$ is the state of vertex v_i. Due to the fact that states of all the vertices are not always available, we employ the widely-used displacement-based control law for networked control systems:

$$u_i(t) = \sum_{j \in \mathcal{N}_i} \big(x_j(t) - x_i(t)\big). \tag{2}$$

For convenience, let us denote $x(t)$ as the state of the networked control system, $x(t) = \big[x_1(t), \, x_2(t), \ldots, \, x_N(t)\big]^\top$. In our setup, the adversary conducts time-dependent malicious action $a(t) \in \mathbb{R}$ at the input of vertex v_a:

$$u_a(t) = \sum_{j \in \mathcal{N}_a} \big(x_j(t) - x_a(t)\big) + a(t). \tag{3}$$

The purpose of the adversary is to manipulate the output of a given target vertex v_τ. On the other hand, the detector places a sensor at the output of vertex v_m to monitor attack signals. The system model (1) under the control law (2) can be rewritten in the presence of attack signals at the vertex v_a (3) with two outputs observed at the two vertices v_τ and v_m:

$$\dot{x}(t) = -Lx(t) + e_a a(t), \tag{4}$$

$$y_\tau(t) = e_\tau^\top x(t), \tag{5}$$

$$y_m(t) = e_m^\top x(t). \tag{6}$$

In the scope of this study, we mainly focus on the stealthy data injection attack. This attack will be defined as follows. Consider the above structure of the continuous-time system (4)-(6), which we denote as $\Sigma_{\tau,m} \triangleq (-L, e_a, [e_\tau, e_m]^\top, 0)$, with target output $y_\tau(t) = e_\tau^\top x(t)$ and monitor output $y_m(t) = e_m^\top x(t)$. The input signal $a(t)$ of the system $\Sigma_{\tau,m}$ is called the stealthy data injection attack if the monitor output satisfies $\|y_m\|_{\mathcal{L}_2[0,T]}^2 < \delta$, in which $\delta > 0$ is called an alarm threshold. Further, the impact of the stealthy data injection attack is measured via the energy of the target output over the horizon $[0, T]$, i.e., $\|y_\tau\|_{\mathcal{L}_2[0,T]}^2$. Without loss of generality, let us set the alarm threshold $\delta = 1$ in the remainder of this study.

The worst-case impact of the stealthy data injection attack will be further investigated in the next subsection.

2.2 Optimal stealthy data injection attack

The adversary attacks vertex v_a with the objective of maximizing impact on the output of the target vertex v_τ while remaining undetected at the monitor vertex v_m, which can be formulated as the following non-convex optimal control problem (Teixeira, 2021):

$$J_\tau(v_a, v_m) \triangleq \sup_{a \in \mathcal{L}_{2e},\ x(0)=0} \|y_\tau\|_{\mathcal{L}_2}^2 \qquad (7)$$
$$\text{s.t.} \quad \|y_m\|_{\mathcal{L}_2}^2 \leq 1.$$

Following the details in Teixeira (2021), the above optimal control problem can be equivalently rewritten as the following optimization problem

$$J_\tau(v_a, v_m) \triangleq \min_{\gamma \in \mathbb{R}_+} \gamma \qquad (8)$$
$$\text{s.t.} \quad \|y_\tau\|_{\mathcal{L}_2}^2 \leq \gamma \|y_m\|_{\mathcal{L}_2}^2, \quad \forall\, a \in \mathcal{L}_{2e},$$
$$x(0) = 0,$$

where the constraint may in turn be replaced with a convex Linear Matrix Inequality (Teixeira (2021, Ch. 6.4) and references therein), yielding a convex optimization problem that computes $J_\tau(v_a, v_m)$.

Remark 1. With a similar scenario, another objective function based on $\mathcal{L}_2$-gain for the adversary and the detector has been proposed in Pirani et al. (2021, Sec. 3). The objective function in Pirani et al. (2021) was formulated in terms of the maximal $\mathcal{L}_2$-gains from the attack to the target vertices and from the attack to monitor vertices. More specifically, the objective function in Pirani et al. (2021) is given by

$$G_\tau(v_a, v_m) = \sup_{\|a\|_{\mathcal{L}_2} \neq 0} \frac{\|y_\tau\|_{\mathcal{L}_2}^2}{\|a\|_{\mathcal{L}_2}^2} - \lambda \sup_{\|a\|_{\mathcal{L}_2} \neq 0} \frac{\|y_m\|_{\mathcal{L}_2}^2}{\|a\|_{\mathcal{L}_2}^2}, \ (\lambda \geq 0).$$

The above objective in Pirani et al. (2021) also considers two different outputs $y_\tau(t)$ and $y_m(t)$, but note that the output energies are maximized separately, thus leading to two different optimal input signals $a(t)$ in the general case. By contrast, our objective function (8) investigates the worst-case attack impact that is simultaneously characterized by the two outputs $y_\tau(t)$ and $y_m(t)$ w.r.t. a single input signal $a(t)$.

Next, we tackle the problem of the optimal selection of a monitor vertex through a game-theoretic approach.

2.3 Game-theoretic approach to monitor vertex selection

To defend against adversaries, we consider that the detector tackles the following problem.

Problem 1. (Optimal monitor selection) Given a target vertex and an arbitrary attack vertex, select a monitor vertex that minimizes the worst-case impact of the stealthy data injection attack at the attack vertex.

As the attack vertex is arbitrary, we formulate Problem 1 as a game between the detector and adversary, where the players choose v_a and v_m to respectively maximize and minimize the function $J_\tau(v_a, v_m)$ described in (8). Hence, Problem 1 is formalized as a zero-sum game with $J_\tau(v_a, v_m)$ as the game-payoff, namely

$$\min_{v_m \neq v_\tau \in \mathcal{V}} \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m). \qquad (9)$$

While Problem 1 investigates an optimal selection of the monitor vertex, there is no *a priori* guarantee that a suitable monitor vertex exists for which (9) is bounded from above. The following Problem raises a question of finding feasible monitor vertices such that the worst-case impact of the stealthy data injection attack is bounded.

Problem 2. (Feasible monitor vertices) Given a target vertex and an arbitrary attack vertex, find a set of feasible monitor vertices such that the worst-case impact of the stealthy data injection attack is bounded.

Formally, a set of feasible monitor vertices w.r.t. the target vertex v_τ is defined as $\mathcal{M}_\tau \triangleq \{v_m \neq v_\tau \in \mathcal{V} \mid \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m) < \infty\}$.

By definition, if $\mathcal{M}_\tau \neq \emptyset$, the detector may select a vertex $v_m \in \mathcal{M}_\tau$ to ensure that (8) is feasible for any attack vertex, which in turn guarantees that the zero-sum game (9) admits a bounded value. Furthermore, characterizing the set $\mathcal{M}_\tau$ allows us to restrict the possible choices of the detector to $\mathcal{M}_\tau$. Hence, by addressing Problem 2 and characterizing $\mathcal{M}_\tau$, we can tackle Problem 1 by reformulating the zero-sum game (9) as

$$\min_{v_m \neq v_\tau \in \mathcal{V}} \max_{v_a \neq v_\tau \in \mathcal{V}} J_\tau(v_a, v_m) \qquad (10)$$
$$\text{s.t.} \quad v_m \in \mathcal{M}_\tau.$$

The next section characterizes the set of feasible monitor vertices $\mathcal{M}_\tau$ by investigating the feasibility of (8) with respect to system-theoretic properties of the dynamical system (4)-(6).

3. CHARACTERIZATION OF FEASIBLE MONITOR VERTICES

Let us denote the continuous-time systems $\Sigma_\tau \triangleq (-L, e_a, e_\tau^\top, 0)$ and $\Sigma_m \triangleq (-L, e_a, e_m^\top, 0)$. Inspired by Teixeira et al. (2015a, Th. 2), the feasibility of the optimization problem (8) is related to the invariant zeros of Σ_τ and Σ_m, which are defined as follows.

Definition 2. (Invariant zeros) Consider the strictly proper system $\Sigma \triangleq (A, B, C, 0)$ with A, B, and C are real matrices with appropriate dimensions. A tuple $(\lambda, \bar{x}, g) \in \mathbb{C} \times \mathbb{R}^N \times \mathbb{R}$ is a zero dynamics of Σ if it satisfies

$$\begin{bmatrix} \lambda I - A & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \qquad (11)$$

In this case, a finite λ is called a finite invariant zero of Σ. Further, the strictly proper system Σ always has at least one invariant zero at infinity (Franklin et al., 2002, Ch. 3).

More specifically, the optimization (8) is feasible if and only if the unstable invariant zeros of Σ_m are also invariant zeros of Σ_τ (Teixeira et al., 2015a, Th. 2). To derive a necessary and sufficient condition characterizing the set of feasible monitor vertices, we will investigate both finite and infinite invariant zeros of the two systems Σ_m and Σ_τ. The following Lemma considers the former.

Lemma 3. Consider a networked control system associated with a connected undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$, whose vertex dynamics and control law are described in (1) and (2), respectively. Suppose that the networked control system is driven by the stealthy data injection attack (3) at a single attack vertex v_a, and observed by a single monitor vertex v_m, resulting in the state-space model $\Sigma_m \triangleq (-L, e_a, e_m^\top, 0)$. Then, the networked control system Σ_m has no invariant zero on the closed positive real line.

Proof. The proof follows directly from the results in Briegel et al. (2011, Th. 3.7 & 3.9). ∎

Remark 4. By inheriting the results in Torres and Roy (2015), the other invariant zeros on the closed right half-plane possibly exist if the input and output vertices have short weak paths and long strong paths between them. On the other hand, the graph representing the system (1) under control law (2) is unweighted, i.e., all the edges have the same weight values, conflicting with the above sufficient condition in Torres and Roy (2015). We leave the necessary condition under which the system Σ_m has no invariant zeros on the closed right half-plane for the future research.

Based on the above remarks, assuming that the system Σ_m has no finite unstable zero, we then investigate the infinite zeros of the systems Σ_m and Σ_τ. In the investigation, we make use of known results connecting infinite invariant zeros mentioned in Definition 2 and the relative degree of a linear system, which is defined below.

Definition 5. (Relative degree) (Khalil, 2002, Ch. 13) Consider the strictly proper system $\Sigma \triangleq (A, B, C, 0)$ with $A \in \mathbb{R}^{n \times n}$, B, and C are real matrices with appropriate dimensions. The system Σ is said to have relative degree r $(1 \leq r \leq n)$ if the following conditions satisfy

$$CA^k B = 0, \quad 0 \leq k < r - 1,$$
$$CA^{r-1} B \neq 0. \tag{12}$$

Remark 6. Let $H(s) = C(sI - A)^{-1}B$ be the transfer function of the above system Σ. The relative degree r of the system Σ defined in Definition 5 is also the difference between the degrees of the denominator and the numerator of $H(s)$ (Khalil, 2002), which in turn corresponds to the degree of the infinite zero (Franklin et al., 2002, Ch. 3).

Based on Definition 5, let us denote $r_{\tau a}$ and r_{ma} as the relative degrees of Σ_τ and Σ_m, respectively. In the scope of this study, we have assumed that the cyber-attack (3) has no direct impact on the outputs (5) and (6), resulting in strictly proper systems Σ_τ and Σ_m. This implies that the relative degrees $r_{\tau a}$ and r_{ma} of Σ_τ and Σ_m are positive, yielding their infinite zeros. Those infinite zeros will be considered to present the following Theorem that gives us a necessary and sufficient condition for finding feasible monitor vertices $\mathcal{M}_\tau$.

Theorem 7. Consider the strictly proper systems $\Sigma_\tau \triangleq (-L, e_a, e_\tau^\top, 0)$ and $\Sigma_m \triangleq (-L, e_a, e_m^\top, 0)$, in which the two systems have the same stealthy data injection attack input at a single attack vertex v_a but different output vertices, i.e., v_τ for Σ_τ and v_m for Σ_m. Suppose the systems Σ_τ and Σ_m have relative degrees $r_{\tau a}$ and r_{ma}, respectively. Then, the worst-case impact of the stealthy data injection attack (8) is bounded if and only if the following condition holds

$$r_{ma} \leq r_{\tau a}. \tag{13}$$

Proof. Followed by Teixeira et al. (2015a, Th. 2), the optimization problem (8) is feasible if and only if Σ_m has unstable invariant zeros that are also invariant zeros of Σ_τ. Based on Lemma 3 and Remark 4, Σ_m has no finite unstable invariant zero, which leaves us to analyze infinite zeros of those systems. Recall the equivalence between the relative degree of a SISO system and the degree of its infinite zero. Hence, a necessary condition to guarantee the feasibility of the optimization (8) is that the number of infinite invariant zeros of Σ_m is not greater than that of Σ_τ. This implies $r_{ma} \leq r_{\tau a}$. For sufficiency, it remains to show that if $r_{ma} \leq r_{\tau a}$, any infinite zeros of Σ_m are also infinite zeros of Σ_τ. We will investigate each infinite zero of Σ_m by starting from their transfer functions with zero initial states

$$G_{\tau a}(s) = e_\tau^\top (sI + L)^{-1} e_a = \frac{P_{\tau a}(s)}{Q(s)},$$
$$G_{ma}(s) = e_m^\top (sI + L)^{-1} e_a = \frac{P_{ma}(s)}{Q(s)}, \tag{14}$$

where $s \in \mathbb{C}$. Based on Remark 6 and the minimal realisations Σ_τ and Σ_m, $P_{\tau a}(s)$, $P_{ma}(s)$, and $Q(s)$ are the polynomials of degrees $N - r_{\tau a}$, $N - r_{ma}$, and N, respectively. Let us denote $z_k = \sigma_k + j\omega_k \in \mathbb{C}$, $k \in \{1, 2, \ldots, r_{ma}\}$ with infinite module as infinite zeros of Σ_m. Indeed, (Morris and Rebarber, 2010) z_k $(1 \leq k \leq r_{ma})$ is an infinite zero of maximal degree r_{ma} of Σ_m if it satisfies

$$\lim_{\|z_k\|_2 \to \infty} z_k^q G_{ma}(z_k) = 0, \quad (0 \leq q \leq r_{ma} - 1),$$
$$\lim_{\|z_k\|_2 \to \infty} z_k^{r_{ma}} G_{ma}(z_k) \neq 0. \tag{15}$$

Further, with $0 \leq q \leq r_{ma} - 1$, we also basically have

$$\lim_{\|z_k\|_2 \to \infty} z_k^q G_{\tau a}(z_k) = \lim_{\|z_k\|_2 \to \infty} \frac{z_k^q P_{\tau a}(z_k)}{Q(z_k)} = 0. \tag{16}$$

The above limit (16) holds because the denominator $z^q P_{\tau a}(s)$ is the polynomial of degree $N - r_{\tau a} + q \leq N - 1 < N$, the degree of the polynomial $Q(z_k)$. This implies that any infinite zeros z_k of maximal degree r_{ma} of Σ_m are also infinite zeros of degree r_{ma} of Σ_τ. ∎

The following Lemma introduces a sufficient condition under which feasible monitor vertices guarantee the feasibility of the optimization (8) for an arbitrary attack vertex.

Lemma 8. Consider a networked system associated with a connected undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, \mathcal{A})$, whose vertex dynamics and control law are described in (1) and (2), respectively. The networked system is driven by the stealthy data injection attack at an arbitrary attack vertex v_a with its impact measured at a given target vertex v_τ.

Suppose that there exists a feasible monitor vertex v_m that directly connects to all the neighbors of the target vertex v_τ. Then, the optimisation (8) is feasible. Furthermore, defining $A_m \triangleq I + A$, this vertex v_m satisfies

$$e_\tau^\top A A_m e_m = e_\tau^\top A^2 e_\tau. \tag{17}$$

Proof. Recalling that the relative degrees of Σ_τ and Σ_m are related to the length of the shortest paths (*i.e.*, distance) from v_a to v_τ and v_m, respectively (Briegel et al., 2011, Th. 3.2), the first part of the proof follows directly from the fact that a vertex v_m is connected to all the neighbors of v_τ. This implies that the distance from any arbitrary attack vertex $v_a \neq v_\tau$ to v_m will be less or equal to the distance from v_a to v_τ. Thus, the vertex v_m satisfies (13). The remainder of the proof expresses the relation between v_m and v_τ in terms of the adjacency matrix and is omitted due to space limitations. ∎

Remark 9. To seek a set of feasible monitor vertices, the algebraic condition (17) is simply tested with all the vertices $v_m \neq v_\tau \in \mathcal{V}$.

4. NUMERICAL EXAMPLES

To validate the obtained results, let us take an example of a 10-vertex networked control system depicted in Fig. 2. We simply verify that no pair of attack and monitor vertices exhibits finite unstable zeros. Suppose that v_5 is the target vertex. There are two feasible monitor vertices v_3 and v_6, which satisfy the algebraic condition (17). Indeed, we simulate two scenarios, in which the detector monitors the outputs of the vertices v_3 (feasible) and v_2 (infeasible). Meanwhile, the adversary selects the vertex v_4 to conduct malicious attack signals at frequency 1.67 Hz depicted in Fig. 3a. The outputs of the monitor vertices v_2, v_3 and the target vertex v_5 are shown in Fig. 3b. Fig. 3b shows that the output of the feasible monitor vertex v_3 (red dash-dotted line) approximately tracks the figure for the target vertex v_5 (blue dashed line). The energy produced by the output of the vertices v_5 and v_3 witnesses no noticeable difference, namely around 1.04. By contrast, the output energy of the infeasible monitor vertex v_2 (yellow dotted line) is only 0.27, almost four times as low as the output energy of the target vertex v_5. More specifically, the output energies of those vertices over time horizon are illustrated in Fig. 4. Next, we will investigate how the ratio of the output energy of the above vertices progresses when increasing the frequency of the attack signals (see Fig. 5). As seen in Fig. 5, the gap between the two lines dramatically increases following the rise of the attack signal frequency. While the blue dotted-line ($v_m = v_3$) almost remains unchanged at 1.0, the red dashed-line ($v_m = v_2$) significantly becomes unbounded as the attack signal frequency increases. This implies that with massively high frequencies of the attack signals, the adversary is capable of manipulating the adversarial effect on the output of the target vertex at wish while remaining undetected at the infeasible monitor vertex v_2.

Next, the above results will be verified once again by computing the game payoff $J_5(v_a, v_m)$ with pairs of attack and monitor vertices $(v_a, v_m \neq v_5 \in \mathcal{V})$ (see Tab. 1). Looking at the third column ($v_m = v_3$) and the fifth column ($v_m = v_6$) of Tab. 1, no cell gives infinite value. On the other hand, the other columns show at least one
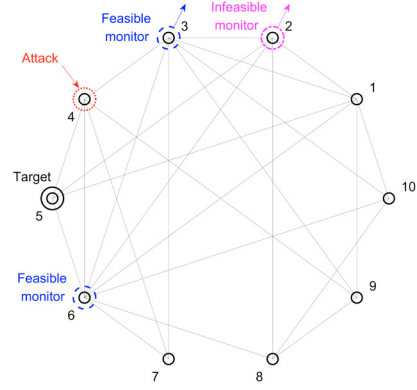

Fig. 2. 10-vertex networked control system with target vertex v_5, attack vertex v_4, and feasible monitor vertices v_3 and v_6.
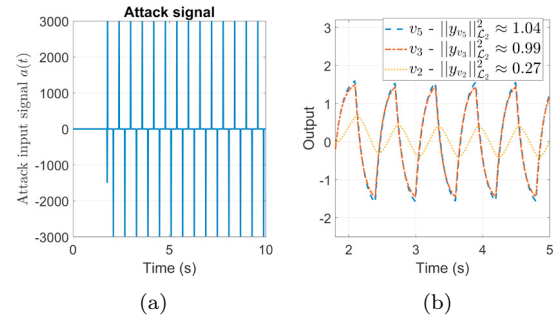

Fig. 3. (a) Attack signals directly injected into the input of v_4 at frequency 1.67 Hz; (b) Outputs of target v_5, feasible v_3, infeasible vertices v_2.
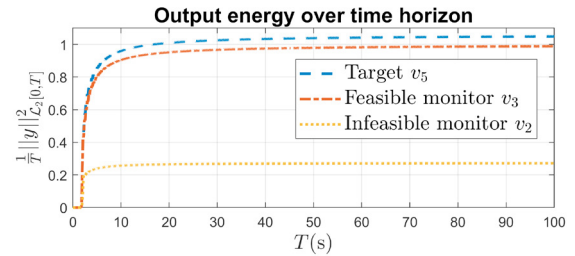

Fig. 4. The output energies of vertices v_2, v_3, and v_5 over time horizon.
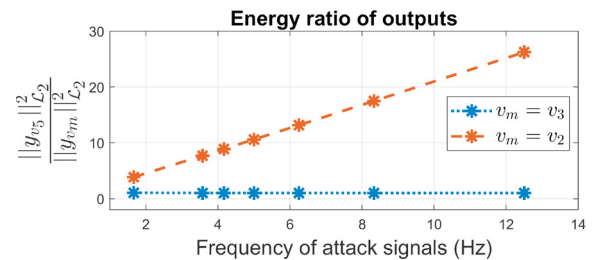

Fig. 5. Energy ratio of the outputs of target v_5 vs. feasible monitor v_3 and target v_5 vs. infeasible monitor v_2.

infinite game payoff. This assessment once again confirms that $v_m = v_3$ and $v_m = v_6$ are the feasible monitor vertices solving Problem 2.

By observing the game payoffs with the target vertex

Table 1. Game payoff (8) w.r.t. target vertex v_5 for the detector and the adversary corresponding to their chosen pair of monitor and attack vertices.

v_a \ v_m	v_1	v_2	v_3	v_4	v_6	v_7	v_8	v_9	v_{10}	$p^\star(v_a)$ (%)
v_1	1	1.0062	1.2405	∞	1.4384	∞	∞	1.2417	1.0074	0
v_2	1.2124	1	1.7737	∞	1.4669	∞	1.1984	∞	∞	≈ 100
v_3	1.0565	1.2329	1	1.0043	1.1905	1.008	∞	1.2369	1.2681	≈ 0
v_4	∞	∞	1.1742	1	1.4407	1	∞	1.0126	∞	0
v_6	1.1886	1.0029	1.1729	1.2122	1	1.0045	1.212	∞	1.0038	0
v_7	∞	2.2853	1	1	1	1	∞	∞	2.405	0
v_8	1	1	1	1.2928	1	∞	1	1	1	0
v_9	1	1	1	1	1	∞	1	1	1	0
v_{10}	1	1	1	∞	1	2.3027	1	1	1	0
$p^\star(v_m)$ (%)	0	≈ 0	0	0	≈ 100	0	0	0	0	

v_5 in Tab. 1, there is no pure Nash equilibrium. However, this game always admits a mixed-strategy Nash equilibrium (Zhu and Basar, 2015). Next, we investigate the mixed-strategy Nash equilibrium for this example. Let us denote $p(v_a)$ and $p(v_m)$ as the probabilities of attack v_a and monitor vertices v_m, respectively. $P(v_a) = [p(v_{a=1}), \ldots, p(v_{a=10})]^\top$, $P(v_m) = [p(v_{m=1}), \ldots, p(v_{m=10})]^\top$. The expected game payoff w.r.t. the target vertex v_5 for attack vertex v_a and monitor vertex v_m is given by

$$Q_5(v_a, v_m) = P(v_a)^\top J_5 P(v_m), \qquad (18)$$

where $J_5 = \left[J_5(v_i, v_j)_{ij} \right]$ is a 9×9-game matrix computed in Tab. 1. There exits a saddle point $(v_a^\star, v_m^\star)$ satisfies

$$-\infty < Q_5(v_a, v_m^\star) \leq Q_5(v_a^\star, v_m^\star) \leq Q_5(v_a^\star, v_m) < \infty,$$
$$\forall v_a, v_m \neq v_\tau \in \mathcal{V}.$$

The saddle point $(v_a^\star, v_m^\star)$ in the condition above indicates that a deviation of selecting $v_a(v_m)$ does not increase(decrease) the optimal expected game payoff $Q_5(v_a^\star, v_m^\star)$. From the numerical results in Tab. 1, while the probability of selecting $v_m = 6$ is approximately 100%, the figures for $v_a = 2$ is approximately 100%. The optimal probabilities $P^\star(v_a)$ and $P^\star(v_m)$ give us the optimal expected game payoff $Q_5(v_a^\star, v_m^\star) = 1.4669$.

5. CONCLUSION

In this paper, we investigated a continuous-time networked control system in the presence of a cyber-attack conducted by an adversary. An optimal sensor placement problem was raised such that a detector places a sensor at a vertex to monitor such a cyber-attack. We invoked a single-adversary-single-detector zero-sum game to describe the optimal sensor placement problem. This game was then formulated by employing a min-max optimization problem. In order to guarantee the feasibility of the min-max optimization problem, this paper presented a necessary and sufficient condition and an algebraic sufficient condition to find feasible monitor vertices. By placing a sensor at one of the feasible monitor vertices, the detector possibly monitors the cyber-attack. Further, the mixed-strategy Nash equilibrium of the zero-sum game was also analyzed to determine the optimal sensor placement. In future works, by inheriting the concept of an untouchable target vertex in this study, our game will be expanded to consider multiple adversaries and multiple detectors.

REFERENCES

Briegel, B., Zelazo, D., Bürger, M., and Allgöwer, F. (2011). On the zeros of consensus networks. In *2011 50th IEEE Conference on Decision and Control and European Control Conference*, 1890–1895. IEEE.

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.

Gupta, A., Langbort, C., and Başar, T. (2016). Dynamic games with asymmetric information and resource constrained players with applications to security of cyber-physical systems. *IEEE Transactions on Control of Network Systems*, 4(1), 71–81.

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

Miao, F., Zhu, Q., Pajic, M., and Pappas, G.J. (2018). A hybrid stochastic game for secure control of cyber-physical systems. *Automatica*, 93, 55–63.

Morris, K. and Rebarber, R. (2010). Invariant zeros of siso infinite-dimensional systems. *International journal of control*, 83(12), 2573–2579.

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

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

Torres, J.A. and Roy, S. (2015). Graph-theoretic analysis of network input–output processes: Zero structure and its implications on remote feedback control. *Automatica*, 61, 73–79.

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.