Security Allocation in Networked Control Systems under Stealthy Attacks

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

***Abstract*— This paper considers the problem of security allocation in a networked control system under stealthy attacks. The system is comprised of interconnected subsystems represented by vertices. A malicious adversary selects a single vertex on which to conduct a stealthy data injection attack with the purpose of maximally disrupting a distant target vertex while remaining undetected. Defense resources against the adversary are allocated by a defender on several selected vertices. First, the objectives of the adversary and the defender with uncertain targets are formulated in a probabilistic manner, resulting in an expected worst-case impact of stealthy attacks. Next, we provide a graph-theoretic necessary and sufficient condition under which the cost for the defender and the expected worst-case impact of stealthy attacks are bounded. This condition enables the defender to restrict the admissible actions to dominating sets of the graph representing the network. Then, the security allocation problem is solved through a Stackelberg game-theoretic framework. Finally, the obtained results are validated through a numerical example of a 50-vertex networked control system.**

***Index Terms*— Cyber-physical security, networked control system, Stackelberg game, stealthy attack.**

I. Introduction

Networked control systems are ubiquitous in modern society and are exemplified by power grids, transportation, and water distribution networks. These systems, utilizing non-proprietary information and communication technologies, such as public Internet and wireless communication, are exposed to the threat of cyber attacks [1]–[3], with potentially severe financial and societal consequences. For instance, an Iranian industrial control system and a Ukrainian power grid have witnessed the catastrophic consequences of malware such as Stuxnet in 2010 [2] and Industroyer in 2016 [3], respectively. Thus, in light of these alarming realities, the issue of security has acquired unprecedented significance in the realm of control systems.

In terms of cyber attacks on control systems, deception attacks that undermine the integrity of control systems have emerged as an area of increasing scholarly interest. For example, Pang and Liu [4] have proposed an encryption-based predictive control mechanism to counteract and mitigate such attacks. Another form of deception attacks, replay attacks, has been unmasked by physical watermarking [5]. Meanwhile, the development of stealthy attacks on control systems has been made to evade the most advanced detection schemes [6]–[9].

Upon review of the above studies [4]–[9], it is noticed that they have concentrated on secure estimation and secure control from the perspective of either the defender or the adversary. Nonetheless, it is crucial to note that both parties are confronted with similar challenges, as the defender has limited resources to counteract malicious activities, while the adversary also faces energy and detectability constraints when executing attacks. As a result, addressing the security problem within a unified framework that encompasses both the defender and the adversary is of utmost importance.

Game theory offers a unified framework to consider the objectives and actions of both strategic players, namely the defender and the adversary [10]. It also 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 [11]. Further, many other concepts of games describing networked systems subjected to cyber attacks such as matrix games [12]–[14], dynamic games [15], stochastic games [16], and network monitoring games [17] have been studied. Recent studies [12], [18], [19] have utilized the common concept of zero-sum games to address the problem of input attacks on cyber-physical systems. Control systems exposed to cyber attacks have been extensively investigated through game theoretic approaches [15]–[17]. However, these approaches have not accounted for the deployment of detectors in an effort to improve the detection of cyber attacks. This creates a significant knowledge gap that must be addressed in order to enhance security measures.

One such effort to close the aforementioned gap has been presented in a game-theoretic formulation outlined by Pirani et al. [20]. The game payoff in [20] has been formulated by combining the maximum $\mathcal{L}_2$ gains of multiple outputs with respect to 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 input signals. Further, the utilization of a maximum gain for characterizing the detectability corresponds to an optimistic perspective, where the adversary attempts to maximize the energy of the detection output, instead of the opposite. Therefore, in order to address the critical issue of cyber security and develop a security metric against cyber attacks, it is imperative to thoroughly investigate the optimal placement of sensors in a

This work is supported by the Swedish Research Council under the grant 2021-06316 and by the Swedish Foundation for Strategic Research.

Anh Tung Nguyen, André M. H. Teixeira, and Alexander Medvedev are with the 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).

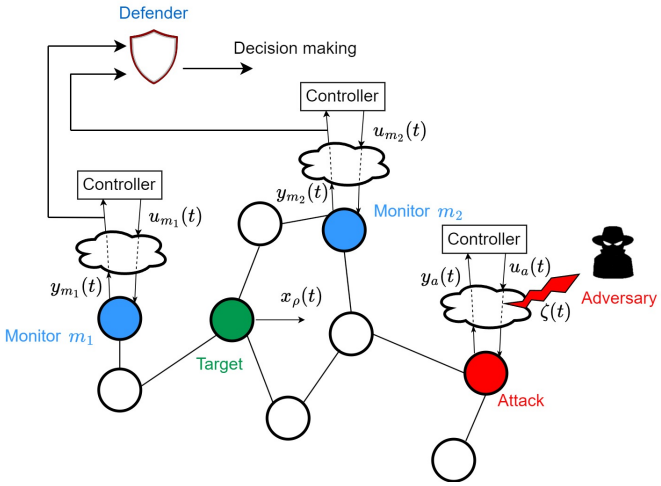

Fig. 1: An illustration of a networked control system with the (green) target vertex. While the defender places sensors at the (blue) monitor vertices, the adversary conducts a stealthy data injection attack on the (red) attack vertex.

networked system to minimize the impact of cyber attacks while maintaining maximum detectability.

Additionally, the above existing studies [12], [13], [15], [17], [19], [20] considered the security problem where the defender and the adversary select their actions simultaneously. However, this formulation is not always applicable in practical situations where an adversary attacks after observing the action of the defender. To deal with this scenario, a game-theoretic Stackelberg framework [21] offers a more practical solution [14], [22], [23]. In the framework, after analyzing possible attack scenarios, the defender called *the leader*, has the power to select and announce their action first, knowing that the malicious adversary bases their actions on the leader's decision. Then, the malicious adversary called *the follower*, finds the best response to the defender's action.

In this paper, we consider a continuous-time networked control system, associated with an undirected connected graph, under stealthy attacks involving two strategic agents: a malicious adversary and a defender. The system is comprised of multiple interconnected one-dimensional subsystems, referred to as vertices. The purpose of the adversary is to maliciously degrade a distant target vertex without being detected. To this end, the adversary selects one vertex on which to launch a stealthy data injection attack on its input. Meanwhile, the defender allocates defense resources by selecting a set of monitor vertices to measure their outputs with the aim of alleviating the attack impact. Given the strategic nature of both agents, we investigate the optimal selection of the monitor vertices using the Stackelberg game-theoretic approach described above. By leveraging the concept of the Stackelberg game in [21], we can elucidate the complex interplay between the two agents and identify their best actions. Figure 1 visualizes the above-defined game in a networked control system. The contributions of this paper are the following:

1) A novel defense cost, the expected output-to-output gain, is proposed to capture the expected worst-case impact of stealthy attacks with an uncertain target vertex.
2) The security allocation problem is cast in a Stackelberg game-theoretic framework with the defender as the leader and the malicious adversary as the follower.
3) We propose a control design that fulfills a graph-theoretic necessary and sufficient condition under which the boundedness of the defense cost is guaranteed.
4) Leveraging the uncertainty of the target vertex, we show that the necessary and sufficient condition in 3) restricts the admissible choices of monitor sets to be dominating sets of the graph.
5) The advantage of the proposed security allocation scheme is highlighted through the alleviation of the computational complexity.

The remainder of this paper is organized as follows. Section II describes a networked control system under stealthy attacks and the adversarial modeling. Then, Section III presents how a malicious adversary and a defender design their strategies. Thereafter, Section IV investigates the boundedness of the defense cost and the worst-case impact of stealthy attacks caused by the malicious adversary. The investigation affords us to restrict the admissible actions of the defender, which is presented at the end of Section IV. In Section V, by employing the Stackelberg game-theoretic framework, we propose two solutions to find the optimal actions for the malicious adversary and the defender. In Section VI, the effectiveness of the proposed security allocation scheme in terms of computational complexity is highlighted, especially in large-scale networks. Section VII presents a numerical example to validate the obtained results while Section VIII concludes the paper. We conclude this section by providing the notation to be used throughout this 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. A vector with the i-th element set to one and the other elements set to zero is denoted $e_i \in \mathbb{R}^n$. For a set $\mathcal{A}$, $|\mathcal{A}|$ stands for the set cardinality. For a given discrete random variable $y \in D_y$ having a probability mass function p, the expected value of a function $f(y)$ is denoted as $\mathbb{E}_{y\sim p}\left[f(y)\right] = \sum_{y\in D_y} p(y)f(y)$. A continuous linear time-invariant (LTI) system with the state-space model $\dot{x}(t) = \bar{A}x(t) + \bar{B}u(t),\ y(t) = \bar{C}x(t) + \bar{D}u(t)$ is denoted as $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, \bar{D})$. The space of square-integrable functions is defined as $\mathcal{L}_2 \triangleq \left\{f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|^2_{\mathcal{L}_2[0,\infty]} < \infty\right\}$ and the extended space is defined as $\mathcal{L}_{2e} \triangleq \left\{f : \mathbb{R}_+ \to \mathbb{R} \mid \|f\|^2_{\mathcal{L}_2[0,T]} < \infty,\ \forall\ 0 < T < \infty\right\}$. The notation $\|x\|^2_{\mathcal{L}_2}$ is used as shorthand for the norm $\|x\|^2_{\mathcal{L}_2[0,T]} \triangleq \frac{1}{T}\int_0^T \|x(t)\|_2^2\ \mathrm{d}t$ if the time horizon $[0,T]$ is clear from the context. Let $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$ be an undirected graph with the set of N vertices $\mathcal{V} = \{1, 2, ..., N\}$, the set of edges $\mathcal{E} \subseteq \mathcal{V}\times\mathcal{V}$, and the adjacency matrix $A = [a_{ij}]$. For any $(i,j) \in \mathcal{E},\ i \neq j$, the element of the adjacency matrix a_{ij} is positive, and with $(i,j) \notin \mathcal{E}$ or $i = j$, $a_{ij} = 0$. The degree of vertex i is denoted as $\Delta_i \triangleq \sum_{j=1}^n a_{ij}$ and the degree matrix of graph $\mathcal{G}$ is defined as $\Delta \triangleq \mathbf{diag}\big(\Delta_1, \Delta_2, \ldots, \Delta_N\big)$,

where **diag** stands for a diagonal matrix. The Laplacian matrix is defined as $L = [\ell_{ij}] \triangleq \Delta - A$. Further, $\mathcal{G}$ is called an undirected connected graph if and only if matrix 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 $\mathcal{N}_i = \{j \in \mathcal{V} \mid (i,j) \in \mathcal{E}\}$. We denote the subset of $\mathcal{V}$ excluding a vertex i as $\mathcal{V}_{-i} \triangleq \mathcal{V} \setminus \{i\}$.

II. Problem Description

We first describe a networked control system under stealthy attacks in the presence of a defender and a malicious adversary. Then, the malicious goal and the attack strategy are modeled in the remainder of this section.

A. Networked control system under stealthy attacks

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

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

where $x_i(t) \in \mathbb{R}$ and $u_i(t) \in \mathbb{R}$ are the state and the local control input of vertex i, respectively. Each vertex $i \in \mathcal{V}$ is controlled by the control law:

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

where $\theta_i \in \mathbb{R}_+$ is an adjustable self-loop control gain at vertex i. This self-loop control gain will be used to improve the security of the entire network later in this paper. For convenience, let us denote $x(t)$ as the state of the entire network, $x(t) \triangleq \big[x_1(t),\ x_2(t), \ldots,\ x_N(t)\big]^\top$.

To get prepared for facing malicious activities, the defender selects a subset of the vertex set $\mathcal{V}$ as a set of monitor vertices, denoted as $\mathcal{M} \triangleq \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}$, on which to place a sensor at each selected monitor vertex. Due to practical reasons, the number of utilized sensors should be constrained. Let us denote n_s as the sensor budget that is the maximum number of utilized sensors, i.e., $|\mathcal{M}| \leq n_s$.

Given the defense strategy, the malicious adversary selects a vertex $a \in \mathcal{V}$ on which to conduct an additive time-dependent attack signal $\zeta(t) \in \mathbb{R}$, where $\zeta \in \mathcal{L}_{2e}$, at its input as follows:

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

Based on the above descriptions of the network, the defense strategy, and the malicious plan, the system model (1) under the control law (2)-(3) can be rewritten in the presence of the attack signal at the attack vertex a with output of the target vertex ρ and outputs observed at the monitor vertices $m_k \in \mathcal{M}$ as follows:

$$\dot{x}(t) = -\bar{L}x(t) + e_a\zeta(t), \tag{4}$$

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

$$y_\mathcal{M}(t) = C_\mathcal{M}^\top x(t), \tag{6}$$

where $C_\mathcal{M} \triangleq [e_{m_1}, e_{m_2}, \ldots, e_{m_{|\mathcal{M}|}}]$, $\bar{L} \triangleq L + \Theta$, and $\Theta \triangleq \mathbf{diag}(\theta_1, \theta_2, \ldots, \theta_N)$. The Laplacian matrix L associated with the undirected connected graph $\mathcal{G}$ and $\theta_i \in \mathbb{R}_+,\ \forall i \in \mathcal{V}$ result in that all the eigenvalues of the matrix $\bar{L}$ are positive real. This property of $\bar{L}$ ensures that the state of the network $x(t)$ asymptotically converges to the origin in the attack-free case, affording us to employ the following assumption.

Assumption 1: The system (4) is at its equilibrium $x_e = 0$ before being affected by the attack signal $\zeta(t)$. ◁

Remark 1: The system (4)-(6) is guaranteed to be asymptotically stable in the attack-free case. Unfortunately, the stability of an attack-free system is not enough to determine the impact of stealthy additive false data injection attacks (3), which are mainly studied in this paper. The attack impact needs to be evaluated through the invariant zeros of the system (4)-(6), which will be described in Section IV. ◁

B. Stealthy attack model

The purpose of the malicious adversary is to maximally disrupt a distant target vertex (denoted as ρ) by compromising an attack vertex a, while remaining stealthy to the defender (see the discussion on the importance of the stealthiness in [13, Sec. II.E]). This attack strategy is motivated by existing scenarios considered in the literature such as a single target vertex in networked control systems [20], malicious control in competitive power systems [24], Crossfire attacks in computer security [25], and adversarial reachable sets [26], where the malicious goal is to impact other vertices beyond the initially compromised vertex. Based on these motivating examples, we employ the following assumption.

Assumption 2: For any given attack vertex a, the target vertex ρ is distinct from the attack vertex a, i.e., $\rho \in \mathcal{V}_{-a}$.

The above malicious purpose allows us to mainly focus on the stealthy data injection attack that will be defined in the following. Consider the above structure of the continuous LTI system (4)-(6), which we denote as $\Sigma_{\rho\mathcal{M}} \triangleq (-\bar{L}, e_a, [e_\rho, C_\mathcal{M}]^\top, 0)$, with the monitor outputs $y_{m_k}(t) = e_{m_k}^\top x(t),\ \forall m_k \in \mathcal{M}$. The input signal $\zeta(t)$ of the system $\Sigma_{\rho\mathcal{M}}$ is called the stealthy data injection attack if the monitor outputs satisfy $\|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}$, for all $m_k \in \mathcal{M}$, in which $\delta_{m_k} > 0$ is given for each corresponding monitor vertex m_k and called an alarm threshold. This means that the adversary is said to be detected if there exists at least one monitor vertex $m_k \in \mathcal{M}$ whose output energy crosses its corresponding alarm threshold δ_{m_k}. The impact of the stealthy data injection attack is measured via the output energy of the target vertex ρ over the horizon $[0, T]$, i.e., $\|y_\rho\|_{\mathcal{L}_2[0,T]}^2$. This performance specification is commonly used in the literature on secure control systems [5], [8], [10], [18], [20] where it captures the average impact on the target in a certain time interval. The long time horizon considered in the attack impact is motivated by a common assumption in the literature that adversaries aim for a long-term malicious impact after they have made a significant investment to infiltrate the network and acquire system parameters [13]. Further, akin to the $\mathcal{H}_-/\mathcal{H}_\infty$ metrics [11] and the LQ controller design, designing problems with energy costs and linear systems can be formulated into tractable problems.

The worst-case impact of the stealthy data injection attack conducted by the malicious adversary on the target will be

further investigated. Then, this worst-case attack impact will be utilized to formulate the objectives of the adversary and the defender in the following section.

Remark 2: In the absence of *Assumption 2*, the resulting allocation problem based on (7) has a single trivial solution that is to monitor all the vertices. *Assumption 2* overcomes this limitation and results in richer and more interesting allocation problems in the following sections. Section V discusses this matter in more detail.

III. Attack and Defense Strategies

In the first two parts of this section, the malicious and defense objectives are formulated to design the strategies for the malicious adversary and the defender. In the remainder of this section, the security allocation methodology that is the main focus of this paper is presented to show how the defender designs their defense strategy.

A. Attack strategy

Practically, the malicious adversary designs their attack policies after acquiring enough system parameters and observing defense strategies. Given the set of monitor vertices $\mathcal{M}$, the malicious adversary selects an attack vertex a that maximizes the following worst-case impact of stealthy attacks on the distant target vertex $\rho \in \mathcal{V}_{-a}$:

$$J_\rho(a,\mathcal{M}) \triangleq \sup_{x(0)=0,\ \zeta\in\mathcal{L}_{2e}} \|y_\rho\|_{\mathcal{L}_2}^2 \quad \text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \le \delta_{m_k},\ \forall m_k\in\mathcal{M},\ (4)-(6). \tag{7}$$

The dual problem of (7) is given as follows:

$$\inf_{\gamma_{m_k}>0}\left[\sup_{x(0)=0,\ \zeta\in\mathcal{L}_{2e}}\left(\|y_\rho\|_{\mathcal{L}_2}^2-\sum_{m_k\in\mathcal{M}}\gamma_{m_k}\|y_{m_k}\|_{\mathcal{L}_2}^2\right)+\sum_{m_k\in\mathcal{M}}\gamma_{m_k}\delta_{m_k}\right] \quad \text{s.t.} \quad (4)-(6). \tag{8}$$

The dual problem (8) is bounded only if $\|y_\rho\|_{\mathcal{L}_2}^2 - \sum_{m_k\in\mathcal{M}}\gamma_{m_k}\|y_{m_k}\|_{\mathcal{L}_2}^2 \le 0,\ \forall\zeta\in\mathcal{L}_{2e}$ and $x(0)=0$, which results in the following minimization problem:

$$J_\rho(a,\mathcal{M}) = \min_{\gamma_{m_k}>0} \sum_{m_k\in\mathcal{M}}\gamma_{m_k}\delta_{m_k} \quad \text{s.t.} \quad \|y_\rho\|_{\mathcal{L}_2}^2-\sum_{m_k\in\mathcal{M}}\gamma_{m_k}\|y_{m_k}\|_{\mathcal{L}_2}^2\le 0,\ (4)-(6),\ x(0)=0,\ \forall\zeta\in\mathcal{L}_{2e}. \tag{9}$$

The strong duality can be proven by utilizing S-Procedure [27, Ch. 4]. Recalling the key results in dissipative system theory for linear systems with quadratic supply rates [28], the optimization problem (9) can be translated into the following semidefinite programming (SDP) problem:

$$J_\rho(a,\mathcal{M}) = \min_{\gamma_{m_k}>0,\ P=P^\top\ge 0} \sum_{m_k\in\mathcal{M}}\gamma_{m_k}\delta_{m_k} \quad \text{s.t.} \quad \begin{bmatrix} -\bar{L}P-P\bar{L} & Pe_a \\ e_a^\top P & 0\end{bmatrix}+\begin{bmatrix} e_\rho \\ 0\end{bmatrix}\begin{bmatrix} e_\rho^\top & 0\end{bmatrix} - \sum_{m_k\in\mathcal{M}}\gamma_{m_k}\begin{bmatrix} e_{m_k} \\ 0\end{bmatrix}\begin{bmatrix} e_{m_k}^\top & 0\end{bmatrix}\le 0. \tag{10}$$

It is worth noting that to guarantee the existence of a solution to the optimization problem (10), we need to show the boundedness of the optimization problem (7) [29], which will be discussed in Section IV. The following subsection presents how the defender designs their defense strategy without knowing the exact target of the malicious adversary.

Remark 3: In a similar scenario, another objective function based on $\mathcal{L}_2$-gain for both the adversary and the defender has been proposed in [20, Sec. 3]. The objective function in [20, Sec. 3] was formulated in terms of the maximal $\mathcal{L}_2$-gains from the attack vertex a to the target vertex ρ and from the attack vertex a to the monitor vertex m_k. More specifically, the objective function in [20, Sec. 3] is given by

$$W_\rho(a,m_k) \triangleq \sup_{\|\zeta\|_{\mathcal{L}_2}\neq 0}\frac{\|y_\rho\|_{\mathcal{L}_2}^2}{\|\zeta\|_{\mathcal{L}_2}^2}-\lambda\sup_{\|\zeta\|_{\mathcal{L}_2}\neq 0}\frac{\|y_{m_k}\|_{\mathcal{L}_2}^2}{\|\zeta\|_{\mathcal{L}_2}^2},\ (\lambda\ge 0).$$

The above objective $W_\rho(a,m_k)$ also considers two different outputs $y_\rho(t)$ and $y_{m_k}(t)$, but note that the output energies are maximized separately, thus leading to two different optimal input signals $\zeta(t)$ in general cases. By contrast, our objective function (7) considers the worst-case impact of stealthy attacks that is simultaneously characterized by the multiple outputs $y_\rho(t)$ and $y_{m_k}(t)$ with respect to a single input signal $\zeta(t)$. ◁

B. Defense strategy

We assume that the defender does not know the exact location of a distant target vertex ρ that parameterizes the attack policy (7). This assumption closely aligns with practical situations where the defender seldom foresees the exact intentions of malicious adversaries. To design a suitable defense strategy despite such uncertainty, the defender can conduct a risk assessment [30] to assess and reason about the impact and the likelihood of potential malicious activities (namely pairs of attack and target vertices in our context). To this end, the defender considers the malicious target, represented by the location of the vertex ρ, in a probabilistic manner. For a given attack vertex a, the uncertain target vertex ρ is characterized probabilistically through a conditional belief $\pi_a(\rho)$, which is assumed to be positive $\forall\rho\in\mathcal{V}_{-a}$. This belief model aligns partially with the concept of attack types in games with incomplete information [13], [31]. Therefore, instead of minimizing (7) as in games with complete information, the defender utilizes the above-defined conditional belief $\pi_a(\rho)$ to consider an expected worst-case impact of stealthy attacks as a proxy for (7). Then, the defender desires to choose a set of monitor vertices $\mathcal{M}$ that minimizes the following defense cost:

$$R(a,\mathcal{M}) \triangleq \mathfrak{c}(|\mathcal{M}|)+Q(a,\mathcal{M}), \tag{11}$$

where the expected worst-case impact of stealthy attacks is defined as:

$$Q(a,\mathcal{M}) \triangleq \mathbb{E}_{\rho\sim\pi_a}\left[J_\rho(a,\mathcal{M})\right] = \sum_{\rho\in\mathcal{V}_{-a}} \pi_a(\rho) J_\rho(a,\mathcal{M}), \tag{12}$$

and $\mathfrak{c}(|\mathcal{M}|)$ is a cost for the number of utilized sensors, which is assumed to be bounded for any monitor set $\mathcal{M}\subseteq\mathcal{V}$. In the following subsection, we present how the defender plans their defense strategy by addressing the above-defined objectives (11)-(12).

C. Security Allocation Methodology

The security allocation entails that the defender strategically allocates defense resources to monitor specific vertices, aiming to enhance the security level of the network. The strategic selection of a monitor set is computed offline in the design phase, where the defender simulates and evaluates all the possible attack scenarios in order to seek the best monitor set that minimizes the defense cost (11).

To accomplish the design, the defender first evaluates the defense cost (11) based on the potential target of the malicious adversary, which is generally uncertain, in a probabilistic way (see more discussions in [13, Sec. II.E]). Secondly, the defender changes the attack scenario to other vertices and repeats the investigation conducted in the previous step for all potential attack vertices. In the end, the defender obtains the result of the enumeration of all the action scenarios, which is in line with other Stackelberg security games found in the literature [14]. Finally, the result from the enumeration enables the defender to find the best monitor set, which will be discussed in Section V.

In the steps mentioned above, the defender can neglect monitor sets that yield unbounded defense costs, reducing the defender's action space. This reduction saves computing resources and fosters the design procedure. From (7), $J_\rho(a,\mathcal{M})$ is non-negative for every pair of attack vertex a and monitor set $\mathcal{M}$. Thus, the defense cost $R(a,\mathcal{M})$ and the expected worst-case impact of stealthy attacks $Q(a,\mathcal{M})$ are bounded when the worst-case impact of stealthy attacks (7) on every target vertex $\rho\in\mathcal{V}_{-a}$ is bounded. In the following section, we will present how the defender finds a set of admissible monitor vertices $\mathcal{M}$ that guarantees the boundedness of the worst-case impact of stealthy attacks (7) for every attack vertex.

IV. Characterizing the Set of Monitor Vertices

In this section, we first provide an upper bound of the worst-case impact of stealthy attacks (7). The boundedness of this upper bound is guaranteed by a necessary and sufficient condition. By analyzing this upper bound, we provide a graph-theoretic necessary and sufficient condition under which the cost (11) and the expected worst-case impact (12) are bounded. This condition, then, allows us to limit the admissible actions of the defender. In the remainder of this section, we show how the admissible actions of the defender are characterized.

A. Evaluating the worst-case impact of stealthy attacks

The following lemma states a key property of the worst-case impact of stealthy attacks (7).

Lemma 1: Consider the continuous LTI system $\Sigma_{\mathcal{M}} = (-\bar{L}, e_a, C_{\mathcal{M}}^\top, 0)$ with a given attack vertex a, a target vertex $\rho\in\mathcal{V}_{-a}$, and a non-empty monitor vertex set $\mathcal{M}$, the worst-case impact (7) has an upper bound:

$$J_\rho(a,\mathcal{M}) \;\le\; \overline{J}_\rho(a,\mathcal{M}), \tag{13}$$

where

$$\overline{J}_\rho(a,\mathcal{M}) = \min_{m_k\in\mathcal{M}} \left\{ \begin{array}{ll} \sup\limits_{x(0)=0,\ \zeta\in\mathcal{L}_{2e}} & \|y_\rho\|_{\mathcal{L}_2}^2 \\ \text{s.t.} & \|y_{m_k}\|_{\mathcal{L}_2}^2 \le \delta_{m_k} \end{array} \right\}. \tag{14}$$

◁

Proof: See Appendix I. ■

Lemma 1 enables us to guarantee the boundedness of the worst-case impact of stealthy attacks (7) through considering the isolated worst-case impact of stealthy attacks (14) at a single monitor vertex $m_k\in\mathcal{M}$. Next, at the first stage in the investigation into the boundedness of the worst-case impact of stealthy attacks (14), we adopt a result in [29, Th. 2]. The boundedness of the optimization problem (14) is related to the invariant zeros of $\Sigma_\rho \triangleq (-\bar{L}, e_a, e_\rho^\top, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$, which are defined as follows.

Definition 1 (Invariant zeros): Consider the strictly proper LTI system $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$ where $\bar{A}, \bar{B}$, 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 $\bar{\Sigma}$ if it satisfies

$$\left[\begin{array}{cc} \bar{\lambda}I - \bar{A} & -\bar{B} \\ \bar{C} & 0 \end{array}\right] \left[\begin{array}{c} \bar{x} \\ \bar{g} \end{array}\right] = \left[\begin{array}{c} 0 \\ 0 \end{array}\right], \quad \bar{x}\neq 0. \tag{15}$$

A finite $\bar{\lambda}$ is called a finite invariant zero of the system $\bar{\Sigma}$. The strictly proper system $\bar{\Sigma}$ always has at least one invariant zero at infinity [32, Ch. 3]. Further, invariant zeros that have positive real parts are called unstable invariant zeros. ◁

More specifically, to guarantee the boundedness of the worst-case impact of stealthy attacks (14), let us state the following lemma.

Lemma 2 ([29, Th. 2]): Consider the following continuous LTI systems $\Sigma_\rho \triangleq (-\bar{L}, e_a, e_\rho^\top, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$, $\forall m_k\in\mathcal{M}$. The optimization problem (14) is bounded if, and only if, there exists at least one system Σ_{m_k} such that its unstable invariant zeros are also invariant zeros of Σ_ρ. ◁

Proof: Follows directly the result in [29, Th. 2]. ■

The result in *Lemma 2* prompts us to investigate invariant zeros of Σ_{m_k}. Let us adopt the following lemma from our previous work [19] that considers finite invariant zeros of Σ_{m_k}.

Lemma 3 ([19, Lem. 4.4]): Consider a networked control system associated with an undirected connected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$, whose closed-loop dynamics is described in (4). Suppose that the networked control system is driven by the stealthy data injection attack at a single attack vertex a, and observed by a single monitor vertex m_k, resulting in the state-space model $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$. Then, there exist self-loop control gains θ_i, $\forall i \in \{1, 2, \ldots, N\}$, in (2) such that Σ_{m_k} has no finite unstable invariant zero. ◁

Proof: See Appendix II. ■

Lemma 3 enables us to carefully design the control law (2), i.e. select θ_i, such that for every pair of an input vertex a and an output vertex m_k, the corresponding LTI system $\Sigma_{m_k} = (-\bar{L}, e_a, e_{m_k}^\top, 0)$ has no unstable invariant zero. Hence, it leaves us to investigate infinite invariant zeros of systems $\Sigma_{m_k},\ \forall m_k \in \mathcal{M}$ in the following subsection.

B. Infinite invariant zeros

We investigate the infinite invariant zeros of the systems Σ_ρ and $\Sigma_{m_k},\ \forall m_k \in \mathcal{M}$. In the investigation, we make use of known results connecting infinite invariant zeros mentioned in *Definition 1* and the relative degree of a linear system, which is defined below.

Definition 2 (Relative degree [33, Ch. 13]): Consider a strictly proper LTI system $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$ with $\bar{A} \in \mathbb{R}^{n\times n}$, $\bar{B}$, and $\bar{C}$ are real matrices with appropriate dimensions. The system $\bar{\Sigma}$ is said to have a relative degree r $(1 \le r \le n)$ if the following conditions satisfy

$$\begin{aligned} &\bar{C}\bar{A}^k\bar{B} = 0, \quad 0 \le k < r-1, \\ &\bar{C}\bar{A}^{r-1}\bar{B} \neq 0. \end{aligned} \tag{16}$$

◁

Remark 4: Let $\bar{H}(s) = \bar{C}(sI - \bar{A})^{-1}\bar{B}$ be the transfer function of the above system $\bar{\Sigma}$. The relative degree r of the system $\bar{\Sigma}$ defined in *Definition 2* is also the difference between the degrees of the denominator and the numerator of $\bar{H}(s)$ [33], which in turn corresponds to the degree of the infinite zero if $\bar{\Sigma}$ is minimal realization [32, Ch. 3]. ◁

Based on *Definition 2*, let us denote $r_{(\rho,a)}$ and $r_{(m_k,a)}$ as the relative degrees of Σ_ρ and $\Sigma_{m_k},\ \forall m_k \in \mathcal{M}$, respectively. In the scope of this study, we have assumed that the attack signal $\zeta(t)$ in (3) has no direct impact on the outputs (5) and (6), resulting in strictly proper systems Σ_ρ and Σ_{m_k}. This implies that the relative degrees $r_{(\rho,a)}$ and $r_{(m_k,a)}$ of the systems Σ_ρ and Σ_{m_k} are positive, yielding their infinite invariant zeros. Let us state the following theorem that considers infinite invariant zeros of the systems Σ_ρ and Σ_{m_k} to provide a necessary and sufficient condition under which the boundedness of the worst-case impact of stealthy attacks (14) is guaranteed.

Theorem 1: Consider the strictly proper LTI systems $\Sigma_\rho \triangleq (-\bar{L}, e_a, e_\rho^\top, 0)$ and $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0),\ \forall m_k \in \mathcal{M}$, in which the systems have the same stealthy data injection attack input (3) at a single attack vertex $a \in \mathcal{V}_{-\rho}$ but different output vertices (5)-(6), i.e., ρ for Σ_ρ and m_k for Σ_{m_k}. Suppose the systems Σ_ρ and Σ_{m_k} have relative degrees $r_{(\rho,a)}$ and $r_{(m_k,a)}$, respectively. Then, the worst-case impact of stealthy attacks (14) is bounded if, and only if, there exists at least one system Σ_{m_k} such that the following condition holds

$$r_{(m_k,a)} \le r_{(\rho,a)}. \tag{17}$$

◁

Proof: See Appendix III. ■

Given an arbitrary attack vertex a and a distant target vertex $\rho \in \mathcal{V}_{-a}$, *Theorem 1* hints a solution to monitoring malicious activities. The defender chooses a non-empty monitor set $\mathcal{M} \subset \mathcal{V}$ such that there exists at least one monitor vertex $m_k \in \mathcal{M}$ that fulfills the condition (17). The following subsection presents how to find such a monitor set $\mathcal{M}$.

Remark 5: Let us consider the following continuous LTI system $\Sigma_\mathcal{M} = (-\bar{L}, e_a, C_\mathcal{M}^\top, 0)$ where its input is at the vertex a and its outputs are at monitor vertices $m_k \in \mathcal{M}$. By employing the definition of the relative degree of single-input-multiple-output systems, adapted from [34], the relative degree of the system $\Sigma_\mathcal{M}$ is the least relative degree from its input to its single monitor vertex. Thus, we need to find at least one monitor vertex m_k such that it fulfills the condition (17), resulting in the boundedness of (14). This result eventually allows us to guarantee that the worst-case impact of stealthy attacks in (7) is bounded according to the property in (13). ◁

C. Admissible monitor sets and dominating sets

Consider a subset $\mathcal{M} \subset \mathcal{V}$ where its cardinality is not greater than the sensor budget n_s, the maximum number of available sensors, i.e., $\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}$ and $|\mathcal{M}| \le n_s$. Inspired by the discussions in the previous subsection, a monitor set $\mathcal{M}$ is admissible if it contains at least one monitor vertex $m_k \in \mathcal{M}$ such that this vertex m_k fulfills the necessary and sufficient condition (17) in *Theorem 1*. This set $\mathcal{M}$ is called a dominating set which is defined below.

Definition 3 (Dominating set): Given an undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$, a subset of the vertex set $\mathcal{D} \subset \mathcal{V}$ is called a dominating set if, for every vertex $u \in \mathcal{V}\setminus\mathcal{D}$, there is a vertex $v \in \mathcal{D}$ such that $(u, v) \in \mathcal{E}$. ◁

The following lemma presents a necessary and sufficient condition that allows us to examine whether a subset of the vertex set $\mathcal{V}$ is a dominating set.

Lemma 4: Consider an undirected graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A)$, a subset $\mathcal{M} \subset \mathcal{V}$ is a dominating set of $\mathcal{V}$ if, and only if, the following condition holds

$$e_i^\top \mathcal{C}(\mathcal{M}) > 0,\ \forall i \in \mathcal{V}, \tag{18}$$

where $\mathcal{C}(\mathcal{M}) = (A + I)\sum_{m_k\in\mathcal{M}} e_{m_k}$. ◁

Proof: See Appendix IV. ■

By investigating all the subsets of $\mathcal{V}$, we can find all the dominating sets which fulfill the condition (18). Let us make use of the following assumption.

Assumption 3: The vertex set $\mathcal{V}$ has at least one dominating set with a cardinality of at most n_s. ◁

Based on *Assumptions 2-3* and the above results in *Lemma 1* and *Theorem 1*, we are now ready to state the following theorem that provides a graph-theoretic necessary and sufficient condition under which the cost (11) and the expected worst-case impact of stealthy attacks (12), caused by the stealthy data injection attack at an arbitrary attack vertex a, are bounded.

Theorem 2: Suppose that *Assumptions 2-3* hold. Consider the networked control system (4) associated with an undirected connected graph $\mathcal{G}$ where the system has the stealthy data injection attack (3) at the input of an arbitrary attack vertex a and outputs (6) at monitor vertices $m_k \in \mathcal{M}$. The defense cost $R(a, \mathcal{M})$ in (11) and the expected worst-case impact of stealthy attacks $Q(a, \mathcal{M})$ in (12) are bounded if, and only if, the monitor set $\mathcal{M}$ is a dominating set of $\mathcal{G}$. ◁

Proof: Let us consider the following continuous LTI systems $\Sigma_\rho \triangleq (-\bar{L}, e_a, e_\rho^\top, 0)$ and $\Sigma_{m_k} \triangleq$

$(-\bar{L}, e_a, e_{m_k}^\top, 0)$, $\forall m_k \in \mathcal{M}$. The systems have the same stealthy data injection attack at the input of an arbitrary attack vertex a but Σ_ρ has an output at an arbitrary target vertex $\rho \in \mathcal{V}_{-a}$ and Σ_{m_k} has an output at monitor vertex $m_k \in \mathcal{M}$. Based on *Definition 2*, *Assumption 2* guarantees that the relative degree of Σ_ρ is not lower than one, i.e., $r_{(\rho,a)} \geq 1$.

We begin by providing sufficiency. *Assumption 3* ensures that there exists at least one dominating set that has at most n_s elements. Therefore, the defender selects the monitor set $\mathcal{M}$ as one of such dominating sets. According to *Definitions 2-3*, there exists at least one system Σ_{m_k}, where its input is at an arbitrary attack vertex a and its output is at the monitor vertex m_k ($m_k \in \mathcal{M}$), such that its relative degree is not greater than one, i.e., $r_{(m_k,a)} \leq 1$. Based on the above observation, one has $r_{(m_k,a)} \leq 1 \leq r_{(\rho,a)}$, fulfilling (17). From the results in *Theorem 1* and *Lemma 1*, the satisfaction of (17) allows us to guarantee the boundedness of the worst-case impact of stealthy attacks (7). Therefore, the defense cost $R(a, \mathcal{M})$ and the expected worst-case impact of stealthy attacks $Q(a, \mathcal{M})$ are bounded based on their definitions in (11)-(12).

For necessity, let us present a contradiction argument by assuming that the defense cost $R(a, \mathcal{M})$ and the expected worst-case impact of stealthy attacks $Q(a, \mathcal{M})$ are bounded while the monitor set $\mathcal{M}$ is not a dominating set of $\mathcal{G}$. Based on the definitions of $Q(a, \mathcal{M})$ and $R(a, \mathcal{M})$ in (11)-(12), they are bounded if, and only if, $J_\rho(a, \mathcal{M})$ is bounded for all pairs of ρ and a. Since the attack vertex a can be chosen arbitrarily and the monitor set $\mathcal{M}$ is not a dominating set, the attack vertex a can be chosen such that it does not belong to $\mathcal{M}$ and none of its neighbors belongs to $\mathcal{M}$, resulting in $r_{(m_k,a)} > 1$ $\forall m_k \in \mathcal{M}$. On the other hand, the adversary considers all the possibilities of the target vertex ρ including $(\rho, a) \in \mathcal{E}$, resulting in $r_{(\rho,a)} = 1$. The above observation gives us $r_{(\rho,a)} = 1 < r_{(m_k,a)}$, $\forall m_k \in \mathcal{M}$, violating the necessary and sufficient condition (17). Hence, for this particular pair of ρ and a, the worst-case impact of stealthy attacks $J_\rho(a, \mathcal{M})$ is unbounded, contradicting the assumption. ■

Lemma 4 enables us to determine whether a subset of $\mathcal{V}$ is a dominating set. On the other hand, *Theorem 2* affords us to restrict the admissible actions of the defender to dominating sets of $\mathcal{V}$. This step is beneficial to the defender in selecting monitor vertices such that the defense cost (11) and the expected worst-case impact of stealthy attacks (12) are always bounded. More detail on how the defender and the malicious adversary select their actions is given in the following section.

Remark 6: The condition (18) enables us to seek all the dominating sets of a given network. Leveraging the structure of (18), we sequentially multiply each row of $(A + I)$ with $\sum_{m_k \in \mathcal{M}} e_{m_k}$. Whenever the result is equal to zero, we stop the examination and determine that the subset $\mathcal{M}$ is not a dominating set. Otherwise, it is a dominating set. Moreover, since the examination of each subset of the vertex set $\mathcal{V}$ is independent, it can be executed by parallel computations with the help of computer clusters. ◁

TABLE I: Components of the Stackelberg security game between a defender and a malicious adversary.

Component	Description
Players	Defender and Adversary
Model knowledge of two players	The vertex set $\mathcal{V}$, the edge set $\mathcal{E}$, the self-loop gains θ_i, the alarm threshold δ_i ($\forall i \in \mathcal{V}$)
Action Space	Defender: $\mathbb{D} = \{\mathcal{M} \mid \mathcal{M} \subset \mathcal{V}, \lvert\mathcal{M}\rvert \leq n_s, (18)\}$ Adversary: $\mathbb{A} = \mathcal{V}$
Game Payoff & Goal	Defender minimizes $R(a, \mathcal{M})$ defined in (11) Adversary maximizes $Q(a, \mathcal{M})$ defined in (12)
Information Structure	Defender takes action first Adversary responds to Defender's action

V. Stackelberg Security Game

In this section, to assist the defender and the malicious adversary in selecting their best actions, we employ the Stackelberg game-theoretic framework where the defender acts as *the leader* and the malicious adversary acts as *the follower* of the game. Subsequently, we provide an algorithm to illustrate the procedure of how the two agents seek their best actions.

A. Game setup

To investigate the best actions of the defender and the adversary, we assume that they are two strategic players in a game. The defender can select at most n_s monitor vertices on which to place one sensor at each selected vertex with the purpose of monitoring malicious activities. Given *Assumption 3*, let us denote the collection of dominating sets as $\mathbb{D}$, where each dominating set has at most n_s elements, i.e., $\mathbb{D} = \{\mathcal{M} \mid \mathcal{M} \subset \mathcal{V},\ \lvert\mathcal{M}\rvert \leq n_s,\ \mathcal{M} \text{ satisfies } (18)\}$. This collection $\mathbb{D}$ is chosen as the action space of the defender. Meanwhile, the malicious adversary is able to select any vertex to conduct the stealthy data injection attack, i.e., the action space of the malicious adversary is $\mathbb{A} = \mathcal{V}$.

Based on the catastrophic consequences caused by famous malware such as Stuxnet and Industroyer [2], [3], the defender should decide their defense strategy regardless of the presence of malicious adversaries since the defender does not know when adversaries attack the system. Consequently, it is reasonable to let the defender select and announce their action publicly before the presence of the adversary [14], [22], [23]. The defender is called *the leader* while the malicious adversary is called *the follower*. The purpose of the defender is to minimize the defense cost $R(a, \mathcal{M})$ in (11) with knowing that the malicious adversary bases their action on the leader's decision. Thus, the leader considers the following problem.

Problem 1: Given that the malicious adversary maximizes (12), the defender selects an optimal dominating set $\mathcal{M}^\star \in \mathbb{D}$ that minimizes the cost (11). ◁

We cast the *Problem 1* in the Stackelberg game-theoretic framework with the defender as the leader, who selects and announces their action first, and the malicious adversary as the follower. The components of the Stackelberg game between the defender and the malicious adversary are summarized in Table I. This Stackelberg game always admits an optimal action [21], which is defined below.

Definition 4 (Stackelberg optimal action [35]): If there exists a mapping $\mathcal{T} : \mathbb{D} \to \mathbb{A}$ such that, for any fixed $\mathcal{M} \in \mathbb{D}$,

one has $Q(\mathcal{TM},\mathcal{M}) \geq Q(a,\mathcal{M})$ for all $a \in \mathbb{A}$, and if there exists $\mathcal{M}^\star \in \mathbb{D}$ such that $R(\mathcal{TM}^\star,\mathcal{M}^\star) \leq R(\mathcal{TM},\mathcal{M})$ for all $\mathcal{M} \in \mathbb{D}$, then the pair $(a^\star(\mathcal{M}^\star),\mathcal{M}^\star) \in \mathbb{A}\times\mathbb{D}$, where $a^\star(\mathcal{M}^\star)=\mathcal{TM}^\star$, is called a Stackelberg optimal action with the defender as the leader and the adversary as the follower of the game. ◁

Based on *Definition 4*, we first analyze the Stackelberg optimal action and then provide two solutions that find it in the following subsection.

B. Stackelberg optimal action

Recall *Problem 1* and *Definition 4*, the defender finds their optimal action by solving the following optimization problem:

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\in\mathbb{D}} \; R(a^\star(\mathcal{M}),\mathcal{M}), \tag{19}$$

where

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \; Q(a,\mathcal{M}). \tag{20}$$

One can verify that the optimal solution $(a^\star(\mathcal{M}^\star),\mathcal{M}^\star)$ found through solving the optimization problems (19)-(20) is equivalent to the one in *Definition 4*. To obtain the best monitor set $\mathcal{M}^\star$ by solving (19), we provide the following proposition.

Proposition 1: Consider the networked control system (4)-(6) associated with an undirected connected graph $\mathcal{G}$. Denote $\mathbb{D}$ as a non-empty collection of all the dominating sets $\mathcal{D}_i$ of the graph $\mathcal{G}$ with a cardinality of at most n_s, i.e., $\mathbb{D}=\{\mathcal{D}_1,\mathcal{D}_2,\ldots,\mathcal{D}_{|\mathbb{D}|}\}$. For each dominating set $\mathcal{D}_i$, let $z_i=\sum_{m\in\mathcal{D}_i} e_m$ be an N-dimensional binary vector, where j-th entry of z_i being equal to 1 indicates that vertex j belongs to $\mathcal{D}_i$. Define v as a $|\mathbb{D}|$-dimensional binary vector where i-th entry of v being equal to 1 indicates that D_i is chosen as a monitor set. Then, the optimal monitor set is determined by $v^\star$, which is the optimal solution to the following mixed-integer semidefinite programming problem:

$$\begin{aligned}
\min_{\bar{z}_{(a,\rho)}\in\mathbb{R}^N,\, v\in\{0,1\}^{|\mathbb{D}|},\, P_{(a,\rho)}\in\mathbb{R}^{N\times N},\, \beta>0} \quad & \mathfrak{c}(|\mathcal{M}|)+\beta \qquad (21)\\
\text{s.t.} \quad & \mathbf{1}_{|\mathbb{D}|}^\top v = 1,\; P_{(a,\rho)}=P_{(a,\rho)}^\top \geq 0,\\
& \sum_{\rho\in\mathcal{V}_{-a}} \pi_a(\rho)\,\delta^\top \bar{z}_{(a,\rho)} \leq \beta,\\
& 0\leq \bar{z}_{(a,\rho)} \leq \tilde{M}\,[z_1,z_2,\ldots,z_{|\mathbb{D}|}]\,v,\\
& \begin{bmatrix} -\bar{L}P_{(a,\rho)}-P_{(a,\rho)}\bar{L} & P_{(a,\rho)}e_a \\ e_a^\top P_{(a,\rho)} & 0 \end{bmatrix} + \mathbf{diag}\left(\begin{bmatrix} e_\rho \\ 0 \end{bmatrix}\right)\\
& - \mathbf{diag}\left(\begin{bmatrix} \bar{z}_{(a,\rho)} \\ 0 \end{bmatrix}\right) \leq 0, \quad \forall\,(a\,,\,\rho)\in\mathcal{V}\times\mathcal{V}_{-a},
\end{aligned}$$

where $\mathbf{1}_{|\mathbb{D}|}$ stands for a $|\mathbb{D}|$-dimensional all-one vector, $\delta=[\delta_1,\delta_2,\ldots,\delta_N]^\top$ is the alarm threshold vector of all the vertices, and $\tilde{M}$ is a large positive number, also called a "big M" [17]. ◁

Proof: The proof is omitted due to limited space. ■

Successfully solving (21) gives us the best monitor set $\mathcal{M}^\star$ represented by the optimal solution $v^\star$. However, dealing with the large mixed-integer SDP (21), which contains $N\times(N-1)$ attack scenarios for all possible pairs (a,ρ), poses efficiency challenges in very large networks. To deal with such an issue, we leverage parallel computations mentioned in *Remark 6* and propose *Algorithm 1*. The following section discusses how the proposed concept of dominating sets significantly alleviates the computational complexity in large networks.

Algorithm 1 Stackelberg optimal action through parallel computations

Input: The vertex set $\mathcal{V}$, the edge set $\mathcal{E}$, the self-loop gains θ_i, the alarm thresholds $\delta_i,\ \forall i\in\mathcal{V}$, the sensor budget n_s, the cost of utilized sensors $\mathfrak{c}(|\mathcal{M}|)$, the conditional belief $\pi_a(\rho)$, and n_c computer cores where j-th core is denoted as $U_j,\ j\in\{1,2,\ldots,n_c\}$.
Output: The best monitor set $\mathcal{M}^\star$ and the best attack vertex $a^\star(\mathcal{M}^\star)$.
Initialize: $\mathbb{D}=\{\mathcal{M}\,|\,\mathcal{M}\subset\mathcal{V},\ |\mathcal{M}|\leq n_s,\ (18)\}$
Equally divide $\mathbb{D}$ into n_c partitions $\{\mathbb{D}_1,\mathbb{D}_2,\ldots,\mathbb{D}_{n_c}\}$ where partition $\mathbb{D}_j$ is assigned to computer core U_j.
for every computer core U_j **do**
  for every dominating set $\mathcal{M}$ in $\mathbb{D}_j$ **do**
    for every pair $(a\,,\,\rho)\in\mathcal{V}\times\mathcal{V}_{-a}$ **do**
      solve (10).
    end for
    Compute (11).
  end for
end for
Solve (19) to obtain $\mathcal{M}^\star$ and $a^\star(\mathcal{M}^\star)$.

Remark 7: Let us discuss the solution to (19) in the absence of *Assumption 2*. Given that the attack and the distant target vertices are the same, the worst-case impact of stealthy attacks (7) is bounded when the attack vertex belongs to the set of monitor vertices according to *Theorem 1*. Therefore, to guarantee the boundedness of (7) for an arbitrary attack vertex, the defender has to trivially monitor all the vertices, i.e., (19) only admits a single trivial solution $\mathcal{M}\equiv\mathcal{V}$. To have a richer and more interesting allocation problem, we desire to use *Assumption 2*.

VI. Computational Complexity

In this section, we highlight the benefits of characterizing admissible monitor sets as dominating sets to the computation, especially in large-scale networked control systems.

Without the consideration of the collection $\mathbb{D}$ in *Proposition 1*, the security allocation problem requires the defender to solve (21) with the collection of all the subsets of the vertex set $\mathcal{V}$, whose cardinality is denoted as $S(N,n_s)$ where N is the number of vertices in the network and n_s is the sensor budget. This number $S(N,n_s)$ can be computed as follows:

$$S(N,n_s)=\sum_{k=1}^{n_s}\binom{N}{k}. \tag{22}$$

This number $S(N,n_s)$ grows dramatically when either the number of vertices N or the sensor budget n_s increases due to $S(N,n_s)=\mathcal{O}(N^{n_s})$, where $\mathcal{O}$ stands for Big O notation.

An illustration of the dramatic increase of $S(N,n_s)$ with respect to N (blue dashed-dotted line) can be found in Figure 2

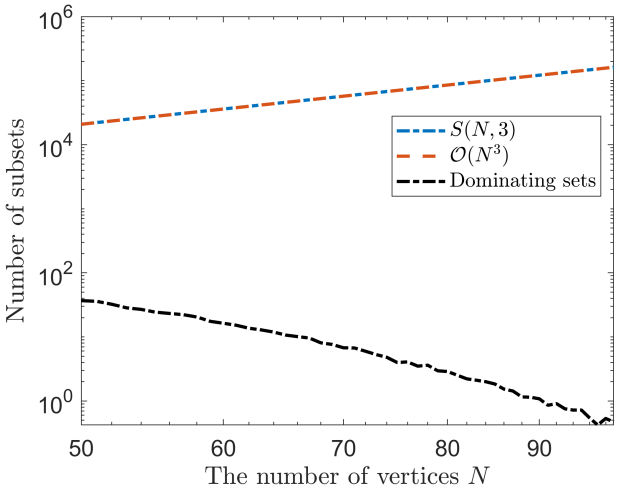

Fig. 2: Given $n_s = 3$, the number of subsets of the vertex set $\mathcal{V}$ with respect to the number of vertices has the same slope as $\mathcal{O}(N^3)$. The average number of dominating sets is given through the Monte-Carlo simulation with 500 samples.

where it has the same slope as $\mathcal{O}(N^3)$ (red dashed line). In Figure 2, we also conduct Monte-Carlo simulations with 500 samples to count the number of dominating sets with respect to the size of the graph N, which is denoted as the black dashed-dotted line. In the Monte-Carlo simulations, we examine Erdős–Rényi random undirected connected graphs $G(N, q)$, where N is the number of vertices and an edge is included to connect two vertices with a probability $q = 0.5$ [36]. By observing the results in Figure 2, the number of dominating sets with a fixed sensor budget dramatically decreases when the size of networks increases. Therefore, adopting the concept of dominating sets in solving (21) enables us to significantly reduce its computational complexity.

Regarding the parallel computation proposed in *Algorithm 1*, the concept of dominating sets plays a crucial role in practice. The number of possible actions computed by (22) possibly requires the defender to employ a large number of working hours of computer cores, which are limited in practice. In fact, as the number of vertices increases, the number of possible actions grows significantly (see Figure 2), making the solution methodology impractical in dealing with the security problem in very large networks. In contrast, the number of dominating sets with a fixed sensor budget typically decreases with respect to the size of random graphs (as seen in the example in Figure 2), requiring greatly fewer working hours of computer cores. As a result, the concept of dominating sets enables us to practically handle the security allocation problem in very large networks.

It is worth noting that the proposed method is carried out in the design phase, which can be computed offline. Moreover, the proposed method can be improved by utilizing parallel computation toolboxes and computer clusters as discussed above (see *Remark 6* and *Algorithm 1*). Thus, the computational complexity does not significantly impact the implementation of the proposed method (see more discussions in [14, Sec. V]). In the next section, we are likely to show the effectiveness of the proposed security allocation scheme with the notion of dominating sets through a numerical example.

VII. Numerical Example

In the first part of this section, we validate the main result of this paper presented in *Theorem 2* and find the Stackelberg optimal action for the defender and the malicious adversary in a numerical example. In the remainder of this section, the alleviation in the computational complexity will be discussed. The simulation is performed using Matlab 2023b with YALMIP 2021 [37] and MOSEK solver on a personal computer with 2.9-GHz, 8-core Intel i7-10700 processor and 16 GB of RAM.

To demonstrate the obtained results, let us consider an example of a 50-vertex networked control system depicted in Figure 3. The 50-vertex graph is an Erdős–Rényi random undirected connected graph where an edge is included to connect two vertices with a probability of 0.5. Parameters of the system are selected as follows: $\theta_i = 0.5$, $\delta_i = 1$, $\forall i \in \mathcal{V}$; the cost for the number of utilized sensors is set as $\mathfrak{c}(|\mathcal{M}|) = \kappa|\mathcal{M}|$ where $\kappa = 5$; the beliefs of the defender and the malicious adversary in the location of the target vertex given an attack vertex are assumed to be uniformly distributed; and the sensor budget $n_s = 3$. It is worth noting that the mixed-integer SDP (21) considers all possible pairs of $(a, \rho) \in \mathcal{V} \times \mathcal{V}_{-\rho}$, yielding $50 \times 49 = 2450$ attack scenarios, which are considerable.

A. The Stackelberg optimal action

First, we begin with finding all the dominating sets of the considered 50-vertex graph (see Figure 3). By investigating all the subsets $\mathcal{M} \subset \mathcal{V}$ where $|\mathcal{M}| \leq n_s$, twenty subsets satisfy the necessary and sufficient condition (18), which are dominating sets. One of those dominating sets is illustrated in Figure 3 where elements of the dominating set are coded blue. The computational time for finding dominating sets with the sensor budget $n_s = 3$ is under one second.

Next, we validate the obtained result of *Theorem 2*. From Figure 3, let us consider a system $\Sigma_{m_k} \triangleq (-\bar{L}, e_a, e_{m_k}^\top, 0)$ where e_a represents the input at any vertex and e_{m_k} represents the monitor output at a blue vertex. We simply examine that there exists at least one blue vertex such that the relative degree of Σ_{m_k} is never greater than one. Thus, the cost for the defender and the expected worst-case impact of stealthy attacks are always bounded according to the result in *Theorem 2*. To validate their boundedness, we compute the defense cost (11) and the expected worst-case impact of stealthy attacks (12) for an arbitrary pair of a vertex $a \in \mathcal{V}$ and a dominating set $\mathcal{M}$. Through the computation, the maximum cost for the defender and the maximum expected worst-case impact of stealthy attacks are obtained as follows: $R(a, \mathcal{M}) \leq 50.2456$ and $Q(a, \mathcal{M}) \leq 48.4235$, which verifies the result in *Theorem 2*.

Finally, the best monitor set $\mathcal{M}^\star$ is found by directly solving (21). The optimal action $\mathcal{M}^\star$ for the defender consists of three blue vertices in Figure 3 that yields the minimum cost of $R(a^\star(\mathcal{M}^\star), \mathcal{M}^\star) = 49.7985$. Given such an optimal action $\mathcal{M}^\star$, the corresponding attack vertex $a^\star(\mathcal{M}^\star)$ yields

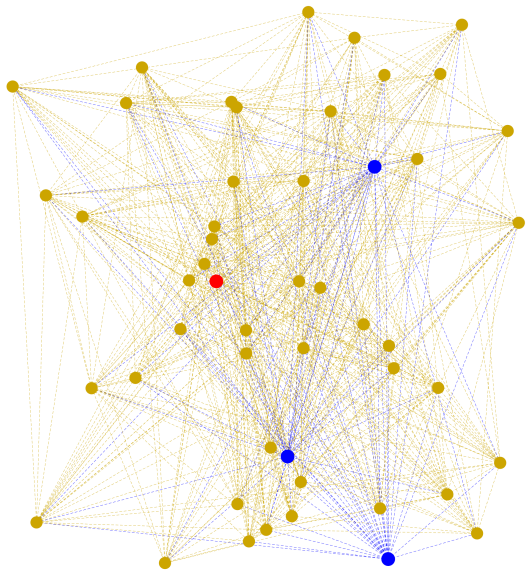

Fig. 3: 50-vertex graph where the optimal monitor vertices are coded blue and the optimal attack vertex is coded red.

the maximum expected worst-case impact of stealthy attacks $Q(a^\star(\mathcal{M}^\star), \mathcal{M}^\star) = 47.9764$.

B. Computational complexity

As discussed above, the 50-vertex networked control system (see Figure 3) gives us twenty dominating sets where the sensor budget is three ($n_s = 3$). This number is extremely smaller than the number of subsets of the vertex set which has at most n_s elements, i.e., $S(50, 3) = 20875$. Solving the mixed-integer SDP (21) normally employs the branch-and-bound algorithm. Adopting the concept of dominating sets considers 20 branches instead of 20875 branches, significantly saving computational resources. On the other hand, if we go for the parallel computation suggested in *Algorithm 1*, we only need to request 20 computer cores for those dominating sets, which are suitable for many computer cluster platforms.

VIII. Conclusion

In this paper, we investigated the security allocation problem in a networked control system faced with a stealthy data injection attack. The uncertain target vertex allowed us to formulate the objective functions of the defender and the adversary by considering probabilistic locations of the malicious target. We presented a necessary and sufficient condition based on dominating sets under which the defender guarantees the boundedness of their cost and the expected worst-case impact of stealthy attacks. The security allocation problem was cast in the Stackelberg game-theoretic framework where the defender plays the leader and the malicious adversary acts as the follower. Then, we provided an algorithm to show the procedure of finding the Stackelberg optimal action. The advantage of the proposed security allocation scheme was highlighted in the context of large-scale networks via a discussion on the computational burden and several numerical simulations. In future work, we can empower the adversary by allowing them to conduct attack signals on multiple vertices or sophisticated attacks such as multiplicative false data injection attacks and communication edge removal attacks. Further, we plan to characterize the Stackelberg optimal action for the defender and the adversary through graph properties such as centrality measures.

Appendix I
Proof of Lemma 1

Showing (13) is trivial when the monitor vertex set $\mathcal{M}$ has only one vertex. We assume that $\mathcal{M}$ has more than one monitor vertex. From the worst-case impact of stealthy attacks (7), let us introduce the following optimization by removing $|\mathcal{M}| - 1$ constraints except the constraint corresponding to a monitor vertex $m_k \in \mathcal{M}$ as follows:

$$J_\rho(a, m_k) = \sup_{x(0)=0,\ \zeta \in \mathcal{L}_{2e}} \|y_\rho\|_{\mathcal{L}_2}^2 \quad \text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}. \tag{23}$$

The design of the optimization problem (23) tells us that its feasible set contains the feasible set of the optimization problem (7). Further, the two optimization problems (7) and (23) have the same objective function. This implies that $J_\rho(a, \mathcal{M}) \leq J_\rho(a, m_k)$ for all $m_k \in \mathcal{M}$, directly resulting in (13).

Appendix II
Proof of Lemma 3

Let us denote a tuple $(\bar{\lambda}_{m_k}, \bar{x}_{m_k}, \bar{g}_{m_k}) \in \mathbb{C} \times \mathbb{C}^N \times \mathbb{C}$ as a zero dynamics of Σ_{m_k}, where a finite $\bar{\lambda}_{m_k}$ is called a finite invariant zero of Σ_{m_k}. From *Definition 1*, one has that the tuple $(\bar{\lambda}_{m_k}, \bar{x}_{m_k}, \bar{g}_{m_k})$ satisfies

$$\begin{bmatrix} \bar{\lambda}_{m_k} I + \bar{L} & -e_a \\ e_{m_k}^\top & 0 \end{bmatrix} \begin{bmatrix} \bar{x}_{m_k} \\ \bar{g}_{m_k} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{24}$$

The above equation is rewritten as

$$\begin{bmatrix} (\bar{\lambda}_{m_k} - \theta_0) I + \bar{L} + \theta_0 I & -e_a \\ e_{m_k}^\top & 0 \end{bmatrix} \begin{bmatrix} \bar{x}_{m_k} \\ \bar{g}_{m_k} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \tag{25}$$

where $\theta_0 \in \mathbb{R}_+$ is a uniform offset self-loop control gain. From (25), the finite value $(\bar{\lambda}_{m_k} - \theta_0) \in \mathbb{C}$ is an invariant zero of a new state-space model $\tilde{\Sigma}_{m_k} \triangleq (-\bar{L} - \theta_0 I, e_a, e_{m_k}^\top, 0)$. For all $\bar{\lambda}_{m_k} \in \mathbb{C}$ satisfying (25), the control gain θ_0 can be adjusted such that $\theta_0 > \mathrm{Re}(\bar{\lambda}_{m_k})$, resulting in that $\tilde{\Sigma}_{m_k}$ has no finite unstable zero. Then, the self-loop control gains $\theta_i,\ i \in \{1, 2, \ldots, N\}$, in (2) are tuned with θ_0 such that the system Σ_{m_k} is identical with $\tilde{\Sigma}_{m_k}$. By this tuning procedure, the system Σ_{m_k} also has no finite unstable invariant zero.

APPENDIX III
PROOF OF THEOREM 1

The result in *Lemma 2* enables us to investigate invariant zeros of the systems Σ_ρ and Σ_{m_k}, $\forall m_k \in \mathcal{M}$. Based on *Lemma 3*, Σ_{m_k} has no finite unstable invariant zero, which leaves us to analyze infinite invariant zeros of those systems. Recall the equivalence between the relative degree of an SISO system and the degree of its infinite zero (see *Remark 4*), a necessary condition to guarantee the boundedness of the optimization problem (14) is that there exists at least one system $\Sigma_{m_k}(m_k \in \mathcal{M})$ such that the number of its infinite invariant zeros is not greater than that of the system Σ_ρ. This implies $r_{(m_k,a)} \leq r_{(\rho,a)}$. For sufficiency, it remains to show that if $r_{(m_k,a)} \leq r_{(\rho,a)}$, all the infinite zeros of the system Σ_{m_k} are also infinite zeros of the system Σ_ρ. The following proof is adapted from our previous results in [12, Th. 7]. In the investigation, we make use of the definition of infinite invariant zeros in [38, Def. 2.4]. We investigate infinite zeros of Σ_{m_k} and Σ_ρ by starting from their transfer functions with zero initial states

$$G_{(\rho,a)}(s) = e_\rho^\top (sI + \bar{L})^{-1} e_a = \frac{P_{(\rho,a)}(s)}{Q(s)},$$
$$G_{(m_k,a)}(s) = e_{m_k}^\top (sI + \bar{L})^{-1} e_a = \frac{P_{(m_k,a)}(s)}{Q(s)}, \quad (26)$$

where $s \in \mathbb{C}$ is the Laplace complex variable. Based on *Remark 4*, it gives that $P_{(\rho,a)}(s)$, $P_{(m_k,a)}(s)$, and $Q(s)$ are the polynomials of degrees $N - r_{(\rho,a)}$, $N - r_{(m_k,a)}$, and N, respectively. Let us denote $z_\tau = \sigma_\tau + j\omega_\tau \in \mathbb{C}$, $\tau \in \{1, 2, \ldots, r_{(m_k,a)}\}$ with infinite module as infinite invariant zeros of Σ_{m_k}. Indeed, the zero z_τ $(1 \leq \tau \leq r_{(m_k,a)})$ is an infinite invariant zero of maximal degree $r_{(m_k,a)}$ of the system Σ_{m_k} [38, Def. 2.4] if it satisfies

$$\lim_{\|z_\tau\| \to \infty} z_\tau^q G_{(m_k,a)}(z_\tau) = 0, \ (0 \leq q \leq r_{(m_k,a)} - 1),$$
$$\lim_{\|z_\tau\| \to \infty} z_\tau^{r_{(m_k,a)}} G_{(m_k,a)}(z_\tau) \neq 0. \quad (27)$$

Further, with $0 \leq q \leq r_{(m_k,a)} - 1$, we also basically have

$$\lim_{\|z_\tau\| \to \infty} z_\tau^q G_{(\rho,a)}(z_\tau) = \lim_{\|z_\tau\| \to \infty} \frac{z_\tau^q P_{(\rho,a)}(z_\tau)}{Q(z_\tau)} = 0. \quad (28)$$

The above limit (28) holds because the denominator $z_\tau^q P_{(\rho,a)}(z_\tau)$ is the polynomial of degree $N - r_{(\rho,a)} + q \leq N - 1 < N$, where N is the degree of the polynomial $Q(z_\tau)$. This implies that any infinite zeros z_τ of maximal degree $r_{(m_k,a)}$ of the system Σ_{m_k} are also infinite zeros of degree $r_{(m_k,a)}$ of the system Σ_ρ.

APPENDIX IV
PROOF OF LEMMA 4

Let us decompose $\mathcal{C}(\mathcal{M}) \triangleq \mathcal{C}_A(\mathcal{M}) + \mathcal{C}_I(\mathcal{M})$ where $\mathcal{C}_A(\mathcal{M}) \triangleq \sum_{m_k \in \mathcal{M}} A e_{m_k}$ and $\mathcal{C}_I(\mathcal{M}) \triangleq \sum_{m_k \in \mathcal{M}} e_{m_k}$. Entry i-th of $\mathcal{C}_I(\mathcal{M})$ takes 0 if vertex i does not belong to $\mathcal{M}$ and 1 if vertex i belongs to $\mathcal{M}$. Entry i-th of $\mathcal{C}_A(\mathcal{M})$ takes 0 if all the neighbors of vertex i do not belong to $\mathcal{M}$ and a non-zero value if at least one neighbor of vertex i belongs to $\mathcal{M}$. Thus, entry i-th of $\mathcal{C}(\mathcal{M})$ takes 0 if vertex i and all of its neighbors do not belong to $\mathcal{M}$; takes a non-zero value if vertex i or one of its neighbors belong to $\mathcal{M}$. If the condition (18) fulfills, the vector $\mathcal{C}(\mathcal{M})$ has no zero entry. This implies that an arbitrary vertex in $\mathcal{V}$ is either a vertex of $\mathcal{M}$ or a neighbor of a vertex of $\mathcal{M}$, resulting in that $\mathcal{M}$ is a dominating set.

REFERENCES

[1] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[2] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011.

[3] N. Kshetri and J. Voas, "Hacking power grids: A current problem," *Computer*, vol. 50, no. 12, pp. 91–95, 2017.

[4] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334–1342, 2011.

[5] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2009, pp. 911–918.

[6] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 4907–4919, 2019.

[7] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber–physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.

[8] X.-X. Ren and G.-H. Yang, "Kullback–leibler divergence-based optimal stealthy sensor attack against networked linear quadratic gaussian systems," *IEEE Transactions on Cybernetics*, vol. 52, no. 11, pp. 11 539–11 548, 2021.

[9] Z. Li, A. T. Nguyen, A. M. Teixeira, Y. Mo, and K. H. Johansson, "Secure state estimation with asynchronous measurements against malicious measurement-data and time-stamp manipulation," in *2023 62nd IEEE Conference on Decision and Control (CDC)*. IEEE, 2023, pp. 7073–7080.

[10] Q. Zhu and T. Basar, "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*, vol. 35, no. 1, pp. 46–65, 2015.

[11] J. L. Wang, G.-H. Yang, and J. Liu, "An lmi approach to $\mathcal{H}$-index and mixed $\mathcal{H}_-/\mathcal{H}_\infty$ fault detection observer design," *Automatica*, vol. 43, no. 9, pp. 1656–1665, 2007.

[12] A. T. Nguyen, A. M. H. Teixeira, and A. Medvedev, "A single-adversary-single-detector zero-sum game in networked control systems," *IFAC-PapersOnLine*, vol. 55, no. 13, pp. 49–54, 2022.

[13] D. Umsonst, S. Sarıtaş, G. Dán, and H. Sandberg, "A bayesian nash equilibrium-based moving target defense against stealthy sensor attacks," *IEEE Transactions on Automatic Control*, 2023.

[14] P. Shukla, L. An, A. Chakrabortty, and A. Duel-Hallen, "A robust stackelberg game for cyber-security investment in networked control systems," *IEEE Transactions on Control Systems Technology*, vol. 31, no. 2, pp. 856–871, 2022.

[15] A. Gupta, C. Langbort, and T. Başar, "Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 71–81, 2016.

[16] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "A hybrid stochastic game for secure control of cyber-physical systems," *Automatica*, vol. 93, pp. 55–63, 2018.

[17] J. Milošević, M. Dahan, S. Amin, and H. Sandberg, "Strategic monitoring of networked systems with heterogeneous security levels," *IEEE Transactions on Control of Network Systems*, 2023.

[18] C. Wu, X. Li, W. Pan, J. Liu, and L. Wu, "Zero-sum game-based optimal secure control under actuator attacks," *IEEE Transactions on Automatic Control*, vol. 66, no. 8, pp. 3773–3780, 2020.

[19] A. T. Nguyen, S. C. Anand, and A. M. Teixeira, "A zero-sum game framework for optimal sensor placement in uncertain networked control systems under cyber-attacks," in *2022 IEEE 61st Conference on Decision and Control (CDC)*. IEEE, 2022, pp. 6126–6133.

[20] M. Pirani, E. Nekouei, H. Sandberg, and K. H. Johansson, "A game-theoretic framework for security-aware sensor placement problem in networked control systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 7, pp. 3699–3706, 2021.

[21] T. Başar and G. J. Olsder, *Dynamic noncooperative game theory*. SIAM, 1998.
[22] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A stackelberg game analysis," *IEEE Transactions on Automatic Control*, vol. 63, no. 10, pp. 3503–3509, 2018.
[23] H. Yuan, Y. Xia, J. Zhang, H. Yang, and M. S. Mahmoud, "Stackelberg-game-based defense analysis against advanced persistent threats on cloud control system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1571–1580, 2019.
[24] C. L. DeMarco, J. Sariashkar, and F. Alvarado, "The potential for malicious control in a competitive power systems environment," in *Proceeding of the 1996 IEEE International Conference on Control Applications IEEE International Conference on Control Applications held together with IEEE International Symposium on Intelligent Contro*. IEEE, 1996, pp. 462–467.
[25] M. S. Kang, S. B. Lee, and V. D. Gligor, "The crossfire attack," in *2013 IEEE symposium on security and privacy*. IEEE, 2013, pp. 127–141.
[26] M. Pirani, J. A. Taylor, and B. Sinopoli, "Strategic sensor placement on graphs," *Systems & Control Letters*, vol. 148, p. 104855, 2021.
[27] I. R. Petersen, V. A. Ugrinovskii, and A. V. Savkin, *Robust control design using H-8 methods*. Springer Science & Business Media, 2000.
[28] H. L. Trentelman and J. C. Willems, *The dissipation inequality and the algebraic Riccati equation*. Springer, 1991.
[29] A. Teixeira, H. Sandberg, and K. H. Johansson, "Strategic stealthy attacks: the output-to-output ℓ_2-gain," in *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 2015, pp. 2582–2587.
[30] R. S. Ross, "Guide for conducting risk assessments," 2012.
[31] J. C. Harsanyi, "Games with incomplete information played by "bayesian" players, i–iii part i. the basic model," *Management science*, vol. 14, no. 3, pp. 159–182, 1967.
[32] G. F. Franklin, J. D. Powell, A. Emami-Naeini, and J. D. Powell, *Feedback control of dynamic systems*. Prentice hall Upper Saddle River, NJ, 2002, vol. 4.
[33] H. K. Khalil, "Nonlinear systems third edition," *Patience Hall*, vol. 115, 2002.
[34] M. Mueller, "Normal form for linear systems with respect to its vector relative degree," *Linear algebra and its applications*, vol. 430, no. 4, pp. 1292–1312, 2009.
[35] M. Simaan and J. B. Cruz Jr, "On the stackelberg strategy in nonzero-sum games," *Journal of Optimization Theory and Applications*, vol. 11, no. 5, pp. 533–555, 1973.
[36] B. Bollobás and B. Bollobás, *Random graphs*. Springer, 1998.
[37] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *2004 IEEE international conference on robotics and automation (IEEE Cat. No. 04CH37508)*. IEEE, 2004, pp. 284–289.
[38] K. Morris and R. Rebarber, "Invariant zeros of siso infinite-dimensional systems," *International journal of control*, vol. 83, no. 12, pp. 2573–2579, 2010.

Anh Tung Nguyen received the degree of engineer in automatic control from Hanoi University of Science and Technology, Vietnam, in 2018 and the M.Sc. degree in aerospace engineering from Sejong University, South Korea, in 2021. Currently, he is working toward a Ph.D. degree in automatic control with the Division of Systems and Control, Department of Information Technology, Uppsala University, Sweden. He was visiting scholars at the Kyushu University, Japan (2018), the University of Cyprus, Cyprus (2023), and the Lund University, Sweden (2024). His research interests include control theory, multi-agent systems, and cyber-physical security.

André M. H. Teixeira (Member, IEEE) received the M.Sc. degree in electrical and computer engineering from the Faculdade de Engenharia da Universidade do Porto, Porto, Portugal, in 2009, and the Ph.D. degree in automatic control from the KTH Royal Institute of Technology, Stockholm, Sweden, in 2014. He is an Associate Professor at the Department of Information Technology, Uppsala University, Sweden. Before this, he was an Associate Senior Lecturer at the Department of Electrical Engineering, Uppsala University (2017-2021). From 2015 to 2017, he was an Assistant Professor at the Faculty of Technology, Policy and Management, Delft University of Technology. Dr. Teixeira was awarded a Starting Grant by the Swedish Research Council in 2019, and the Future Research Leaders grant by the Swedish Foundation for Strategic Research in 2020. He received the Lilly and Sven Thuréus prize in 2023 from The Royal Society of Sciences at Uppsala. In 2023, the Knut and Alice Wallenberg Foundation appointed him as a Wallenberg Academy Fellow. Dr. Teixeira serves as Associate Editor for Automatica. His research interests include secure and resilient control systems, distributed anomaly detection, distributed optimization, and power systems.

Alexander Medvedev is a Professor of Control Engineering at Uppsala University, Sweden. He is also Director of Program in Automatic Control since 2013. Prof. Medvedev has received his MSc (honors, 1981) and PhD (1987) in automatic control from Leningrad Electrical Engineering Institute (LEEI), USSR. He was promoted to Associate Professor (docent) at LEEI in 1991. After a research visit to Åbo Akademi, Finland, (1990-1991), Prof. Medvedev joined Luleå University of Technology, Sweden, and served there as Lecturer, Acting Professor, and Full Professor from 1991 until 2003. In 2002 he moved to Uppsala, where he was appointed Full Professor and started a research group in Biomedical Systems and Control. Besides safe control, the current research interests of Prof. Medvedev are mathematical modeling in life sciences and medicine, feedback control of therapies, and quantification of symptoms in neurological diseases. He chaired the IEEE Technical Committee on Healthcare and Medical Systems for two terms in 2018-2023.