# Power Grid State Estimation Following a Joint Cyber and Physical Attack

Saleh Soltan, *Student Member, IEEE,* Mihalis Yannakakis, and Gil Zussman, *Senior Member, IEEE*

***Abstract*—This paper focuses on *joint cyber and physical attacks* on power grids and presents methods to retrieve the grid state information following such an attack. We consider a model where an adversary attacks a zone by physically disconnecting some of its power lines and blocking the information flow from the zone to the grids control center. We use tools from linear algebra and graph theory and leverage the properties of the power flow DC approximation to develop methods for information recovery. *Using information observed outside the attacked zone, these methods recover information about the disconnected lines and the phase angles at the buses.* We identify *sufficient conditions on the zone structure* and *constraints on the attack characteristics* such that these methods can recover the information. We also show that it is NP-hard to find an approximate solution to the problem of partitioning the power grid into the minimum number of attack-resilient zones. However, since power grids can often be represented by planar graphs, we develop a *constant approximation partitioning algorithm for these graphs* and numerically demonstrate its performance on real power grids.**

## I. Introduction

Cyber and physical attacks on power grids may cause large-scale blackouts due to a domino effect on power lines with major disruption in everyday life [2]–[6]. For example the December 2015 cyber attack on Ukraine's grid left 225,000 people without power for days [2] and the April 2014 physical attack on a California substation interfered with the power grid operation [3].

Power grids are comprised of two components: (i) the physical infrastructure of the power transmission system (power lines, substations, power stations), and (ii) the Supervisory Control and Data Acquisition (SCADA) system that monitors and controls the grid (the control network) (Fig. 1). The physical infrastructure is the target of physical attacks and SCADA is the target of cyber attacks.

In the case of a physical attack, the system's stability can be maintained if SCADA receives precise information about the location of the attack and takes proper action accordingly. If however, the flow of information is obstructed by a cyber attack, the SCADA is prevented from taking necessary and appropriate actions. This problem, the joint cyber and physical attacks on power grids, is the focus of our work. We develop methods to *estimate the state of the power grid following a joint cyber and physical attack, and study the resilience of different topologies as well as the resilience to different kinds of attacks.*

S. Soltan and G. Zussman are with the Elec. Eng. Dept. (e-mails: {saleh,gil}@ee.columbia.edu), and Mihalis Yannakakis is with the Comp. Sci. Dept. (email: mihalis@cs.columbia.edu) in Columbia University, New York, NY. A partial and preliminary version appeared in Proc. ACM SIGMETRICS'15 [1].

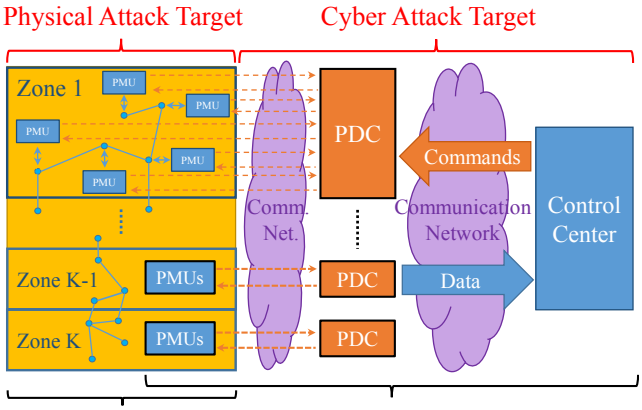



Fig. 1: Components of the power grid and potential attacks: physical attacks target the physical infrastructure (lines, substations, etc.); Cyber attacks target the SCADA system – an adversary can obstruct the flow of information from the PMUs within the zone to the control center.

We use the linearized *direct-current (DC) power flow model*,[1] a practical relaxation of the alternating-current (AC) model. We also use a modified version of the *control network model* [10] that includes Phasor Measurement Units (PMU), Phasor Data Concentrators (PDC), and a control center (Fig. 1). We define a *zone* as a set of buses (nodes), power lines (edges), PMUs, and an associated PDC. We analyze an attack that disconnects lines within a zone (physical attack) and obstructs the flow of information from the PMUs within the zone to the control center (cyber attack). For example, an adversary can perform the cyber attack by disabling the zone's associated PDC. Alternatively, the adversary can attack the communication network between the PMUs and the PDC, or between the PDC and the control center. Because our control network model is a generic model of SCADA that monitors the status of the grid, most of the results and methods provided in this paper can be interpreted and used for more complicated control systems and scenarios.

As a result of an attack, some lines get disconnected, and the phase angles and the status of the lines within the *attacked zone* $H = (V_H, E_H)$ become unavailable (Fig. 2). Our objective is to recover the phase angles and detect the disconnected lines using the information available outside of the attacked zone.

Power flows are governed by the laws of physics, where a line failure results in changes to flows and node phase angles throughout the power grid [11]. We use this property and

[1]The DC model is commonly used in large-scale contingency analysis of power grids [7]–[9].

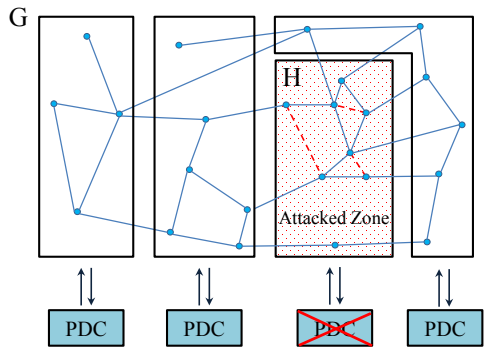



Fig. 2: $G$ is the power grid graph and $H$ is an induced subgraph of $G$ that represents the attacked zone. An adversary attacks a zone by disconnecting some of its power lines (red dashed lines) and disallowing the information from the PMUs within the zone to reach the control center.

show that it is possible to estimate the state in the attacked zone using the information available outside of the zone. Specifically, we *develop methods for retrieving information from the attacked zone* by applying matrix analysis and graph theoretical tools to the matrix representation of the DC equations.

We present *necessary and sufficient conditions on the structure of a zone such that our methods are guaranteed to recover the state of the grid inside the attacked zone*. We prove that if there is a *matching* between the nodes inside and outside the attacked zone that covers the inside nodes ($V_H$), then the phase angles of the nodes in the attacked zone are recoverable by solving a set of linear equations of size $|V_H|$. We also prove that if $H$ is *acyclic*, the disconnected lines in $H$ are detectable by solving a set of linear equations of size $|E_H|$. Moreover, we show that if $H$ is *planar*, under some constraints, the disconnected lines are detectable by solving a Linear Programming (LP) problem.

We develop another method for simultaneous recovery of phase angles and detection of disconnected lines by solving a single LP problem. We show that this method is guaranteed to recover the information under certain constraints on the attack (i.e., on the disconnected lines) if there is a *partial matching* between the nodes inside and outside of $H$, and if $H$ is *planar*. Based on these results, we present the Post-Attack Recovery and Detection (PARD) Algorithm. We propose that our methods can be generalized to the case where multiple zones are attacked simultaneously. We show that if the attacked zones are relatively distant from each other, any of the methods provided in this paper can be applied to recover the information and detect the failures in the attacked zones.

We briefly study the problem of information recovery in the presence of measurement noise. By relaxing some of the constraints introduced in developing the methods used in the PARD Algorithm, we provide a method for information recovery in the noisy scenarios as well. We numerically evaluate the performance of the method and show that if the Signal to Noise Ratio (SNR) is high enough, it can successfully recover the information.

We study the problem of partitioning power grids into the minimum number of attack-resilient zones (i.e., zones in which the information can be recovered by the methods mentioned above). We show that this problem is not approximable to within $n^{1-\epsilon}$ for all $\epsilon > 0$, unless P=NP. However, since power grids are often represented by planar graphs, we introduce our Zone Selection (ZS) Algorithm and demonstrate that the AZ Algorithm provides a constant approximation ratio for these graphs. We present numerical results to demonstrate the operation of the ZS Algorithm on several power grids. This algorithm can also be used for designing a secure control network for smart grids.

This paper presents three main contributions. We use matrix analysis and graph theoretical tools: (i) to develop methods to recover the phase angles and detect the disconnected lines after a joint cyber and physical attack, (ii) to find graph classes for which these methods are guaranteed to recover the information, and (iii) to develop an algorithm for partitioning the power grid into attack-resilient zones.

This paper is organized as follows. Section II reviews related work. Section III describes the models and reviews graph theoretical terms. In Section IV, we focus on information recovery and in Section V, we present the PARD Algorithm. Section VI provides results for the noisy scenario. In Section VII, we study the grid partitioning problem. Section VIII provides numerical results and Section IX provides concluding remarks and directions for future work. Due to space constraints some of the proofs are omitted and can be found in [1].

## II. Related Work

The vulnerability of general networks to attacks has been studied extensively (e.g., [12]–[14] and references therein). In particular, attacks and failures in power grids has been studied using probabilistic failure propagation models (e.g., [15]–[17], and references therein) as well as using deterministic DC power flows [7], [11], [18]–[20]. Malicious data attacks on the power grid control network have also been studied [21]–[24]. To the best of our knowledge however, no previous work has focused on vulnerability of power grids to joint cyber and physical attacks.

In Section IV, we study the problem of recovering the phase angles and detecting disconnected lines after a joint cyber and physical attack, a problem related to line outage identification from changes in phase angles [25], [26] [27]. These studies however, were based on complete knowledge of phase angle measurements and in the case of [25], [26] were limited to two line failures. The problem of line failure identification in an internal system using the information from an external system was studied in [9], where a heuristic algorithm was proposed for only one and two line failures.

In Section VII, we disucss the problem of partitioning the power grid into the minimum number of attack-resilient zones. This problem is similar to PMU placement problems [28]–[30]. Recently, PMU placemnet problem has attracted much attention in India after the major blackouts of 2013 [29]. In [30] the problem of PMU placement for line outage detection was studied. However, none of these previous works addressed the problem of PMU placement from the security point of view where both the PDC/PMUs and the physical network are under attack.

In Section VII, we reduce the attack-resilient zone partitioning problem to the problem of partitioning a graph into subgraphs where each subgraph is (i) acyclic, and (ii) there is a matching between nodes inside and outside the subgraph that covers all the subgraph nodes. This problem is closely related to the problems of *vertex arboricity* (which is known to be NP-hard to be determined [31, p.193]) and *k-matching cover* of a graph (which can be found in $O(n^3)$ time [32]). However, to the best of our knowledge, the joint problem ((i) and (ii) above) was not studied before.

## III. Model and Definitions

### A. DC Power Flow Model

We adopt the linearized (or DC) power flow model, which is widely used as an approximation for the non-linear AC power flow model [33]. In particular, we follow [7], [34]and represent the power grid by a connected undirected graph $G = (V, E)$ where $V = \{1, 2, \ldots, n\}$ and $E = \{e_1, \ldots, e_m\}$ are the set of nodes and edges corresponding to the buses and transmission lines, respectively. Each edge $e_i$ is a set of two nodes $e_i = \{u, v\}$. $p_v$ is the active power *supply* ($p_v > 0$) or *demand* ($p_v < 0$) at node $v \in V$ (for a *neutral node* $p_v = 0$). We assume *pure reactive* lines, implying that each edge $\{u, v\} \in E$ is characterized by its *reactance* $r_{uv} = r_{vu}$.

Given the power supply/demand vector $\vec{p} \in \mathbb{R}^{|V|\times 1}$ and the reactance values, a *power flow* is a solution $\mathbf{P} \in \mathbb{R}^{|V|\times|V|}$ and $\vec{\theta} \in \mathbb{R}^{|V|\times 1}$ of:

$$\sum_{v\in N(u)} p_{uv} = p_u, \ \forall\ u \in V \tag{1}$$

$$\theta_u - \theta_v - r_{uv}p_{uv} = 0, \ \forall\ \{u, v\} \in E \tag{2}$$

where $N(u)$ is the set of neighbors of node $u$, $p_{uv}$ is the power flow from node $u$ to node $v$, and $\theta_u$ is the phase angle of node $u$. Eq. (1) guarantees (classical) flow conservation and (2) captures the dependency of the flow on the reactance values and phase angles. Additionally, (2) implies that $p_{uv} = -p_{vu}$. When the total supply equals the total demand in each connected component of $G$, (1)-(2) has a unique solution [7, lemma 1.1].[2] Eq.(1)-(2) are equivalent to the following matrix equation:

$$\mathbf{A}\vec{\theta} = \vec{p} \tag{3}$$

where $\mathbf{A} \in \mathbb{R}^{|V|\times|V|}$ is the *admittance matrix* of $G$,[3] defined as follows:

$$a_{uv} = \begin{cases} 0 & \text{if } u \neq v \text{ and } \{u, v\} \notin E, \\ -1/r_{uv} & \text{if } u \neq v \text{ and } \{u, v\} \in E, \\ -\sum_{w\in N(u)} a_{uw} & \text{if } u = v. \end{cases}$$

Note that in power grids nodes can be connected by multiple edges, and therefore, if there are $k$ multiple edges between nodes $u$ and $v$, $a_{uv} = -\sum_{i=1}^{k} 1/r_{uv_i}$. Once $\vec{\theta}$ is computed, the flows, $p_{uv}$, can be obtained from (2).

[2]The uniqueness is in the values of $p_{uv}$s rather than $\theta_u$s (shifting all $\theta_u$s by equal amounts does not violate (2)).

[3]When $r_{uv} = 1\ \forall\{u, v\} \in E$, the admittance matrix $\mathbf{A}$ is the *Laplacian matrix* of the graph.

**Notation.** Throughout this paper we use bold uppercase characters to denote matrices (e.g., $\mathbf{A}$), italic uppercase characters to denote sets (e.g., $V$), and italic lowercase characters and overline arrow to denote column vectors (e.g., $\vec{\theta}$). For a matrix $\mathbf{Q}$, $q_{ij}$ denotes its $(i, j)^{\text{th}}$ entry. For a column vector $\vec{y}$, $\vec{y}^t$ denote its transpose, $y_i$ denotes its $i^{\text{th}}$ entry, $\|\vec{y}\|_1 := \sum_{i=1}^{n} |y_i|$ is its $l_1$-norm, $\|\vec{y}\|_2 := (\sum_{i=1}^{n} y_i^2)^{1/2}$ is its $l_2$-norm, and $\text{supp}(\vec{y}) := \{i | y_i \neq 0\}$ is its support.

### B. Control Network

We use a modified version of the model described in [10] to model the SCADA system to which we refer as the control network. Fig. 1 illustrates the components of the control network. We assume that there is a Phasor Measurement Unit (PMU) at each node of $G$. The PMU at node $i$ reports the phase angle $\theta_i$ as well as the status of the lines (either *operational* or *failed*) adjacent to node $i$. Phasor Data Concentrators (PDC) gather the data collected by PMUs. The data gathered by PDCs is sent to a control center which monitors and controls the entire grid. A *zone* is a subgraph induced by a subset of nodes with a single associated PDC.

### C. Attack Model

We study attacks on power grids that affect both the physical infrastructure and the control network. We assume that an adversary attacks a zone by: (i) disconnecting some edges within the attacked zone (physical attack), and (ii) obstructing the flow of information from the PMUs within the zone to the control center (cyber attack). An adversary can perform the cyber attack by, for example, disabling the zone's associated PDC. Alternatively, the communication network between the PMUs and the PDC or between the PDC and the control center can be attacked. We assume that disconnecting edges within a zone does not make $G$ disconnected.

Fig. 2 shows an example of an attack on the zone represented by $H$. Due to the attack, some edges are disconnected (we refer to these edges as *failed lines*) and the phase angles and the status of the lines within the *attacked zone* become unavailable. We denote the set of failed lines in zone $H$ by $F \subseteq E_H$. Upon failure, the failed lines are removed from the graph and the flows are redistributed according to (1)-(2).

**Notation.** Throughout this paper, we denote an attacked zone by $H = (V_H, E_H)$. Without loss of generality we assume that the indices are such that $V_H = \{1, 2, \ldots, |V_H|\}$ and $E_H = \{e_1, e_2, \ldots, e_{|E_H|}\}$. We denote the complement of the zone $H$ by $\bar{H} = G\backslash H$. If $X, Y$ are two subgraphs of $G$, $\mathbf{A}_{X|Y}$ and $\mathbf{A}_{V_X|V_Y}$ both denote the submatrix of the admittance matrix of $G$ with rows from $V_X$ and columns from $V_Y$. For instance, $\mathbf{A}$ can be written in any of the following forms,

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{H|H} & \mathbf{A}_{H|\bar{H}} \\ \mathbf{A}_{\bar{H}|H} & \mathbf{A}_{\bar{H}|\bar{H}} \end{bmatrix}, \mathbf{A} = \begin{bmatrix} \mathbf{A}_{G|H} & \mathbf{A}_{G|\bar{H}} \end{bmatrix}, \mathbf{A} = \begin{bmatrix} \mathbf{A}_{H|G} \\ \mathbf{A}_{\bar{H}|G} \end{bmatrix}.$$

We use the very same notation for the vectors. For instance $\vec{\theta}_H$ and $\vec{\theta}_{\bar{H}}$ are the vectors of phase angle of the nodes in $H$ and $\bar{H}$, respectively. We use the prime symbol ($'$) to denote the values after an attack. For instance, $G'$, $\mathbf{A}'$, and $\vec{\theta}'$ are used to represent the graph, the admittance matrix of the graph, and the phase angles of the nodes after an attack.

TABLE I: Summary of notation.

| Notation | Description |
|---|---|
| $G=(V,E)$ | The graph representing the power grid |
| $\mathbf{A}$ | Admittance matrix of $G$ |
| $\vec{\theta}$ | Vector of the phase angles of the nodes in $G$ |
| $H$ | A subgraph of $G$ representing the attacked zone |
| $F$ | Set of failed lines due to an attack |
| $\mathbf{D}$ | Incidence matrix of $G$ |
| $\bigcirc'$ | The value of $\bigcirc$ after an attack |
| $\overline{\bigcirc}$ | The complement of $\bigcirc$ |
| $\bigcirc^*$ | The dual of $\bigcirc$ |

### D. Graph Theoretical Terms

In this paper, we use several graph theoretical terms and theorems mostly borrowed from [35]. We briefly review some of the important definitions in this subsection.

**Subgraphs, Cuts, and Cycles:** Let $X$ and $Y$ be subsets of the nodes of a graph $G$. $G[X]$ denotes the subgraph of $G$ *induced* by $X$. We denote by $E[X,Y]$ the set of edges of $G$ with one end in $X$ and the other end in $Y$. We denote the complement of a set $X$ by $\bar{X}=V\backslash X$. The *coboundary* of $X$ is the set $E[X,\bar{X}]$ and is denoted by $\partial(X)$. $\partial(v)$ denotes the coboundary of $X=\{v\}$. $G[X,\bar{X}]$ denotes the subgraph of $G$ induced by the edges from $E[X,\bar{X}]$. $N(X)$ is the set of neighbors of the nodes in $X$ excluding $X$ itself, and $N_c(X)=X\cup N(X)$. We say that $Q\subseteq E$ is *$G$-separable*, if there are pairwise edge-disjoint cycles $C_q(q\in Q)$, such that $\forall q\in Q, q\in C_q$ [36].

**Planar Graphs:** A graph $G$ is *planar*, if it can be drawn in the plane so that its edges intersect only at their ends. A planar graph $G$ partitions the rest of the plane into a number of edgewise-connected open sets called the *faces* of $G$.

Given a planar graph $G$, its dual graph $G^*$ is defined as follows. Corresponding to each face $c$ of $G$ there is a node $c^*$ of $G^*$, and corresponding to each edge $e$ of $G$ there is an edge $e^*$ of $G^*$. Two nodes $c_1^*$ and $c_2^*$ are joined by the edge $e^*$ in $G^*$, if and only if their corresponding faces $c_1$ and $c_2$ are separated by the edge $e$ in $G$. It is easy to see that the dual $G^*$ of a planar graph $G$ is itself a planar graph [35].

**Incidence Matrix:** Suppose we assign an arbitrary orientation to the edges of $G$. We denote the set of oriented edges by $\mathcal{E}=\{\epsilon_1,\epsilon_2,\dots,\epsilon_m\}$. The (node-edge) *incidence matrix* of $G$ is denoted by $\mathbf{D}\in\{-1,0,1\}^{|V|\times|E|}$ and defined as follows,

$$d_{ij}=\begin{cases}0 & \text{if } \epsilon_j \text{ is not incident to node } i,\\ 1 & \text{if } \epsilon_j \text{ is coming out of node } i,\\ -1 & \text{if } \epsilon_j \text{ is going into node } i.\end{cases}$$

When we use the incidence matrix, we assume an arbitrary orientation for the edges unless we mention an specific orientation. $\mathbf{D}_H\in\{-1,0,1\}^{|V_H|\times|E_H|}$ is the submatrix of $\mathbf{D}$ with rows from $V_H$ and columns from $E_H$.

## IV. Attack Analysis

In this section, we study the effects of an attack and provide analytical methods for recovering the phase angles and detecting failed lines in the attacked zone $H$. We find conditions on the structural properties of a zone and constraints on the failed lines for which these methods successfully recover the phase angles and detect the failed lines. These conditions depend on the connections between $V_H$ and $\bar{V}_H$ as well as the inner connections of the nodes in $H$. Therefore, we refer to them as *external* and *internal* conditions on $H$, respectively. Finally, we briefly study the case in which multiple zones are attacked simultaneously. Table II summarizes the results regarding the resilience of a zone based on its internal and external conditions, and the constraints on the set of failed lines $F$.

In this section, when we describe our methods, we assume that there are no edges $\{i,j\}\in E_H$ for which $\theta_i'=\theta_j'$ (we refer to these edges as *null-edges*). Following (2), a null-edge does not carry any flow. Thus, we cannot detect the status of those edges since they cannot be distinguished from failed lines. However, we can detect the null-edges and treat them separately (we consider this in the PARD Algorithm provided in the next section).

### A. Recovery of Phase Angles

In this subsection, we introduce a method to recover the phase angles of the nodes in an attacked zone $H$. We provide sufficient conditions on $G[V_H,\bar{V}_H]$ such that the method recovers the phase angles of the nodes in $V_H$ successfully. As we mentioned, since these conditions depend only on the connections between $V_H$ and $\bar{V}_H$, we refer to them as the *external conditions* on $H$.

The following lemma is the first step towards designing the method for recovering the phase angles and for detecting the failed lines (see Subsection IV-B).

*Lemma 1:* $\mathrm{supp}(\mathbf{A}(\vec{\theta}-\vec{\theta}'))\subseteq V_H$.

*Proof:* Suppose $F=\{e_{i_1},e_{i_2},\dots,e_{i_k}\}\subseteq E_H$ are the edges that are disconnected from the grid after the attack on the zone $H$. Define the column vectors $\vec{x_1},\vec{x_2}\dots\vec{x_k}\in\{-1,0,1\}^n$ associated with the failed lines as follows. If $e_{i_j}=\{s_j,t_j\}$ then $\vec{x_j}$ is 1 in its $s_j{}^{th}$ entry, $-1$ in its $t_j^{\text{th}}$ entry, and 0 everywhere else. It is easy to see that $\mathbf{A}'$ is related to $\mathbf{A}$ as $\mathbf{A}'=\mathbf{A}-\sum_{j=1}^k a_{s_jt_j}\vec{x_j}\vec{x_j}^t$. Since the graph $G$ does not get disconnected after an attack, the flow equations in $G'$ are $\mathbf{A}'\vec{\theta}'=\vec{p}$. On the other hand, $\mathbf{A}\vec{\theta}=\vec{p}$, therefore $\mathbf{A}\vec{\theta}-\mathbf{A}'\vec{\theta}'=0$. Thus,

$$0=\mathbf{A}\vec{\theta}-\mathbf{A}'\vec{\theta}'=\mathbf{A}\vec{\theta}-\mathbf{A}\vec{\theta}'+\sum_{j=1}^k a_{s_jt_j}\vec{x_j}\vec{x_j}^t\vec{\theta}'$$

$$\Rightarrow \mathrm{supp}(\mathbf{A}(\vec{\theta}-\vec{\theta}'))\subseteq\bigcup_{i=1}^k\{s_j,t_j\}\subseteq V_H.\blacksquare$$

One of the immediate results of Lemma 1 is the following corollary. This corollary gives a true statement about $\vec{\theta}'$ (recall that $\vec{\theta}'$ is partly unknown). It states that $\vec{\theta}'$ is in the solution space of the matrix equation (4).

*Corollary 1:* For any $U\subseteq\bar{H}$, $\mathbf{A}_{U|N_c(U)}(\vec{\theta}_{N_c(U)}-\vec{\theta}'_{N_c(U)})=0$. In particular, when $U=\bar{H}$,

$$\mathbf{A}_{\bar{H}|G}(\vec{\theta}-\vec{\theta}')=0. \tag{4}$$

For simplicity of the notations and equations, through the most of this paper we consider the case in which $U=\bar{H}$. However, as we briefly describe in Subsection IV-D, using a smaller $U$ allows the recovery of the phase angles after an attack on multiple zones.

We find sufficient conditions such that the solution $\vec{\theta'}_H$ to (4) is unique (given $\vec{\theta}$ and $\vec{\theta'}_{\bar{H}}$), and consequently $\vec{\theta'}_H$ can be recovered after any attack on $H$. We first define a *well-supported* zone.

*Definition 1:* A zone $H$ is called *well-supported*, if $\vec{\theta'}_H$ can be recovered after any attack on $H$.

Using Corollary 1, the following theorem gives sufficient condition for a zone $H$ to be *well-supported*.

*Theorem 1:* A zone $H$ is *well-supported*, if $\mathbf{A}_{\bar{H}|H}$ has linearly independent columns.

*Proof:* From Corollary 1 we know that $\mathbf{A}_{\bar{H}|G}(\vec{\theta}-\vec{\theta'}) = 0$, therefore $\mathbf{A}_{\bar{H}|H}\vec{\theta'}_H = \mathbf{A}_{\bar{H}|\bar{H}}(\vec{\theta}_{\bar{H}} - \vec{\theta'}_{\bar{H}}) + \mathbf{A}_{\bar{H}|H}\vec{\theta}_H$. The only unknown in this equation is $\vec{\theta'}_H$. Now since $\mathbf{A}_{\bar{H}|H}$ has linearly independent columns, this equation has a unique solution $\vec{\theta'}_H$ which can be computed in polynomial time. Thus, $\vec{\theta'}_H$ can be recovered in this case and zone $H$ is well-supported. ∎

It can be seen that the sufficient condition in Theorem 1 depends on the reactance values. However, the following corollary relaxes the condition in Theorem 1. It shows that if $G[V_H, \bar{V}_H]$ has a matching that covers $V_H$, then for almost any reactance values for the edges in $E[V_H, \bar{V}_H]$, $H$ is *well-supported*. The idea is that the set of reactance values for the edges in $E[V_H, \bar{V}_H]$ for which $\mathbf{A}_{\bar{H}|H}$ does not have linearly independent columns is a measure zero set in the real space [37].

*Corollary 2:* If there is a matching in $G[V_H, \bar{V}_H]$ that covers $V_H$, then $H$ is *well-supported* almost surely.[4]

*Proof:* Suppose $M = (U, V_H)$ is the matching for $G[V_H, \bar{V}_H]$ that covers $V_H$, and suppose $U \subseteq \bar{V}_H$ are the matched nodes which are in $\bar{V}_H$. Since $M$ is the matching in $G[V_H, \bar{V}_H]$ that covers $H$, thus $|U| = |V_H|$. Regarding Theorem 1, to show that $H$ is well-supported almost surely, we need to show that the columns of the matrix $\mathbf{A}_{\bar{H}|H}$ are linearly independent almost surely. For this reason, we show that $\det(\mathbf{A}_{U|V_H}) \neq 0$ almost surely. $\det(\mathbf{A}_{U|V_H})$ can be considered as a polynomial of the nonzero entries of the admittance matrix using Leibniz formula. Now assume $U = \{u_1, u_2, \ldots, u_{|V_H|}\}$ are matched to $V_H = \{v_1, v_2, \ldots, v_{|V_H|}\}$ in order. It can be seen that $\prod_{i=1}^{|V_H|} a_{u_i v_i}$ is a term with nonzero coefficient in $\det(\mathbf{A}_{U|V_H})$. Therefore, $\det(\mathbf{A}_{U|V_H})$ is not a zero polynomial in terms of its nonzero entries. Now since the set of reactance values for the edges in $E[V_H, \bar{V}_H]$ such that $\det(\mathbf{A}_{U|V_H}) = 0$ is a measure zero set in the real space, thus $\det(\mathbf{A}_{U|V_H}) \neq 0$ almost surely. ∎

In reality, since the reactance values are derived by the physical properties of the lines, we expect that these values are relatively random around a mean value. Thus, following Corollary 2, the existence of a matching that covers every node in $V_H$ is enough for a zone to be well-supported (see Fig. 3 for an example of a graph in which every node in a zone is covered by a matching). Hence, in the following sections we consider the existence of a matching as a sufficient external condition on $H$ to be well-supported.

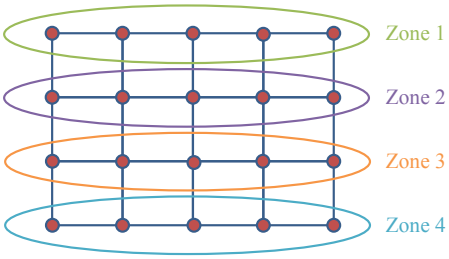



Fig. 3: An example of a graph and set of zones such that each zone is both well-supported and acyclic.

### B. Detecting Failed Lines

In this subsection, we assume that after an attack, the phase angles are recovered using the method in Subsection IV-A (i.e., by solving (4)). We introduce methods to detect the failed lines using $\vec{\theta'}$. We provide sufficient conditions on $H$ such that these methods detect the failed lines successfully. As we mentioned, since these conditions depend only on the connections between the nodes in $H$, we refer to them as *internal conditions* on $H$.

The following Lemma is the foundation for our approach to find the failed lines. It limits the set of failed lines to the solution space of the matrix equation (5). It can be considered as the complement of Corollary 1.

*Lemma 2:* There exists a vector $\vec{x} \in \mathbb{R}^{|E_H|}$ such that $\text{supp}(\vec{x}) = \{i | e_i \in F\}$ and

$$\mathbf{D}_H \vec{x} = \mathbf{A}_{H|G}(\vec{\theta} - \vec{\theta'}). \tag{5}$$

Moreover, for any $W \subseteq G$ such that $N_c(H) \subseteq W$, $\mathbf{D}_H \vec{x} = \mathbf{A}_{H|W}(\vec{\theta}_W - \vec{\theta'}_W)$.

*Proof:* We use the notation that we used in proof of Lemma 1. Recall from the proof of Lemma 1 that $\mathbf{A}(\vec{\theta}-\vec{\theta'}) = -\sum_{j=1}^{k} a_{s_j t_j} \vec{x_j} \vec{x_j}^t \vec{\theta'}$. It is easy to see that if $\vec{d}_1, \vec{d}_2, \ldots, \vec{d}_m$ are the columns of the incidence matrix $\mathbf{D}$, then $\forall j (1 \leqslant j \leqslant k)$, there exists $b_j \in \mathbb{R}$ such that $b_j \vec{d}_{i_j} = -a_{s_j t_j} \vec{x_j} \vec{x_j}^t \vec{\theta'}$. Therefore, $\mathbf{A}(\vec{\theta} - \vec{\theta'}) = \sum_{j=1}^{k} b_j \vec{d}_{i_j}$. Thus, if we define $\vec{y} \in \mathbb{R}^m$ such that $\forall e_{i_j} \in F, y_{i_j} = b_j$ and 0 elsewhere, then $\mathbf{A}(\vec{\theta}-\vec{\theta'}) = \mathbf{D}\vec{y}$ and $\text{supp}(\vec{y}) \subseteq \{i_1, i_2, \ldots, i_k\}$. However, from the Corollary 1 we know that $\mathbf{A}_{\bar{H}|G}(\vec{\theta} - \vec{\theta'}) = 0$. Moreover, since $F \subseteq E_H$, $\vec{y}_{\bar{H}} = 0$. Thus, we can restrict the equation only to the components of the zone $H$, which means that $\mathbf{A}_{H|G}(\vec{\theta} - \vec{\theta'}) = \mathbf{D}_H \vec{y}_H$. Now it is easy to see that since we assumed that no null-edges are in $F$, all the $b_i$s are nonzero and $\text{supp}(\vec{y}_H) = \{i_1, i_2, \ldots, i_k\}$. Therefore, $\vec{x} = \vec{y}_H$ is a solution to (5) and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$. Now, since for any $i \in H$ and $j \notin N_c(H)$ we have $a_{ij} = 0$, it is easy to see that for any $W \subseteq G$ such that $N_c(H) \subseteq W$, $\mathbf{D}_H \vec{x} = \mathbf{A}_{H|W}(\vec{\theta}_W - \vec{\theta'}_W)$. ∎

Lemma 2 provides important information regarding the failed lines. It states that there exists a solution $\vec{x}$ to (5) such that $\text{supp}(\vec{x})$ reveals the set of failed lines. However, the solution to (5) may not be unique. Again, for simplicity of the notations and equations, through the most of this paper we consider the case in which $W = G$. However, as we briefly describe in Subsection IV-D, using a smaller $W$ allows the failed lines detection after an attack on multiple zones.

[4] In probability theory, one says that an event happens almost surely, if it happens with probability one.

TABLE II: Summary of the results in Section IV. The external/internal conditions on the structural properties of a zone $H$ such that after an attack with certain constraints, the phase angles can be recovered and the failed lines can be detected by solving (8). Matching and partial matching refer to matchings in $G[V_H, \bar{V}_H]$ that cover $V_H$ and $V_H \backslash (V_H^{\text{in}} \cup V_H^{\text{out}})$, respectively.

| Case | External conditions | Internal conditions | Attack constraints | Resilience | Results |
|---|---|---|---|---|---|
| I | Matching | Acyclic | None | attack-resilient | Corollary 2/Lemma 3 |
| II | Matching | Planar | $\forall$ cycle $C$, $\lvert C \cap F\rvert < \lvert C \backslash F\rvert$<br>$F^*$ is $H^*$-separable | weakly-attack-resilient | Corollary 2/Theorem 2 |
| III | Partial matching | Acyclic | $\forall v \in V_H^{\text{in}}$, $\lvert\partial(v) \cap F\rvert < \lvert\partial(v) \backslash F\rvert$ | weakly-attack-resilient | Lemmas 3,6/Corollary 5 |
| IV | Partial matching | Planar<br>No cycle contains an inner-connected-node | $\forall$ cycle $C$, $\lvert C \cap F\rvert < \lvert C \backslash F\rvert$<br>$\forall v \in V_H^{\text{in}}$, $\lvert\partial(v) \cap F\rvert < \lvert\partial(v) \backslash F\rvert$<br>$F^*$ is $H^*$-separable | weakly-attack-resilient | Theorem 3/Corollary 5 |

The lemma below provides a necessary and sufficient condition on $H$ such that the solution to (5) is unique.

*Lemma 3:* The solution to (5) is unique and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$, if and only if $H$ is acyclic.

*Proof:* It is easy to see that the solution to (5) is unique if and only if $\mathbf{D}_H$ has linearly independent columns. It is known that $\text{rank}(\mathbf{D}_H) = |V_H| - c$ in which $c$ is the number of connected components of $H$ [38, Theorem 2.3]. Therefore, $\mathbf{D}_H$ has linearly independent columns if and only if each connected component of $\mathbf{D}_H$ is a tree, which means that $\mathbf{D}_H$ should be acyclic. ∎

According to Lemma 3 the set of failed lines for any attack can be detected, if and only if $H$ is acyclic. Fig. 3 shows an example of a graph and set of zones such that each zone is both well-supported and acyclic (case I in Table II).

Although Lemma 3 requires $H$ to be an acyclic graph in order for the solution of (5) to be unique, by setting some constraints on the failed lines $F$, we provide a method to detect the failed lines in broader class of graphs. The underlying idea is that the set of failed lines is expected to be relatively sparse compared to the overall set of edges within a zone. Thus, we are interested in the solutions of (5) that are relatively sparse. The $l_0$-norm should be used to capture the sparseness of a vector. However, since minimizing $l_0$-norm is a combinatorial problem in general cases, we prefer to use $l_1$-norm which is known to be a good approximation of the $l_0$-norm. Thus, we consider the following minimization problem,

$$\min \|\vec{x}\|_1 \text{ s.t. } \mathbf{D}_H \vec{x} = \mathbf{A}_{H|G}(\vec{\theta} - \vec{\theta}'). \tag{6}$$

Notice that (6) is still linear and can be solved using Linear Programming. Moreover, when the solution to (6) also appears to be sparse, which is usually the case in the considered scenario, there are very fast algorithms to solve it [39].

The Lemma below states that by solving (6), the failed lines can be detected in more cases than by solving (5). The idea that we use in proof of Lemma 4 is the core idea in proofs of Theorems 2 and 3, as well. Namely, the null space of $D_H$ is in one-to-one correspondence with the cycle space of the graph $H$. Therefore, there are graph theoretical interpretations to the solution space of (5). Hence, by using tools from graph theory and linear algebra, we find the solution to (5) with the minimum $l_1$-norm.

*Lemma 4:* If $H$ is a cycle and $|E_H \cap F| < |E_H \backslash F|$, the solution to (6) is unique and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$.

*Proof:* Here without loss of generality, we assume that $\mathbf{D}_H$ is the incidence matrix of $H$ when edges of $H$ has been oriented clockwise. Since $H$ is connected, it is known that $\text{rank}(\mathbf{D}_H) = |V_H| - 1$ [38, Theorem 2.2]. Therefore, $\dim(\text{Null}(\mathbf{D}_H)) = 1$. Suppose $\vec{e} \in \mathbb{R}^{|E_H|}$ is the all one vector. It is easy to see that $\mathbf{D}_H \vec{e} = 0$. Since $\dim(\text{Null}(\mathbf{D}_H)) = 1$, $\vec{e}$ is the basis for the null space of $\mathbf{D}$. Suppose $\vec{x}$ is a solution to (5) such that $\text{supp}(\vec{x}) = \{i | e_i \in F\}$ (from Lemma 2 we know that such a solution exists). To prove that $\vec{x}$ is the unique solution for (6), we only need to prove that $\forall c \in \mathbb{R} \backslash \{0\}$, $\|\vec{x}\|_1 < \|\vec{x} - c\vec{e}\|_1$. Without loss of generality we can assume that $x_1, x_2, \ldots, x_k$ are the nonzero elements of $\vec{x}$, in which $k = |F|$. From the assumption we know that $|E_H \cap F| < |E_H \backslash F|$, therefore $k < |E_H|/2$. Hence, we have

$$\begin{aligned}
\|\vec{x} - c\vec{e}\|_1 &= \sum_{i=1}^{k} |x_i - c| + (|E_H| - k)|c| \\
&= \sum_{i=1}^{k} (|x_i - c| + |c|) + (|E_H| - 2k)|c| \\
&\geqslant \sum_{i=1}^{k} |x_i| + (|E_H| - 2k)|c| > \sum_{i=1}^{k} |x_i| = \|\vec{x}\|_1.
\end{aligned}$$

Thus, the solution to (6) is unique. ∎

*Corollary 3:* If all the cycles in $H$ are edge-disjoint and for any cycle $C$ in $H$, $|C \cap F| < |C \backslash F|$, then the solution to (6) is unique and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$.

The following Theorem extends the idea in the proof of Lemma 4 and provides sufficient conditions for failed lines in a planar graph $H$ to be detected by solving (6) (recall from subsection III-D that $H^*$ is the dual of the planar graph $H$ and $F^*$ is the dual of the set of failed lines). For the proof details see [1].

*Theorem 2:* In a planar graph $H$, the solution to (6) is unique and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$, if (i) for any cycle $C$ in $H$, $|C \cap F| < |C \backslash F|$, and (ii) $F^*$ is $H^*$-separable.

Fig. 4 shows an example of a zone $H$ for which the set of failed lines can be detected by solving (6) based on Theorem 2 (case II in Table II).

The Corollary below states that in planar bipartite graphs, condition (ii) in Theorem 2 immediately holds, if condition (i) holds. For the proof details see [1].

*Corollary 4:* In a planar bipartite graph $H$, the solution to (6) is unique and $\text{supp}(\vec{x}) = \{i | e_i \in F\}$, if for any cycle $C$ in $H$, $|C \cap F| < |C \backslash F|$.

Theorem 2 and Corollary 4 are important since power grids are usually considered to be planar. For instance, lattice graphs are planar bipartite.

### C. Simultaneous Phase Angles Recovery and Failed Lines Detection

In Subsection IV-A we showed that the phase angles of the zone $H$ are recoverable, if there is a matching in $G[V_H, \bar{V}_H]$

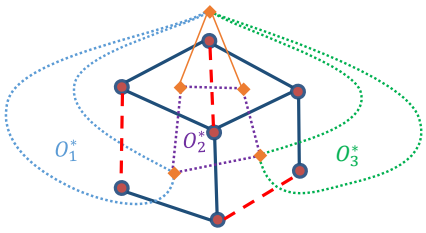



Fig. 4: An example of a zone $H$ and a set of failed lines (shown by red dashed lines) that can be detected by solving (6) based on Theorem 2. The diamond orange nodes are the nodes of the dual graph $H^*$. As can be seen, the dual of the failed lines can be covered by three edge disjoint cycles $O_1^*, O_2^*, O_3^*$ (shown by dotted lines) in $H^*$. Thus, as Theorem 2 requires, $F^*$ is $H^*$-separable.

that covers $V_H$. However, in reality, this condition might be very difficult and costly to maintain (i.e., it may require to increase the number of zones). Therefore, in this subsection, using similar ideas as in subsection IV-B, we relax the external conditions on $H$.

The key idea which is summarized in the following Lemma, is to combine Corollary 1 and Lemma 2.

*Lemma 5:* There exist vectors $\vec{x} \in \mathbb{R}^{|E_H|}$ and $\vec{\delta}_H \in \mathbb{R}^{|V_H|}$ such that $\text{supp}(\vec{x}) = \{i | e_i \in F\}$, $\vec{\delta}_H = \vec{\theta}_H - \vec{\theta}'_H$, and

$$\begin{aligned} &\mathbf{D}_H \vec{x} = \mathbf{A}_{H|H} \vec{\delta}_H + \mathbf{A}_{H|\bar{H}} \vec{\delta}_{\bar{H}} \\ &\mathbf{A}_{\bar{H}|H} \vec{\delta}_H + \mathbf{A}_{\bar{H}|\bar{H}} \vec{\delta}_{\bar{H}} = 0 \end{aligned} \tag{7}$$

where $\vec{\delta}_{\bar{H}} = \vec{\theta}_{\bar{H}} - \vec{\theta}'_{\bar{H}}$ and is known.

From Subsections IV-A and IV-B we know that the solution to (7) is unique, if and only if $H$ is acyclic and $\mathbf{A}_{\bar{H}|H}$ has linearly independent columns. Therefore, to deal with cases for which $\mathbf{A}_{\bar{H}|H}$ does not have linearly independent columns, we consider a similar optimization problem as in (6) but with more constraints. For this reason, as we mentioned in Subsection IV-B, since the set of failed lines is expected to be relatively sparse compared to the overall set of edges, we consider the following optimization problem,

$$\begin{aligned} &\min \|\vec{x}\|_1 \text{ s.t.} \\ &\mathbf{D}_H \vec{x} = \mathbf{A}_{H|H} \vec{\delta}_H + \mathbf{A}_{H|\bar{H}} \vec{\delta}_{\bar{H}} \\ &\mathbf{A}_{\bar{H}|H} \vec{\delta}_H + \mathbf{A}_{\bar{H}|\bar{H}} \vec{\delta}_{\bar{H}} = 0. \end{aligned} \tag{8}$$

The following Lemma states that if there is an independent set of nodes in $H$ with no neighbors in $\bar{H}$, then under some conditions on $F$, we can recover $F$ and $\vec{\theta}'_H$ by solving (8) even when $\mathbf{A}_{\bar{H}|H}$ does not have linearly independent columns (case III in Table II). First, we define *inner-connected* nodes.

*Definition 2:* A node $v \in V_H$ is called *$H$-inner-connected* if $N(v) \subseteq V_H$. It is called *$H$-outer-connected* if $N(v) \subseteq V_{\bar{H}}$. We denote the set of *$H$-inner-connected* and *$H$-outer-connected* nodes by $V_H^{\text{in}}$ and $V_H^{\text{out}}$, respectively.

*Lemma 6:* Suppose $H$-inner-connected nodes form an independent set. If $H$ is acyclic, $\text{rank}(\mathbf{A}_{\bar{H}|H}) = |V_H| - |V_H^{\text{in}}|$, and $\forall v \in V_H^{\text{in}}, |\partial(v) \cap F| < |\partial(v) \backslash F|$, then the solution $\vec{x}, \vec{\delta}$ to (8) is unique. Moreover, $\text{supp}(\vec{x}) = \{i | e_i \in F\}$ and $\vec{\delta}_H = \vec{\theta}_H - \vec{\theta}'_H$.

*Proof:* The idea of the proof is very similar to the proof of Lemma 4. Suppose $\vec{x}, \vec{\delta}_H$ is the solution to (7) such that $\text{supp}(\vec{x}) = \{i | e_i \in F\}$ and $\vec{\delta}_H = \vec{\theta}_H - \vec{\theta}'_H$. From Lemma 5 we know that such a solution exists. We show that this solution is the unique solution to (8) in this setting.

Without loss of generality in addition to assuming $V_H = \{1, 2, 3, \ldots, |V_H|\}$ and $E_H = \{e_1, e_2, \ldots, e_{|E_H|}\}$, we can assume the labeling of the nodes in $G$ is such that $V_H^{\text{in}} = \{1, 2, \ldots, t\}$ is the set of $H$-inner-connected nodes. Suppose $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_t \in \mathbb{R}^{|V_H|}$ are the coordinate vectors, in other words $\vec{\alpha}_i$ is 1 at its $i^{\text{th}}$ entry and 0 everywhere else. It is easy to see that $\forall i \in V_H^{\text{in}} : A_{\bar{H}|H} \vec{\alpha}_i = 0$. On the other hand, since $\text{rank}(\mathbf{A}_{\bar{H}|H}) = |V_H| - t$ and $\vec{\alpha}_i$s are linearly independent, $\vec{\alpha}_1, \vec{\alpha}_2, \ldots, \vec{\alpha}_t$ form a basis for $\text{Null}(\mathbf{A}_{\bar{H}|H})$.

Assume $\mathbf{D}_H$ is the incidence matrix of $H$ when its edges are oriented such that for each $i \in V_H^{\text{in}}$, the edges are coming out of $i$. Now suppose $\vec{z}$ is another solution to (8), it is easy to see that $\mathbf{D}_H(\vec{z} - \vec{x}) = \mathbf{A}_{H|H} \vec{\alpha}$ for a vector $\vec{\alpha} \in \text{Null}(\mathbf{A}_{\bar{H}|H})$. Since $\vec{\alpha} \in \text{Null}(\mathbf{A}_{\bar{H}|H})$, there are unique coefficients $c_1, c_2, \ldots, c_t \in \mathbb{R}$ such that $\vec{\alpha} = c_1 \vec{\alpha}_1 + c_2 \vec{\alpha}_2 + \cdots + c_t \vec{\alpha}_t$. Thus,

$$\begin{aligned} \mathbf{D}_H(\vec{z} - \vec{x}) &= \mathbf{A}_{H|H} \vec{\alpha} = \mathbf{A}_{H|H}(c_1 \vec{\alpha}_1 + c_2 \vec{\alpha}_2 + \cdots + c_t \vec{\alpha}_t) \\ &= c_1 \mathbf{A}_{H|H} \vec{\alpha}_1 + c_2 \mathbf{A}_{H|H} \vec{\alpha}_2 + \cdots + c_t \mathbf{A}_{H|H} \vec{\alpha}_t. \end{aligned}$$

Suppose $\vec{d}_j$ is the column associated with edge $e_j$ in $D_H$. Notice that for each $i \in V_H^{\text{in}}$, $\partial(i) \subseteq E_H$. Therefore, $\forall i \in V_H^{\text{in}}$ and $\forall e_j \in \partial(i)$, $\vec{d}_j$ is a column of $\mathbf{D}_H$. It is easy to see that for any $i \in V_H^{\text{in}}$, $\sum_{j : e_j \in \partial(i)} \vec{d}_j = \mathbf{A}_{H|H} \vec{\alpha}_i$. If for any $i \in V_H^{\text{in}}$ we define vector $\vec{b}_i \in \{0, 1\}^{|E_H|}$ as follows,

$$b_{ij} := \begin{cases} 1 & \text{if } e_j \in \partial(i) \\ 0 & \text{otherwise,} \end{cases}$$

then $\mathbf{D}_H \vec{b}_i = \mathbf{A}_{H|H} \vec{\alpha}_i$ for any $i \in V_H^{\text{in}}$. Thus,

$$\begin{aligned} &\mathbf{D}_H(c_1 \vec{b}_1 + \cdots + c_t \vec{b}_t) = c_1 \mathbf{A}_{H|H} \vec{\alpha}_1 + \cdots + c_t \mathbf{A}_{H|H} \vec{\alpha}_t \\ &\Rightarrow \mathbf{D}_H(\vec{z} - \vec{x}) = \mathbf{D}_H(c_1 \vec{b}_1 + c_2 \vec{b}_2 + \cdots + c_t \vec{b}_t). \end{aligned}$$

Now since $H$ is acyclic, $\mathbf{D}_H$ has linearly independent columns. Thus, from the equation above we can conclude that,

$$\begin{aligned} &\vec{z} - \vec{x} = c_1 \vec{b}_1 + c_2 \vec{b}_2 + \cdots + c_t \vec{b}_t \\ &\Rightarrow \vec{z} = \vec{x} + c_1 \vec{b}_1 + c_2 \vec{b}_2 + \cdots + c_t \vec{b}_t. \end{aligned}$$

Using equation above, we show that $\|\vec{z}\|_1 > \|\vec{x}\|_1$ unless $c_1 = c_2 = \cdots = c_t = 0$. First, notice that since $V_H^{\text{in}}$ is an independent set, $\forall i \neq j \in V_H^{\text{in}}$, $\partial(i) \cap \partial(j) = \varnothing$. Suppose $\forall i \in V_H^{\text{in}}, |\partial(i) \cap F| = k_i$, we have

$$\begin{aligned} \|\vec{z}\|_1 &= \|\vec{x} + c_1 \vec{b}_1 + c_2 \vec{b}_2 + \cdots + c_t \vec{b}_t\|_1 \\ &= \sum_{i \in V_H^{\text{in}}} \Big( (|\partial(i)| - k_i)|c_i| + \sum_{j \in F \cap \partial(i)} |x_j + c_i| \Big) + \sum_{i \in F \backslash \partial(V_H^{\text{in}})} |x_i| \\ &= \sum_{i \in V_H^{\text{in}}} \Big( (|\partial(i)| - 2k_i)|c_i| + \sum_{j \in F \cap \partial(i)} \big( |x_j + c_i| + |c_i| \big) \Big) + \sum_{i \in F \backslash \partial(V_H^{\text{in}})} |x_i| \\ &\geqslant \sum_{i \in V_H^{\text{in}}} \Big( (|\partial(i)| - 2k_i)|c_i| + \sum_{j \in F \cap \partial(i)} |x_j| \Big) + \sum_{i \in F \backslash \partial(V_H^{\text{in}})} |x_i| \\ &= \sum_{i \in V_H^{\text{in}}} \big( (|\partial(i)| - 2k_i)|c_i| \big) + \sum_{i \in V_H^{\text{in}}} \sum_{j \in F \cap \partial(i)} |x_j| + \sum_{i \in F \backslash \partial(V_H^{\text{in}})} |x_i| \\ &= \sum_{i \in V_H^{\text{in}}} \big( (|\partial(i)| - 2k_i)|c_i| \big) + \|\vec{x}\|_1. \end{aligned}$$

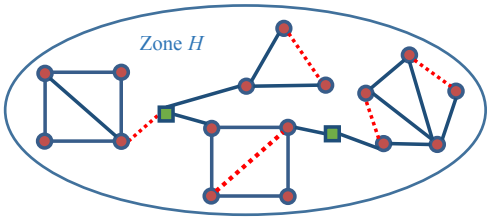



Fig. 5: An example of a zone $H$ and an attack such that the phase angles can be recovered and the failed lines can be detected by solving (8) based on Theorem 3. The squared green nodes are the $H$-inner-connected nodes. The failed lines are shown by red dashed edges.

Now, since from the assumptions $\forall i \in V_H^{\text{in}}, k_i < |\partial(i)|/2$, it is easy to see that $\sum_{i\in V_H^{\text{in}}}((\partial(i)-2k_i)|c_i|) + \|\vec{x}\|_1 > \|\vec{x}\|_1$, unless $c_1 = c_2 = \cdots = c_t = 0$. Since $\vec{z}$ is a solution to (8), we should have $c_1 = c_2 = \cdots = c_t = 0$, and $\vec{z} = \vec{x}$. Thus, $\vec{x}$ is the unique solution to (8) and $\text{supp}(\vec{x}) = \{i|e_i \in F\}$. From the proof, it is easy to see that $\vec{\delta}_H$ is also unique. ■

To generalize Lemma 6, first let us consider cases in which $H$ contains $H$-outer-connected nodes. The Lemma below shows that the value of $\delta$ for these nodes is unique.

*Lemma 7:* If $v$ is $H$-outer-connected and $\vec{\delta}_H$ is a solution to (7), then $\delta_v$ is unique and equal to $\delta_v = 1/d(v)\sum_{u\in N(v)}\delta_u$, where $d(v)$ is the degree of node $v$.

*Proof:* First, notice that since $v$ is $H$-outer-connected, $N(v) \subseteq \bar{V}_H$. Thus, $\delta_v = 1/d(v)\sum_{u\in N(v)}\delta_u$ implies that $\delta_v$ is unique. Now, let us compute the $v^{\text{th}}$ entry of the vectors on the both side of the equation $\mathbf{D}_H\vec{x} = \mathbf{A}_{H|H}\vec{\delta}_H + \mathbf{A}_{H|\bar{H}}\vec{\delta}_{\bar{H}}$. Since $v$ is $H$-outer-connected, the $v^{\text{th}}$ row of $\mathbf{D}_H$ is a zero vector. Thus, $(\mathbf{D}_H\vec{x})_v = 0$ for any $\vec{x}$. It is also easy to see that $(\mathbf{A}_{H|H}\vec{\delta}_H)_v = \delta_v d(v)$ and $(A_{H|\bar{H}}\vec{\delta}_{\bar{H}})_v = -\sum_{u\in N(v)}\delta_u$. Since $(\mathbf{D}_H\vec{x})_v = (\mathbf{A}_{H|H}\vec{\delta}_H)_v + (A_{H|\bar{H}}\vec{\delta}_{\bar{H}})_v$, we can conclude that $\delta_v = 1/d(v)\sum_{u\in N(v)}\delta_u$. Thus, the proof is complete. ■

In the following theorem, we generalize Lemma 6. This theorem combines Lemma 6 and Theorem 2, and provides a broader class of graphs in which solving (8) recovers phase angles and detects the failed lines after an attack. For the proof details see [1].

*Theorem 3:* In a planar graph $H$, the solution $\vec{x}, \vec{\delta}_H$ to (8) is unique with $\text{supp}(\vec{x}) = \{i|e_i \in F\}$ and $\vec{\delta}_H = \vec{\theta}_H - \vec{\theta}'_H$, if the following conditions hold: (i) $\forall v \in V_H^{\text{in}}, |\partial(v)\cap F| < |\partial(v)\backslash F|$, (ii) for any cycle $C$ in $H$, $|C \cap F| < |C\backslash F|$, (iii) $F^*$ is $H^*$-separable, (iv) in $\mathbf{A}_{\bar{H}|H}$, columns associated with nodes that are neither $H$-inner-connected nor $H$-outer-connected are linearly independent, (v) no cycle in $H$ contains a $H$-inner-connected node, and (vi) $H$-inner-connected nodes form an independent set.

Note that when $H$ is well-supported, there are no $H$-inner-connected or $H$-outer-connected nodes. Thus, conditions (i), (iv), (v), and (vi) immediately hold and Theorem 3 reduces to Theorem 2.

Fig. 5 shows an example of a zone $H$ and an attack such that the phase angles can be recovered and the failed lines can be detected by solving (8) using Theorem 3 (case IV in Table II). As it can be seen, this theorem covers a broad set of graphs and attacks for which we can recover the phase angles and detect the failed lines. Notice that here, with similar argument as in Corollary 2 we can replace condition (iv) in Theorem 3 with a simpler matching condition as follows.

*Corollary 5:* If there is a matching in $G[V_H, \bar{V}_H]$ that covers $V_H\backslash(V_H^{\text{in}} \cup V_H^{\text{out}})$, then condition (iv) in Theorem 3 holds almost surely.

To conclude, we define the *attack-resilient* and *weakly-attack-resilient* notions to summarize the resilience of a zone to joint cyber and physical attacks.

*Definition 3:* A zone $H$ is called *attack-resilient*, if it is both well-supported and acyclic.

*Definition 4:* A zone $H$ is called *weakly-attack-resilient*, if $\vec{\theta}'_H$ and $F$ can be uniquely found after a constrained attack on the zone $H$ by solving (8).

It is easy to see that an attack-resilient zone is also weakly-attack-resilient.

### D. Recovery and Detection After Attacks on Multiple Zones

In this subsection, we study the case in which multiple zones are attacked simultaneously. When the attacked zones are close to each other, it may not always be possible to recover information. However, if the attacked zones are relatively distant from each other, any of the methods provided in the previous subsections (depending on the conditions on the zones and attacks) can be applied to recover the information and detect the failures in the attacked zones.

The idea is to use Corollary 1 and Lemma 2 for sets $U$ and $W$ much smaller than $\bar{H}$ and $G$, respectively. Assume $H_1$ and $H_2$ are two attacked zones. Let $U_1$ and $U_2$ be two sets with the minimum size such that $U_1 \subseteq \bar{H}_1$, $H_1 \subseteq N_c(U_1)$, $U_2 \subseteq \bar{H}_2$, and $H_2 \subseteq N_c(U_2)$. Following Corollary 1, $\mathbf{A}_{U_1|N_c(U_1)}(\vec{\theta}_{N_c(U_1)} - \vec{\theta}'_{N_c(U_1)}) = 0$ and $\mathbf{A}_{U_2|N_c(U_2)}(\vec{\theta}_{N_c(U_2)} - \vec{\theta}'_{N_c(U_2)}) = 0$. Now if $N_c(U_1)\cap H_2 = N_c(U_2)\cap H_1 = \varnothing$ (i.e., $H_1$ and $H_2$ are distant enough), and both $\mathbf{A}_{U_1|H_1}$ and $\mathbf{A}_{U_2|H_2}$ have linearly independent columns, then similar to the proof of Theorem 1, the phase-angles of the nodes in $H_1$ and $H_2$ can be recovered by solving a set of linear equations.

To detect the failed lines, let $W_1$ and $W_2$ be two sets with the minimum size such that $W_1, W_2 \subseteq G$, $N_c(H_1) \subseteq W_1$, and $N_c(H_2) \subseteq W_2$. Following Lemma 2, there exist vectors $\vec{x_1}, \vec{x_2} \in \mathbb{R}^{|E_H|}$ such that $\text{supp}(\vec{x_1})$ and $\text{supp}(\vec{x_2})$ give the failed lines in $H_1$ and $H_2$, and also $\mathbf{D}_{H_1}\vec{x_1} = \mathbf{A}_{H_1|W_1}(\vec{\theta}_{W_1} - \vec{\theta}'_{W_1})$ and $\mathbf{D}_{H_2}\vec{x_2} = \mathbf{A}_{H_2|W_2}(\vec{\theta}_{W_2} - \vec{\theta}'_{W_2})$. Now, if $H_1$ and $H_2$ are acyclic and $W_1 \cap H_2 = W_2 \cap H_1 = \varnothing$, then similar to the Lemma 3, the solutions to $\mathbf{D}_{H_1}\vec{x_1} = \mathbf{A}_{H_1|W_1}(\vec{\theta}_{W_1} - \vec{\theta}'_{W_1})$ and $\mathbf{D}_{H_2}\vec{x_2} = \mathbf{A}_{H_2|W_2}(\vec{\theta}_{W_2} - \vec{\theta}'_{W_2})$ are unique and the failed lines can be detected by $\text{supp}(\vec{x_1})$ and $\text{supp}(\vec{x_2})$.

Notice that the methods in subsection IV-C can also be simply used to recover the phase angles and detect the failed lines in the attacked zones that are distant enough. The following corollary summarizes our discussion in this subsection.

*Corollary 6:* The phase angles and the failed lines can be recovered/detected after a simultaneous attack on zones $H_1, H_2, \ldots, H_k$, if followings hold: (i) for any $1 \leqslant i \leqslant k$, if $H_i$ was the only attacked zone, then the phase angle of the nodes and the failed lines could be recovered/detected using

**Algorithm 1** - Post-Attack Recovery & Detection (PARD)

**Input:** A connected graph $G$, phase angles before the attack $\vec{\theta}$, and partial phase angles after the attack $\vec{\theta}'_{\bar{H}}$.

1: Detect the attacked zone $H$ by checking for missing data.
2: Compute $\vec{x}, \vec{\delta}_H$ the solution to (8) by Linear Programming.
3: Compute $\vec{\theta}'_H = \vec{\theta}_H - \vec{\delta}_H$.
4: Compute $F = \{e_i | i \in \text{supp}(\vec{x})\}$.
5: Detect the set of null-edges that appear after the attack as $N = \{\{i,j\} \in E_H | \theta'_i = \theta'_j\}$.
6: **return** $N$, $F$, $\vec{\theta}'_H$.

the methods in subsections IV-A,IV-B, and IV-C, (ii) there exist $U_1, U_2, \ldots, U_k \subseteq G$ and $W_1, W_2, \ldots W_k \subseteq G$ such that:

1. For any $1 \leqslant i \leqslant k$, $U_i \subseteq \bar{H}_i$, $H_i \subseteq N_c(U_i)$, and $N_c(H_i) \subseteq W_i$.
2. For any $1 \leqslant i \neq j \leqslant k$, $N_c(U_i) \cap H_j = \varnothing$ and $W_i \cap H_j = \varnothing$.

*Proof:* For any $1 \leqslant i \leqslant k$, consider equations $\mathbf{A}_{U_i|N_c(U_i)}(\vec{\theta}_{N_c(U_i)} - \vec{\theta}'_{N_c(U_i)}) = 0$ and $\mathbf{D}_{H_i}\vec{x_i} = \mathbf{A}_{H_i|W_i}(\vec{\theta}_{W_i} - \vec{\theta}'_{W_i})$ instead of (4) and (5). Then, recover the phase angle of the nodes and detect the failed lines at each $H_i$ separately using any of the methods provided in subsections IV-A,IV-B, and IV-C. ■

## V. Post-Attack Recovery and Detection Algorithm

In this section, we present the Post-Attack Recovery and Detection (PARD) Algorithm for recovering the phase angles and detecting the failed lines after an attack on a zone $H$. Based on the results provided in previous subsections, if a zone $H$ is weakly-attack-resilient, the PARD Algorithm will recover the phase angles and detect the failed lines after a constrained attack.

Notice that if there are some failed lines but no data is missing, then from the data that is gathered by the PDCs from the PMUs, all the information regarding the status of the lines and phase angles is available and there is no need for the algorithm. Thus, as the first step, the PARD Algorithm detects the attacked zone $H$ by checking the missing data (line 1). Then, it solves (8) by Linear Programming to obtain $\vec{x}, \vec{\delta}_H$. If $H$ is weakly-attack-resilient, from the results in previous subsections, we know that $\vec{x}, \vec{\delta}_H$ are unique, $\vec{\theta}'_H = \vec{\theta}_H - \vec{\delta}_H$ (line 3), and $F = \{e_i | i \in \text{supp}(\vec{x})\}$ (line 4). Finally, using $\vec{\theta}'$ computed in previous line, the PARD Algorithm detects the set of null-edges $N$ (line 5), and returns $N$, $F$, and $\vec{\theta}'_H$.

## VI. Attack Analysis in the Presence of Measurement Noise and Uncertainty

In this section, we briefly discuss the problem of information recovery after an attack in the presence of a measurement noise and uncertainty. We follow [21] and model the measurement noise by changing (3) to $\mathbf{A}(\vec{\theta} - \vec{e}) = \vec{p}$ where $\vec{e} \in \mathbb{R}^{|V|\times 1}$ is a Gaussian measurement noise with a diagonal covariance matrix $\Sigma$. Following [9], $\vec{e}$ can also account for the perturbations in $\vec{p}$ after failures. It is obvious that in the presence of noise, the optimization problem (8) has no feasible solution. However, since the $l_1$-norm is relatively robust against noise, one possible approach to generalize the optimization problem (8) to the noisy case is to relax the conditions as follows:

$$\begin{aligned} &\min \|\vec{x}\|_1 \text{ s.t.} \\ &\|\mathbf{D}_H\vec{x} - \mathbf{A}_{H|H}\vec{\delta}_H - \mathbf{A}_{H|\bar{H}}\vec{\delta}_{\bar{H}}\|_2 < \epsilon \\ &\|\mathbf{A}_{\bar{H}|H}\vec{\delta}_H + \mathbf{A}_{\bar{H}|\bar{H}}\vec{\delta}_{\bar{H}}\|_2 < \epsilon. \end{aligned} \tag{9}$$

It is easy to see that the optimization problem (9) is a *second-order cone program* that can be solved using gradient decent methods. After solving (9), the line failures can then be detected as before by $F = \{e_i | i \in \text{supp}(\vec{x})\}$.

Generalizing Theorem 3 to take into account the noisy case modeled by (9) is part of the future work. However, in Section VIII, we show via simulation that solving the optimization problem (9) can correctly recover the phase angles and detect the failed lines depending on the level of the Signal to Noise Ratio (SNR).[5]

**Algorithm 2** - 3-Acyclic Partition of Planar (3APP)

**Input:** A non-empty planar graph $G$.

1: Find a node $v \in V$ such that $\deg(v) \leqslant 5$.
2: **if** $G \backslash v = \varnothing$ **then** set $Q_1 = Q_2 = Q_3 = \varnothing$.
3: **else** Find 3-partition of $G \backslash v$ using 3APP Algorithm as $Q_1, Q_2, Q_3$.
4: Add $v$ to the partition that $|N(v) \cap Q_i|$ is minimum.
5: **return** $Q_1, Q_2, Q_3$.

**Algorithm 3** - Zone Selection (ZS)

**Input:** A connected graph $G$.

1: Find an optimal matching cover $M_1, M_2, \ldots, M_t$ of $G$ [32].
2: For each $M_i$, separate the matched nodes into two set of nodes $V_{2i-1}, V_{2i}$ such that $\forall \{v,u\} \in M$, $v \in V_{2i-1}$ and $u \in V_{2i}$.
3: For any $1 \leqslant i \leqslant 2t$, $Q_i = V_i \backslash \bigcup_{j=1}^{i-1} Q_j$.
4: **for** each $Q_i$ **do**
5: **if** $G[Q_i]$ is acyclic **then continue**
6: **if** $G[Q_i]$ is a planar graph **then**
7: Use 3APP Algorithm to partition $G[Q_i]$.
8: **else**
9: Use any greedy algorithm to partition $G[Q_i]$ into acyclic subgraphs.
10: Name the resulted partitions $P_1, \ldots, P_k$.
11: **return** $P_1, \ldots, P_k$.

## VII. Zone Selection Algorithm

In this section we use the results from Section IV to provide an algorithm for partitioning the power grid into the minimum number of attack-resilient zones. From Lemma 3 and Corollary 2, for a zone $H$ to be attack-resilient, it is sufficient that $H$ is acyclic and there is a matching in $G[V_H, \bar{V}_H]$ that covers every node in $V_H$. Fig. 3 shows an example of a partitioning such that each zone is attack-resilient. Thus, we define a *matched-forest* partition of a graph $G$ as follows.

*Definition 5:* A *matched-forest* partition of a graph $G$ into $H_1, H_2, \ldots, H_k$ is a partition such that for any $i$, $H_i$ is acyclic and $G[V_{H_i}, \bar{V}_{H_i}]$ has a matching that covers $V_{H_i}$.

The problem of finding a matched-forest partition of $G$ is closely related to two previously known problems of *vertex arboricity* and *$k$-matching cover* of a graph. The vertex arboricity

[5] We define the SNR (in dB) as $20\log_{10}(\|\vec{\theta}\|_2/\|\vec{e}\|_2)$.

$a(G)$ of a graph $G$ is the minimum number of subsets into which the nodes of $G$ can be partitioned so that each subset induces an acyclic graph. It is known that determining $a(G)$ is NP-hard [31, p.193].

A $k$-matching cover of a graph $G$ is a union of $k$ matchings of $G$ which covers $V$. The matching cover number of $G$, denoted by $mc(G)$, is the minimum number $k$ such that $G$ has a $k$-matching cover. An optimal matching cover of a graph on $n$ nodes can be found in $O(n^3)$ time [32].

Using these results, we study the time complexity of the *minimum matched-forest* partition problem.[6] The following Lemma shows that it is hard to find the minimum matched-forest partition of a graph. For the proof details see [1].

*Lemma 8:* The problem of finding the minimum matched-forest partition of a graph $G$ is NP-hard.

Moreover, we show that finding the minimum matched-forest partition is even hard to approximate. We use the well-known result by Zuckerman [40] that for all $\epsilon > 0$, it is NP-hard to approximate *chromatic number* to within $n^{1-\epsilon}$.

*Lemma 9:* For all $\epsilon > 0$, it is NP-hard to approximate the minimum matched-forest partition of a graph $G$ to within $n^{1-\epsilon}$.

*Proof:* For a graph $G$, assume $\chi(G)$ is its chromatic number. Since each color gives an independent set of $G$, induced subgraph by the nodes with the same color is acyclic with no edges. Thus, it is easy to see that $a(G) \leqslant \chi(G)$. Suppose there is an $\alpha$-approximation algorithm for the minimum matched-forest problem. Define $\hat{G}$ as in proof of Lemma 8. Assume this algorithm partitions $\hat{G}$ into $k$ subsets. From the proof of Lemma 8, it is easy to see that $k \leqslant \alpha a(G)$. On the other hand, since each acyclic graph has the chromatic number of at most 2, this algorithm gives the $2k$ coloring of graph $G$. However, $2k \leqslant 2\alpha a(G) \leqslant 2\alpha\chi(G)$. Thus, this algorithm gives a $2\alpha$-approximation of the chromatic number of $G$. However, the result by Zuckerman [40] states that for all $\epsilon > 0$, it is NP-hard to approximate chromatic number to within $n^{1-\epsilon}$. Therefore, for all $\epsilon > 0$, it is NP-hard to approximate the minimum matched-forest problem to within $n^{1-\epsilon}$ as well. ■

Despite these hardness results, we provide the polynomial-time Zone Selection (ZS) Algorithm to find a matched-forest partition of a graph. We prove that the ZS Algorithm provides a constant approximation for the minimum matched-forest partition of a graph $G$ when $G$ is planar.

Before describing the ZS Algorithm in detail, we first describe an algorithm that is used in the ZS Algorithm, when $G$ is planar. It is known that for a planar graph $G$, $a(G) \leqslant 3$ [41]. Based on the proof provided in [41], we introduce a recursive 3-Acyclic Partition of Planar (3APP) Algorithm. The Lemma below shows the correctness of this Algorithm.

*Lemma 10:* The 3APP Algorithm partitions the nodes of a planar graph $G$ into 3 subsets such that each subset induces an acyclic graph.

*Proof:* It is known that every planar graph has a node of degree less than or equal to 5 [42]. Therefore, line 1 of the algorithm can always find $v$. At line 4, recursively we know that subgraphs induced by $Q_1, Q_2, Q_3$ in $G \backslash v$ are acyclic. Now since $\deg(v) \leqslant 5$, there exists a partition such that $|N(v) \cap Q_i| \leqslant 1$. Without loss of generality we can assume that $|N(v) \cap Q_1| \leqslant 1$. Hence, adding $v$ to $Q_1$ does not produces any cycles. Thus, subgraphs induced by $Q_1 \cup \{v\}, Q_2, Q_3$ in $G$ are acyclic. ■

[6]To the best of our knowledge, this is the first time that the problem is studied.

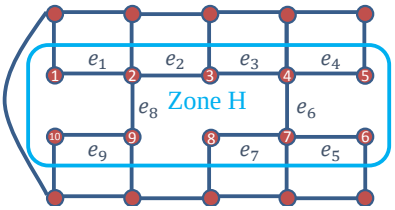



Fig. 6: The graph and the zone $H$ that are used in the simulations in Subsection VIII-A. All the edges in the graph have admittance value equal 1. The supply/demand values are chosen randomly.

We now present the ZS Algorithm. The ZS Algorithm first finds an optimal matching cover $M_1, M_2, \ldots, M_t$ of $G$ using an $O(n^3)$ algorithm introduced in [32] (line 1). Then, in lines 2 and 3, it uses this matching cover to partition $V$ into $Q_1, Q_2, \ldots, Q_{2t}$. It is easy to see that for each $Q_i$, $M_{\lceil i/2 \rceil} \cap E[Q_i, \bar{Q}_i]$ is the matching in $G[Q_i, \bar{Q}_i]$ that covers nodes in $Q_i$. Then, in order to satisfy the acyclicity condition on the partitions, it partitions $Q_i$s that do not induce an acyclic graph, into subsets so that each subset induces an acyclic graph. When $G[Q_i]$ is a planar graph, it uses 3APP Algorithm to partition $G[Q_i]$. When it is not, it uses any *greedy algorithm* to do so. Thus, the resulted partition $P_1, P_2, \ldots, P_k$ satisfies the conditions of a matched-forest partition.

The lemma below states that when $G$ is planar, the ZS Algorithm provides a constant approximation of the optimal matched-forest partition. We demonstrate the results obtained by the algorithm in the following section. For the proof details see [1].

*Lemma 11:* If $G$ is planar, the ZS Algorithm provides a 6-approximation of the minimum *matched-forest* partition of $G$ in $O(n^3)$.

Notice that the planarity of $G$ is a sufficient but not a necessary condition for the successful execution of the 3APP Algorithm. Hence, as we show in Section VIII, the ZS algorithm can be applied to almost any power grid network without checking its planarity as long as the 3APP algorithm is executed successfully.

## VIII. Numerical Results

### A. Recovering the Information in the Presence of a Measurement Noise

In this subsection, we show via simulation that solving the optimization problem (9) can correctly recover the phase angles and detect the failed lines in the presence of the measurement noise depending on the SNR level. To evaluate the results, we count number of *false negatives* and *false positives*. False negatives are the failed lines that are not detected in the solution of (9). False positives are the edges that are detected as failed lines in the solution of (9) despite the fact that they were not failed. We use the Matlab-based solver *CVX* [43] for solving the optimization problem (9).

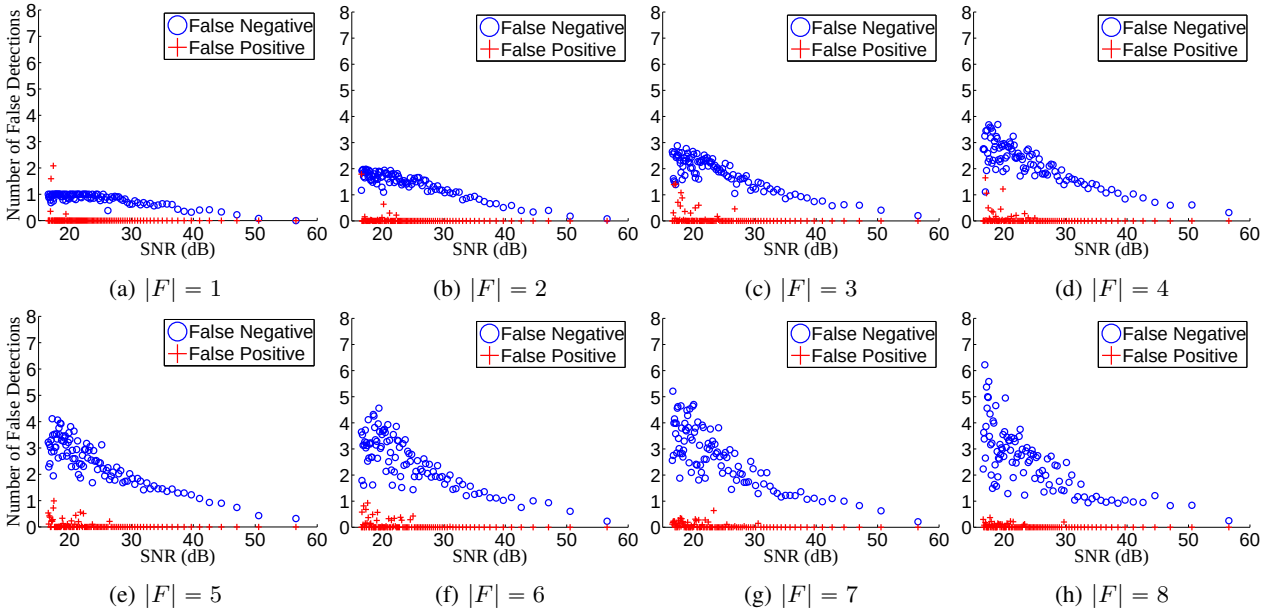
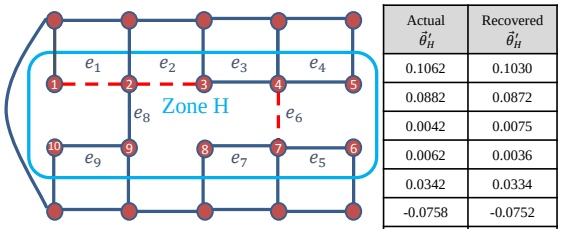


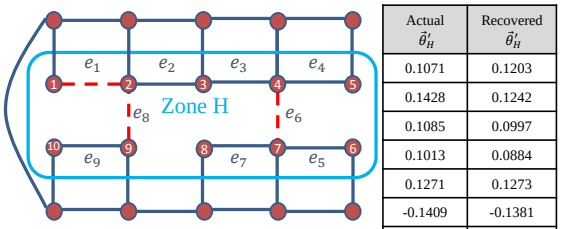

Fig. 9: The average number of false negatives and positives in detecting line failures by solving (9) in the presence of the measurement noise versus the SNR. Each data point is the average over 100 trials. (a)-(h) Show this relationship for different number of line failures ($|F|$). Figs. 7 and 8 provide the detailed information for two of the points in (c).




| Actual $\vec{\theta}'_H$ | Recovered $\hat{\theta}'_H$ |
|---|---|
| 0.1062 | 0.1030 |
| 0.0882 | 0.0872 |
| 0.0042 | 0.0075 |
| 0.0062 | 0.0036 |
| 0.0342 | 0.0334 |
| -0.0758 | -0.0752 |
| -0.0971 | -0.0937 |
| -0.0925 | -0.0919 |
| 0.0442 | 0.0441 |
| 0.0322 | 0.0321 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\vec{x}$ | -0.0074 | -0.0068 | 0 | 0 | 0 | -0.0857 | 0 | 0 | 0 |
| supp($\vec{x}$) | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |

Fig. 7: An example of an attack and recovered information in the presence of the measurement noise for SNR= 50dB. Red dashed lines show the attacked lines. As can be seen, the attacked lines can be detected successfully in this case.




| Actual $\vec{\theta}'_H$ | Recovered $\hat{\theta}'_H$ |
|---|---|
| 0.1071 | 0.1203 |
| 0.1428 | 0.1242 |
| 0.1085 | 0.0997 |
| 0.1013 | 0.0884 |
| 0.1271 | 0.1273 |
| -0.1409 | -0.1381 |
| -0.1623 | -0.1496 |
| -0.1576 | -0.1563 |
| -0.0429 | -0.0299 |
| -0.0329 | 0.0321 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $\vec{x}$ | 0 | 0 | 0 | 0 | 0 | -0.1938 | 0 | -0.1164 | 0 |
| supp($\vec{x}$) | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |

Fig. 8: An example of an attack and recovered information in the presence of the measurement noise for SNR= 30dB. Red dashed lines show the attacked lines. As can be seen, 2 out of the 3 attacked lines can be detected in this case.

We provide simulation results with the graph and zone $H$ shown in Fig. 6 (it is easy to see that $H$ is attack-resilient). Notice that the graph in Fig. 6 can be part of a much bigger graph, however following Corollary 1 and Lemma 2, only the local information is needed to recover the information inside the attacked zone. As we mentioned in Section VI, in the simulations, we assume that the readings from the PMUs somewhat differ from the solution of (3) (i.e., to the DC power flow). Hence, if $\vec{\theta}$ and $\vec{\theta}'$ are the phase angles obtained from the PMUs (before and after the attack, respectively), then $\mathbf{A}(\vec{\theta} - \vec{e}) = \vec{p}$ and $\mathbf{A}'(\vec{\theta}' - \vec{e}') = \vec{p}$ for unknown Gaussian noise vectors $\vec{e}$ and $\vec{e}'$ with equal covariance matrices.

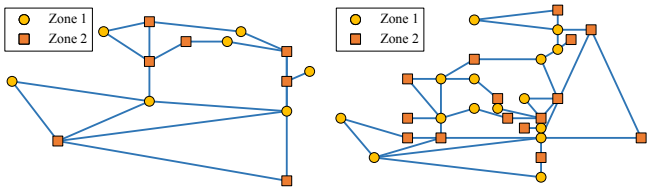
Figs. 7 and 8 show two attack scenarios with different SNR values and the information recovered by solving (9). Fig. 9 shows the average number of false negatives and positives in detecting line failures by solving (9) versus the SNR level for different numbers of line failures. As can be seen, for any number of line failures, when the SNR is above a certain level (e.g., 40 dB) the solution to (9) can detect the line failures with acceptable accuracy (less than one false negative and zero false positives on average). Using the *CVX* solver, the solution to the optimization problem (9) can be found in 0.07 sec in our system with Intel Core i7-2600 @3.40GHz CPU and 16GB RAM for the graph depicted in Fig. 6.

### *B. Evaluating the Performance of the ZS Algorithm*

In this subsection, we demonstrate the results obtained by the ZS Algorithm in several known power grid networks. Table III lists the considered grids and number of resulting partitions. For example, Fig. 10 shows the partitions obtained

TABLE III: Number of partitions into which the ZS Algorithm divides different networks.

| Network | Nodes | Edges | Partitions |
|---|---|---|---|
| IEEE 14-Bus | 14 | 20 | 2 |
| IEEE 30-Bus | 30 | 41 | 2 |
| IEEE 118-Bus | 118 | 179 | 5 |
| IEEE 300-Bus | 300 | 409 | 14 |
| Polish grid | 3120 | 3684 | 10 |
| Colorado state grid | 662 | 864 | 6 |
| Western interconnection | 13135 | 16860 | 9 |




(a) IEEE 14 bus (b) IEEE 30 bus

Fig. 10: Partitioning of the IEEE 14 and IEEE 30 bus systems into 2 attack resilient zones (using the ZS Algorithm).

by ZS Algorithm in the IEEE 14-Bus and 30-Bus benchmark systems [44]. As can be seen, in both cases the graphs can be partitioned into two attack-resilient zones. We also evaluated the ZS Algorithm on the IEEE 118 and 300-bus systems, the Polish grid (available with MATPOWER [45]), the Colorado state grid, and the U.S. Western Interconnection network.[7] Recall form Section VII that when $G$ is planar, the ZS Algorithm is a 6-approximation algorithm for the minimum matched-forest problem. However, as can be seen from the examples above, in practice, it partitions the networks into few zones.

We note that the ZS Algorithm does not take the geographical constraints into account. Thus, when partitioning very large networks such as the Western Interconnection (see Fig. 11), the nodes in the same partition may be geographically distant from each other. This is impractical, since the PMUs from the same zone should send the data to a single PDC. However, it is easy to see that if a zone is attack-resilient, any of its subgraphs is also attack-resilient. Therefore, the partitions obtained by the ZS Algorithm can be further divided into smaller zones based on geographical constraints (e.g., into zones within different states in Fig. 11). This approach does not result in an optimal partitioning. Hence, obtaining an efficient partitioning with geographical constraints is a subject of future work.

## IX. Conclusion

We studied joint cyber and physical attacks on power grids. We developed methods to estimate the state of the grid inside the attacked zone using only the information available outside of the attacked zone. We identified graph topologies and constraints on the attacked edges for which these methods are guaranteed to recover the state information. We briefly studied the problem of information recovery in the presence of measurement noise and showed that by relaxing some of the constraints the same methods can be used for information recovery in noisy scenarios. Moreover, we showed that the problem of partitioning the grid into the minimum number of attack-resilient zones is not approximable to within $n^{1-\epsilon}$ for all $\epsilon > 0$ unless P=NP. However, for planar graphs, we developed an approximation algorithm for the partitioning problem and numerically illustrated the operation of the algorithm.

[7]The data of the Western Interconnection (and of Colorado) was obtained from the Platts Geographic Information System (GIS) [46].

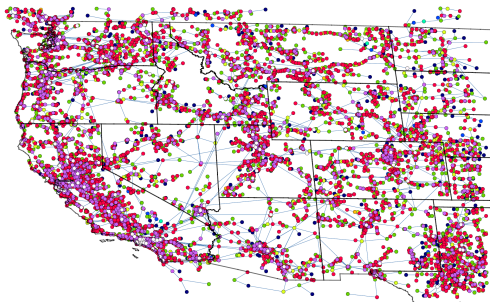


Fig. 11: Partitioning of the U.S. Western Interconnection into 9 attack-resilient zones (using the ZS Algorithm). Nodes with the same color are in the same zone.

This is one of the first steps towards understanding the vulnerabilities of power grids to joint cyber and physical attacks and developing methods to mitigate their effects. Hence, there are still many open problems. In particular, we have been evaluating the performance of the recovery method presented in Section VI when the phase angles are obtained using the AC power flow model. Preliminary results are promising, and therefore, future work will focus on its large scale evaluation using MATPOWER [45]. We also plan to generalize Theorems 2 and 3 to a broader class of graphs, noisy scenarios, and when the control network is limited (e.g, limited number of PMUs). Moreover, we will develop algorithms to partition the grid into weakly-attack-resilient zones while taking into account geographical constraints and constraints on the number and positions of the PDCs.

## Acknowledgement

This work was supported in part by DTRA grant HDTRA1-13-1-0021, DARPA RADICS under contract #FA-8750-16-C-0054, funding from the U.S. DOE OE as part of the DOE Grid Modernization Initiative, and NSF under grant CCF-1320654 and CCF-1423100. The work of G.Z. was also supported in part by the Blavatnik ICRC and the BSF. We thank Janet Kayfetz for her helpful comments.

## References

[1] S. Soltan, M. Yannakakis, and G. Zussman, "Joint cyber and physical attacks on power grids: Graph theoretical approaches for information recovery," in *Proc. ACM SIGMETRICS'15*, June 2015.

[2] P. Fairley, "Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [news]," *IEEE Spectrum*, vol. 53, no. 5, pp. 11–13, May 2016.

[3] "Assault on California power station raises alarm on potential for terrorism," 2014, source: http://goo.gl/RiuhI1.

[4] "U.S.-Canada Power System Outage Task Force. Report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," 2004.

[5] "Report of the enquiry committee on grid disturbance in Northern region on 30th July 2012 and in Northern, Eastern and North-Eastern region on 31st July 2012," Aug. 2012.

[6] "The Federal Energy Regulatory Comission (FERC) and the North American Electric Reliability Corporation (NERC). Arizona-Southern California Outages on September 8, 2011," 2012.

[7] D. Bienstock and A. Verma, "The $N - k$ problem in power grids: New models, formulations, and numerical experiments," *SIAM J. Optimiz.*, vol. 20, no. 5, pp. 2352–2380, 2010.

[8] A. Pinar, J. Meza, V. Donde, and B. Lesieutre, "Optimization strategies for the vulnerability analysis of the electric power grid," *SIAM J. Optimiz.*, vol. 20, no. 4, pp. 1786–1810, 2010.

[9] H. Zhu and G. B. Giannakis, "Sparse overcomplete representations for efficient identification of power line outages," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 2215–2224, 2012.

[10] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 33–43, 2012.

[11] S. Soltan, D. Mazauric, and G. Zussman, "Cascading failures in power grids – analysis and algorithms," in *Proc. ACM e-Energy'14*, June 2014.

[12] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[13] C. Phillips, "The network inhibition problem," in *Proc. ACM STOC'93*, May 1993.

[14] J. Kleinberg, M. Sandler, and A. Slivkins, "Network failure detection and graph connectivity," in *Proc. ACM-SIAM SODA'04*, Jan. 2004.

[15] H. Xiao and E. M. Yeh, "Cascading link failure in the power grid: A percolation-based analysis," in *Proc. IEEE Int. Work. on Smart Grid Commun.*, June 2011.

[16] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabsi–Albert network model," *Phys. A*, vol. 355, no. 2-4, pp. 667 – 677, 2005.

[17] S. Buldyrev, R. Parshani, G. Paul, H. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[18] J. Liu, C. H. Xia, N. B. Shroff, and H. D. Sherali, "Distributed optimal load shedding for disaster recovery in smart electric power grids: A second-order approach," in *Proc. ACM SIGMETRICS'14 (poster description)*, June 2014.

[19] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Sensitivity analysis of the power grid vulnerability to large-scale cascading failures," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 40, no. 3, pp. 33–37, 2012.

[20] I. Dobson, B. Carreras, V. Lynch, and D. Newman, "Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization," *Chaos*, vol. 17, no. 2, p. 026103, 2007.

[21] J. Kim and L. Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun*, vol. 31, no. 7, pp. 1294–1305, 2013.

[22] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[23] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. IEEE SmartGridComm'10*, 2010.

[24] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," in *Proc. IEEE SmartGridComm'11*, 2011.

[25] J. E. Tate and T. J. Overbye, "Line outage detection using phasor angle measurements," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1644–1652, 2008.

[26] ——, "Double line outage detection using phasor angle measurements," in *Proc. IEEE PES'09*, July 2009.

[27] M. Garcia, T. Catanach, S. Vander Wiel, R. Bent, and E. Lawrence, "Line outage localization using phasor measurement data in transient state," *to appear in IEEE Trans. Power Syst.*, preprint available at http://public.lanl.gov/rbent/2015_03_02TransPS.pdf.

[28] N. M. Manousakis, G. N. Korres, and P. S. Georgilakis, "Taxonomy of PMU placement methodologies," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 1070–1077, 2012.

[29] K. Khandeparkar, P. Patre, S. Jain, K. Ramamritham, and R. Gupta, "Efficient PMU data dissemination in smart grid," in *Proc. ACM e-Energy'14 (poster description)*, June 2014.

[30] Y. Zhao, A. Goldsmith, and H. V. Poor, "On PMU location selection for line outage detection in wide-area transmission networks," in *Proc. IEEE PES'12*, July 2012.

[31] M. R. Garey and D. S. Johnson, "Computers and intractability: a guide to the theory of np-completeness," 1979.

[32] X. Wang, X. Song, and J. Yuan, "On matching cover of graphs," *Math. Program.*, vol. 147, no. 1-2, pp. 499–518, 2014.

[33] A. R. Bergen and V. Vittal, *Power Systems Analysis*. Prentice-Hall, 1999.

[34] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures - analysis and control implications," in *Proc. IEEE INFOCOM'14*, Apr. 2014.

[35] J. A. Bondy and U. Murty, "Graph theory, volume 244 of graduate texts in mathematics," 2008.

[36] P. D. Seymour, "On odd cuts and plane multicommodity flows," *P. Lond. Math. Soc.*, vol. 3, no. 1, pp. 178–192, 1981.

[37] W. Rudin, *Real and complex analysis*. McGraw-Hill Education, 1987.

[38] R. Bapat, *Graphs and matrices*. Springer, 2010.

[39] D. Donoho and Y. Tsaig, "Fast solution of l1-norm minimization problems when the solution may be sparse, 2006," *Preprint at http://statweb.stanford.edu/~donoho/Reports/2006/kstep-20061005.pdf*.

[40] D. Zuckerman, "Linear degree extractors and the inapproximability of max clique and chromatic number," in *Proc. ACM STOC'06*, May 2006.

[41] G. Chartrand, D. Geller, and S. Hedetniemi, "Graphs with forbidden subgraphs," *J. Combin. Theory Ser. B*, vol. 10, no. 1, pp. 12–41, 1971.

[42] D. B. West *et al.*, *Introduction to graph theory*. Prentice hall Upper Saddle River, 2001, vol. 2.

[43] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.

[44] "Power systems test case archive," available at: http://www.ee.washington.edu/research/pstca/.

[45] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, 2011.

[46] "Platts GIS Data," http://www.platts.com/Products/gisdata.


**Saleh Soltan** is a Ph.D. student in the department of electrical engineering at Columbia University. He received B.S. degrees in Electrical Engineering and Mathematics (double major) from Sharif University of Technology, Iran in 2011 and the M.S. degree in Electrical Engineering from Columbia University in 2012. He is the Gold Medalist of the 23rd National Mathematics Olympiad in Iran in 2005 and the recipient of Columbia University Electrical Engineering Armstrong Memorial Award in 2012.

**Mihalis Yannakakis** is the Percy K. and Vida L. W. Hudson Professor of Computer Science at Columbia University. Prior to joining Columbia, he was Head of the Computing Principles Research Department at Bell Labs and at Avaya Labs, and Professor of Computer Science at Stanford University. Dr. Yannakakis received his PhD from Princeton University. He has served on the editorial boards of several journals, including as editor-in-chief of the SIAM Journal on Computing, and has chaired various conferences, including the IEEE Symposium on Foundations of Computer Science, the ACM Symposium on Theory of Computing, and the ACM Symposium on Principles of Database Systems. Dr. Yannakakis is a recipient of the Knuth Prize, a member of the National Academy of Engineering, of Academia Europaea, a Fellow of the ACM, and a Bell Labs Fellow.

**Gil Zussman** received the Ph.D. degree in electrical engineering from the Technion in 2004 and was a postdoctoral associate at MIT in 2004-2007. He is currently an Associate Professor of Electrical Engineering at Columbia University. He is a co-recipient of 6 paper awards including the ACM SIGMETRICS'06 Best Paper Award and the 2011 IEEE Communications Society Award for Outstanding Paper on New Communication Topics. He received two Marie Curie Fellowships, the DTRA Young Investigator Award, and the NSF CAREER Award.