Efficient Computations of a Security Index for False Data Attacks in Power Networks

Julien M. Hendrickx, Karl Henrik Johansson, *Fellow, IEEE*, Raphaël M. Jungers,
Henrik Sandberg, and Kin Cheong Sou

***Abstract*—The resilience of Supervisory Control and Data Acquisition (SCADA) systems for electric power networks for certain cyber-attacks is considered. We analyze the vulnerability of the measurement system to false data attack on communicated measurements. The vulnerability analysis problem is shown to be NP-hard, meaning that unless $P = NP$ there is no polynomial time algorithm to analyze the vulnerability of the system. Nevertheless, we identify situations, such as the full measurement case, where the analysis problem can be solved efficiently. In such cases, we show indeed that the problem can be cast as a generalization of the minimum cut problem involving nodes with possibly nonzero costs. We further show that it can be reformulated as a standard minimum cut problem (without node costs) on a modified graph of proportional size. An important consequence of this result is that our approach provides the first exact efficient algorithm for the vulnerability analysis problem under the full measurement assumption. Furthermore, our approach also provides an efficient heuristic algorithm for the general NP-hard problem. Our results are illustrated by numerical studies on benchmark systems including the IEEE 118-bus system.**

***Index Terms*—Mathematical programming, network theory (graph), power system security, SCADA systems, smart grids.**

I. Introduction

OUR society depends heavily on the proper operation of cyber-physical systems, examples of which include, but not limited to, intelligent transport systems, industrial automation systems, health care systems, and electric power distribution and transmission systems. These cyber-physical systems are supervised and controlled through Supervisory Control And Data Acquisition (SCADA) systems. For instance, in the electric power transmission grid, SCADA systems collect measurements through remote terminal units (RTUs) and send them to the state estimator to estimate the system states. The estimated states are used for subsequent operations such as system health monitoring and control. Any malfunctioning of these operations can lead to significant social and economical consequences such as the northeast US blackout of 2003 [1].

The technology and the use of the SCADA systems have evolved a lot since they were introduced. The SCADA systems now are interconnected to office LANs, and through them they are connected to the Internet. Hence, today there are more access points to the SCADA systems, and also more functionalities to tamper with. For example, the RTUs can be subjected to denial-of-service attacks. The communicated data can be subjected to false data attacks. Furthermore, the SCADA master itself can be attacked. In the context of secured cyber-physical systems in general, [2], [3] have considered denial-of-service-like attacks and their impact. Reference [4] has studied replay attacks on the sensor measurements and [5], [6] have considered false data attacks. This paper investigates the cyber security issues related to false data attacks with the special focus on the measurement systems of power networks. The negative effects of false data attacks on SCADA systems have been exemplified by malware such as Stuxnet and Duqu. False data attacks have received a lot of attention in the literature (e.g., [7]–[14]). Reference [7] was the first to point out that a coordinated intentional data attack can be staged without being detected by the state estimation bad data detection (BDD) algorithm, a standard part of today's SCADA/EMS system. References [7]–[9], [11]–[14] investigate the construction problem for such "unobservable" data attack, especially the sparse ones involving relatively few meters to compromise, under various assumptions of the network (e.g., DC power flow model [15], [16]). In particular, [7] poses the attack construction problem as a cardinality minimization problem to find the sparsest attack including a given set of target measurements. References [8], [9], [12] set up similar optimization problems for the sparsest attack including a given measurement. References [11], [14] seek the sparsest nonzero attack and [13] finds the sparsest attack including exactly two injection measurements and possibly more line power flow measurements, under the assumption that all power injections are measured. The solution information of the above optimization problems can help network operators identify the vulnerabilities in the network and strategically assign protection resources (e.g., encryption of measurements and secured PMUs) to their best effect (e.g., [9], [10], [14]). On the other hand, the unobservable data attack problem has its

Manuscript received February 15, 2013; revised December 4, 2013; accepted January 15, 2014. Date of publication August 28, 2014; date of current version November 18, 2014. This work was supported by the "Communauté francaise de Belgique-Actions de Recherche Concertées", the Belgian Programme on Interuniversity Attraction Poles initiated by the Belgian Federal Science Policy Office, the European Commission through the VIKING project, the Swedish Foundation for Strategic Research (SSF), the Swedish Research Council (VR), and the Knut and Alice Wallenberg Foundation. Recommended by Associate Editor P. Tabuada.

J. M. Hendrickx and R. M. Jungers are with the Université Catholique de Louvain, ICTEAM, B-1348 Louvain-la-Nueve, Belgium (e-mail: julien.hendrickx@uclouvain.be; raphael.jungers@uclouvain.be).

K. H. Johansson and H. Sandberg are with the ACCESS Linnaeus Center and the Automatic Control Lab, The School of Electrical Engineering, KTH Royal Institute of Technology, SE-10044 Stockholm, Sweden (e-mail: hsan@kth.se; kallej@kth.se).

K. C. Sou is with the Department of Mathematical Sciences, Chalmers University of Technology, SE-41296 Goteborg, Sweden (e-mail: kincheong.sou@chalmers.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2014.2351625

connection to another vital EMS functionality—observability analysis [15], [16]. In particular, solving the attack construction problem can also solve an observability analysis problem (this was explained in [17, Section II-C]). This connection was first reported in [11], and was utilized in [18] to compute the sparsest critical p-tuples for some integer p. This is a generalization of critical measurements and critical sets [15].

To perform the cyber-security analysis in a timely manner, it is important to solve the data attack construction problem efficiently. This effort has been discussed, for instance, in [7]–[9], [11]–[14], [17]. The efficient solution to the attack construction problem in [8] is the focus of this paper. The matching pursuit method [19] employed in [7] and the basis pursuit method [20] (l_1 relaxation and its weighted variant) employed in [14] are common efficient (i.e., polynomial time) approaches to obtain suboptimal solutions to the attack construction problem. However, these methods do not guarantee exact optimal solutions, and they might not be sufficiently accurate. For instance, [12] describes a naive application of basis pursuit and its consequences. While [11], [14] provide polynomial time solution procedures for their respective attack construction problems, the problems therein are different from the one in this paper in that the considered problem in this paper is not a special case of the ones in [11], [14]. In particular, in [11] the attack vector contains at least one nonzero entry. However, this nonzero entry cannot be given *a priori*. This means that the problem considered in this paper is more general than the one in [11]. Reference [14] needs to restrict the number of nonzero injection measurements attacked, while there is no such constraint in the problem considered in this paper.

Other relevant previous work include [12], [17], [18], which also consider the data attack construction problem in this paper. In [12], [18] the attack construction problem is formulated as a graph generalized minimum cut problem (to be defined in Section IV-C). However, it is not known in [12], [18] whether the generalized minimum cut problem can be solved efficiently (i.e., in polynomial time) or not. Indeed, [12], [18] only provide approximate solutions. Instead, the current work establishes that the generalized minimum cut problem is indeed *exactly solvable in polynomial time*. This work establishes the result by constructing a practical polynomial time algorithm. Regarding [17], one of the main distinctions is that [17] makes an assumption that no bus injections are metered. The current result requires a different assumption that the network is *fully measured* as in [13] (i.e., all bus injections and line power flows are metered). In addition, [17] considers a more general case where the constraint matrix is totally unimodular, whereas the focus of the current paper is a graph problem. The setup considered by this paper is specific to network applications and thus it enables a more efficient solution algorithm. Finally, note that the notion of minimum cut problem has been explored also in other power network applications (e.g., [21], [22]).

Outline: In the next section, we present the optimization problem of interest, namely the security index problem, and discuss its applications. Then Sections III–V present the technical contributions of this paper, focusing on a specialized version of the security index problem defined in (8) in the end of Section II-B. In Section III the complexity of the security index problem is analyzed. We show that the security index problem is NP-hard in general, but in Section IV we demonstrate that under some realistic assumptions it can be restated as a generalized minimum cut (`Min Cut`) problem. In Section V we show that the generalized `Min Cut` problem can be solved efficiently, by reformulating it as a classical `Min Cut` problem. The specialized version considered in Sections III–V turns out to be not restrictive, as far as the application of the proposed results is concerned. This will be explained in Section VI. In Section VII a simple numerical example is first presented to illustrate that the proposed solution correctly solves the generalized `Min Cut` problem. Then the efficiency and accuracy of the proposed solution to the security index problem are demonstrated through a case study with large-scale benchmark systems. We also demonstrate that our method provides an efficient and high quality approximate solution to the general problem security index problem which is NP-hard.

II. The Security Index Problem

In Section II-A, the mathematical model of the power networks considered is first described. Then in Section II-B, the security index of power networks is defined.

A. Power Network Model and State Estimation

A power network is modeled as a graph with $n+1$ nodes and m edges. The nodes and edges model the buses and transmission lines in the power network, respectively. In the present text, the terms node and bus are used interchangeably, and the same is true for edges and transmission lines (or simply lines). The topology of the graph is described by a directed incidence matrix $A \in \mathbb{R}^{(n+1)\times m}$, in which the directions along the edges are arbitrarily specified [12]. The physical property of the network is described by a nonsingular diagonal matrix $D \in \mathbb{R}^{m\times m}$, whose nonzero entries are the reciprocals of the reactance of the transmission lines. In general, the reactance is positive (i.e., inductive) and hence the matrix D is assumed to be positive definite throughout this paper.

In the sequel, the set of all nodes and the set of all directed edges of the power network graph are denoted V^0 and E^0, respectively. The edge directions are consistent with those in A. An element of V^0 is denoted by $v_i \in V^0$, and an element of E^0 is denoted by $(v_i, v_j) \in E^0$ for $v_i \in V^0$ and $v_j \in V^0$. The set of all neighbors of v_i is denoted by $N(v_i)$. A node v_j is a neighbor of v_i if either $(v_i, v_j) \in E^0$ or $(v_j, v_i) \in E^0$.

The states of the network include bus voltage phase angles and bus voltage magnitudes, the latter of which are typically assumed to be constant (one in the per unit system). Therefore, the network states can be captured in a vector $\theta \in [0, 2\pi)^{n+1}$. The state estimator estimates θ based on the measurements obtained from the network. In reality the model relating the states and the measurements is nonlinear. However, for state estimation data attack analysis [7]–[14], [17] (and more traditionally bad data analysis [15], [16], [23]) it suffices to consider the DC power flow model [15], [16]. In addition, the DC power flow model is accurate for security analysis even if control actions taken by the control center are considered. Because of the slow time

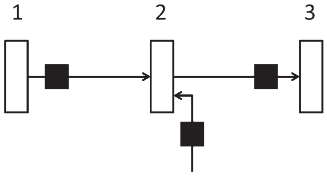


Fig. 1. Simple power network with three buses and two transmission lines. With the assumed directions of the transmission lines, the incidence matrix A, according to MATLAB notation, is $A = [1, 0; -1, 1; 0, -1]$. The matrix D is $D = [1/x_{12}, 0; 0, 1/x_{23}]$, where x_{12} and x_{23} are the reactances of lines (1,2) and (2,3), respectively. The black squares indicate the meters. The measurement selection matrices are $P_1 = [1, 0]$, $P_2 = [0, 1]$, and $P_3 = [0, 1, 0]$.

scale at which today's control centers operate, it is accurate to assume the power system reaches steady state after each new control decision the control center makes. For instance, the sampling period of the control center is at least 10 s, whereas power system transients die out in less than a second (assuming of course it is stable). Reference [24] analyzes how the control center would react under the influence of unobservable data attack.

In the DC power flow model the measurement vector, denoted as z, is related to θ by

$$z = H\theta + \Delta z, \quad \text{where} \quad H \triangleq \begin{bmatrix} P_1 DA^T \\ -P_2 DA^T \\ P_3 ADA^T \end{bmatrix}. \tag{1}$$

In (1), Δz can either be a vector of random error or intentional additive data attack (e.g., [7]), and P_1, P_2, and P_3 consist of subsets of rows of identity matrices of appropriate dimensions, indicating which measurements are actually taken. The term $P_1 DA^T \theta$ contains line power flow measurements, measured at the outgoing ends of the lines. Similarly, $-P_2 DA^T \theta$ contains the line power flow measurements at the incoming ends of the lines. The term $P_3 ADA^T \theta$ contains bus power injection measurements, one entry for each measured bus. For example, P_1 has as many rows as the number of flow measurements at outgoing ends of the lines, and each column of P_1 corresponds to an edge in the network. See Fig. 1 for an illustration of the matrices in (1).

Measurement redundancy is a common practice in power networks [15], [16]. Therefore, it is assumed in this paper that the measurement system described by H is observable—meaning that if any column of H is removed the remaining submatrix still has rank n [15], [16]. Note that H cannot have rank $n+1$ since the sum of all columns of H is always a zero column vector (a property of any incidence matrix A). In the practice of power system state estimation, it is customary to designate an arbitrary node as the reference and set the corresponding entry of θ to zero. Without loss of generality, it is assumed that the first entry of θ is zero (i.e., $\theta(1) = 0$) and denote $\theta_{2:}$ as the rest of the entries of θ. For convenience, let $H_{2:}$ denote H with the first column removed. By definition, $H\theta = H_{2:}\theta_{2:}$ and $H_{2:}$ has full column rank ($= n$) since H is observable. Given measurements z, the estimate of the network states is typically determined via the least squares approach [15], [16]:

$$\hat{\theta}_{2:} = \left(H_{2:}^T W H_{2:}\right)^{-1} H_{2:}^T W z \tag{2}$$

where W is a given positive-definite diagonal matrix, whose nonzero entries are typically the reciprocals of the variances of the measurement noise. The state estimate $\hat{\theta} = \left[0 \ \hat{\theta}_{2:}^T\right]^T$ is subsequently fed to other vital SCADA functionalities such as optimal power flow (OPF) calculation and contingency analysis (CA). Therefore, the accuracy and reliability of $\hat{\theta}$ is of paramount concern.

Notice that in addition to the alternating current (AC) electric power transmission/distribution networks mentioned in this paper, the DC power flow measurement model in (1) can in fact characterize the measurement system of any potential flow network in steady state under certain assumptions, i.e., the potential flows depend linearly on potential differences and the flow conservation law is satisfied. For example, model (1) can describe water distribution networks where the potentials are water pressures and the potential flows (i.e., edge flows) are along distribution pipes where the Hagen-Poiseuille model is valid [25]. Alternatively, model (1) can describe high-voltage direct current (HVDC) electric power transmission networks where the potentials are voltages and the edge flows are DC flows on transmission lines. The edge flows are linearly related to the voltage differences between the end nodes of transmission lines through the Ohm's law.

B. Security Index

To detect possible faults or data attacks in the measurements z, the BDD test is commonly performed [15], [16]. In a typical strategy, if the norm of the residual

$$\text{residual} \triangleq z - H_{2:}\hat{\theta}_2 = \left(I - H_{2:}\left(H_{2:}^T W H_{2:}\right)^{-1} H_{2:}^T W\right) \Delta z \tag{3}$$

is too big, then the BDD alarm is triggered. The BDD test is in general sufficient to detect the presence of a random error Δz [15], [16]. However, in face of a coordinated malicious attack the BDD test can fail. In particular, in [7] it was reported that an attack of the form

$$\Delta z = H\Delta\theta \tag{4}$$

for an arbitrary $\Delta\theta \in \mathbb{R}^{n+1}$ would result in a zero residual in (3) since $H\Delta\theta = H_{2:}\Delta\theta_{2:}$ for some $\Delta\theta_{2:} \in \mathbb{R}^n$. Data attack in the form of (4) is unobservable from the BDD perspective, and this was also experimentally verified in [26] in a realistic SCADA system testbed. Since [7], there has been a significant amount of literature studying the unobservable attack in (4) and its consequences to state estimation data integrity (e.g., [8]–[11], [13], [14]). In particular, [8] introduced the notion of security index α_k for a measurement k as the optimal objective value of the following cardinality minimization problem:

$$\begin{aligned} \alpha_k \triangleq \min_{\Delta\theta \in \mathbb{R}^{n+1}} \quad & \text{card}(H\Delta\theta) \\ \text{subject to} \quad & H(k,:)\Delta\theta = 1 \end{aligned} \tag{5}$$

where card($\cdot$) denotes the cardinality of its argument, k is the label of the measurement for which the security index α_k is computed, and $H(k,:)$ denotes the kth row of H. α_k is the minimum number of measurements an attacker needs to compromise in order to attack measurement k without being detected. In particular, a small α_k implies that measurement k is relatively easy to compromise in an unobservable attack. As a result, the knowledge of the security indices for all measurements allows the network operator to pinpoint the security vulnerabilities of the network, and to better protect the network with limited resource. For example, [9] proposed a method to optimally assign limited encryption protection resources to improve the security of the network based on its security indices.

It should be emphasized that the security index defined in (5) can provide a security assessment that the standard power network BDD procedure [15], [16] might not be able to provide. As a concrete example [8], consider the simple network whose $H_{2:}$ matrix is

$$H_{2:} = \begin{pmatrix} -1 & -1 & 0 \\ -1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}. \tag{6}$$

From (2), the "hat matrix" [15], [16], denoted K is defined according to

$$\hat{z} = H_{2:}\hat{\theta}_2 = H_{2:}\left(H_{2:}^T W H_{2:}\right)^{-1} H_{2:}^T W z \triangleq Kz.$$

Assuming $W = I$, the K matrix associated with $H_{2:}$ in (6) is

$$K = \begin{pmatrix} 0.6 & 0.2 & -0.2 & 0 & 0.4 \\ 0.2 & 0.4 & -0.4 & 0 & -0.2 \\ -0.2 & -0.4 & 0.4 & 0 & 0.2 \\ 0 & 0 & 0 & 1 & 0 \\ 0.4 & -0.2 & 0.2 & 0 & 0.6 \end{pmatrix}. \tag{7}$$

The hat matrix K shows how the measurements z are weighted together to form a power flow estimate $\hat{z}$. The rows of the hat matrix can be used to study the measurement redundancy in the system [15], [16]. Typically a large degree of redundancy (many non-zero entries in each row) is desirable to compensate for noisy or missing measurements. In (7), it is seen that all measurements are redundant except the fourth which is called a *critical measurement*. Without the critical measurement observability is lost. From the hat matrix one is led to believe that the critical measurement is sensitive to attacks. This is indeed the case, but some other measurements can also be vulnerable to attacks. It can be shown—for example using the method that we develop, that the security indices α_k, $k = 1, \ldots, 5$, respectively, are 2, 3, 3, 1, 2. Therefore, the fourth measurement (critical measurement) has security index one, indicating that it is indeed vulnerable to unobservable attacks. However, the first and the last measurements also have relatively small security indices. This is not obvious from K in (7). Hence, we cannot rely on the hat matrix for vulnerability analysis of power networks.

For ease of exposition but without loss of generality, instead of (5) the following version of the security index problem with a specialized constraint will be the focus of the parts of the paper where the main technical contributions are presented (i.e., Sections III–V):

$$\begin{aligned} \underset{\Delta\theta\in\mathbb{R}^{n+1}}{\text{minimize}} \quad & \operatorname{card}(H\Delta\theta) \\ \text{subject to} \quad & A(:,\bar{e})^T\Delta\theta \neq 0 \end{aligned} \tag{8}$$

where $\bar{e} \in \{1, 2, \ldots, m\}$ is given. The restriction introduced in (8) is that it can only enforce constraints on edge flows but not on node injections as directly allowed by (5). We will see however in Section VI that all results obtained for (8) can be extended to the general case in (5).

III. The Security Index Problem is NP-Hard

Consider a variant of (5) where k is not fixed (i.e., one wishes to minimize $\operatorname{card}(H\Delta\theta)$ under the constraint that at least one entry of $H\Delta\theta$ is nonzero). This variant of (5) is known to be the cospark of $H_{2:}$ in compressed sensing [27]. The cospark of $H_{2:}$ is the same as the spark of F, where F is a matrix of full row rank such that $FH_{2:} = 0$ [27]. The spark of F is defined as the minimum number of columns of F which are linearly dependent [28]. It is established that computing the spark of a general matrix F is NP-hard [29], [30]. Consequently, because of the equivalence between spark and cospark, unless $P = NP$ there is no efficient algorithm to solve the security index problem in (5) if the H matrix is not assumed to retain any special structure. In power network applications, the H matrix in fact possesses special structure as defined in (1). Nevertheless, the security index problem, even the specialized version in (8), is still computationally intractable as indicated by the following statement:

Theorem 1: Unless $P = NP$, there is no polynomial time algorithm that solves the problem (8), with H defined in (1), even if D is the identity matrix and P_2 is an emtpy matrix.

Proof: Our proof proceeds by reduction from the positive one-in-three 3SAT problem [31]: *Given a set of M triples of indices $C_j = (\alpha_j, \beta_j, \gamma_j) \in \{1, \ldots, n\}^3$, does there exist a vector $\tilde{x} \in \{0,1\}^n$ such that for every j, exactly one among $\tilde{x}_{\alpha_j}, \tilde{x}_{\beta_j}, \tilde{x}_{\gamma_j}$ is 1 and the others 0.*

Consider an instance of the positive one-in-three 3SAT problem, and let us build an equivalent instance of (5). We take an empty matrix as P_2, and set D as the identity matrix. P_1 and P_3 consist by definition of selected rows of the identity matrices of dimensions respectively equal to the number of edges and the number of nodes. Each row selected in P_1 corresponds univocally to an edge of the graph. We say that an edge for which there is a corresponding row in P_1 is *measured*. Similarly, each row selected in P_3 corresponds to a node, and we will say that this node is measured. Other nodes and edges will be called *floating*. The sets of measured edges and nodes entirely characterize P_1 and P_3, and it is more convenient in this proof to describe these sets instead of the matrices. Note that if the edge (v_i, v_j) is measured, then $H\Delta\theta$ contains a corresponding entry $\Delta\theta_j - \Delta\theta_i$. Similarly, if v_i is measured, then $H\Delta\theta$ contains an entry $\sum_{v_j\in N(v_i)}(\Delta\theta_j - \Delta\theta_i)$.

We begin by defining a node 1 and a node 0 connected by a *measured* edge. We set $\bar{e}$ such that the constraint $A(\bar{e},:)\Delta\theta = 1$

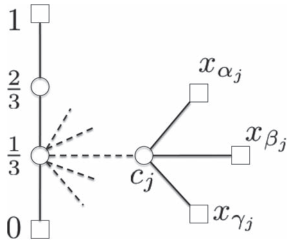


Fig. 2. Representation of a part of the construction of the proof of Theorem 1, including the reference values of $\Delta\theta$ and one clause C_j. Edges are represented by dashed line when they are measured and continuous lines when they are floating. Nodes are represented by squares when they are measured and circles when they are floating. If $\mathrm{card}(H\Delta\theta) = n + 1$, the rest of the construction ensures that $\Delta\theta$ takes only values 1 and 0 for the x_i, and that all entries of $H\Delta\theta$ other than those corresponding to the nodes x_i must be zero. As a result, a measured (dashed) edge transmits no current and enforces equality between the values of the nodes to which it is incident, and measured (circle) nodes enforce that the sum of the currents on the incident edges should be 0. These constraints can only be satisfied if $\Delta\theta_{c_j} = 1/3$, and if exactly one of the nodes involved in each clause is at 1 while the others are at 0.

in (8), corresponds to this edge, so that there must hold $\Delta\theta_1 - \Delta\theta_0 = 1$ for any solution of the problem. Since $H\Delta\theta$ is not modified when adding a constant to all entries of $\Delta\theta$, we assume without loss of generality that $\Delta\theta_1 = 1$ and $\Delta\theta_0 = 0$.

The goal of the first part of our construction is to represent the n variables. For every $i = 1, \ldots, n$, we define a floating node x_i, and we connect it to both 1 and 0 by measured edges. Observe that the two entries of $H\Delta\theta$ corresponding to these two edges are $1 - \Delta\theta_{x_i}$ and $0 - \Delta\theta_{x_i}$, which cannot be simultaneously 0. Moreover, one of them is equal to zero if and only if $\Delta\theta_{x_i}$ is either 0 or 1.

Taking into account the fact the entry of $H\Delta\theta$ corresponding to the edge (1,0) is by definition 1, it follows that $\mathrm{card}(H\Delta\theta) \geq n + 1$ for any $\Delta\theta$, independently of the rest of the construction. Moreover, $\mathrm{card}(H\Delta\theta) = n + 1$ only if $\Delta\theta_{x_i} \in \{0, 1\}$ for every i, and if the entries of $H\Delta\theta$ corresponding to all the measured edges and nodes introduced in the sequel are 0. The remainder of the construction, represented in Fig. 2, is designed to ensure that all these entries can be 0 only if the (binary) values $\Delta\theta_{x_i}$ solves the initial instance of the positive one-in-three 3SAT problem.

We first generate a reference value at 1/3: We define two measured nodes indexed by 2/3 and 1/3. We then add floating edges (1, 2/3), (2/3, 1/3), (1/3, 0). Besides, we define for every clause $j = 1, \ldots, M$ a measured clause node c_j connected to 1/3 by a measured edge.

The entries of $H\Delta\theta$ corresponding to the edges between 1/3 and c_j are $\Delta\theta_{1/3} - \Delta\theta_{c_j}$. We have seen that, if $\mathrm{card}(H\Delta\theta) = n + 1$, all these entries must be equal to 0, so that $\Delta\theta_{c_j} = \Delta\theta_{1/3}$ for every j. Observe then that the entry of $H\Delta\theta$ corresponding to 1/3 is in that case

$$\Delta\theta_{\frac{2}{3}} + \Delta\theta_0 + \sum_{j=1}^{M} \Delta\theta_{c_j} - (2 + M)\Delta\theta_{\frac{1}{3}} = \Delta\theta_{\frac{2}{3}} + 0 - 2\Delta\theta_{\frac{1}{3}}$$

while the entry corresponding to 2/3 is $1 + \Delta\theta_{1/3} - 2\Delta\theta_{2/3}$. These two entries are thus equal to zero if and only if $\Delta\theta_{2/3} = 2/3$ and $\Delta\theta_{c_j} = \Delta\theta_{1/3} = 1/3$ for every j, as intended.

We now represent the clauses. For each j, we connect the (measured) clause node c_j to the (floating) nodes x_{α_j}, x_{β_j}, and x_{γ_j} of the three variables involved in the clause by floating edges. The entry of $H\Delta\theta$ corresponding to each clause node c_j is then

$$\begin{aligned}\Delta\theta x_{\alpha_j} + \Delta\theta x_{\beta_j} + \Delta\theta x_{\gamma_j} - 3\Delta\theta_{c_j}& \\ = \Delta\theta x_{\alpha_j} + \Delta\theta x_{\beta_j} + \Delta\theta x_{\gamma_j} - 1.&\end{aligned}$$

Remembering that $\Delta\theta_{x_i}$ is either 1 or 0 for any i, this latter expression can be zero only if exactly one among $\Delta\theta x_{\alpha_j}$, $\Delta\theta x_{\beta_j}$, and $\Delta\theta x_{\gamma_j}$ is 1. If that is the case, setting $\tilde{x}_i = \Delta\theta_{x_i}$ for every i yields a vector x that solves the instance of positive one-in-three 3SAT.

We have thus shown that there exists a $\Delta\theta$ for which $\mathrm{card}(H\Delta\theta) = n + 1$ only if the $\Delta\theta_{x_i}$ are binary and the binary vector $\tilde{x}$ obtained by setting $\tilde{x}_i = \Delta\theta_{x_i}$ solves the instance of positive one-in-three 3SAT. Conversely, one can verify that if a binary vector $\tilde{x}$ solves the instance of the one-in-three 3SAT problem, then setting $\Delta\theta_{x_i} = \tilde{x}_i$ for every i, $\Delta\theta_{c_j} = \Delta\theta_{1/3} = 1/3$ for every j and $\Delta\theta_{2/3} = 2/3$ yields a cost $\mathrm{card}(H\Delta\theta) = n + 1$. The latter cost can thus be obtained if and only if the initial positive one-in-three 3SAT problem is achievable. This achieves the proof because our construction clearly takes an amount of time that grows polynomially with the size of the instance C, and unless $P = NP$ there is no polynomial time algorithm that solves the positive one-in-three 3SAT [31]. ■

Remark 1: (5) is also NP-hard since (8) is a special case of (5).

IV. Tractable Cases of Security Index Problem

In Section IV-A, we show that, under the full measurement assumption, the security index problem can be solved by solving its restriction where decision variables take binary values. Section IV-B presents the proof of the statement which implies our finding in Section IV-A. Section IV-B also discusses the relationship between the security index problem and its binary restriction defined in Section IV-A. Section IV-C describes the consequences of Section IV-A and B, explaining how the security index problem can be reformulated as a generalized minimum cut problem with node costs, a graph problem whose efficient solution will be discussed in Section V.

A. The Security Index Problem Under Full Measurement Assumption

Even though in general the security index problem in (8) is NP-hard for H defined in (1), there exist interesting specializations that are solvable in polynomial time. One such case is the *full measurement* situation where $P_1 = I$, $P_2 = I$, and $P_3 = I$. In [12], [13], the full measurement assumption is also considered, motivated by the situations where all power flows and injections are measured in future smart grid applications. The polynomial time complexity of (8) under the full measurement assumption can be established in three steps. Firstly, it can be shown that problem (8) can be solved by solving a restriction where the decision vector $\Delta\theta$ is a binary vector. Secondly, in

Section IV-C it will be shown that the binary restriction of (8) can be expressed in a generalized `Min Cut` problem with node costs. Finally, this generalized `Min Cut` problem can be shown to be solvable in polynomial time. This is to be explained in Section V.

The first step is formalized in the following statement, whose preliminary version appeared in [12].

Proposition 1: Let H in (1) satisfy the full measurement assumption that $P_1 = I$, $P_2 = I$, and $P_3 = I$. Consider the restriction of problem (8) with 0–1 binary decision vector

$$\begin{aligned} \underset{\Delta\theta\in\{0,1\}^{n+1}}{\text{minimize}} \quad & \operatorname{card}(H\Delta\theta) \\ \text{subject to} \quad & A(:,\bar{e})^T\Delta\theta \neq 0. \end{aligned} \tag{9}$$

It holds that every optimal solution of (9) is an optimal solution of (8) (i.e., the problem with the same formulation except that $\Delta\theta$ is not restricted to binary values).

Proof: Proposition 1 is a corollary of the more general Theorem 2 to be described in Section IV-B. ■

Remmark 2: Since there cannot be any all-zero column in any incidence matrix A, problem (8) and (9) are always feasible. Proposition 1 states that, under the full measurement assumption, an optimal solution of (8) can always be obtained by solving (9). The later problem will be shown to be solvable in polynomial time.

B. The Security Index Problem With Binary Decision Vector

This subsection establishes Proposition 1, providing the first step in the efficient solution method for problem (8) under the full measurement assumption. Recall that V^0 and E^0 denote the sets of all nodes and all edges of the power network graph, respectively. In the sequel, let $p_i \geq 0$ represent the cost of attacking the injection measurement at bus $v_i \in V^0$, and $c_e \geq 0$ represent the cost of attacking the power flow measurements at both ends of an edge $e \in E^0$ (it is impossible to modify the measurement at one end without affecting the one at the other end). Problem (8) can be generalized to model the situation where tampering with certain measurements may be more expensive than with some others:

$$\begin{aligned} \underset{\Delta\theta\in\mathbb{R}^{n+1}}{\text{minimize}} \quad & c^T g(DA^T\Delta\theta) + p^T g(ADA^T\Delta\theta) \\ \text{subject to} \quad & A(:,\bar{e})^T\Delta\theta \neq 0 \end{aligned} \tag{10}$$

where $p \in \mathbb{R}_+^{n+1}$ is the node measurement attack cost vector whose entries are indexed by p_i for each $v_i \in V^0$, and $c \in \mathbb{R}_+^m$ is the edge measurement attack cost vector whose entries are indexed by c_e for each $e \in E^0$. Similar to the change from (8) to (10), the binary variable version in (9) is generalized to

$$\begin{aligned} \underset{\Delta\theta\in\{0,1\}^{n+1}}{\text{minimize}} \quad & c^T g(DA^T\Delta\theta) + p^T g(ADA^T\Delta\theta) \\ \text{subject to} \quad & A(:,\bar{e})^T\Delta\theta \neq 0. \end{aligned} \tag{11}$$

In (10) and (11), g is a vector-valued indicator function such that for any vector x, $g_i(x) = 1$ if $x_i \neq 0$ and $g_i(x) = 0$ otherwise. An instance of (10) or (11) can be reduced, respectively, to an instance of (8) or (9) if the following rules are applied: In (10) or (11), for each $v_i \in V^0$, let $p_i \in \{0,1\}$ be the total number of nonzero entry in the column of P_3 corresponding to v_i (P_3 defined in H in (1)). For each $e \in E^0$, set $c_e \in \{0,1,2\}$ to be the total number of nonzero entries in the column of $[P_1^T P_2^T]^T$ corresponding to e. Then, (8) or (9) is recovered. The following theorem characterizes the relationship between the security index problem in (8) and its binary restriction in (9) by studying their respective generalizations of (10) and (11) for arbitrary nonnegative vectors c and p.

Theorem 2: Let J_c and J_b, respectively, denote the optimal objective values of (10) and of its restriction to binary variables (11) with A and D defined in (1), $c \in \mathbb{R}_+^m$, $p \in \mathbb{R}_+^{n+1}$, and $\bar{e} \in \{1,2,\ldots,m\}$ given. Then

$$0 \leq J_b - J_c \leq \sum_{v_i\in V^0} \max\left\{0, \max_{e\to v_i}\{p_i - c_e\}\right\} \tag{12}$$

where the symbol $e \to v_i$ denotes that $e \in E^0$ is incident to node v_i (i.e., $\exists v_j \in V^0$ such that e connects v_i and v_j).

Proof: The proof requires the following notations: In (10) and (11), the vector $DA^T\Delta\theta$ has as many rows as the number of edges in the power network graph (with node set V^0 and edge set E^0). Each row of $DA^T\Delta\theta$ corresponds to some edge $e \in E^0$. We denote by $[DA^T\Delta\theta]_e$ the row of $DA^T\Delta\theta$ corresponding to edge e. Similarly, the vector $ADA^T\Delta\theta$ has as many rows as the number of nodes, and each row corresponds to some node $v \in V^0$. We denote by $[ADA^T\Delta\theta]_v$ the row of $ADA^T\Delta\theta$ corresponding to node v. With a slight abuse of notation, the symbol $g([DA^T\Delta\theta]_e)$ denotes the entry of $g(DA^T\Delta\theta)$ corresponding to e. In addition, $g([ADA^T\Delta\theta]_v)$ corresponds to the entry of $g(ADA^T\Delta\theta)$ associated with node v. We remind the reader that $N(v_i)$ denote the set of all nodes neighboring v_i.

First note that both (10) and (11) are always feasible with finite optimal objective values attained by some optimal solutions. In addition, $0 \leq J_b - J_c$ holds because (11) is a restriction of (10). To show the upper bound in (12) the main idea is that for each feasible solution $\Delta\theta$ of (10) it is possible to construct a feasible solution $\Delta\phi$ of (11), such that the objective value difference is bounded from above by $\sum_{v_i\in V^0}\max\{0, \max_{e\to v_i}\{p_i - c_e\}\}$. The construction is as follows. Let $\Delta\theta$ be a feasible solution of (10), and let $\Delta\theta_i$ be its entry corresponding to node $v_i \in V^0$. Since $\Delta\theta$ is feasible, the constraint $A(:,\bar{e})^T\Delta\theta \neq 0$ implies that there exist two nodes denoted v_s and v_t with $\bar{e}$ corresponding to either (v_s, v_t) or (v_t, v_s) such that $\Delta\theta_s \neq \Delta\theta_t$. Without loss of generality, it is assumed that $\Delta\theta_s > \Delta\theta_t$. Define $\Delta\phi \in \{0,1\}^{n+1}$ by

$$\Delta\phi_i = \begin{cases} 1 & \text{if } \Delta\theta_i > \Delta\theta_t \\ 0 & \text{if } \Delta\theta_i \leq \Delta\theta_t \end{cases} \quad \forall\, v_i \in V^0. \tag{13}$$

Note that $\Delta\phi$ is feasible to (11), since $\Delta\phi_s \neq \Delta\phi_t$ by construction. Also notice that for any two nodes v_i and v_j if $\Delta\theta_i = \Delta\theta_j$ then $\Delta\phi_i = \Delta\phi_j$. Hence, in the objective functions of (10) and (11) it holds that

$$c_e g\left([DA^T\Delta\theta]_e\right) \geq c_e g\left([DA^T\Delta\phi]_e\right), \quad \forall\, e \in E^0. \tag{14}$$

In other words, for each edge the contribution to the objective function with the new solution $\Delta\phi$ is smaller than or equal to that with the initial one $\Delta\theta$. To finish the proof, the objective function contributions due to the node injections, i.e., the terms $p^T g(ADA^T\Delta\theta)$ and $p^T g(ADA^T\Delta\phi)$, need to be investigated. We will see that for some nodes the difference of nodal objective contributions between the solutions $\Delta\phi$ and $\Delta\theta$ is positive, and in fact equal to p_i for each such node v_i. On the other hand we will show that to each of these nodes one can associate a distinct incident edge $\tilde{e}(i)$ for which the corresponding difference of edge objective contributions is $-c_{\tilde{e}(i)}$. To investigate the the aforementioned cost change, let $V_b \subset V^0$ be the set of nodes defined by

$$v_i \in V_b \iff g\left([ADA^T\Delta\theta]_{v_i}\right) = 0,\ g\left([ADA^T\Delta\phi]_{v_i}\right) = 1. \tag{15}$$

In essence, V_b encompasses all potential causes for $J_b > J_c$. Consider $v_i \in V_b$, since $g([ADA^T\Delta\phi]_{v_i}) = 1$, there exists $v_k \in N(v_i)$ such that $\Delta\phi_k \neq \Delta\phi_i$, and therefore $\Delta\theta_k \neq \Delta\theta_i$ (by the definition (13)). Consequently, the fact that $g([ADA^T\Delta\theta]_{v_i}) = 0$ (i.e., $\sum_{v_j\in N(v_i)} D^{i,j}(\Delta\theta_j - \Delta\theta_i) = 0$ with $D^{i,j} > 0$ denoting the diagonal entry of D associated with the edge linking v_i and v_j) implies that (i) there exists $v_{i^+} = \text{argmax}_{v_k\in N(v_i)}\{\Delta\theta_k\}$ such that $\Delta\theta_{i^+} > \Delta\theta_i$; and (ii) there exists $v_{i^-} = \text{argmin}_{v_k\in N(v_i)}\{\Delta\theta_k\}$ such that $\Delta\theta_{i^-} < \Delta\theta_i$. For each node $v_i \in V_b$, we then define $\tilde{e}(i) \in E^0$ as the edge linking v_i to v_{i^+} if $\Delta\theta_i > \Delta\theta_t$, and as the edge linking v_i to v_{i^-} if $\Delta\theta_i \leq \Delta\theta_t$. It follows from the definition of v_{i^+} and v_{i^-} that in both cases, $\tilde{e}(i)$ connects v_i with a node whose corresponding entry in $\Delta\theta$ is more distant from $\Delta\theta_t$ than $\Delta\theta_i$ is. As a result, there holds

$$v_i \neq v_j \Rightarrow \tilde{e}(i) \neq \tilde{e}(j), \quad \forall\, v_i, v_j \in V_b. \tag{16}$$

We now prove that for every $v_i \in V_b$,

$$g\left([DA^T\Delta\theta]_{\tilde{e}(i)}\right) = 1, \quad g\left([DA^T\Delta\phi]_{\tilde{e}(i)}\right) = 0. \tag{17}$$

We suppose first that $\Delta\theta_i > \Delta\theta_t$, and thus that $\tilde{e}(i)$ connects v_i to v_{i^+}. The equalities of (17) can in that case be written $\Delta\theta_{i^+} \neq \Delta\theta_i$ and $\Delta\phi_{i^+} = \Delta\phi_i$. By definition of v_{i^+}, there holds $\Delta\theta_{i^+} > \Delta\theta_i > \Delta\theta_t$, which directly proves the first one, and implies moreover that $\Delta\phi_{i^+} = \Delta\phi_i = 1$ thanks to the definition of $\Delta\phi$, so that the second equality also holds. A symmetric reasoning applies if $\Delta\theta_i \leq \Delta\theta_t$.

We can now deduce the second inequality of (12): For all feasible solutions $\Delta\theta$ of (10), it holds that

$$\begin{aligned} J_b &- c^T g(DA^T\Delta\theta) - p^T g(ADA^T\Delta\theta) \\ &\leq c^T g(DA^T\Delta\phi) + p^T g(ADA^T\Delta\phi) \\ &\qquad - c^T g(DA^T\Delta\theta) - p^T g(ADA^T\Delta\theta) \end{aligned} \tag{18}$$

because $\Delta\phi$ is a feasible solution of (11) and J_b is the optimal objective value of (11). The second member of the inequality (18) can be rewritten as

$$\begin{aligned} &\sum_{v_i\in V_b} p_i\left(g\left([ADA^T\Delta\phi]_{v_i}\right) - g\left([ADA^T\Delta\theta]_{v_i}\right)\right) \\ &+ \sum_{v_i\in V^0\setminus V_b} p_i\left(g\left([ADA^T\Delta\phi]_{v_i}\right) - g\left([ADA^T\Delta\theta]_{v_i}\right)\right) \\ &+ \sum_{v_i\in V_b} c_{\tilde{e}(i)}\left(g\left([DA^T\Delta\phi]_{\tilde{e}(i)}\right) - g\left([DA^T\Delta\theta]_{\tilde{e}(i)}\right)\right) \\ &+ \sum_{\substack{e\in E^0 \\ e\neq\tilde{e}(i),\ \forall\, v_i\in V_b}} c_e\left(g\left([DA^T\Delta\phi]_e\right) - g\left([DA^T\Delta\theta]_e\right)\right). \end{aligned} \tag{19}$$

It follows indeed from (16) that every edge $e \in E_0$ appears exactly once in the summation (19), either in the third or the fourth term, so that the sum of these two terms equals $c^T g(DA^T\Delta\phi) - c^T g(DA^T\Delta\theta)$. The definition of V_b (15) implies that the first term of (19) is equal to $\sum_{v_i\in V_b} p_i$, and that the second is zero. Equation (17) implies then that the third term is equal to $\sum_{v_i\in V_b} c_{\tilde{e}(i)}$. Finally, (14) implies the nonpositivity of the fourth term. We have thus

$$\begin{aligned} J_b &- c^T g(DA^T\Delta\theta) - p^T g(ADA^T\Delta\theta) \\ &\leq \sum_{v_i\in V_b}\left(p_i - c_{\tilde{e}(i)}\right) \\ &\leq \sum_{v_i\in V_b}\max_{e\to v_i}\{p_i - c_e\} \\ &\leq \sum_{v_i\in V^0}\max\left\{0, \max_{e\to v_i}\{p_i - c_e\}\right\}. \end{aligned} \tag{20}$$

Finally, since (20) applies to all feasible solutions $\Delta\theta$ of (10), the upper bound in (12) follows. ■

Remark 3: The full measurement assumption in Proposition 1 corresponds to a special case in Theorem 2 where $c_e = 2$ for all $e \in E^0$ and $p_i = 1$ for all $v_i \in V^0$. The inequalities in (12) imply Proposition 1.

Remark 4: Theorem 2 suggests other situations where (8) and (9) are equivalent. One example is when there is a meter on each edge and there is at most one meter in each node. In this case, $[P_1^T\ P_2^T]^T$ does not have a zero column and P_3 consists of subsets of rows of an identity matrix. This corresponds to $c_e = 1$ for all e and $p_i \leq 1$ for all i, j in Theorem 2. Another situation suggesting equivalence is as follows: if an edge is not metered, then its two terminal nodes are not metered either. This corresponds to a case when $p_i \leq \min_{e\to v_i} c_e$ for all $v_i \in V^0$, implying that $\max_{e\to v_i}\{p_i - c_e\} = 0$.

Remark 5: Without the full measurement assumption or conditions such as those described in Remark 4, solving (9) can lead to an approximate solution to (8) with an error upper bound provided by (12). This error bound, however, is rather conservative since the summation is over all nodes $v_i \in V^0$. As developed in the proof, the summation is in fact over a subset V_b of V^0. However, in general it is difficult to characterize the V_b which leads to the tightest possible upper bound without first solving (8) to optimality.

Remark 6: The argument in Remark 4 provides the basis for obtaining a lower bound for the optimal objective value of (8) even without the full measurement assumption: Construct a modified measurement matrix $\tilde{H}$ corresponding to a modified measurement system in which each edge has exactly the same number of meters as in the original measurement system. However, the set of node meters in the modified measurement system is a subset of the node meter set in the original case. All node meters in nodes incident to any unmetered edge are removed in the modified setup. Solving (8) with $\tilde{H}$ leads to a lower bound of the optimal objective value of (8) with H because the objective function in the former case is always less than or equal to that of the later case. In addition, by Remark 4 solving (9) with $\tilde{H}$ leads to the exact optimal objective value of (8) with $\tilde{H}$. Therefore, solving (9) with $\tilde{H}$ leads to an efficient approach to obtain a lower bound for the original problem of (8) with H, provided that (9) with $\tilde{H}$ can be solved efficiently.

C. Reformulating the Security Index Problem into Generalized Min Cut Problem With Node Costs

The above discussion suggests that the (exact or approximate) solution to the security index problem is obtained by solving (11), whose graph interpretation will be the focus of this subsection. In (11) the choice of 0 or 1 for each entry of $\Delta\theta$ is a partitioning of the nodes into two parts. The constraint $A(:,\bar{e})^T\Delta\theta \neq 0$ enforces that the two end nodes of edge $\bar{e}$, denoted as v_s and v_t, must be in two different parts of the partition. In the objective function, the term $c^T g(DA^T\Delta\theta)$ is the sum of the edge weights of the edges whose two ends are in different parts (i.e., edges that are "cut", in an undirected sense). In addition, since $\Delta\theta$ has binary entries, a row of $ADA^T\Delta\theta$ is zero if and only if the corresponding node and all its neighbors are in the same part of the partition (i.e., none of the incident edges are cut). Therefore, the term $p^T g(ADA^T\Delta\theta)$ in the objective function is the sum of the node weights of the nodes connected to at least one cut edge. In summary, (11) can be reinterpreted as a generalized minimum cut problem on an undirected graph (i.e., the original power network graph with the edge direction ignored). The generalization is due to the presence of the node weights.

We now define formally the `Min Cut with node costs` problem (on any given directed graph) of which (11) and the standard `Min Cut` problem are special cases. Let $G(V, E)$ be a directed graph (we will see that the problem can be particularized to undirected graphs), where V denotes the set of nodes $\{v_1, \ldots, v_{n+1}\}$, and E the set of directed edges; and suppose that a cost $c_{ij} \geq 0$ is associated to each directed edge (v_i, v_j) and a cost $p_i \geq 0$ is associated to each node v_i. We designate two special nodes: a source node v_s and a sink node v_t. The problem is the following:

Problem 1: **The** `Min Cut with node costs` **problem**. Find a partition of V, denoted as $P = \{S_s, S_t\}$, such that $S_s, S_t \subset V$, $S_s \cap S_t = \emptyset$, $S_s \cup S_t = V$, $s \in S_s$, $t \in S_t$ which minimizes the cost

$$C(P) = \sum_{(v_i,v_j)\in E : v_i \in S_s, v_j \in S_t} c_{ij} + \sum_{v_i \in S_s : \exists (v_i,v_j)\in E : v_j \in S_t} p_i + \sum_{v_j \in S_t : \exists (v_i,v_j)\in E : v_i \in S_s} p_j. \quad (21)$$

When the node costs are all set to zero (i.e., $p_i = 0$ for all $v_i \in V$), Problem 1 reduces to the standard `Min Cut` problem (see, for instance, [32] for more detail). By convention, if $v_i \in S_s$, $v_j \in S_t$, for two nodes v_i, v_j, we will say that both these nodes, and the edge (v_i, v_j), are *in the cut*, or that this edge is cut.

Notice that in a directed graph an edge (v_i, v_j) is cut if $v_i \in S_s$ and $v_j \in S_t$ but not in the reverse case, where $v_i \in S_t$ and $v_j \in S_s$, and the cost c_{ij} is not incurred in that latter case. This asymmetry disappears however in symmetric graphs, in which to each edge (v_i, v_j) with weight c_{ij} corresponds a symmetric edge (v_j, v_i) with same weight. For these symmetric graphs, the cost c_{ij} is incurred as soon as v_i and v_j are not in the same set. Indeed, exactly one among (v_i, v_j) and (v_j, v_i) is in the cut in that case. The cost (21) consists then of the sum of the $c_{ij} (= c_{ji})$ over all pairs of nodes v_i, v_j that are in different sets, and consists of the sum of the p_i over all nodes that are adjacent to nodes in a different set. Thus, (11) defined on the power network graph $G(V^0, E^0)$ could be modeled by Problem 1 defined on a symmetric graph $G(V, E)$ if the following holds: Let $V = V^0$ with node cost p_i for each $v_i \in V$. In addition, for each $e = (v_i, v_j) \in V^0$ with cost c_e let both (v_i, v_j) and (v_j, v_i) be in E with cost $c_{ij} = c_{ji} = c_e$. In addition, by letting $c_{ij} = c_{ji} = 2$ for every edge $e = (v_i, v_j)$ and $p_i = 1$ for every node, one recovers problem (9) under the full measurement assumption. We will show in Section V how to solve Problem 1, and hence the problems in (11), (9), and (8).

V. An Efficient Solution to the Generalized Min Cut Type Security Index Problem

This section presents the efficient solution to the `Min Cut with node costs` problem (i.e., Problem 1) introduced in Section IV-C. The proposed solution method also solves the security index problem under the full measurement assumption, since this problem is a special case of the `Min Cut with node costs` problem.

A. Construction of an Auxiliary Graph

Consider a directed graph $G(V, E), V = \{v_1, \ldots, v_{n+1}\}$ with a set of nonnegative weights $c_{ij} \geq 0$, and $p_i \geq 0$ for each node $v_i \in V$, a source node v_s and a sink node v_t. We build an auxiliary graph $\tilde{G}$ using the following algorithm, illustrated in Fig. 3 on an example:

1) Define the set $\tilde{V} = \{\tilde{v}_i, \tilde{w}_i, \tilde{z}_i : 1 \leq i \leq n+1\}$ of nodes of the auxiliary graph.
2) Designate $\tilde{v}_s$ and $\tilde{v}_t$ as source and sink nodes respectively.
3) For all $1 \leq i \leq n+1$, add the two directed edges $(\tilde{w}_i, \tilde{v}_i)$ and $(\tilde{v}_i, \tilde{z}_i)$, both with cost p_i.
4) For all $1 \leq i, j \leq n+1 : (v_i, v_j) \in E$
   - add the edge $(\tilde{v}_i, \tilde{v}_j)$ with cost c_{ij}.
   - add the two edges $(\tilde{v}_i, \tilde{w}_j)$ and $(\tilde{z}_i, \tilde{v}_j)$, both with a cost $C > \max_i p_i$.

The intuition behind the construction of $\tilde{G}$ is the following: Suppose that one wants to cut the edge $(\tilde{v}_i, \tilde{v}_j)$, then one must also cut at least either $(\tilde{v}_i, \tilde{z}_i)$ or $(\tilde{z}_i, \tilde{v}_j)$ (see Fig. 3). Because the latter has a higher cost C, one will naturally cut $(\tilde{v}_i, \tilde{z}_i)$, incurring a cost p_i. Moreover, since that edge does not depend

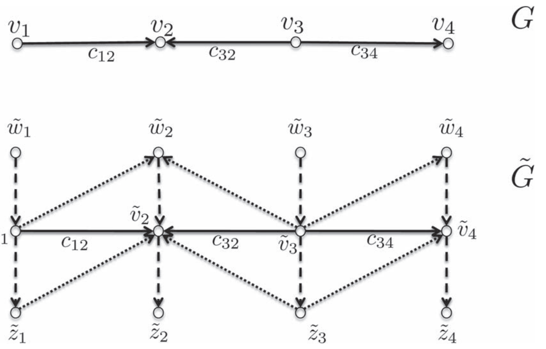


Fig. 3. Representation of the auxiliary graph $\tilde{G}$ associated to the graph G. The dotted diagonal edges all have the same weight $C > \max p_i$. The vertical dashed edges linking $\tilde{w}_i$ to $\tilde{v}_i$ and $\tilde{v}_i$ to $\tilde{z}_i$ have weight p_i.

on j, one just needs to cut it (and pay the associated cost) once, independently of the number of other edges $(\tilde{v}_i, \tilde{v}_k)$ that will be cut. A similar reasoning applies to the path $(\tilde{v}_i, \tilde{w}_j)$ or $(\tilde{w}_j, \tilde{v}_j)$. Therefore, the cost of a minimum cut on $\tilde{G}$ will consists of the sum of all c_{ij} for all edges $(\tilde{v}_i, \tilde{v}_j)$ in the cut, and of the sum of all p_i for nodes incident to one or several edges $(\tilde{v}_i, \tilde{v}_j)$ or $(\tilde{v}_j, \tilde{v}_i)$ in the cut, i.e., to the cost of the equivalent cut on the initial graph G, taking the node costs into account.

B. Equivalence With Min Cut on the Auxiliary Graph

We now show formally that solving the standard `Min Cut` problem on this weighted graph provides a solution to Problem 1 on the initial graph, and that a solution is obtained by directly translating the partition of the $\tilde{v}_i$ into the equivalent partition of the v_i.

Theorem 3: Consider a graph $G(V, E)$ with a set of weights $c_{ij} \geq 0$ for each edge $(v_i, v_j) \in E$, and $p_i \geq 0$ for each node $v_i \in V$, a source node v_s and a sink node v_t. Let $\tilde{G}(\tilde{V}, \tilde{E})$ be the modified graph obtained from G by the procedure described above, and the partition $\tilde{V} = \{\tilde{S}_s, \tilde{S}_t\}$ be an optimal solution of the standard `Min Cut` problem for $\tilde{G}$. Then the partition $\{S_s, S_t\}$ of V, obtained by letting $v_i \in S_s$ if and only if $\tilde{v}_i \in \tilde{S}_s$, is an optimal solution to Problem 1 on G.

Proof: Let us call respectively c^* and $\tilde{c}^*$ the optimal cost of Problem 1 on the graph G and `Min Cut` problem on the graph $\tilde{G}$. In the sequel, we always assume that the source and sink nodes belong to the appropriate set of the partition.

We first prove that $\tilde{c}^* \leq c^*$, by showing that for any cut in G with cost c (i.e., the sum of the costs of the edges **and** the nodes in the cut is c), one can build a cut in $\tilde{G}$ whose cost is equal to c in the following way: For any $1 \leq i \leq n+1$,

1) If $v_i \in S_s$, and all the out-neighbors of v_i are in S_s, put $\tilde{v}_i$, $\tilde{w}_i$ and $\tilde{z}_i$ in $\tilde{S}_s$.
2) if $v_i \in S_t$, and all the in-neighbors of v_i are in S_t, put $\tilde{v}_i$, $\tilde{w}_i$ and $\tilde{z}_i$ in $\tilde{S}_t$.
3) if $v_i \in S_s$, and at least one out-neighbor of v_i is in S_t, put $\tilde{v}_i$, $\tilde{w}_i$ in $\tilde{S}_s$ and $\tilde{z}_i$ in $\tilde{S}_t$.
4) if $v_i \in S_t$, and at least one in-neighbor of v_i is in S_s, put $\tilde{v}_i$, $\tilde{z}_i$ in $\tilde{S}_t$ and $\tilde{w}_i$ in $\tilde{S}_s$.

One can verify that no edge with cost C is in the cut, and that an edge $(\tilde{v}_i, \tilde{v}_j)$ is in the cut if and only if the corresponding edge (v_i, v_j) (which has the same weight) is in the initial cut. Moreover, for every node i, the edge $(\tilde{w}_i, \tilde{v}_i)$, of weight p_i, will be in the cut if and only if at least one edge arriving at v_i was in the initial cut. Similarly, the edge $(\tilde{v}_i, \tilde{z}_i)$ will be in the cut if and only if at least one edge leaving v_i is in the initial cut. So, there will be a contribution p_i to the total cost if at least an edge arriving at v_i is in the cut or at least one edge leaving v_i is in the cut (note that the two situations cannot happen simultaneously). As a conclusion, the cost of the cut $\{S_s, S_t\}$ in G (counting the weights of the nodes) is equal to the cost of the cut $\{\tilde{S}_s, \tilde{S}_t\}$ in $\tilde{G}$.

Consider now an arbitrary cut in $\tilde{G}$, and the corresponding cut in G obtained by putting v_i in S_s if and only if $\tilde{v}_i \in \tilde{S}_s$, as explained in the statement of this theorem. We show that the cut of G obtained has a cost (taking the vertex costs p_i into account) smaller than or equal to the cost of the initial cut. This will imply that $\tilde{c}^* \geq c^*$.

The cost of this new cut $\{S_s, S_t\}$ consists indeed of all the c_{ij} of edges (v_i, v_j) in the cut, and all the p_i of the nodes at which arrives, or from which leaves an edge in the cut.

Consider first an edge (v_i, v_j) in the cut, i.e., $v_i \in S_s, v_j \in S_t$. By construction, this implies that $\tilde{v}_i \in \tilde{S}_s$ and $\tilde{v}_j \in \tilde{S}_t$ so that the edge $(\tilde{v}_i, \tilde{v}_j)$ was also in the cut in $\tilde{G}$, incurring a same cost c_{ij}.

Consider now a node v_i from which leaves at least one edge in the cut, incurring thus a cost p_i. (A symmetric reasoning applies if an edge in the cut arrives at v_i, and no node has edges in the cut both leaving from and arriving at it.) Call v_j the node at which arrives that edge. We have thus $v_i \in S_s$ and $v_j \in S_t$, and therefore $\tilde{v}_i \in \tilde{S}_s$, $\tilde{v}_j \in \tilde{S}_t$ in $\tilde{G}$. This implies that one edge of the path consisting of $(\tilde{v}_i, \tilde{z}_i)$ and $(\tilde{z}_i, \tilde{v}_j)$ is in the cut. These edges have respective costs p_i and $C > p_i$, so that a cost at least p_i will be incurred by the cut in $\tilde{G}$. Note moreover that none of these edges will appear when considering other nodes and be counted more than once.

We have thus shown that to each cost in the cut $\{S_s, S_t\}$ for Problem 1 corresponds a larger or equal cost in $\{\tilde{S}_s, \tilde{S}_t\}$ for the `Min Cut` problem, and thus that the former has a smaller cost.

Therefore, if one takes any cut of optimal cost $\tilde{c}^*$ for the `Min Cut` problem on $\tilde{G}$, and applies the procedure described in the theorem, one obtains a cut of G with a smaller or equal cost for Problem 1. Since we have proved that the optimal cost of the latter problem is at least $\tilde{c}^*$, this implies that $\tilde{c}^* = c^*$ and that the cost obtained is optimal for Problem 1 on G. ■

There exist many efficient polynomial time algorithms solving the `Min Cut` problem exactly when the weights are nonnegative (e.g., [33], [34]). Theorem 3 implies that the same algorithms can be used to solve efficiently Problem 1, and therefore problem (9), and problem (8) in the fully measured case. Moreover, observe that the size of this new graph $\tilde{G}$ is proportional to that of G, as it has $3n$ nodes and $3|E| + 2n$ edges. The order of the polynomial measuring the efficiency of the algorithms remains therefore unchanged. In particular, if the standard `Min Cut` problem on the new graph $\tilde{G}$ is solved using the algorithm in [33] whose complexity is $O(n|E| + n^2 \log(n))$, our algorithm has the same complexity.

It is well known that `Min Cut` problems are particular cases of submodular function optimization, and this type of optimization problems are solvable by polynomial-time algorithms [35].

Since we show that our problem can be recast as a `Min Cut` problem, it enjoys the submodularity property. Hence, it could be solved in polynomial time by classical submodular function optimization routines. However, our reduction to a `Min Cut` formulation allows one to apply better algorithms tailored for the particular structure of `Min Cut` problems.

Finally, consider a slight generalization of Problem 1 in which each node contains two different weights (one for cutting outgoing edges and the other for cutting incoming edges). Then with a corresponding modification in the auxiliary graph construction procedure in Section V-A (in the fourth bullet), the proposed method can still solve the generalization in polynomial time.

VI. The Original Security Index Problem Targeting Edge and Node

The relationship between the original security index problem in (5), the problem in (8) and its binary restriction in (9) is summarized as follows: In the case where $H(k,:)$ in (5) corresponds to the row of P_1DA^T or $-P_2DA^T$, (5) can be restated as (8) with an appropriate choice of $\bar{e}$. Consequently, solving (9) either exactly solves (5) or approximately solves (5) with an error bound provided by (12), depending on whether the full measurement assumption or similar ones in Remark 4 are satisfied or not.

Next, consider the case where $H(k,:)$ corresponds to a row of P_3ADA^T. The constraint $H(k,:)\Delta\theta = 1$ means that the power injection at the target node, denoted v_s, is nonzero. This implies that at least one edge incident to v_s should have nonzero edge flow. Let e_i with $i = 1, 2, \ldots$ denote the column indices of A of the incident edges of v_s. For any given k, consider the following instances (parameterized by e_i)

$$\begin{aligned} J^i_{(22)} \triangleq \min_{\Delta\theta\in\mathbb{R}^{n+1}} \quad & \mathrm{card}\,(H\Delta\theta) \\ \text{subject to} \quad & H(k,:)\Delta\theta \neq 0 \\ & A(:,e_i)^T\Delta\theta \neq 0. \end{aligned} \tag{22}$$

The minimum of $J^i_{(22)}$, over all e_i, is the optimal objective value of (5). In addition, consider a relaxation of (22), obtained by keeping only the constraint $A(:,e_i)^T\Delta\theta \neq 0$:

$$\begin{aligned} J^i_{(23)} \triangleq \min_{\Delta\theta\in\mathbb{R}^{n+1}} \quad & \mathrm{card}(H\Delta\theta) \\ \text{subject to} \quad & A(:,e_i)^T\Delta\theta \neq 0 \end{aligned} \tag{23}$$

and its binary restriction

$$\begin{aligned} J^i_{(24)} \triangleq \min_{\Delta\theta\in\{0,1\}^{n+1}} \quad & \mathrm{card}(H\Delta\theta) \\ \text{subject to} \quad & A(:,e_i)^T\Delta\theta \neq 0. \end{aligned} \tag{24}$$

(23) is an instance of (8), and the fact that (23) has one fewer constraint than (22) implies that

$$J^i_{(23)} \le J^i_{(22)}, \quad \forall i. \tag{25}$$

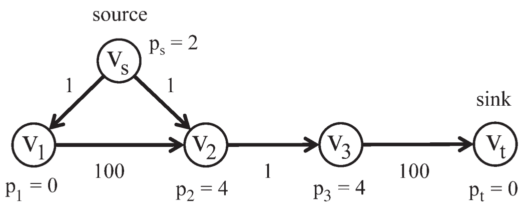


Fig. 4. An instance of Problem 1. v_s and v_t are the source and sink nodes, respectively. The numbers next to the edges are the edge weights, and the node weights are labeled, for example, as $p_2 = 4$ for node v_2.

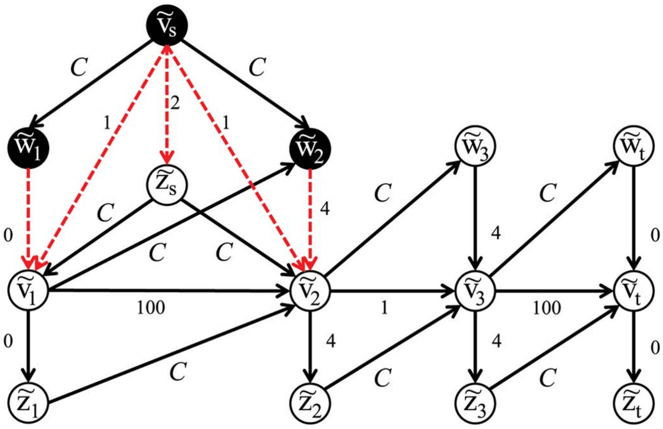


Fig. 5. Solving the standard `Min Cut` problem in the auxiliary graph corresponding to the instance in Fig. 4 (the irrelevant node w_s is not shown). C is a large scalar constant defined in the auxiliary graph construction procedure in Section V-A. The black nodes form the optimal source set (in the auxiliary graph), and the dotted red edges are cut. The optimal objective value is 8.

On the other hand, (24) is an instance of (9), and

$$J^i_{(24)} \ge J^i_{(22)}, \quad \forall i \tag{26}$$

because if $\Delta\theta \in \{0,1\}^{n+1}$ is feasible to (24), then it is also feasible to (22) since the injection at v_s is nonzero with $\Delta\theta \in \{0,1\}^{n+1}$. Notice, however, that a feasible solution of (23) need not be feasible to (22). Let $i^\star$ be defined such that $J^{i^\star}_{(22)} = \min_i J^i_{(22)}$. The full measurement assumption or similar ones in Remark 4 implies that $J^{i^\star}_{(24)} = J^{i^\star}_{(23)}$, since $J^i_{(24)} = J^i_{(23)}$ holds for all i. This, together with (25) and (26), suggests that

$$J^{i^\star}_{(22)} \le J^{i^\star}_{(24)} = J^{i^\star}_{(23)} \le J^{i^\star}_{(22)}.$$

This implies that the equalities above hold throughout, and solving (9) (by solving (24)) indeed solves the original security index problem in (5) (by solving (22)). On the other hand, if the full measurement assumption does not hold, then

$$J^{i^\star}_{(22)} \le J^{i^\star}_{(24)} \le J^{i^\star}_{(23)} + \Delta J \le J^{i^\star}_{(22)} + \Delta J$$

where the error upper bound ΔJ can be obtained from (12). In conclusion, all exact or approximate results pertaining to the case between (8) and (9) apply to the case between (5) and (9). As discussed in Remark 5, the above error bound might be conservative. The approximation quality in practice will be demonstrated in Section VII containing some numerical examples on benchmark power networks.

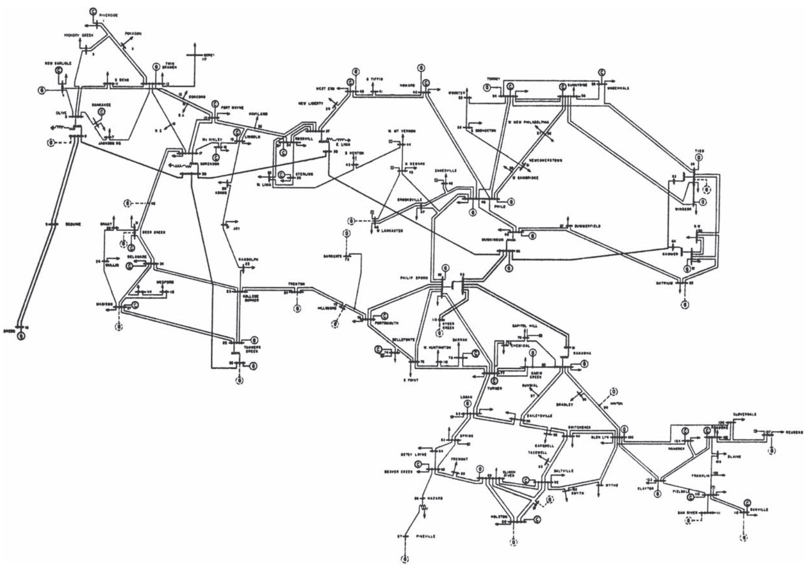


Fig. 6. IEEE 118-bus benchmark system [36].

VII. Numerical Examples

A. Simple Illustrative Example of Problem 1

To illustrate the proposed method, consider an instance of Problem 1 depicted in Fig. 4. By inspection, the optimal solution corresponds to the optimal source set $S_s = \{v_s\}$, with objective value being 8. Constructing the auxiliary graph as described in Section V and solving the corresponding standard `Min Cut` problem leads to the node partitioning in Fig. 5. In the auxiliary graph the optimal source set is $\{v_s, w_1, w_2\}$, with the objective value being 8. According to the rule in Theorem 3, $\{v_s\}$ is the source set returned by the proposed procedure in this paper. It correctly solves Problem 1.

B. The Security Index Problem on Benchmark Systems

To demonstrate the effectiveness and accuracy of the proposed solution, the security index problem for two benchmark systems is considered (IEEE 118-bus [36] and Polish 2383-bus [37]). See Fig. 6 for an illustration of the 118-bus system.

First, the full measurement case is considered. The security index problem in (5) is solved for each measurement, using the proposed solution and the methods from [12], [18]. The proposed method is guaranteed to provide the exact optimal solutions, as explained earlier in the paper. Both for the 118-bus and 2383-bus cases, the methods from [12], [18] are experimentally found to provide the exact solutions (though this is not guaranteed theoretically). The computation times for the three methods are listed in Table I, indicating that the methods have similar efficiency. The guarantee of optimality provided by our approach is obtained at no additional computational cost. The computation was performed on a PC with 2.4 GHz CPU and 2 GB of RAM. The minimum cut problems are solved using the MATLAB Boost Graph Library [38], [39].

Next, (5) is considered when the full measurement assumption is removed. That is, the matrices P_1, P_2, and P_3 in (1) need not be identities. In this test, the 118-bus system is considered. In the measurement system about 50% of power injections and power flows are measured. The measurements are chosen randomly (uniform over all possible measurements), and the measurement system is verified to be observable (i.e., the corresponding $H_{2:}$ has full column rank $(= n)$). Since (5) is NP-hard in general, no efficient solution algorithm has been known. Enumerative algorithms include, for instance, enumeration on the support of $H\Delta\theta$, finding the maximum feasible subsystem for an appropriately constructed system of infeasible inequalities [40], and the big M method to be described. The authors' implementations of the first two methods turn out to be too inefficient for the applications concerned. Therefore, the big M method is used, which sets up and solves the following optimization problem:

TABLE I
Computation Times for all Security Indices in the Full Measurement Case for the IEEE 118-Bus and Polish 2383-Bus Benchmarks

	our method	[12]	[18]
IEEE 118-bus	0.18s	0.23s	0.24s
2383-bus	29s	29s	33s

$$\begin{aligned} \underset{\Delta\theta, y}{\text{minimize}} \quad & \sum_j y(j) \\ \text{subject to} \quad & H\Delta\theta \le My \\ & -H\Delta\theta \le My \\ & H(k,:)\Delta\theta = 1 \\ & y(j) \in \{0,1\} \quad \forall j. \end{aligned} \tag{27}$$

In (27), M is a user-defined constant. If $M \ge \|H\Delta\theta^\star\|_\infty$ for at least one optimal solution $\Delta\theta^\star$ of (5), then (27) provides the exact solution to (5). Otherwise, solving (27) yields a suboptimal solution, optimal among all solutions $\Delta\theta$ such that $\|H\Delta\theta\|_\infty \le M$. In principle a sufficiently large M can be found to ensure that the big M method indeed provides the optimal solution to (5) [41]. However, this choice of M is typically too large to be practical. In the numerical example

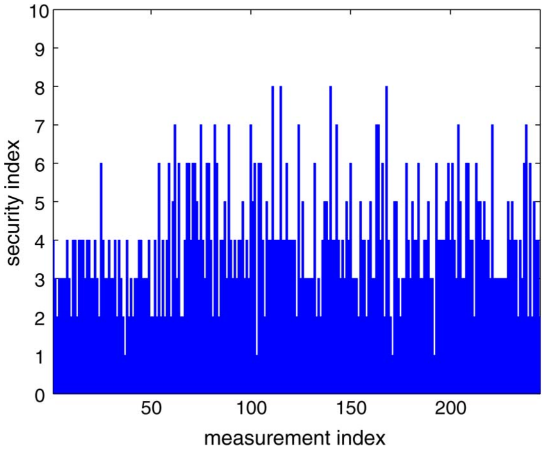


Fig. 7. Security indices for the partially measured 118-bus system. Security indices are computed using the big M method with $M = 10^4$.

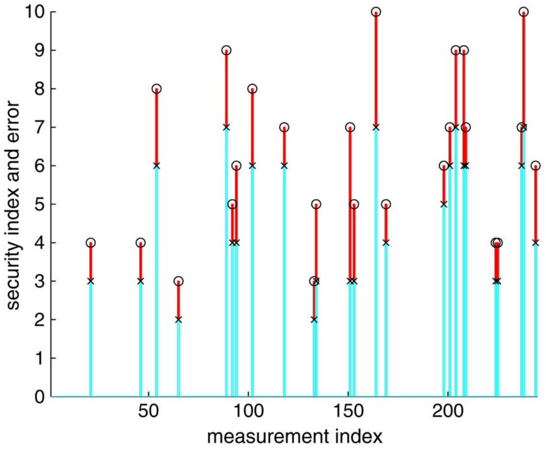


Fig. 8. Security index estimates for the partially measured 118-bus system. Security index estimates are computed using the method in [12]. The figure shows only the inexact security index estimates (in circles) and the corresponding ones by the big M method (in crosses).

in this section, M is simply chosen to be 10^4. (27) can be solved as a mixed integer linear program [32] using solvers such as CPLEX [42]. The solutions by the big M method are treated as references for accuracy for the rest of the case study. Fig. 7 shows the (big M) security indices for all chosen measurements.

Alternatively, as described in Section VI a suboptimal solution to (5) can be obtained by solving (9) exactly using the proposed method in Section V (see Remark 5 for detail) or the ones from [12], [18]. As explained earlier, (9) can be formulated as Problem 1 with $p_i = 1$ if and only if the injection measurement at bus v_i is taken and $c_{ij} = c_{ji} \in \{0, 1, 2\}$ being the total number of line power flow meters on the line connecting buses v_i and v_j. Figs. 8–10, respectively, show the security index test results with the three `Min Cut` based methods (i.e., [12], [18] and the one proposed in this paper). These figures show only the big M security indices (in light blue, the heights of the crosses) and the overestimation (in red, the heights between the crosses and the circles) for the measurements where the `Min Cut` based methods do not agree with big M. The case study indicates that, among the three `Min Cut` based methods, the proposed method provides the most accurate suboptimal solutions to (5). In particular, only in two cases is the security index overestimated by the proposed method. In terms of computation time, the proposed method is most efficient as suggested by Table II. Finally, the lower bounds for the optimal objective values for (5) (or (8)) can be obtained following the computation procedure described in Remark 6. Fig. 11 shows the lower bounds, the exact values of the security indices, as well as the upper bounds for the two cases where they are overestimations. Note that even though without the full measurement assumption the exact security indices cannot be computed efficiently, the bounds obtained by the proposed method provide valuable insight about the security of the network. For instance, the relatively small upper bounds of the security indices necessarily imply the corresponding measurements are vulnerable to unobservable data attack. This is because the true security indices can only be smaller than the already small upper bounds provided by the proposed computation procedure.

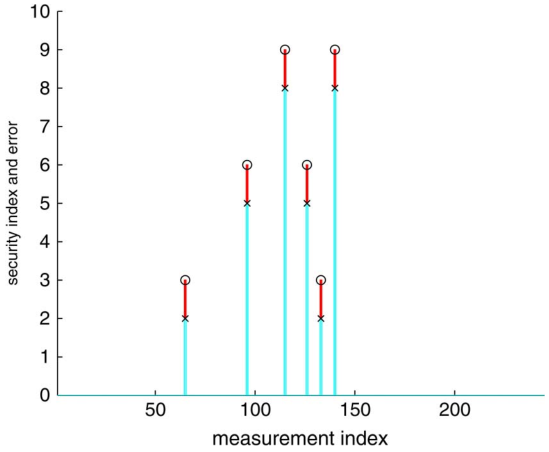


Fig. 9. Security index estimates for the partially measured 118-bus system. Security index estimates are computed using the method in [18]. The figure shows only the inexact security index estimates (in circles) and the corresponding ones by the big M method (in crosses).

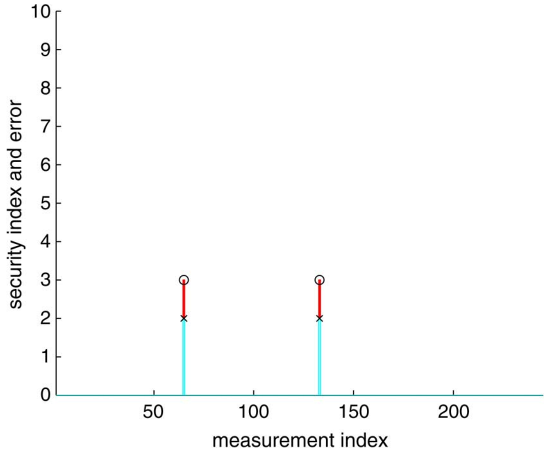


Fig. 10. Security index estimates for the partially measured 118-bus system. Security index estimates are computed using the method proposed in this paper. The figure shows only the inexact security index estimates (in circles) and the corresponding ones by the big M method (in crosses).

TABLE II
COMPUTATION TIMES FOR ALL SECURITY INDICES IN THE PARTIAL MEASUREMENT CASE FOR THE IEEE 118-BUS BENCHMARK

	our method (s)	[12]	[18]	big M
IEEE 118-bus	0.17s	4.4s	0.21s	118s

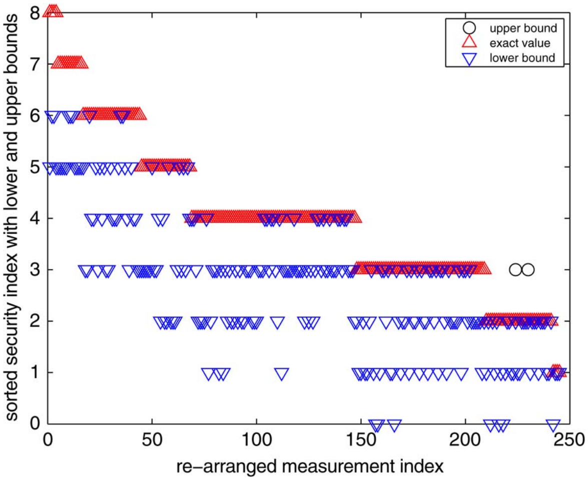


Fig. 11. The lower bounds and the upper bounds of the security indices in the 118-bus system with partial measurements. In this figure, the measurement indices are re-arranged so that the security indices are non-increasing. While the proposed procedure provides very accurate upper bounds (there are only two cases with overestimations), the quality of the lower bounds obtained using the method described in Remark 6 is not as good.

VIII. CONCLUSION

It has been assumed that the security index problem, formulated as a cardinality minimization problem, cannot be solved efficiently. This paper formally confirms this conjecture by showing that the security index problem is indeed NP-hard. Nevertheless, the security index problem can be shown to be reducible to a `Min Cut with node costs` problem (Problem 1) under the full measurement assumption. In this paper, we show that this problem is equivalent to a standard `Min Cut` problem on an auxiliary graph of proportional size, and can therefore be solved exactly and efficiently using standard techniques for the `Min Cut` problem. Under the full measurement assumption, this allows computing the minimal number of measurements with which one must tamper in order to feed incorrect information on the SCADA system without being detected by a BDD method. The knowledge of this number can help strategically assigning protection resources (e.g., [9], [43]). Our method also solves a mathematically equivalent problem of robustness of the observability properties of the system with respect to the failure of some measurements, assuming again full measurement. It remains to be determined if the solution could be efficiently approximated in the general (not fully measured) case. Indeed, even though our approach already provides an approximate solution to such general problems we do not know if this approximation comes with any guarantee of accuracy.

Another interesting issue is the design question: in view of the exact solution of the security index problem presented in this paper, could one build efficient design methods in order to optimize the security index under some natural constraints?

REFERENCES

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 major grid blackouts in North America and Europe, recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.

[2] S. Amin, A. Cárdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Hybrid Systems: Computation and Control*, *Lecture Notes in Computer Science*. Berlin/Heidelberg: Springer, April 2009, pp. 31–45.

[3] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. 49th IEEE Conf. Decision and Control (CDC)*, Dec. 2010.

[4] Y. Mo and B. Sinopoli, "Secure control against replay attack," in *Proc. 47th Annu. Allerton Conf. Communication, Control, Computing*, Oct. 2009.

[5] R. Smith, "A decoupled feedback structure for covertly appropriating networked control systems," in *Proc. 18th IFAC World Congr.*, Milano, Italy, Aug./Sep. 2011.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proc. 50th IEEE Conf. Decision and Control and European Control Conf.*, Orlando, FL, Dec. 2011.

[7] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Computer and Communication Security*, New York, 2009, pp. 21–32.

[8] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *1st Workshop on Secure Control Systems, CPSWEEK*, 2010.

[9] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *IEEE SmartGridComm*, 2010.

[10] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on dc state estimation," in *1st Workshop on Secure Control Systems, CPSWEEK*, 2010.

[11] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, pp. 645–658, 2011.

[12] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. IEEE Conf. Decision and Control*, Dec. 2011.

[13] A. Giani, E. Bitar, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: Characterizations and countermeasures," in *IEEE SmartGridComm*, 2011.

[14] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, pp. 326–333, Jun. 2011.

[15] A. Abur and A. Expósito, *Power System State Estimation*. New York: Marcel Dekker, 2004.

[16] A. Monticelli, *State Estimation in Electric Power Systems A Generalized Approach*. Norwell, MA: Kluwer, 1999.

[17] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the exact solution to a smart grid cyber-security analysis problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, Jun. 2013.

[18] K. C. Sou, H. Sandberg, and K. H. Johansson, "Computing critical k-tuples in power networks," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1511–1520, 2012.

[19] S. Mallat and Z. Zhang, "Matching pursuit with time-frequency dictionaries," *IEEE Trans. Signal Process.*, vol. 41, pp. 3397–3415, 1993.

[20] S. S. Chen, D. L. Donoho, and M. A. Saunders, "Atomic decomposition by basis pursuit," *SIAM J. Scientif. Comput.*, vol. 20, 1998.

[21] B. Lesieutre, S. Roy, V. Donde, and A. Pinar, "Power system extreme event screening using graph partitioning," in *Proc. 38th North American Power Symp. (NAPS 2006)*, Sep. 2006, pp. 503–510.

[22] A. Pinar, Y. Fogel, and B. C. Lesieutre, "The Inhibiting Bisection Problem," Lawrence Berkeley National Laboratory, Tech. Rep. LBNL-62142, 2006.

[23] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. 94, no. 2, pp. 329–337, Mar. 1975.

[24] A. Teixeira, H. Sandberg, G. Dan, and K. Johansson, "Optimal power flow: Closing the loop over corrupted data," in *Proc. American Control Conf. (ACC)*, 2012, pp. 3534–3540.

[25] J. Burgschweiger, B. Gnädig, and M. Steinbach, "Optimization models for operative planning in drinking water networks," *Optimiz. and Eng.*, vol. 10, no. 1, pp. 43–73, 2009.

[26] A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, "Cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator," in *IFAC World Congr.*, Milan, Italy, 2011.

[27] E. Candès and T. Tao, "Decoding by linear programming," *IEEE Trans. Inform. Theory*, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[28] D. L. Donoho and M. Elad (2003). Optimally sparse representation in general (nonorthogonal) dictionaries via l1 minimization. *Proc. Nat. Acad. Sci.*, vol. 100, no. 5, pp. 2197–2202. [Online]. Available: http://www.pnas.org/content/100/5/2197.abstract

[29] A. Tillmann and M. Pfetsch, The Computational Complexity of the Restricted Isometry Property, the Nullspace Property, Related Concepts in Compressed Sensing, 2012. [Online]. Available: http://arxiv.org/abs/1205.2081

[30] S. McCormick, "A Combinatorial Approach to Some Sparse Matrix Problems," Ph.D. dissertation, Stanford University, Stanford, CA, 1983.

[31] P. Gopalan, P. Kolaitis, E. Maneva, and C. Papadimitriou, "The connectivity of boolean satisfiability: Computational and structural dichotomies," *Automata, Lang. and Programm.*, pp. 346–357, 2006.

[32] J. Tsitsiklis and D. Bertsimas, *Introduction to Linear Optimization*. New York: Athena Scientific, 1997.

[33] M. Stoer and F. Wagner, "A simple min-cut algorithm," *J. ACM*, vol. 44, pp. 585–591, July 1997.

[34] L. Ford and D. Fulkerson, "Maximal flow through a network," *Canadian J. Mathemat.*, vol. 8, pp. 399–404, 1956.

[35] G. Nemhauser, L. Wolsey, and M. Fisher, "An analysis of approximations for maximizing submodular set functions I," *Mathemat. Programm.*, vol. 14, no. 1, pp. 265–294, 1978.

[36] R. Christie, Power System Test Case Archive, 1993. [Online]. Available: http://www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm

[37] R. Zimmerman, C. Murillo-Sánchez, and R. 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.

[38] D. Gleich, Contents Matlab BGL v4.0, 2006. [Online]. Available: http://www.stanford.edu/~dgleich/programs/matlab_bgl/

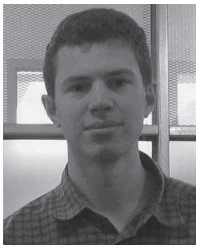
[39] , *The Boost Graph Library: User Guide and Reference Manual*. Boston, MA: Addison-Wesley Longman, 2002.

[40] S. Jokar and M. E. Pfetsch (2008, Oct.). Exact and approximate sparse solutions of underdetermined linear equations. *SIAM J. Sci. Comput.* [Online]. *31(1)*, pp. 23–44. Available: http://dx.doi.org/10.1137/070686676

[41] A. Schrijver, *Theory of linear and integer programming*. New York: Wiley, 1986.

[42] CPLEX. [Online]. Available: http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/

[43] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Select. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.



Julien M. Hendrickx received the engineering degree in applied mathematics and the Ph.D. degree in mathematical engineering from the Université Catholique de Louvain, Louvain-la-Neuve, Belgium, in 2004 and 2008, respectively.

He was a Visiting Researcher at the University of Illinois at Urbana Champaign in 2003–2004, at the National ICT Australia in 2005 and 2006, and at the Massachusetts Institute of Technology in 2006 and 2008. He was a postdoctoral fellow at the Laboratory for Information and Decision Systems of the Massachusetts Institute of Technology, Cambridge, MA, in 2009 and 2010, holding postdoctoral fellowships of the Fund for Scientific Research (F.R.S.-FNRS) and of the Belgian American Education Foundation. Since September 2010, he has been an Assistant Professor (chargé de cours) at the Université Catholique de Louvain, in the Ecole Polytechnique de Louvain.

Dr. Hendrickx is the recipient of the 2008 EECI award for the best Ph.D. thesis in Europe in the field of Embedded and Networked Control, and of the Alcatel-Lucent-Bell 2009 award for a Ph.D. thesis on original new concepts or application in the domain of information or communication technologies.

Karl Henrik Johansson (F'13) received the M.Sc. and Ph.D. degrees in electrical engineering from Lund University, Lund, Sweden.

He is Director of the KTH ACCESS Linnaeus Centre and Professor at the School of Electrical Engineering, Royal Institute of Technology, Stockholm, Sweden. He is a Wallenberg Scholar and has held a six-year Senior Researcher Position with the Swedish Research Council. He is Director of the Stockholm Strategic Research Area ICT The Next Generation. He has held visiting positions at the University of California Berkeley (1998–2000) and California Institute of Technology (2006–2007). His research interests are in networked control systems, hybrid and embedded system, and applications in transportation, energy, and automation systems.

Dr. Johansson has been a member of the IEEE Control Systems Society Board of Governors and the Chair of the IFAC Technical Committee on Networked Systems. He has been on the Editorial Boards of several journals, including *Automatica*, IEEE TRANSACTIONS ON AUTOMATIC CONTROL, and IET Control Theory and Applications. He is currently on the Editorial Board of IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS and the European Journal of Control. He has been Guest Editor for special issues, including the one on "Wireless Sensor and Actuator Networks" of IEEE TRANSACTIONS ON AUTOMATIC CONTROL 2011. He was the General Chair of the ACM/IEEE Cyber-Physical Systems Week 2010 in Stockholm and IPC Chair of many conferences. He has served on the Executive Committees of several European research projects in the area of networked embedded systems. In 2009, he received the Best Paper Award of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems. In 2009, he was also awarded Wallenberg Scholar, as one of the first ten scholars from all sciences, by the Knut and Alice Wallenberg Foundation. He was awarded an Individual Grant for the Advancement of Research Leaders from the Swedish Foundation for Strategic Research in 2005. He received the triennial Young Author Prize from IFAC in 1996 and the Peccei Award from the International Institute of System Analysis, Austria, in 1993. He received Young Researcher Awards from Scania in 1996 and from Ericsson in 1998 and 1999.

Raphaël M. Jungers received the engineering degree in applied mathematics from the Ecole Centrale Paris, Paris, France, in 2004 and the Université Catholique de Louvain, Louvain-la-Neuve, Belgium, in 2005, a minor degree in electrical engineering from the Université Catholique de Louvain, in 2005, and the Ph.D. degree in mathematical engineering from the Université Catholique de Louvain in 2008.

He is a FNRS Research Associate and Professor at the Université Catholique de Louvain. His main interests lie in the fields of computer science, graph theory, optimization and control. He has held various invited researcher positions at the Department of Computer Science, Université Libre de Bruxelles (2008–2009), at the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology (2009–2010), and at the University of L'Aquila (2011 and 2013).

Dr. Jungers is a FNRS Fellow and a BAEF Fellow. He was the recipient of the IBM Belgium 2009 Award and a finalist of the ERCIM Cor Baayen Award 2011.

Henrik Sandberg received the M.Sc. degree in engineering physics and the Ph.D. degree in automatic control from Lund University, Lund, Sweden, in 1999 and 2004, respectively.

He is an Associate Professor with the Automatic Control Laboratory, KTH Royal Institute of Technology, Stockholm, Sweden. From 2005 to 2007, he was a Post-Doctoral Scholar with the California Institute of Technology, Pasadena. In 2013, he was a visiting scholar at the Laboratory for Information and Decision Systems (LIDS) at MIT, Cambridge, MA. He has also held visiting appointments with the Australian National University and the University of Melbourne, Australia. His current research interests include secure networked control, power systems, model reduction, and fundamental limitations in control.

Dr. Sandberg was a recipient of the Best Student Paper Award from the IEEE Conference on Decision and Control in 2004 and an Ingvar Carlsson Award from the Swedish Foundation for Strategic Research in 2007. He is currently an Associate Editor of the *IFAC Journal Automatica*.

Kin Cheong Sou received the Ph.D. degree in electrical engineering and computer science at Massachusetts Institute of Technology, Cambridge, in 2008.

From 2008 to 2010, he was a Postdoctoral Researcher at Lund University, Lund, Sweden. From 2010 to 2013, he was a postdoctoral researcher at KTH Royal Institute of Technology, Stockholm, Sweden. Since 2013, he has been an Assistant Professor with the Department of Mathematical Sciences, Chalmers University of Technology, Gothenburg, Sweden. His research interests include power system cyber-security analysis, environment-aware building and community, convex/non-convex optimization and model reduction for dynamical systems.