Robust Structural Analysis and Design of Distributed Control Systems to Prevent Zero Dynamics Attacks

Sean Weerakkody Xiaofei Liu Bruno Sinopoli

***Abstract*— We consider the design and analysis of robust distributed control systems (DCSs) to ensure the detection of integrity attacks. DCSs are often managed by independent agents and are implemented using a diverse set of sensors and controllers. However, the heterogeneous nature of DCSs along with their scale leave such systems vulnerable to adversarial behavior. To mitigate this reality, we provide tools that allow operators to prevent zero dynamics attacks when as many as p agents and sensors are corrupted. Such a design ensures attack detectability in deterministic systems while removing the threat of a class of stealthy attacks in stochastic systems. To achieve this goal, we use graph theory to obtain necessary and sufficient conditions for the presence of zero dynamics attacks in terms of the structural interactions between agents and sensors. We then formulate and solve optimization problems which minimize communication networks while also ensuring a resource limited adversary cannot perform a zero dynamics attacks. Polynomial time algorithms for design and analysis are provided.**

I. Introduction

Distributed control systems (DCSs) have become prevalent in today's world. A DCS is a system where components such as sensors, actuators, and controllers are separated over a large network. DCSs allows operators to control multiple local environments while simultaneously meeting various global objectives. The ability of a DCS to meet society's demands for large scale control has made such systems common in a variety of applications including sensor networks, the smart grid, vehicular systems, and manufacturing.

Nonetheless, distributed control systems provide attack surfaces for potential adversaries [1]. Indeed DCS rely on spatially distributed heterogenous subsystems and components, many of which are left unsupervised, creating vulnerability. Moreover, the health of a DCS may be dependent on the actions of multiple, possibly colluding, agents. Serious breaches have occured in control systems, for instance the Stuxnet attack [2] and the Maroochy Shire Incident [3].

We consider the setting of a DCS with up to p malicious agents or sensors. Our goal is to provide tools which allow an operator to characterize and design DCSs that can not be targeted by zero dynamics attacks. We demonstrate that implementing a zero dynamics attack is both necessary and sufficient for an adversary to remain stealthy in a DCS with deterministic dynamics and unknown initial state. We also show such an attack allows an adversary to remain hidden in stochastic systems. Remaining stealthy is a powerful capability, allowing attackers to act on a DCS unencumbered.

For a fixed set of attacked nodes, a zero dynamics attacks does not exist if and only if the attacker's subsystem is left invertible and strongly observable. Prior work [4]–[6] proves that these properties are, for almost all valid numerical realizations, linked to the structure of a system, defined by the interactions of the inputs, states, and outputs. Boukhobza et al. [5] derive sufficient and necessary graphical conditions which ensure structural left invertibility and strong observability. From a security perspective, these results assume the set of adversarial nodes is known. We extend this work by providing sufficient and necessary conditions, which guarantee no zero dynamics attacks exist from any feasible set of malicious nodes. We call a system that does not satisfy these conditions discreetly attackable. In special cases, we offer efficient algorithms that can verify these conditions.

From a design perspective, we address tradeoffs between the costs of communication and sensing and security requirements. Here, we formulate and solve optimization problems which minimize a linear function of the number of communication links and sensors in our DCS while ensuring our system is not discreetly attackable. In addition, we include constraints on which agents are allowed to communicate. We show that if communication is more costly than sensing, it is optimal to observe all agents, while if sensing is more costly than communicating it is optimal to observe the fewest number of agents that enable secure system design.

Prior work has characterized when systems are vulnerable to undetectable attacks to motivate robust design. Liu et al. [7] provided algebraic conditions which determine when the smart grid is vulnerable to stealthy attacks. Additionally, Mo et al. [8] consider stochastic systems and determine the extent to which an adversary can covertly bias a system's state. Zero dynamics attacks have been previously considered in both centralized control systems [9] and [10] and distributed algorithms [11], [12]. Here, Sundaram et al. in [11] determine graphical conditions under which a set of agents can resiliently compute an arbitrary function of their initial states. Pasqualetti et al. in [12] characterize attack identifiability/detectability from each node using connectivity.

We extend the work of Sundaram et al. [11] by focusing on the problem of attack detection and providing graphical conditions for the absence of zero dynamics attacks in the more general case that there are no self-loops among system agents. We also extend the work of Pasqualetti et al. in [12] which considers consensus systems and requires the

S. Weerakkody, X. Liu, and B. Sinopoli are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA 15213. Email: {sweerakk,xiaofeil,brunos}@andrew.cmu.edu.

This work is supported by the Department of Energy grant DE-OE0000779 and by the National Science Foundation grant CCF 1646526. S. Weerakkody is also supported in part by a Department of Defense National Defense Science & Engineering Graduate Fellowship.

network to be strongly connected. Specifically, we focus on general control systems and a DCS which may or may not be connected and derive conditions under which a single central operator can perform detection and identification. Moreover, we extend the works of both [11] and [12] by considering the problem of minimal robust DCS design.

Additionally, we examined the analysis and design of DCSs to prevent perfect attacks in our prior work [13], [14]. The set of perfect attacks are the complete set of stealthy attacks in deterministic control systems when the defender knows the initial state. We extend these prior results by considering a richer attack model, the zero dynamics attack, where we remove the defender's knowledge of the initial state. Designing a DCS to avoid perfect attacks will be insufficient to prevent zero dynamics attack (which are practically just as stealthy), thus motivating our efforts.

Notation: M^i and M_j are the ith row and jth column of matrix M. $M(i,j)$ or M_{ij} is the entry of M at row i, column j. M^T is the transpose of M. $|A|$ is the size of set A

II. System Model

Graphical Model: In this section we describe the modeling for our DCS. We assume there exists n agents, $\mathcal{X} \triangleq \{x_1, \cdots, x_n\}$ which communicate with each other and are observed by m sensors, $\mathcal{Y} \triangleq \{y_1, \cdots, y_m\}$ where $m \leq n$. We model interactions using a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with vertices $\mathcal{V} \triangleq \mathcal{X} \cup \mathcal{Y}$. The edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ capture agent/sensor interactions. If $(x_i, x_j) \in \mathcal{E}$, agent x_i sends messages to x_j. If sensor y_j measures state x_i, $(x_i, y_j) \in \mathcal{E}$. Each agent $x_i \in \mathcal{X}$ has a self-loop so $(x_i, x_i) \in \mathcal{E}$. The incoming neighbors to a node v_i or $N_{v_i}^I \subset \mathcal{V}$, and the outgoing neighbors $N_{v_i}^O \subset \mathcal{V}$ from v_i are

$$N_{v_i}^I \triangleq \{v_j | \; (v_j, v_i) \in \mathcal{E}\}, \quad N_{v_i}^O \triangleq \{v_j | \; (v_i, v_j) \in \mathcal{E}\}. \quad (1)$$

Algebraic Model: We assume each agent x_i has a scalar time dependent state $\mathbf{x}_i(k)$ with dynamics given as follows:

$$\mathbf{x}_i(k+1) = a_{ii}\mathbf{x}_i(k) + \mathbf{u}_i(k). \quad (2)$$

The input $\mathbf{u}_i(k)$ is a linear function of the states of x_i's incoming neighbors and a centrally known input $\mathbf{u}_i^{ff}(k)$ so

$$\mathbf{u}_i(k) = \mathbf{u}_i^{ff}(k) + \sum_{j \neq i} a_{ij}\mathbf{x}_j(k), \quad (3)$$

where $x_j \notin N_{x_i}^I \cap \mathcal{X} \implies a_{ij} = 0$. Without loss of generality $\mathbf{u}_i^{ff}(k) = 0$. Each agent is assumed to have a scalar state though vector states can be examined. The state $\mathbf{x}_i(k)$ can refer to a physical quantity such as temperature or simply a quantity for distributed processing (e.g. consensus).

A set of dedicated sensors $\mathcal{Y}$ measure the state of a subset of agents. The outputs are sent to a central operator for estimation and detection. A dedicated sensor measures the state of one agent and no two sensors measure the same agent. The output of sensor y_i measuring x_j at time k is

$$\mathbf{y}_i(k) = \mathbf{x}_j(k). \quad (4)$$

Remark 1: The assumption of dedicated sensors is made since the system is distributed and no one sensor likely can measure the states of multiple agents. Redundant sensors are ignored as it is assumed that if an attacker can corrupt one sensor measuring x_i, it can corrupt all sensors measuring x_i, especially if the hardware is identical.

For simplicity, we concatenate state and output vectors

$$\mathbf{x}(k) \triangleq \left[\mathbf{x}_1(k) \cdots \mathbf{x}_n(k)\right]^T, \; \mathbf{y}(k) \triangleq \left[\mathbf{y}_1(k) \cdots \mathbf{y}_m(k)\right]^T,$$

so that the dynamics of the full control system are given by

$$\mathbf{x}(k+1) = A\mathbf{x}(k), \quad \mathbf{y}(k) = C\mathbf{x}(k). \quad (5)$$

The pair (A, C) is assumed to be observable. Letting $\mathbf{1}$ be the indicator function, A and C can be defined entrywise:

$$A(i,j) = a_{ij}, \quad C(i,j) = \mathbf{1}_{(x_j, y_i) \in \mathcal{E}}.$$

The state $\mathbf{x}(0)$ is unknown to the operator. Since (A, C) is observable, the state can be estimated using a linear filter.

$$\hat{\mathbf{x}}(k+1) = (A - KCA)\hat{\mathbf{x}}(k) + K\mathbf{y}(k+1), \quad (6)$$

$$\mathbf{z}(k+1) = \mathbf{y}(k+1) - CA\hat{\mathbf{x}}(k). \quad (7)$$

Here, K is chosen so $(A - KCA)$ is Schur stable. The residue $\mathbf{z}(k)$ is a statistic often used to perform detection. Smaller residues are often indicative of normal behavior while larger residues are associated with faulty or malicious behavior.

III. Attack Model

Graphical Model: In this section we define our DCS model under attack. At time 0 an unknown subset of the agents and sensors F are compromised. No more than p agents and sensors can be corrupted. In other words, the operator would like the system to be resilient to up to p malicious failures. The set of all feasible sets of attacked nodes is given by $\mathcal{F}$:

$$\mathcal{F} = \{F \subset \mathcal{V} || F| \leq p\}. \quad (8)$$

We define the graph $\mathcal{G}_F^a = (\mathcal{V}_F^a, \mathcal{E}_F^a)$ of a DCS when a set $F = \{x_{l_1}, \cdots, x_{l_q}, y_{l_{q+1}}, \cdots, y_{l_{p'}}\}$, $(p' \leq p)$ of agents/sensors is compromised. We introduce attack input vertices $\mathcal{U}_F^a = \{u_1^a, \cdots, u_{p'}^a\}$. We assume there exists directed edges from $\mathcal{U}_F^a$ to F given by $\mathcal{E}_{\mathcal{U}_F^a, \mathcal{X}} \triangleq \{(u_1^a, x_{l_1}), \cdots, (u_q^a, x_{l_q})\}$ and $\mathcal{E}_{\mathcal{U}_F^a, \mathcal{Y}} \triangleq \{(u_{q+1}^a, y_{l_{q+1}}), \cdots, (u_{p'}^a, y_{l_{p'}})\}$. We then define $\mathcal{E}_F^a \triangleq \mathcal{E} \cup \mathcal{E}_{\mathcal{U}_F^a, \mathcal{X}} \cup \mathcal{E}_{\mathcal{U}_F^a, \mathcal{Y}}$ and $\mathcal{V}_F^a \triangleq \mathcal{V} \cup \mathcal{U}_F^a$.

Algebraic Model: We let $\mathbf{x}_i^a(k)$ represent the state of x_i under attack. If $(u_l^a, x_i) \in \mathcal{E}_F^a$, then the dynamics are

$$\mathbf{x}_i^a(k+1) = a_{ii}\mathbf{x}_i^a(k) + \sum_{j \neq i} a_{ij}\mathbf{x}_j^a(k) + \mathbf{u}_l^a(k), \quad (9)$$

where $\mathbf{u}_l^a(k)$ is an input from node u_l^a at time k. If x_i is secure then $\mathbf{u}_l^a(k) = 0$. We define $\mathbf{y}_i^a(k)$ as the output of y_i at time k under attack. If $(u_l^a, y_i) \cup (x_j, y_i) \subset \mathcal{E}_F^a$, then

$$\mathbf{y}_i^a(k) = \mathbf{x}_j^a(k) + \mathbf{u}_l^a(k). \quad (10)$$

If y_i is secure then in (10), $\mathbf{u}_l^a(k) = 0$. Concatening $\mathbf{x}_i^a(k)$, $\mathbf{y}_i^a(k)$, and $\mathbf{u}_i^a(k)$ into $\mathbf{x}^a(k), \mathbf{y}^a(k)$, and $\mathbf{u}^a(k)$, we have :

$$\mathbf{x}^a(k+1) = A\mathbf{x}^a(k) + B_F^a\mathbf{u}^a(k), \quad \mathbf{x}^a(0) = \mathbf{x}(0), \quad (11)$$

$$\mathbf{y}^a(k) = C\mathbf{x}^a(k) + D_F^a\mathbf{u}^a(k), \quad (12)$$

with $B_F^a(i,j) \triangleq \mathbf{1}_{(u_j^a,x_i)\in\mathcal{E}_{\mathcal{U}_F^a,\mathcal{X}}}, D_F^a(i,j) \triangleq \mathbf{1}_{(u_j^a,y_i)\in\mathcal{E}_{\mathcal{U}_F^a,\mathcal{Y}}}$. We assume the attacker knows (A, B_F^a, C, D_F^a). The estimator policy remains unchanged during an attack.

$$\hat{\mathbf{x}}^a(k+1) = (A - KCA)\hat{\mathbf{x}}^a(k) + K\mathbf{y}^a(k+1), \qquad (13)$$

$$\mathbf{z}^a(k+1) = \mathbf{y}^a(k+1) - CA\hat{\mathbf{x}}^a(k). \qquad (14)$$

IV. Zero Dynamics Attacks

In this section we determine the conditions which allow an adversary to inject an undetectable attack. We assume the goal of an attacker is to affect the state of the DCS without being detected, thus preventing operator interference.

Theorem 2 ([12]): A nonzero attack $\mathbf{u}^a(k)$ is stealthy for time $k \geq 0$, if and only if there exists $\delta\mathbf{x}(0)$ which satisfies

$$\delta\mathbf{x}(k+1) = A\delta\mathbf{x}(k) + B_F^a\mathbf{u}^a(k), \qquad (15)$$

$$0 = \delta\mathbf{y}(k) = C\delta\mathbf{x}(k) + D_F^a\mathbf{u}^a(k). \qquad (16)$$

Such an attack is known as a zero dynamics attack [9], [10]. Zero dynamics attacks are the only set of attacks which allow an adversary to remain stealthy in deterministic systems with unknown initial state. Even if the defender has some understanding of the initial state, a zero dynamics attack remains stealthy for sufficiently small $\delta\mathbf{x}(0)$.

Theorem 3: Consider the system under attack (11),(12),(13),(14) and the system operating normally (5),(6),(7). Define the residue bias due to an attack to be $\Delta\mathbf{z}(k) \triangleq \mathbf{z}^a(k) - \mathbf{z}(k)$. Then

$$\Delta\mathbf{z}(k) = -C(A - AKC)^k\delta\mathbf{x}(0). \qquad (17)$$

The proof is omitted due to space considerations. Since the matrix $A - KCA$ is Schur stable, $A - AKC$ is also Schur stable and the residue bias $\Delta\mathbf{z}(k)$ approaches 0, allowing an adversary to remain stealthy against operators who use residue based detectors. For general detectors, it can be shown that a quadratic function of the residue bias is linked to optimal decay rates on the probability of false alarm [15].

Remark 4: Zero dynamics attacks are also stealthy in more realistic stochastic systems where there exists both process and sensor noise. It can be shown that Theorem 3 holds in this case as well. Thus, designing systems which do not contain zero dynamics attacks, is a necessary condition for attack detectability in stochastic systems.

To design systems with no feasible zero dynamics attacks we introduce strong observability and left invertibility.

Definition 5: For fixed attack F, a system (A, B_F^a, C, D_F^a) is strongly observable if $\mathbf{y}^a(k) = 0$ for $k \geq 0$ in (11), (12) implies $\mathbf{x}^a(0) = 0$. It is left invertible if $\mathbf{y}^a(k) = 0$ for $k \geq 0$ and $\mathbf{x}^a(0) = 0$ in (11), (12) implies $\mathbf{u}^a(k) = 0$ for $k \geq 0$. We now obtain the following as a result of Theorem 2.

Theorem 6: Suppose (A, C) is observable. A zero dynamics attack on F does not exist if and only if the system (A, B_F^a, C, D_F^a) is strongly observable and left invertible.

Algebraic conditions for strong observability/left invertibility related to the matrix pencil are given in [16] (pg 165, 181).

We wish to design (A, C) so that (A, B_F^a, C, D_F^a) remains strongly observable and left invertible for all feasible attack vectors. We can use structural conditions to obtain a graphical characterization of these properties. We associate $\mathcal{G}_F^a$ with a tuple of structural matrices $([A], [B_F^a], [C], [D_F^a])$. Here, for a matrix M, $[M](i,j) \neq 0$ implies $M(i,j)$ is a free parameter. Alternatively, $[M](i,j) = 0$ implies $M(i,j) = 0$.

Observe that $\mathcal{E}_F^a = \mathcal{E}_{\mathcal{X},\mathcal{X}} \cup \mathcal{E}_{\mathcal{U}_F,\mathcal{X}} \cup \mathcal{E}_{\mathcal{X},\mathcal{Y}} \cup \mathcal{E}_{\mathcal{U}_F,\mathcal{Y}}$ where $\mathcal{E}_{\mathcal{X},\mathcal{X}} = \{(x_i, x_j) : [A](j,i) \neq 0\}$, $\mathcal{E}_{\mathcal{U}_F,\mathcal{X}} = \{(u_i, x_j) : [B_F^a](j,i) \neq 0\}$, $\mathcal{E}_{\mathcal{X},\mathcal{Y}} = \{(x_i, y_j) : [C](j,i) \neq 0\}$, and $\mathcal{E}_{\mathcal{U}_F,\mathcal{Y}} = \{(u_i, y_j) : [D_F^a](j,i) \neq 0\}$.

We note here that $\mathcal{G}$ is associated with the structural system $([A], [C])$. It can be shown that a system's structure can be linked to left invertibility and strong observability.

Definition 7: $([A], [B_F^a], [C], [D_F^a])$ is structurally left invertible and strongly observable if an admissible realization of (A, B_F^a, C, D_F^a) is left invertible and strongly observable.

We remark that if $([A], [B_F^a], [C], [D_F^a])$ is structurally strongly observable and left invertible, then every valid realization of (A, B_F^a, C, D_F^a) is strongly observable and left invertible except for a set of zero Lebesgue measure. Additionally, if $([A], [B_F^a], [C], [D_F^a])$ is not structurally strongly observable and left invertible, no valid realization of (A, B_F^a, C, D_F^a) is strongly observable and left invertible. Thus, we aim to design DCSs that are structurally strongly observable and left invertible for all feasible attack sets F since this will almost surely prevent zero dynamics attacks.

For ease of reference, we introduce the following definition to characterize vulnerable systems.

Definition 8: A system (A, C) is discreetly attackable if there is a set $F \in \mathcal{F}$ for which $([A], [B_F^a], [C], [D_F^a])$ is not structurally strongly observable and left invertible.

Remark 9: In [13], [14], we designed DCSs to avoid a class of stealthy attacks knowns as perfect attacks. The set of zero dynamics attacks is a richer set of attacks. As we will later show, designing minimal DCSs that avoid perfect attacks leaves a system vulnerable to zero dynamics attacks.

Remark 10: While we have designed our system to ensure deterministic detection, this work also allows us to design a DCS that can perform perfect attack identification. Specifically, a system which can detect $2p$ adversaries, can perform perfect identification in the presence of p attackers.

V. Graph Theory Preliminaries

In this section we introduce necessary preliminaries from graph theory. Consider a graph $G = (V, E)$. Two edges (v_1, v_2) and (v_1', v_2') are vertex disjoint or *v-disjoint* if $v_1 \neq v_1'$ and $v_2 \neq v_2'$. A set of edges are v-disjoint if each pair are v-disjoint. Consider sets $\mathcal{A} \subset V$ and $\mathcal{B} \subset V$. An edge (v_1, v_2) from $\mathcal{A}$ to $\mathcal{B}$ has $v_1 \in \mathcal{A}$ and $v_2 \in \mathcal{B}$. We define

$$\theta(\mathcal{A}, \mathcal{B}) \triangleq \text{max number of } v-\text{disjoint edges from } \mathcal{A} \text{ to } \mathcal{B}.$$

A *path* from a set $\mathcal{A} \subset V$ to $\mathcal{B} \subset V$, is a sequence $v_1, v_2, \cdots, v_r$ where $v_1 \in \mathcal{A}$, $v_r \in \mathcal{B}$, and $(v_i, v_{i+1}) \in E$ for $1 \leq i \leq r-1$. An *input output path* from $\mathcal{A} \subset V$ to $\mathcal{B} \subset V$ or IOP from $(\mathcal{A}, \mathcal{B})$ is a path from $\mathcal{A}$ to $\mathcal{B}$ with $v_j \notin \mathcal{A} \cup \mathcal{B}$, $2 \leq j \leq r-1$. A *simple* path has no repeated vertices. An *$\mathcal{A}$-rooted (topped) path* is a simple path with begin (end) vertex in $\mathcal{A}$. Two paths are *disjoint* if they contain no common vertices. Two paths are *internally disjoint* if they have no common vertices except for possibly the starting and ending vertices. In general l paths are (internally) disjoint if every pair of paths are (internally) disjoint. A set of l disjoint and simple paths from $\mathcal{A} \subset V$ to $\mathcal{B} \subset V$ is referred to as a *linking* of size l or a l-linking from $\mathcal{A}$ to $\mathcal{B}$. We define

$$\rho(\mathcal{A}, \mathcal{B}) \triangleq \text{size of the largest linking between } \mathcal{A} \text{ and } \mathcal{B}.$$

A *vertex separator* between $a \in V$ and $b \in V$ is a set $S \subset V \backslash \{a, b\}$ whose removal deletes all paths from a to b. As shorthand, we refer to S as a vertex separator between (a, b). A *minimum vertex separator* S between (a, b) is a vertex separator between (a, b) with the smallest size.

Theorem 11 (Menger [17]): The size of a minimum vertex separator S between (a, b) is equal to the maximum number of internally disjoint paths between a and b.

We define the set of *essential vertices*, $V_{ess}(\mathcal{A}, \mathcal{B}) \subset V$:

$$V_{ess}(\mathcal{A}, \mathcal{B}) \triangleq \{x | x \in \text{all } \rho(\mathcal{A}, \mathcal{B}) - \text{ linkings from } \mathcal{A} \text{ to } \mathcal{B}\}.$$

Suppose we add new vertices $\underline{a}$ and $\underline{b}$ to graph G where $\underline{a}$ has directed edges to $\mathcal{A}$ and $\underline{b}$ has directed edges coming from $\mathcal{B}$. Then, we have $V_{ess}(\mathcal{A}, \mathcal{B}) = \cup_{S \in \mathcal{S}} S$, where $\mathcal{S}$ is the set of all minimum vertex separators between (a, b).

VI. Structural Analysis of Stealthy Attacks

In this section, we obtain structural conditions to describe when our DCS is discreetly attackable. To obtain the most general result, we first remove our prior assumption that each agent has its own self-loop and each sensor measures a dedicated state. Moreover we define the graph $f(\mathcal{G}) \triangleq (\mathcal{V} \cup o, \mathcal{E}')$ by adding a node o with incoming directed edges from all sensors $\mathcal{Y}$ to graph $\mathcal{G}$. We have the following:

Theorem 12: A DCS is not discreetly attackable iff:

C1 For all $\mathcal{T} \subset \mathcal{X} \cup \mathcal{Y}$ with $|\mathcal{T}| = p$, $\theta(\mathcal{X}, (\mathcal{X} \cup \mathcal{Y}) \backslash \mathcal{T}) = n$.
C2 For all $x_i \in \mathcal{X}$, the minimum vertex separator S_i between (x_i, o) in $f(\mathcal{G})$ has size $|S_i| \geq p + 1$.

Proof: Sufficiency: We leverage the following result:

Lemma 13 ([5], [6]): For fixed $\mathcal{U}_F^a$, $|\mathcal{U}_F^a| = p$, a system is structurally strongly observable + left invertible iff for $\mathcal{G}_F^a$

ci $\theta(\mathcal{X} \cup \mathcal{U}_F^a, \mathcal{X} \cup \mathcal{Y}) = n + p$.
cii Every agent $x_i \in \mathcal{X}$ has a path to $\mathcal{Y}$.
ciii $\Delta_0 \subset V_{ess}(\mathcal{U}_F^a, \mathcal{Y})$

where $\Delta_0 = \{x \in \mathcal{X} | \rho(x \cup \mathcal{U}_F^a, \mathcal{Y}) = \rho(\mathcal{U}_F^a, \mathcal{Y})\}$.

C1 $\implies$ ci : Suppose C1 holds. WLOG we define $F = \{x_{l_1}, \cdots, x_{l_q}, y_{l_{q+1}}, \cdots, y_{l_p}\}$. We know by construction that $\theta(\mathcal{U}_F^a, F) = p$. Moreover, from C1 we know $\theta(\mathcal{X}, (\mathcal{X} \cup \mathcal{Y}) \backslash F) = n$. ci immediately follows for all feasible $F \in \mathcal{F}$.

C2 $\implies$ cii, ciii: Suppose C2 holds. Then, cii trivially follows for all $F \in \mathcal{F}$. Now, WLOG, assume $F = \{x_{l_1}, \cdots, x_{l_q}, y_{l_{q+1}}, \cdots, y_{l_p}\}$. Suppose ciii does not hold so there exists $x_i \in \mathcal{X}$ satisfying $x_i \in \Delta_0,\ x_i \notin V_{ess}(\mathcal{U}_F^a, \mathcal{Y})$.

Define $f^a(\mathcal{G}_F^a) \triangleq (\mathcal{V}_F^a \cup o \cup u \cup u_i, \mathcal{E}_F^{a\prime})$ by adding to graph $\mathcal{G}_F^a$, a node o with edges from $\mathcal{Y}$, a node u with edges to $\mathcal{U}_F^a$, and a node u_i with edges to $\mathcal{U}_F^a \cup x_i$. Then, there is a vertex separator S_F in $f^a(\mathcal{G}_F^a)$ between (u_i, o) of size $\rho(\mathcal{U}_F^a, \mathcal{Y}) \leq p$, which is also a vertex separator between (u, o). Thus, $S_F \subset V_{ess}(\mathcal{U}_F^a, \mathcal{Y})$. $x_i \notin V_{ess}(\mathcal{U}_F^a, \mathcal{Y})$ implies $x_i \notin S_F$. Since x_i has $p + 1$ disjoint paths to o, removing S_F from $f^a(\mathcal{G}_F^a)$, does not delete all paths from u_i to o, contradicting S_F as a vertex separator. Thus, ciii holds $\forall F \in \mathcal{F}$.

Necessity: $\sim$ C1 $\implies$ $\sim$ ci. Suppose C1 does not hold for some $F' \subset \mathcal{X} \cup \mathcal{Y}$ with $|F'| = p$. Assume an adversary attacks F'. Since $\mathcal{U}_{F'}^a$ only has directed edges to F', and $\theta(\mathcal{X}, (\mathcal{X} \cup \mathcal{Y}) \backslash F') < n$, we have $\theta(\mathcal{X} \cup \mathcal{U}_{F'}^a, \mathcal{X} \cup \mathcal{Y}) < n + p$.

Suppose C2 fails to hold. We show an attack to illustrate zero dynamics (15),(16). We begin with the following.

Lemma 14 ([4]): $\exists$ a unique minimum vertex separator S_i^* between (x_i, o) in $f(\mathcal{G})$ where every IOP from $(V_{ess}(N_{x_i}^O / \{x_i\}, \mathcal{Y}), o)$ in $f(\mathcal{G})$ has begin vertex in S_i^*.

We let $\delta \mathbf{x}(0) = e_i$, the ith canonical basis vector. WLOG, let $S_i^* = \{x_1, \cdots, x_l, y_{s_{l+1}}, \cdots, y_{s_{p'}}\}$, $p' \leq p$ and $p' > 0$ (needed for cii). Let $F = S_i^*$ and add inputs $\mathcal{U}_F^a$. Moreover, select $\mathbf{u}^a(k)$ so $\delta \mathbf{y}^{S_i^* \cap \mathcal{Y}}(k), \delta \mathbf{x}_1(k), \cdots, \delta \mathbf{x}_l(k) = 0$ for all $k \geq 0$. Here, $\delta \mathbf{y}^H(k)$ corresponds to values of $\delta \mathbf{y}(k)$ for sensors in H. WLOG $\mathcal{Y}/S_i^* \neq \emptyset$ and we must show $\delta \mathbf{y}^{\mathcal{Y}/S_i^*}(k) = 0$. $\mathcal{X}$ can be partitioned as follows:

$\mathcal{X}_1 = \{x \in \mathcal{X} | x \notin x_i\text{-rooted path}, x \in \mathcal{Y}/S_i^*\text{-topped path}\}$,
$\mathcal{X}_2 = \{x \in \mathcal{X} | x \notin x_i\text{-rooted path}, x \notin \mathcal{Y}/S_i^*\text{-topped path}\}$,
$\mathcal{X}_3 = \{x \in \mathcal{X} | x \in x_i\text{-rooted path}, x \notin \mathcal{Y}/S_i^*\text{-topped path}\}$,
$\mathcal{X}_4 = \{x \in \mathcal{X} | x \in x_i\text{-rooted path}, x \in \mathcal{Y}/S_i^*\text{-topped path}\}$.

Note any vertex $x_j \in \mathcal{X}$ not in a x_i-rooted path, cannot be part of a $\mathcal{U}_F^a$-rooted path. Otherwise, if there was a $\mathcal{U}_F^a$-rooted path, then $\exists$ a simple path from $S_i^*/\mathcal{Y}$ to x_j. Since x_i has a simple path to all $s \in S_i^*/\mathcal{Y}$, x_j is part of an x_i-rooted path, which is a contradiction. Permuting $\delta \mathbf{x}(k)$, we have:

$$A = \begin{bmatrix} A_{11} & 0 & 0 & 0 \\ A_{21} & A_{22} & 0 & 0 \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & 0 & 0 & A_{44} \end{bmatrix}, \ B_F^a = \begin{bmatrix} 0 \\ 0 \\ 0 \\ B_4 \end{bmatrix},$$

$$C^{\mathcal{Y}/S_i^*} = \begin{bmatrix} C_1 & 0 & 0 & C_4 \end{bmatrix},$$

$$\delta \mathbf{x}(k) = \begin{bmatrix} \delta \mathbf{x}^1(k)^T & \delta \mathbf{x}^2(k)^T & \delta \mathbf{x}^3(k)^T & \delta \mathbf{x}^4(k)^T \end{bmatrix}^T.$$

$\delta \mathbf{x}^j(k)$ is associated with agents $\mathcal{X}_j$. $C^{\mathcal{Y}/S_i^*}$ is the portion C associated with $\mathcal{Y}/S_i^*$. Since $\mathcal{X}_1$ and $\mathcal{X}_2$ are not part of x_i-rooted paths, they cannot be affected by $\mathcal{X}_3, \mathcal{X}_4$. Since $\mathcal{X}_2, \mathcal{X}_3$ are not part of $\mathcal{Y}/S_i^*$-topped paths, they do not affect $\mathcal{X}_4$ or $\mathcal{X}_1$. B_F^a is obtained from the fact that $S_i^*/\mathcal{Y} \subset \mathcal{X}_4$. $C^{\mathcal{Y}/S_i^*}$ is obtained since $\mathcal{X}_2, \mathcal{X}_3$ do not have $\mathcal{Y}/S_i^*$-topped paths.

Since $\delta \mathbf{x}^1(k+1) = A_{11} \delta \mathbf{x}^1(k),\ \delta \mathbf{x}^1(0) = 0$, $\delta \mathbf{x}^1(k) = 0$ for all k. Thus, the dynamics of sensors $\mathcal{Y}/S_i^*$ are given by

$$\delta \mathbf{x}^4(k+1) = A_{44} \delta \mathbf{x}^4(k) + B_4 \mathbf{u}^a(k) + 0, \tag{18}$$

$$\delta \mathbf{y}^{\mathcal{Y}/S_i^*}(k) = C_4 \delta \mathbf{x}^4(k) + 0. \tag{19}$$

In the special case that $S_i^* \subset \mathcal{Y}$, $\mathcal{X}_4 = \emptyset$ and the result follows. WLOG, assume $S_i^* \not\subset \mathcal{Y}$. To analyze $\mathcal{X}_4$, consider the partition $\bar{\mathcal{X}}_1, \bar{\mathcal{X}}_2, \bar{\mathcal{X}}_3, \bar{\mathcal{X}}_4, \bar{\mathcal{X}}_5 = S_i^*/\mathcal{Y}, \bar{\mathcal{X}}_6 = x_i$ where

1) $\bar{\mathcal{X}}_1 = \{x \in \mathcal{X}_4 \backslash (\bar{\mathcal{X}}_5 \cup \bar{\mathcal{X}}_6) | x \in \text{ IOP from } (x_i, S_i^*/\mathcal{Y})\}$,
2) $\bar{\mathcal{X}}_2 = \{x \in \mathcal{X}_4 \backslash \bar{\mathcal{X}}_5 | x \in \text{ IOP from } (S_i^*/\mathcal{Y}, \mathcal{Y}/S_i^*)\}$,
3) $\bar{\mathcal{X}}_3 = \{x \in \mathcal{X}_4 | x \in \text{IOP from } (x_i, \mathcal{Y}/S_i^*)\} - (\bar{\mathcal{X}}_1 \cup \bar{\mathcal{X}}_2 \cup \bar{\mathcal{X}}_5 \cup \bar{\mathcal{X}}_6)$,
4) $\bar{\mathcal{X}}_4 = \{x \in \mathcal{X}_4 | x \notin \text{IOP from } (x_i, \mathcal{Y}/S_i^*)\}$.

We verify this is a partition. If $x \in \bar{\mathcal{X}}_1$, $\exists$ an IOP from $(x_i, \mathcal{Y}/S_i^*)$ containing x since $\exists$ a path from $s \in S_i^*/\mathcal{Y}$

to $\mathcal{Y}/S_i^*$ without x_i. Indeed, consider p' internally disjoint paths from x_i to o which WLOG do not contain x_i as an intermediate vertex. Each path contains exactly one vertex of S_i^* and thus $\exists$ a path from $s \in S_i^*/\mathcal{Y}$ to $\mathcal{Y}/S_i^*$ not containing x_i. If $x \in \bar{\mathcal{X}}_2$, $\exists$ an IOP from $(x_i, \mathcal{Y}/S_i^*)$ containing x since there is a path from x_i to any $s \in S_i^*/\mathcal{Y}$ and an IOP from $(S_i^*/\mathcal{Y}, \mathcal{Y}/S_i^*)$ cannot contain x_i. It is clear, $\cup_{j=1}^6 \bar{\mathcal{X}}_1 = \mathcal{X}_4$.

Next, observe $\bar{\mathcal{X}}_3$ and $\bar{\mathcal{X}}_5$ are pairwise disjoint from all other subsets. Additionally, since S_i^* is vertex separator between (x_i, o) we note $x_i \notin \bar{\mathcal{X}}_2$. Thus, since $x_i \notin \bar{\mathcal{X}}_1$ and $x_i \notin \bar{\mathcal{X}}_4$, $\bar{\mathcal{X}}_6$ is pairwise disjoint from all other subsets. We next show $\bar{\mathcal{X}}_1 \cap \bar{\mathcal{X}}_2 = \emptyset$. The existence of $x \in \bar{\mathcal{X}}_1 \cap \bar{\mathcal{X}}_2$, implies $\exists$ a path from x_i to $\mathcal{Y}/S_i^*$ not containing $S_i^*/\mathcal{Y}$, which contradicts S_i^* as a vertex separator. Finally, $(\bar{\mathcal{X}}_1 \cup \bar{\mathcal{X}}_2) \cap \bar{\mathcal{X}}_4 = \emptyset$ since $x \in \bar{\mathcal{X}}_4$ cannot be part of an IOP from $(x_i, \mathcal{Y}/S_i^*)$.

We make the following claims about the partitioned sets.

Lemma 15: Let $x \in \bar{\mathcal{X}}_3$. There is a path from $S_i^*/\mathcal{Y}$ to x.

Proof: Suppose Not. If $x \in \bar{\mathcal{X}}_3$, $\exists$ an IOP from $(x_i, \mathcal{Y}/S_i^*)$ with x. Since $\nexists$ path from $S_i^*/\mathcal{Y}$ to x, $\exists$ an IOP from $(x_i, S_i^*/\mathcal{Y})$ with x, contradicting $\bar{\mathcal{X}}_1 \cap \bar{\mathcal{X}}_3 = \emptyset$. ■

Lemma 16: $\theta(\bar{\mathcal{X}}_1 \cup \bar{\mathcal{X}}_3 \cup \bar{\mathcal{X}}_4 \cup \bar{\mathcal{X}}_6, \bar{\mathcal{X}}_2 \cup \mathcal{Y}/S_i^*) = 0$.

Proof: If there was a directed edge from $a \in \bar{\mathcal{X}}_1 \cup \bar{\mathcal{X}}_6$ to $b \in \bar{\mathcal{X}}_2 \cup \mathcal{Y}/S_i^*$, then there is a path from x_i to $\mathcal{Y}/S_i^*$ containing edge (a, b), not containing $S_i^*/\mathcal{Y}$, contradicting S_i^* as a vertex separator. If there was a directed edge from $a \in \bar{\mathcal{X}}_3$ to $b \in \bar{\mathcal{X}}_2 \cup \mathcal{Y}/S_i^*$, by Lemma 15 there is a IOP from $(S_i^*/\mathcal{Y}, \mathcal{Y}/S_i^*)$ containing edge (a, b). This contradicts $\bar{\mathcal{X}}_3 \cap \bar{\mathcal{X}}_2 = \emptyset$. If there was a directed edge from $a \in \bar{\mathcal{X}}_4$ to $b \in \bar{\mathcal{X}}_2 \cup \mathcal{Y}/S_i^*$, there would be an IOP from $(x_i, \mathcal{Y}/S_i^*)$ containing x, contradicting the definition of $\bar{\mathcal{X}}_4$. ■

Let $\delta\bar{\mathbf{x}}^j(k)$ be states associated with $\bar{\mathcal{X}}_j$. Leveraging Lemma 16 and the fact that only $\bar{\mathcal{X}}_5$ has edges from $\mathcal{U}_F^a$:

$$\begin{aligned} &\delta\bar{\mathbf{x}}^2(k+1) = \bar{A}_{22}\delta\bar{\mathbf{x}}^2(k) + \bar{A}_{25}\delta\bar{\mathbf{x}}^5(k), \\ &\delta\mathbf{y}^{\mathcal{Y}/S_i^*}(k) = \bar{C}_2\delta\bar{\mathbf{x}}^2(k) + \bar{C}_5\delta\bar{\mathbf{x}}^5(k), \ \delta\bar{\mathbf{x}}^2(0) = 0. \end{aligned}$$

Recall, that $\mathbf{u}^a(k)$ is chosen so that $\delta\bar{\mathbf{x}}^5(k) = 0$. We then have that $\delta\mathbf{y}^{\mathcal{Y}/S_i^*}(k) = 0$ and Theorem 12 holds. ■

In prior work [13], [14], it was determined that at least p sensors were required to prevent perfect attacks. Removing knowledge of the initial state increases this requirement.

Corollary 17: A system is not discreetly attackable only if it contains at least $p + 1$ sensors.

Now that we have examined the general case, we wish to consider the instance where each agent has a self-loop.

Corollary 18: Suppose each agent $x_i \in \mathcal{X}$ has a self-loop. A DCS is not discreetly attackable iff the minimum vertex separator S_i between (x_i, o) has size $|S_i| \geq p + 1$.

Proof: It is sufficient to show that the self-loop condition implies ci for all $F \in \mathcal{F}$. WLOG, assume an arbitrary set of nodes F are attacked, $|F| = p$. Construct a maximum linking $\mathcal{L}$ from $\mathcal{U}_F^a$ to $\mathcal{Y}$. Since each agent has $p + 1$ paths to o, we know $\rho(\mathcal{U}_F^a, \mathcal{Y}) = p$ [13]. Let $\mathcal{X}_\mathcal{L}$ be the set of vertices in $\mathcal{X}$ belonging to $\mathcal{L}$. $\mathcal{L}$ gives a maximum set of $v-$ disjoint edges from $\mathcal{U}_F^a \cup \mathcal{X}_\mathcal{L}$ to $\mathcal{X}_\mathcal{L} \cup \mathcal{Y}$. Thus, $\theta(\mathcal{U}_F^a \cup \mathcal{X}_\mathcal{L}, \mathcal{X}_\mathcal{L} \cup \mathcal{Y}) = |\mathcal{X}_\mathcal{L}| + p$. Since each agent has a self-loop, $\theta(\mathcal{X}\backslash\mathcal{X}_\mathcal{L}, \mathcal{X}\backslash\mathcal{X}_\mathcal{L}) = |\mathcal{X}\backslash\mathcal{X}_\mathcal{L}|$. Therefore, $\theta(\mathcal{U}_F^a \cup \mathcal{X}, \mathcal{X} \cup \mathcal{Y}) = n + p$. ■

Remark 19: In [13], [14], we showed that having at least p disjoint paths from each agent x_i to o is necessary and sufficient to avoid perfect attacks. To prevent zero dynamics attacks, an extra disjoint path from x_i to o is required.

If $f(\mathcal{G})$ has self-loops at each agent, we can efficiently determine if a system is discreetly attackable. To determine if a fixed agent (x_i, o) has minimum vertex separator S_i of size $p+1$, we solve a $0-1$ maximum flow problem. We consider a graph $h^i(f(\mathcal{G})) = (\mathcal{V}_{H_i}, \mathcal{E}_{H_i})$, where $|\mathcal{V}_{H_i}| = 2|\mathcal{V}|$ and $|\mathcal{E}_{H_i}| \leq |\mathcal{E}'| + |\mathcal{V}| - 1$. Here, every $v \in \mathcal{V}\backslash x_i$ is converted to a pair of nodes, v_{in} and v_{out}, where $N_{v_{in}}^I = N_v^I$, $N_{v_{in}}^O = v_{out}$, $N_{v_{out}}^I = v_{in}$, $N_{v_{out}}^O = N_v^O$. Moreover, all incoming edges to x_i are removed. All edges in $\mathcal{E}_{H_i}$ have capacity 1. (x_i, o) has minimum vertex separator S_i of size at least $p+1$ if and only if the maximum flow from source x_i to sink o in $h^i(f(\mathcal{G}))$ is at least $p+1$. Using Dinic's algorithm, [18], [19] this can be determined in $O((2|\mathcal{V}|)^{\frac{1}{2}}(|\mathcal{E}'| + |\mathcal{V}| - 1))$ time. Since, we must verify $|S_i| \geq p+1$ for each of n agents, the worst case computational complexity is $O(n(2|\mathcal{V}|)^{\frac{1}{2}}(|\mathcal{E}'| + |\mathcal{V}| - 1))$. This outperforms algebraic methods based on the matrix pencil [16] and graphical methods based on Lemma 13 which verify a system's strong observability/left invertibility for fixed attack nodes. This is a combinatorial task since there exists $\binom{n+m}{p}$ possible attack vectors.

VII. Distributed Control System Design

Now that we determined structural conditions characterizing zero dynamics attacks, we consider the problem of design. Here, we aim to secure our system against p adversaries while minimizing costs of sensing and communication.

Communication Design: We first assume the structure of C, or $[C]$ is given. Due to physical/cost constraints on communication, certain agents can not communicate. This is encoded into $[\bar{A}]$, where $[\bar{A}]_{ji} \neq 0$ iff it is feasible for agent x_i to send messages to agent x_j. Again, let S_i be a minimal vertex separator between (x_i, o) in $f(\mathcal{G})$. We have:

$$\begin{aligned} \underset{[A]}{\text{minimize}} \quad & \|A\|_0 && (20) \\ \text{subject to} \quad & |S_i| \geq p+1, \ [A]_{ii} \geq 0, \ i \in \{1, \ldots, n\}, \\ & [\bar{A}]_{uv} = 0 \implies [A]_{uv} = 0, \ u, v \in \{1, \ldots, n\}. \end{aligned}$$

The objective function represents the number of communication links in our system. The first constraint ensures that our system is not discreetly attackable, while $[\bar{A}]_{uv} = 0 \implies [A]_{uv} = 0$ ensures we only select feasible links. We can leverage prior results from [13], which designs minimal DCSs that are not perfectly attackable. The difference is that eliminating perfect attacks requires $|S_i| \geq p$, while we require $|S_i| \geq p+1$ to prevent zero dynamics attacks.

Theorem 20 ([13]): Suppose Problem (20) is feasible. Then in an optimal solution, $\forall x_i \in \mathcal{X}$, $|N_{x_i}^O| = p+2$. Therefore $\|A\|_0^* = (n-m)(p+2) + m(p+1) = (p+2)n - m$.

(20) is solvable if $([\bar{A}], [C])$ is not discreetly attackable. This can be checked by solving n maximum flow problems.

Remark 21: When Problem (20) is feasible, the optimal value of Problem (20), $(p+2)n - m$, is independent of the communication constraints. Thus, a solution to Problem (20) with constraints defined by $[\bar{A}]$ is also a solution to Problem (20) in the absence of constraints.

As done in [13], we can solve n maximum flow problems to obtain an optimal solution $[A]$ to Problem (20).

Theorem 22 ([13]): Suppose Problem (20) is feasible. An optimal solution is found by performing Algorithm 1.

Algorithm 1 DCS Network Design

```
function OPTIMIZATION($[\bar{A}], [C]$)
    Let graph $\mathcal{G}$ be generated from $[\bar{A}], [C]$, $[A] = [\bar{A}]$.
    for $i = 1 : n$ do
        if $|N^O_{x_i}| > p + 2$ then
            Solve maximum flow algorithm on $h^i(f(\mathcal{G}))$ from source $x_i$ to sink $o$.
            If $x_i$ is observed (or unobserved), keep $p$ (or respectively $p + 1$) neighbors in $\mathcal{X}$ through which $\exists$ a maximum flow. Delete other outgoing neighbors in $\mathcal{X} - x_i$. Update $\mathcal{G}, [A]$.
        end if
    end for    return $[A]$
end function
```

Solving Algorithm 1 can be done through at most n maximum flow problems. Dinic's algorithm leads to the worst case complexity $O(n(2|\mathcal{V}|)^{\frac{1}{2}}(|\mathcal{E}'| + |\mathcal{V}| - 1))$ where $\mathcal{V}$ and $\mathcal{E}'$ are associated with matrices $[\bar{A}], [C]$. For simulations illustrating the efficiency of this approach see [13].

Joint Design: We now wish to minimize both sensing and communication costs through our choice of communication links and dedicated sensor placement. Suppose the cost of a communication link is $\alpha_1 \geq 0$ and the cost of a sensor is $\alpha_2 \geq 0$. We wish to solve the following:

$$\begin{aligned} \underset{[A],[C],m}{\text{minimize}} \quad & \alpha_1 \|A\|_0 + \alpha_2 m \qquad (21) \\ \text{subject to} \quad & |S_i| \geq p + 1,\ [A]_{ii} \geq 0,\ i \in \{1, \ldots, n\}, \\ & [\bar{A}]_{uv} = 0 \implies [A]_{uv} = 0,\ u, v \in \{1, \ldots, n\}, \\ & C \in \mathbb{R}^{m \times n},\ m \in \{p + 1, \cdots, n\}, \\ & \|C_j\|_0 \leq 1,\ j \in \{1, \ldots, n\}, \\ & \|C^t\|_0 = 1,\ t \in \{1, \ldots, m\}. \end{aligned}$$

The last three constraints state conveys that $[C]$ implements a set of m dedicated sensors where $m \in \{p + 1, \cdots, n\}$.

Theorem 23: Suppose communication is more costly than sensing $\alpha_1 > \alpha_2$, then every agent should be observed ($m = n$). Alternatively, if $\alpha_2 > \alpha_1$, then $m = p^*$, where p^* is the fewest number of sensors for which Problem (20) is feasible.

Proof: $\|A\|_0^* = (p + 2)n - m$ so the optimal value of (21) is $(\alpha_2 - \alpha_1)m + \alpha_1(p + 2)n$. The result follows. ■

When $\alpha_1 > \alpha_2$, $m = n$ and an optimal C^* satisfies $C^*_{ij} \neq 0 \iff i = j$. Alternatively, when $\alpha_2 > \alpha_1$ we must first obtain a set of dedicated sensors $[C^*]$ with $C^* \in \mathbb{R}^{p^* \times n}$ which makes Problem (20) feasible. Given C^*, Problem (21) can be then solved using Problem (20). However, determining p^* appears to be a combinatorial problem. Future work aims to discover efficient solutions.

VIII. Conclusion

We considered the analysis and design of distributed control systems to prevent zero dynamics attacks. We obtained a graphical condition to characterize the absence of zero dynamics attacks and demonstrated that in certain cases this condition was efficiently verifiable. We then consider the minimal design of DCSs to balance robustness with the cost of communication/sensing. Future work will consider a defender that has partial knowledge of the initial state and communication links/sensors with unique non-uniform costs.

References

[1] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *The 28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 495–500.

[2] R. Langner, "To kill a centrifuge: A technical analysis of what Stuxnet's creators tried to achieve," Langner Communications, Tech. Rep., November 2013. [Online]. Available: www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

[3] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Critical Infrastructure Protection*. Springer US, 2008, pp. 73–82.

[4] J. van der Woude, "The generic number of invariant zeros of a structured linear system," *SIAM Journal on Control and Optimization*, vol. 38, no. 1, pp. 1–21, 1999.

[5] T. Boukhobza, F. Hamelin, and S. Martinez-Martinez, "State and input observability for structured linear systems: A graph-theoretic approach," *Automatica*, vol. 43, no. 7, pp. 1204–1210, 2007.

[6] T. Boukhobza and F. Hamelin, "State and input observability recovering by additional sensor implementation: A graph-theoretic approach," *Automatica*, vol. 45, no. 7, pp. 1737–1742, 2009.

[7] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, Chicago, IL, 2009.

[8] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control*, Atlanta, Georgia, 2010, pp. 5967–5972.

[9] 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.

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[11] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1495–1508, 2011.

[12] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[13] S. Weerakkody, X. Liu, S. H. Son, and B. Sinopoli, "A graph theoretic characterization of perfect attackability for secure design of distributed control systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 60–70, 2017.

[14] ——, "A graph theoretic characterization of perfect attackability and detection in distributed control systems," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 1171–1178.

[15] S. Weerakkody, B. Sinopoli, S. Kar, and A. Datta, "Information flow for security in control systems," in *55th IEEE Conference on Decision and Control (CDC*. IEEE, 2016, pp. 5065–5072.

[16] H. Trentelman, A. A. Stoorvogel, and M. Hautus, *Control theory for linear systems*. Springer Science & Business Media, 2012.

[17] K. Menger, "Zur allgemeinen kurventheorie," *Fundamenta Mathematicae*, vol. 1, no. 10, pp. 96–115, 1927.

[18] E. A. Dinic, "An algorithm for the solution of the max-flow problem with the polynomial estimation," *Doklady Akademii Nauk*, vol. 194, no. 4, pp. 1277–1280, 1970.

[19] S. Even and R. E. Tarjan, "Network flow and testing graph connectivity," *SIAM Journal on Computing*, vol. 4, no. 4, pp. 507–518, 1975.