Network-Aware Mitigation of Data Integrity Attacks on Power System State Estimation

Ognjen Vuković, Kin Cheong Sou, György Dán, Henrik Sandberg

***Abstract*—Critical power system applications like contingency analysis and optimal power flow calculation rely on the power system state estimator. Hence the security of the state estimator is essential for the proper operation of the power system. In the future more applications are expected to rely on it, so that its importance will increase. Based on realistic models of the communication infrastructure used to deliver measurement data from the substations to the state estimator, in this paper we investigate the vulnerability of the power system state estimator to attacks performed against the communication infrastructure. We define security metrics that quantify the importance of individual substations and the cost of attacking individual measurements. We propose approximations of these metrics, that are based on the communication network topology only, and we compare them to the exact metrics. We provide efficient algorithms to calculate the security metrics. We use the metrics to show how various network layer and application layer mitigation strategies, like single and multi-path routing and data authentication, can be used to decrease the vulnerability of the state estimator. We illustrate the efficiency of the algorithms on the IEEE 118 and 300 bus benchmark power systems.**

***Index Terms*—SCADA communication, state estimation, cyber-physical security.**

I. Introduction

SUPERVISORY control and data acquisition (SCADA) systems are used to monitor and to control large-scale power grids. They collect measurement data taken at the substations, multiplex them in remote terminal units (RTUs) located at the substations, and deliver the multiplexed data through the SCADA network to the SCADA master located at the control center. At the control center the measurement data are fed into the power system state estimator (SE). The SE is an on-line application that relies on redundant measurements and a physical model of the power system to periodically calculate an accurate estimate of the power system's state [1], [2]. It includes a Bad Data Detection (BDD) system to detect faulty measurement data.

The state estimate provided by the SE is the basis for a set of application specific software, usually called energy management systems (EMS). Modern EMS provide information support in the control center for a variety of applications related to power network monitoring and control. One example is the optimal routing of power flows in the network, called optimal power flow (OPF), which is to ensure cost-efficient operation. Another example is contingency analysis, which is an essential application to maintain the power system in a secure and stable state despite potential failures, e.g., by using the $n-1$ security criterion. EMS are also expected to be integral components of future SmartGrid solutions, hence the secure and proper operation of the SE is of critical importance [3], [4].

SCADA systems and communication protocols have traditionally been designed to be efficient and to be resilient to failures in order to achieve cost-efficient system operation. Security has been provided through isolating the SCADA infrastructure from the public and the corporate infrastructures, and by following the principle of security by obscurity. SCADA infrastructures are, however, increasingly integrated with corporate infrastructures and equipment are often left unattended, which together with a large installed base of legacy equipment and protocols implies that SCADA systems are potentially vulnerable to cyber attacks [4], [5].

An attacker that gains access to the SCADA communication infrastructure could potentially inject crafted packets or could manipulate the measurement data sent from the RTUs to the control center. While the BDD is supposed to detect faulty measurement data, it was shown recently [6] that measurement data can be manipulated such that they do not trigger the BDD system in the SE. We term such corruptions *stealth attacks* on the SE. Recent experiments on a SCADA/EMS testbed [7] indeed verify that large stealth attacks can be performed without triggering alarms. By fooling the SE the attacker could manipulate the power markets [8], or could hide that the power system is in an unsecure state and eventually can cause cascading failures. The existence of such attacks and their potential security implications make it important to understand how such attacks can be mitigated using various mitigation schemes at a relatively low cost, e.g., without introducing authentication in all system components.

In this paper we address this important question by proposing a framework that captures the characteristics of the power system and of the SCADA communication infrastructure. Our contributions are twofold. First, we develop quantitative metrics to assess the importance of substations and communication equipment with respect to the SE. Second, we use these metrics to evaluate the potential of various mitigation measures to decrease the SE's vulnerability to stealth attacks. As mitigation measures we consider both network layer solutions, such as single-path and multi-path routing, and application layer solutions such as data authentication. We use IEEE benchmark systems to provide numerical results based on the framework. The framework can be used by SCADA system designers

Manuscript received 30 September 2011; revised 26 January 2012. The work was partially funded by the EU FP7 Viking project and by the Swedish Foundation for Strategic Research.

The authors are with ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden, (e-mail: {vukovic,sou,gyuri,hsan}@ee.kth.se).

Digital Object Identifier 10.1109/JSAC.2012.120709.

and operators to assess the vulnerability of their systems and to evaluate the efficiency of different mitigation schemes to protect the SCADA state estimator against attacks.

The structure of the paper is as follows. In Section II, we discuss the related work. In Section III we outline power system SE and stealth attacks, and a model of modern SCADA communication infrastructures. In Section IV, we introduce system security metrics and show how they can be efficiently computed even for large power systems. In Section V, we propose an algorithm to mitigate attacks efficiently via various mitigation measures. In Section VI, we use the proposed metrics to evaluate the potential of the mitigation measures to improve security. In Section VII we conclude the paper.

II. Related Work

Since power system state estimation is a core component of SCADA/EMS systems, there is a wealth of literature on state estimation and bad data detection algorithms [1], [2].

It has long been known that certain bad data are not detectable [9], [10]. Still, the first to study state estimation from a security perspective was [6], where it was pointed out that measurements can be corrupted so that they do not trigger the BDD system, even though the measurements are erroneous. The observation is built on a linearized model of state estimation, but experiments on a SCADA/EMS testbed verified the possibility of stealth attacks under nonlinear models [7].

Several works aimed to quantify the difficulty of performing stealth attacks against some measurements [6], [11], [12], [13], [14], [15]. A common assumption among most of these works is that the measurement values are delivered individually from the meters to the control center [6], [11], [12], [13], [15]. This assumption, while it simplifies the problem formulation, ignores the fact that measurement data taken by different meters at a substation are multiplexed before being sent to the control center. Multiplexing was treated in [14], [15], where the authors considered that measurements taken at the same substation are delivered to the control center over the same point-to-point communication link. This communication model still ignores the network topology, and captures only a fraction of the SCADA communication infrastructures in use today. We, instead, consider a realistic communication model where measurement data are multiplexed and may be relayed through other substations.

Related to our work are studies that use the betweenness centrality [16] and the vertex connectivity [17] in the context of network reliability and in the context of security, respectively. In [18] the authors use the betweenness centrality to assess the importance of individual nodes in routing messages. In [19] the authors use the vertex connectivity to assess network resilience against attacks that compromise communication nodes and communication links. We provide a joint treatment of the communication network topology and stealth attacks against the state estimator, and use these graph theoretical metrics as a comparison to our security metrics.

In this paper we propose a model of the communication infrastructure used in modern power transmission systems. The model accounts for the fact that measurement data can be delivered from a substation to the control center through point-to-point links but also via other substations. Hence an attacker that gains access to a substation, can potentially access and modify all data that traverse the substation. The combination of the power flow model with the model of the communication infrastructure allows us to provide a realistic treatment of stealth attacks and mitigation schemes for power system SE. To our knowledge this paper is the first to consider such a cyber-physical model of power system SE security.

III. Background and System Model

In this section, we review steady-state power system modeling and state-estimation techniques, and give an overview of the communication infrastructure used in SCADA systems.

A. SCADA Communication Infrastructure

Electric power transmission systems extend over large geographical areas, typically entire countries. Wide-area networks (WANs) are used to deliver the multiplexed measurement data, often together with voice, video and other data traffic, from the RTUs located at the substations to the control center of the transmission system operator (TSO).

For reliability the WAN communication infrastructure is usually owned by the TSO, but the public switched telephone network (PSTN), cellular, and satellite networks are also used. Historically, the WAN infrastructure consisted of point-to-point communication links between RTUs and the control center (e.g., over the PSTN). However, modern WAN infrastructures are increasingly based on overhead ground wire (also called optical ground wire, OPGW) installations that run between the tops of the high voltage transmission towers or along underground cables. In the latter case, SONET or SDH is used to establish communication links (called virtual circuits) between the substations and the control center, but wide-area Ethernet is expected to become prevalent in the near future. As an effect the data sent from a remote substation to the control center might traverse several substations, where switches, multiplexers or cross connects multiplex the data from different substations onto a single OPGW link.

To detect bit errors, SCADA communication protocols include an error detection code calculated by the RTU, which is sent along with the data. The error detection code can be based on, e.g., cyclic redundancy check (CRC) or a cryptographic hash function, such as SHA-1. These codes do not provide message authentication. The operator can achieve message authentication by installing a secret key at the substation in one of two ways. First, by installing a bump-in-the-wire (BITW) device adjacent to a legacy RTU [20]. Data between the RTU and the BITW device are sent in plain-text, hence a BITW does not protect the data if an attacker can gain physical access to the substation. Nevertheless, it protects the data between the BITW device and the control center. Second, by installing an RTU that supports message authentication. A tamper-proof RTU that supports authentication, though more expensive, ensures data integrity even if the attacker can gain physical access to the substation.

B. Power System State Estimation and Stealth Attacks

Measurements are taken and sent at a low frequency in SCADA systems, and therefore steady-state estimators are used for state estimation. For a complete treatment of this topic, see for example [1], [2].

Consider a power system that has $n+1$ buses. We consider models of the active power flows P_{ij} (between bus i and j), active power injections P_i (at bus i), and bus phase angles δ_i, where $i,j=1,\ldots,n+1$. (A negative P_i indicates a power load at bus i.) The state-estimation problem we consider consists of estimating n phase angles δ_i given M active power flow and injection measurement values z_m ($m \in \{1,...,M\}$). One has to fix one (arbitrary) bus phase angle as reference angle, for example $\delta_0 := 0$, and therefore only n angles have to be estimated, i.e., the vector $\delta = (\delta_1, \delta_2, .., \delta_n)^T$. The active power flow measurements are denoted by $z = (z_1, \ldots, z_M)^T$, and are equal to the actual power flow plus independent random measurement noise e, which we assume has a Gaussian distribution of zero mean, $e = \left(e_1, \ldots, e_M\right)^T \in \mathcal{N}(0,R)$ where $R := \mathbf{E}ee^T$ is the diagonal measurement covariance matrix.

When the phase differences $\delta_i - \delta_j$ between the buses in the power system are all small, then a linear approximation, a so called DC power flow model, is accurate, and we can write

$$z = H\delta + e, \tag{1}$$

where $H \in \mathbb{R}^{M\times n}$ is a constant known Jacobian matrix that depends on the power system topology and the measurements, see [1], [2] for details. The state estimation problem can then be solved as

$$\hat{\delta} := (H^T R^{-1} H)^{-1} H^T R^{-1} z. \tag{2}$$

The phase-angle estimates $\hat{\delta}$ are used to estimate the active power flows by [2]

$$\hat{z} = H\hat{\delta} = H(H^T R^{-1} H)^{-1} H^T R^{-1} z. \tag{3}$$

The BDD system uses such estimates to identify faulty sensors and bad data by comparing the estimate $\hat{z}$ with z: if the elements $\hat{z}_m$ and z_m are very different, an alarm is triggered because the received measurement value z_m is not explained well by the model. For a more complete treatment of BDD we refer to [1], [2].

An attacker that wants to change measurement m (its *value* z_m) might have to change several other measurements m' to avoid a BDD alarm to be triggered. Consider that the attacker wants to change the measurements from z into $z_a := z + a$. The *attack vector* a is the corruption added to the real measurement vector z. As was shown in [6], an attack vector must satisfy

$$a = Hc, \quad \text{for some } c \in \mathbb{R}^n, \tag{4}$$

in order for it not to increase the risk of an alarm. The corresponding a is termed a *stealth attack* henceforth.

In the recent study [7] it was verified that, despite the simplifying assumptions, stealth attacks can be made large in real (nonlinear) SE software: in the example considered in [7], a power flow measurement was corrupted by 150 MW (57% of the nominal power flow) without triggering alarms.

C. Power System Communication Model

The $n+1$ buses of the power system are spread over a set of substations $\mathcal{S}$, $|\mathcal{S}| = S$. We denote the substation at which measurement m is taken by $S(m) \in \mathcal{S}$, and we denote the substation at which the control center is located by $s_{cc} \in \mathcal{S}$. We model the communication network by an undirected graph $\mathcal{G} = (\mathcal{S}, E)$; an edge between two substations corresponds to a communication link between the two substations (e.g., a point-to-point link from a substation to the control-center, or an OPGW link between two substations connected by a transmission line). The graph $\mathcal{G}$ is connected but is typically sparse. Every substation $s \in \mathcal{S}$ can have multiple established routes to the control center s_{cc} through $\mathcal{G}$. We represent route i of substation s by the set of substations $r_s^i \subseteq \mathcal{S}$ that it traverses, including substation s and the control center s_{cc}. The order in which the substations appear in the route is not relevant to the considered problem. For substation s, we denote the set of established routes by $\mathcal{R}_s = \{r_s^1, \ldots, r_s^{R(s)}\}$. If $R(s) = 1$ then all measurement data from substation s are sent over a single route to the control center. If $R(s) > 1$ then unless the data sent over all routes get corrupted in an appropriate way, the control center can detect the data corruption. This can be achieved in a number of ways, e.g., by repeating the measurement data on all the routes or by appending a checksum calculated using an error detection code or a cryptographic hash function, and splitting the data among all the routes. We denote the collection of all $\mathcal{R}_s$ by $\mathcal{R}$.

We consider two forms of end-to-end authentication: non tamper-proof and tamper-proof. We denote the set of substations with *non tamper-proof* authentication (e.g., substations with a BITW device to *authenticate* the data sent to the control center, or an RTU with a non tamper-proof data authentication module) by $\mathcal{E}^N \subseteq \mathcal{S}$. For a route r_s^i we denote by $\sigma_{\mathcal{E}^N}(r_s^i)$ the set of substations in which the data are *susceptible* to attack despite non tamper-proof authentication. Data authenticated in a non tamper-proof way is only *susceptible* to attack at the substation where it originates from, if physical access is possible. Therefore, for every route $r_s^i \in \mathcal{R}_s$ it holds that $\sigma_{\mathcal{E}^N}(r_s^i) = \{s\}$ if $s \in \mathcal{E}^N$ and $\sigma_{\mathcal{E}^N}(r_s^i) = r_s^i$ otherwise.

Similarly, we denote the set of substations with *tamper-proof* authentication (e.g., substations with a tamper-proof RTU that *authenticates* the data sent to the control center) by $\mathcal{E}^P \subseteq \mathcal{S}$. Data authenticated in a tamper-proof way is not susceptible to attack at any substation on the route, hence $\sigma_{\mathcal{E}^P}(r_s^i) = \emptyset$ for every route r_s^i.

Finally, a substation can be *protected* against attacks, e.g., by guards, video surveillance or using tamper-proof system components. We denote the set of protected substations by $\mathcal{P} \subseteq \mathcal{S}$. Protected substations are not susceptible to attacks, therefore $\sigma_{\mathcal{P}}(r_s^i) = r_s^i \setminus \mathcal{P}$. We assume that the substation where the control center is located is protected, that is, $s_{cc} \in \mathcal{P}$.

Fig. 1 illustrates a simple power system and its communication infrastructure. Some substations have applied mitigation schemes, such as non tamper-proof authentication, tamper-proof authentication, and protection.

IV. Attack Model and Security Metrics

We consider an attacker whose goal is to perform a *stealth attack* on some power flow or power injection measurement

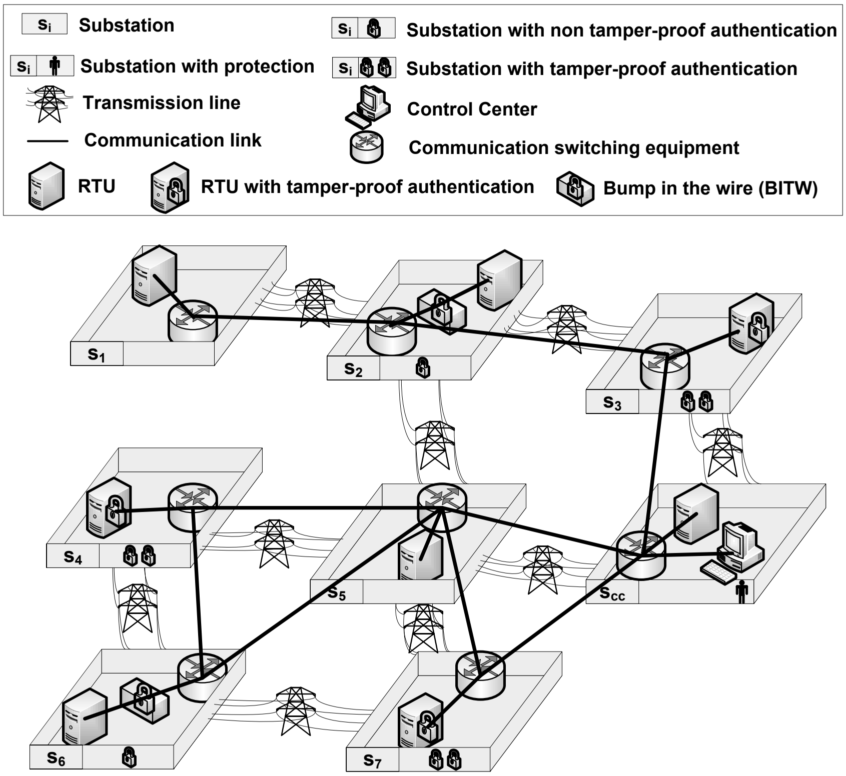

Si Substation
Si Substation with protection
Transmission line
Communication link
RTU
RTU with tamper-proof authentication
Si Substation with non tamper-proof authentication
Si Substation with tamper-proof authentication
Control Center
Communication switching equipment
Bump in the wire (BITW)
S1
S2
S3
S4
S5
Scc
S6
S7

Fig. 1. A simple example of a power system and its communication infrastructure. We have $\mathcal{E}^N = \{s_2, s_6\}$, $\mathcal{E}^P = \{s_3, s_4, s_7\}$, and $\mathcal{P} = \{s_{cc}\}$. A measurement taken at substation $s_1 \notin \mathcal{E}^P \cup \mathcal{E}^N$ is susceptible to attacks at substations s_1, s_2, and s_3. A measurement taken at substation $s_6 \in \mathcal{E}^N$ is only susceptible to attacks at substation s_6 ($\sigma_{\mathcal{E}^N}(r^1_{s_6}) = \{s_6\}$). A measurement taken at substation $s_4 \in \mathcal{E}^P$ is not susceptible to attacks ($\sigma_{\mathcal{E}^P}(r^1_{s_4}) = \emptyset$).

m. To perform the stealth attack, the attacker has to manipulate measurement data from several measurements to avoid a BDD alarm. To manipulate measurement data the attacker gets access to the communication equipment located at a subset of the substations. For example, the attacker could get physical access to the equipment in an unmanned substation or could remotely exploit the improper access configuration of the communication equipment. By gaining access to a substation $s \in \mathcal{S}$ (i.e., the switching equipment and the RTU) the attacker can potentially manipulate the measurement data that are *measured in* substation s and the data that are *routed through* substation s, unless multi-path routing, data authentication or protection make that impossible. To perform a *stealth attack* on a particular measurement m (its value z_m) the attacker might need to attack several substations simultaneously, which increases the cost of performing the attack.

In the following we propose two security metrics to characterize the vulnerability of the system with respect to the importance of individual substations and with respect to the vulnerability of individual measurements. Both metrics depend on the mitigation measures implemented by the operator. We also propose an approximation for each metric based on the communication graph topology.

A. Substation Attack Impact (I_s)

We quantify the importance of substation s by its *attack impact* I_s, which is the number of measurements on which an attacker can perform a *stealth* attack by getting access to a *single* substation s.

By definition $I_s = 0$ if the substation is protected ($s \in \mathcal{P}$). Otherwise, we define I_s as follows. A measurement m can be attacked if and only if the susceptible parts of all routes from $S(m)$ to the control center pass through substation s. Let us denote by $\mathcal{M}_s \subset \{1, \dots, M\}$ the index set of all such attackable measurements. Then measurement $m \in \mathcal{M}_s$ can be *stealthily* attacked if and only if the following system of equations has a solution with respect to unknowns $a \in \mathbb{R}^M$ and $c \in \mathbb{R}^n$

$$a = Hc, \quad a(m') = 0, \forall\, m' \notin \mathcal{M}_s, \quad \text{and } a(m) = 1. \tag{5}$$

We note that due to the bilinearity of matrix multiplication, the constraint on $a(m)$ in (5) is equivalent to $a(m) \neq 0$. We use $a(m) = 1$ for simplicity. The attack impact I_s is then the cardinality of the set of measurements for which (5) has a solution. That is,

$$I_s = \left| \left\{ m \;\middle|\; \exists\, a \text{ satisfying (5)} \right\} \right|. \tag{6}$$

The attack impact of a substation depends on the routing $\mathcal{R}$, the set $\mathcal{E}^N$ of substations with non tamper-proof authentication, the set $\mathcal{E}^P$ of substations with tamper-proof authentication, and the set $\mathcal{P}$ of protected substations.

1) Calculating I_s: By a linear algebra fact [21], $a = Hc$ for some c if and only if there exists a matrix N_s such that $N_s a = 0$, where ${N_s}^T$ is a basis matrix for the null space of H^T. Let us denote by $N_s(:, \mathcal{M}_s)$ the matrix formed by keeping only the columns of N_s in $\mathcal{M}_s$, $a(\mathcal{M}_s)$ as a vector formed by keeping only the entries of a corresponding to $\mathcal{M}_s$. Then (5) is solvable if and only if

$$N_s(:, \mathcal{M}_s) a(\mathcal{M}_s) = 0, \quad \text{and} \quad {v_i}^T a(\mathcal{M}_s) = 1 \tag{7}$$

can be solved, where v_i denotes the i^{th} column of an identity matrix of dimension $|\mathcal{M}_s|$, and the i^{th} entry of $z(\mathcal{M}_s)$ is $z(m)$. Next, let $\tilde{N}_s$ be a basis matrix for the null space of $N_s(:,\mathcal{M}_s)$. Then (7) is solvable if and only if there exists a vector $\tilde{c}$ s.t.

$$\left(v_i{}^T\tilde{N}_s\right)\tilde{c} = 1. \tag{8}$$

This is possible if and only if the i^{th} row of $\tilde{N}_s$ is not identically zero. The above checking procedure applies to indices other than i. Hence, the calculation of I_s can be summarized as

Proposition 1.

$$I_s = \left|\left\{i \mid \tilde{N}_s(i,:)\neq 0\right\}\right|.$$

The complexity of the calculation is dominated by the singular value decomposition needed to find the basis matrix $N_s{}^T$, and is $O(M^3)$.

2) Substation Betweenness $\tilde{I}_s$: An intriguing question is whether one can estimate I_s based on the topology of the communication graph $\mathcal{G}$ only, i.e., without considering the power system. The substation betweenness $\tilde{I}_s$, which we describe in the following is inspired by the betweenness centrality of a vertex in a graph [16]. The betweenness centrality of a vertex corresponds to the importance of the vertex in the graph if all nodes communicate with each other; it is often related to the load the vertex is exposed to and to the dependence of the network on the vertex.

To calculate the substation betweenness $\tilde{I}_s$ we assign to every substation s' as weight the number of measurements taken at substation s' (i.e., $|\{m : S(m) = s'\}|$). For a given set of established routes $\mathcal{R}$ the substation betweenness of substation s is then given by the sum of the weights of the substations s' for which it holds that all their established routes to the control center are susceptible to attack at substation s. This is exactly the cardinality of the index set $\mathcal{M}_s$ used to define I_s

$$\tilde{I}_s \quad = \quad |\mathcal{M}_s| \tag{9}$$

The following proposition establishes the relationship between the attack impact and the betweenness of a substation.

Proposition 2. *The substation betweenness is an upper bound for the attack impact, i.e., $\tilde{I}_s \geq I_s$.*

Proof: The result is trivial if substation $s \in \mathcal{P}$, as $\tilde{I}_s = I_s = 0$. For $s \notin \mathcal{P}$ observe that if a measurement m can be stealthily attacked then by (5) and (6) it must be that $m \in \mathcal{M}_s$. ■

Furthermore, if substation s is susceptible to attacks then $\tilde{I}_s$ is no less than the number of measurements taken at substation s, i.e., $\tilde{I}_s \geq |\{m : S(m) = s\}|$. The complexity of calculating the substation betweenness is that of calculating $\mathcal{M}_s$, which is $O(M)$, and is significantly lower than that of I_s.

B. Measurement Attack Cost (Γ_m)

We quantify the vulnerability of measurement m by the minimum number of substations that have to be attacked in order to perform a stealth attack against the measurement, and denote it by Γ_m. If the substation at which the measurement is located is protected and uses non tamper-proof authentication ($S(m) \in \mathcal{P} \cap \mathcal{E}^N$), or it uses tamper-proof authentication ($S(m) \in \mathcal{E}^P$) then the measurement is not vulnerable and we define $\Gamma_m = \infty$.

Otherwise, for a measurement m we define Γ_m as the cardinality of the smallest set of substations $\omega \subseteq \mathcal{S}$ such that there is a stealth attack against m involving some measurements m' at substations $S(m')$ such that every route of the substations $S(m')$ involved in the stealth attack is susceptible to attack at least in one substation in ω. That is,

$$\begin{aligned}\Gamma_m = \min_{\omega\subseteq\mathcal{S};\omega\bigcap\mathcal{P}=\emptyset} |\omega| \;\; s.t. \;\; \exists\, a,c \;\; s.t. \;\; a = Hc,\;\; a(m) = 1 \text{ and}\\ a(m')\neq 0 \implies \omega\bigcap\sigma_{\mathcal{E}}(r^i_{S(m')})\neq\emptyset, \quad \forall\, r^i_{S(m')}\in\mathcal{R}_{S(m')},\end{aligned} \tag{10}$$

where $\sigma_{\mathcal{E}}(r^i_{S(m')})$ denotes the substations in route $r^i_{S(m')}$ that are susceptible to attack despite the authentication applied at substation $S(m')$, i.e., $\sigma_{\mathcal{E}}(r^i_{S(m')}) = \sigma_{\mathcal{E}^P}(r^i_{S(m')})\bigcap\sigma_{\mathcal{E}^N}(r^i_{S(m')})$. Similar to (5), the constraint on $a(m)$ in (10) is equivalent to $a(m)\neq 0$.

The attack cost of a measurement depends on the routing $\mathcal{R}$, the set $\mathcal{E}^N$ of substations using non tamper-proof authentication, the set $\mathcal{E}^P$ of substations using tamper-proof authentication, and the set $\mathcal{P}$ of protected substations. The following proposition establishes a relationship between the two security metrics; it states that if all measurements have attack cost greater than 1 then all substations have attack impact equal to 0. That is, there is no single substation that would allow attacking a measurement in a stealthy way.

Proposition 3. $I_s = 0\, \forall s\in\mathcal{S} \iff \min_m \Gamma_m > 1$.

Proof: Follows directly from the definitions (6) and (10). If $\nexists s$ $I_s > 0$ then a stealth attack against any measurement requires at least two substations to be attacked, $\Gamma_m \geq 2$. If $\exists s$ $I_s > 0$ then attacking substation s is sufficient to attack some measurement m and hence $\Gamma_m = 1$. ■

1) Calculating Γ_m: We can obtain Γ_m by solving a mixed integer linear programming problem (MILP) as follows. Define decision vectors $a\in\mathbb{R}^M$ and $c\in\mathbb{R}^n$. a is the attack vector to be determined. We need a to be a stealth attack targeting measurement m and for the solution to be unique we require the attack magnitude on m to be unit

$$a(m) = 1 \quad \text{and (4) is satisfied.} \tag{11}$$

To describe the connection between the choice of which substations to attack and the set of measurements that can be attacked as a result of the substation attacks, two 0-1 binary decision vectors are needed. One such binary decision vector is $x\in\{0,1\}^{n+1}$, with $x(s) = 1$ if and only if substation s is attacked. Hence, for protected substations (i.e., $s\in\mathcal{P}$)

$$x(s) = 0 \quad \forall\, s\in\mathcal{P}. \tag{12}$$

The other binary decision vector is denoted as $y\in\{0,1\}^M$, with $y(m) = 1$ meaning measurement m might be attacked because of attacks on relevant substations. Conversely, $y(m) = 0$ means measurement m cannot be attacked. To apply y as an indicator for which measurements can be attacked, we impose

$$a \leq Ky \quad \text{and} \quad -a \leq Ky, \tag{13}$$

where the inequality is entry-wise and K is a scalar which is regarded as "infinity". A nontrivial upper bound for K can be obtained from physical insight. Finally, measurement m' can be attacked if and only if the susceptible part of every route between $S(m')$ and s_{cc} goes through at least one of the attacked substations. This is captured by the following constraints

$$y(m') \le \sum_{s \in \sigma_{\mathcal{E}}(r^i_{S(m')})} x(s), \quad \forall\, r^i_{S(m')} \in \mathcal{R}_{S(m')}, \forall\, m' = 1, \ldots, M \tag{14}$$

Note that by (14) itself it is possible to have $y(m') = 0$ for some m', while the sum on the right-hand-side can be greater than zero. However, this cannot happen at optimality since the objective is to minimize the sum of all entries of x (i.e., the number of substations to be attacked). The following summarizes the calculation.

Proposition 4. *The MILP for finding the attack scheme on measurement m with the minimum number of substation attacks is as follows:*

$$\begin{aligned} \underset{a,c,x,y}{\text{minimize}} \quad & \sum_{s \in \mathcal{S}} x(s) \\ \textit{subject to} \quad & \textit{constraints (11) through (14)} \\ & x(s) \in \{0,1\} \quad \forall\, s \\ & y(m') \in \{0,1\} \quad \forall\, m'. \end{aligned} \tag{15}$$

If (15) is infeasible, then the measurement attack cost is defined to be $\Gamma_m = \infty$. *Otherwise,* Γ_m *is the optimal objective function value in (15).*

MILPs are NP-hard in general, but moderate instances of (15) are feasible to solve offline using off-the-shelf MILP solvers.

2) Measurement Connectivity $\tilde{\Gamma}_m$*:* The measurement connectivity $\tilde{\Gamma}_m$ is an approximation of the attack cost based on the communication network topology. It is inspired by the minimum vertex cut between two vertices of a graph, i.e., the smallest set of vertices within a graph whose removal disconnects the two vertices.

We define the measurement connectivity of measurement m as the cardinality of the minimum vertex cut for substation $S(m)$ and the control center s_{cc}. Intuitively, if an attacker attacks the substations in the minimum vertex cut for substations $S(m)$ and s_{cc} then it can manipulate the value of measurement m if the measurement data are susceptible to attack at the substations specified in the minimum vertex cut. This is the case if there is no data authentication at $S(m)$ and the substations are not protected. For measurements for which $S(m) = s_{cc}$ or $S(m)$ is adjacent to s_{cc} we define $\tilde{\Gamma}_m = \infty$.

To calculate the measurement connectivity, we can use Menger's theorem [17], which states that the cardinality of the minimum vertex cut for two vertices equals the maximum number of vertex-disjoint paths between the two vertices. The maximum number of vertex-disjoint paths can be efficiently calculated using Ford-Fulkerson-like algorithms. In particular, because capacities are unit, Dinitz's algorithm finds the maximum number of vertex-disjoint paths with complexity $O(min(|\mathcal{S}|^{2/3}, |E|^{1/2})|E|)$ [22].

The measurement connectivity $\tilde{\Gamma}_m$ is not an upper bound for the attack cost Γ_m; it captures the minimum number of substations that have to be attacked in order to tamper measurement m given that substation $S(m)$ is protected ($S(m) \in \mathcal{P}$) and given that the maximum number of node disjoint routes is used.

V. Mitigation Measures Against Attacks

In the following we consider how an operator could improve the security of the system by (i) changing the routes used by the substations (ii) by using multipath routing (iii) and by using data authentication and/or protection.

First, we formulate a result regarding mitigation schemes that make stealth attacks impossible to perform, i.e., mitigation schemes such that $\Gamma_m = \infty$, $\forall m$. For this to hold, the minimum number of *measurements* z_m needed to be protected is the number of buses n [6], [14]. The straightforward way to protect this many measurements is to deploy tamper-proof authentication at all substations. The following result suggests that one can mitigate stealth attacks by deploying authentication in significantly less substations.

Proposition 5. *Consider the power system graph, i.e., the graph with vertex set* $\mathcal{S}$*, and edges the transmission lines. If* $\Gamma_m = \infty$ $\forall m$ *then* $\mathcal{E}^P \cup \mathcal{P}$ *is a dominating set of the power system graph.*

Proof: The dominating set of a graph is a subset of the graph's vertices such that every vertex is either a member of the subset or is adjacent to a vertex in the subset. To prove the proposition, we show that if $\mathcal{E}^P \cup \mathcal{P}$ is not a dominating set of the power system graph then there is at least one measurement m with $\Gamma_m < \infty$.

Since $\mathcal{E}^P \cup \mathcal{P}$ is not a dominating set, there is at least one substation s that is unprotected and not authenticated, and is not adjacent to any substation $s' \in \mathcal{E}^P \cup \mathcal{P}$. Take a measurement m at a bus at substation s. This measurement can be attacked by using an attack vector $a = Hc$ for a vector c whose only non-zero component is that corresponding to a bus at substation s. a has nonzero components corresponding to measurements at adjacent buses, and these measurements are located at substations that do not use either authentication or protection. Hence $\Gamma_m < \infty$. This concludes the proof. ■

The cardinality of the dominating set of connected graphs is typically much smaller than the number of vertices, hence perfect protection might be achievable without installing tamper-proof authentication at every substation. The numerical results in Section VI validate this observation as do the results in [14], [15]. Thus, Proposition 5 can be used to achieve perfect protection with low computational complexity, as follows. First, we find a dominating set of the power system graph. Second, we deploy tamper-proof authentication at the substations in the dominating set. Third, we use the CSF (Critical Substation First) algorithm, described later in this section, to select additional substations at which to deploy tamper-proof authentication, one by one, until perfect protection is achieved.

Next, we turn to the problem of decreasing the vulnerability of the system. A natural goal for the operator would be to improve the most vulnerable part of the system, that is, to minimize $\max_{s \in \mathcal{S}} I_s$ or to maximize $\min_{m \in \mathcal{M}} \Gamma_m$, potentially subject to some constraints on the feasible set of mitigation measures (e.g., due to financial reasons). Maximizing the cost of the least cost stealth attack can lead to increased average attack cost as well, compared to maximizing the average attack cost [14].

Instead of the above formulations, we formulate the operator's goal as a multi-objective optimization problem. As we show later, the solution to this problem formulation is a solution to the max-min formulation. We define the objective γ to be the minimization of the number of measurements with attack cost γ, $|\{m|\Gamma_m = \gamma\}|$. The objectives are ordered: objective γ has priority over objective $\gamma' > \gamma$. Formally, we define the objective vector $w \in \mathbb{N}^{S-1}$ whose γ^{th} component is $w_\gamma = |\{m|\Gamma_m = \gamma\}|$. The goal of the operator can then be expressed as

$$\underset{\mathcal{R},\mathcal{E}^N,\mathcal{E}^P,\mathcal{P}}{\text{l}exmin}\ w(\mathcal{R},\mathcal{E}^N,\mathcal{E}^P,\mathcal{P}), \qquad (16)$$

where l*exmin* stands for lexicographical minimization [23], $w(\mathcal{R},\mathcal{E}^N,\mathcal{E}^P,\mathcal{P})$ is the objective vector calculated using Proposition 4 for the established routes $\mathcal{R}$, the sets $\mathcal{E}^N$ and $\mathcal{E}^P$ of authenticated substations, and the set $\mathcal{P}$ of protected substations, and the optimization is performed over all feasible mitigation schemes. The minimal objective vector w, $w_\gamma = 0$ $(1 \leq \gamma \leq S-1)$ corresponds the case when no measurement can be stealthily attacked, i.e., $\Gamma_m = \infty$ for all $m \in \mathcal{M}$.

Proposition 6. *The solution to (16) is a solution to* $\max_{\mathcal{P},\mathcal{E}^N,\mathcal{E}^P,\mathcal{R}} \min_{m\in\mathcal{M}} \Gamma_m$*. Furthermore, if* $\max_{\mathcal{P},\mathcal{E},\mathcal{R}} \min_{m\in\mathcal{M}} \Gamma_m > 1$ *the solution to (16) is a solution to* $\min_{\mathcal{P},\mathcal{E}^N,\mathcal{E}^P,\mathcal{R}} \max_{s\in\mathcal{S}} I_s$.

Proof: We prove the first part of the proposition by contradiction. Let w be the solution to (16), i.e., the lexicographically minimal objective vector, and denote by γ^* the smallest attack cost for which $w_{\gamma^*} > 0$, i.e., $\gamma^* = \min\{\gamma|w_\gamma > 0\}$. Let $\gamma' = max_{\mathcal{P},\mathcal{E}^N,\mathcal{E}^P,\mathcal{R}} \min_{m\in\mathcal{M}} \Gamma_m$ be the max-min solution and w' a corresponding objective vector. Assume now that $\gamma^* < \gamma'$. For $\gamma < \gamma'$ the objective vector has $w'_\gamma = 0$. Since $\gamma^* < \gamma'$, $w'_{\gamma^*} = 0$, and hence according to the definition of lexicographical ordering $w' < w$, which contradicts to the assumption that w is lexicographically minimal.

The second part of the proposition follows directly from Proposition 3 and from the first part of the proposition. ■

We solve the lexicographical minimization in (16) in an iterative way [23]. Consider given $\mathcal{R},\mathcal{E}^N,\mathcal{E}^P,\mathcal{P}$ and let $\gamma^* = \min\{\gamma|w_\gamma > 0\}$. If $\gamma^* = \infty$ the system is not vulnerable. Otherwise, we use the *critical substation first* (CSF) algorithm shown in Table I to decrease w_γ for some $\gamma \geq \gamma^*$ as long as that is possible.

The algorithm starts by calculating the set $\hat{\mathcal{S}}$ of *critical* substations. In order to find the *critical* substations, the algorithm identifies measurements with attack cost $\Gamma_m = \gamma^*$. Each such measurement has at least one stealth attack ω with attack cost $||\omega|| = \gamma^*$. The substations that are contained in ω for every such stealth attack are *critical* substations. There is at least one such substation, the substation $S(m)$. The critical substations are the candidates for route reconfiguration, authentication or protection.

For every *critical* substation $\hat{s}$ the algorithm considers an alternate mitigation scheme. The alternate mitigation scheme could contain a new set of routes $\mathcal{R}'_{\hat{s}}$ between substation $\hat{s}$ and the control center, or it could be the set of authenticated or protected substations augmented by $\hat{s}$ ($\mathcal{E}^{N\prime}(\hat{s}) = \mathcal{E}^N \cup \hat{s}$, $\mathcal{E}^{P\prime}(\hat{s}) = \mathcal{E}^P \cup \hat{s}$ or $\mathcal{P}'(\hat{s}) = \mathcal{P} \cup \hat{s}$). For every alternate mitigation scheme the algorithm calculates the objective vector $w^{\hat{s}}$ using Proposition 4, and selects the one with the minimal objective vector, $w^{\hat{s}}$. If the alternate mitigation scheme improves the system's level of protection, i.e., $w^{\hat{s}} < w$ then the algorithm terminates. Otherwise the algorithm considers a higher attack cost $\gamma^* = \gamma^* + 1$, and continues from Step 1.

TABLE I
CSF ALGORITHM FOR GIVEN $\mathcal{R}$, $\mathcal{E}^N$, $\mathcal{E}^P$, $\mathcal{P}$ AND γ^*

```
1.   Set $\hat{\mathcal{S}} = \emptyset$
2.   for $\forall m$ where $\Gamma_m = \gamma^*$ do
3.     $X = \{x|$ subject to constraints (11) - (14) assuming $\mathcal{E}^N = \mathcal{S}\}$
4.     $\exists X_{\gamma^*} \subseteq X$ s.t. $\forall x \in X_{\gamma^*}, \gamma^* = ||\omega||$
5.     $\hat{\mathcal{S}} = \hat{\mathcal{S}} \cup \{\hat{s}|x(\hat{s}) = 1, \forall x \in X_{\gamma^*}\}$
6.   end for
7.   for $\forall \hat{s} \in \hat{\mathcal{S}}$
8.     create $\mathcal{R}'_{\hat{s}}$ and set $\mathcal{R}'(\hat{s}) = (\mathcal{R} \setminus \mathcal{R}_{\hat{s}}) \cup \mathcal{R}'_{\hat{s}}$ or
9.     set $\mathcal{E}^{N\prime}(\hat{s}) = \mathcal{E}^N \cup \hat{s}$ or $\mathcal{E}^{P\prime}(\hat{s}) = \mathcal{E}^P \cup \hat{s}$ or $\mathcal{P}'(\hat{s}) = \mathcal{P} \cup \hat{s}$
9.     calculate $w^{\hat{s}}(\mathcal{R}'(\hat{s}), \mathcal{E}^{N\prime}(\hat{s}), \mathcal{E}^{P\prime}(\hat{s}), \mathcal{P}'(\hat{s}))$ using Proposition 4
10.  end for
11.  $\hat{s}^* = \arg\min_{\hat{s}} w^{\hat{s}}$
12.  if $w^{\hat{s}^*} < w$
13.    return $\mathcal{R}'(\hat{s}^*)$, $\mathcal{E}^{N\prime}(\hat{s}^*)$, $\mathcal{E}^{P\prime}(\hat{s}^*)$, $\mathcal{P}'(\hat{s}^*)$
14.  else if $\gamma^* < S - 1$
15.    Set $\gamma^* = \gamma^* + 1$ and GOTO (1)
16.  else
17.    return $\mathcal{R}$, $\mathcal{E}^N$, $\mathcal{E}^P$ and $\mathcal{P}$
18.  end if
```

VI. Numerical Results

In the following we show numerical results obtained using the algorithms for two IEEE benchmark power systems: the IEEE 118 and 300 bus power systems. Measurements are assumed to be taken at every power injection and power flow.

We consider two communication network topologies. In the first topology every substation communicates directly to the control center, hence the communication network graph is a star graph of order $|S|+1$: the control center has degree $|S|$ and all substations have degree 1. We refer to this communication network graph as the *star topology*. In the second topology there is an edge between two substations s and s' in the communication network graph if there is a transmission line between any two buses in substations s and s'. The control center is located adjacent to the substation with highest degree s_{cc}. We refer to this communication network graph as the *mesh topology*.

A. Baseline Numerical Results

We start with considering a baseline scenario. Authentication is not used at any substation ($\mathcal{E}^N = \emptyset$, $\mathcal{E}^P = \emptyset$). For the mesh topology we consider that all substations use a *single shortest path* ($|\mathcal{R}_s| = 1$) to the control center s_{cc}, and the substation to which the control center is adjacent is protected ($\mathcal{P} = \{s_{cc}\}$). In the following we show the attack impact and the measurement attack cost for the star and for the mesh communication network topologies.

For the star topology, the substation betweenness of substation s is equal to the number of measurements taken at substation s, i.e., $\tilde{I}_s = |\{m : S(m) = s\}$. Then by Proposition 2, this is an upper bound for the attack impact.

For the mesh topology Fig. 2 shows the attack impact I_s and the substation betweenness $\tilde{I}_s$ for the substations for which $I_s > 0$ and $\tilde{I}_s > 0$ for the two power systems. The results

TABLE II
NUMBER OF MEASUREMENTS WITH PARTICULAR MEASUREMENT ATTACK COST AND MEASUREMENT CONNECTIVITY FOR THE IEEE 118 AND IEEE 300 SYSTEMS

System	Topology	1	2	3	4	5	6
IEEE118	Star (Γ_m)	0	47	279	71	32	26
	Mesh (Γ_m)	374	78	11	0	0	0
	Mesh ($\tilde{\Gamma}_m$)	53	301	52	18	0	0
IEEE300	Star (Γ_m)	209	251	378	188	41	2
	Mesh (Γ_m)	975	89	3	6	0	0
	Mesh ($\tilde{\Gamma}_m$)	217	403	303	44	0	0

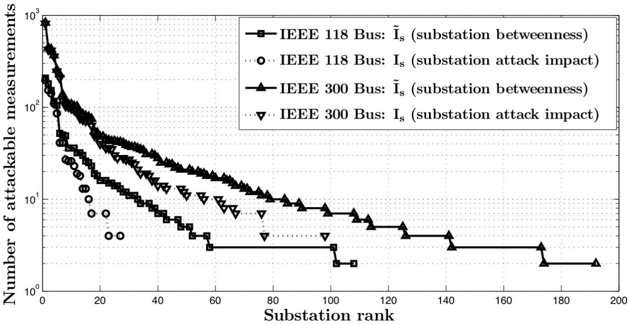


Fig. 2. Attack impact I_s of the substations in the IEEE 118 and 300 b systems in decreasing order of attack impact. The case of shortest path routi

show that there are several substations that would enable a attacker to perform a *stealth* attack on a significant fractio of the measurements in the power system, e.g., on about 100 measurements for the 300 bus system (approx. 90% of all measurements). Almost 50% of the substations have non-zero attack impact, and the attack impact decreases slower than exponentially with the rank of the substation. The substation betweenness $\tilde{I}_s$ is very close to the attack impact for the substations with the highest attack impacts (low ranks), but it overestimates the attack impact significantly for substations with low attack impact.

Table II shows the measurement attack costs for the star and the mesh topologies, and the measurement connectivity for the mesh topology. For the star topology and the 118 bus power system there are no measurements with attack cost 1, and most of the measurements (more than 90%) have an attack cost of at least 3. Interestingly, for the 300 bus power system the attack costs are significantly lower. Almost 20% of the measurements have attack cost 1 and only around 45% of the measurements have an attack cost of at least 3. The reason is that in the 300 bus power system topology there are more substations with several buses, and an attacker can tamper with more measurements by accessing such substations.

The measurement attack costs for the mesh topology are significantly lower than those for the star topology; e.g., for the 118 bus power system more than 75% of the measurements have attack cost 1 for the mesh topology, while none for the star topology. The significant difference in terms of the attack costs shows the importance of considering the communication network topology when estimating the system security. We also note that the measurement connectivity overestimates the actual attack costs for the mesh topology. This is because the attack costs were calculated for the case of a *single shortest path* for every substation.

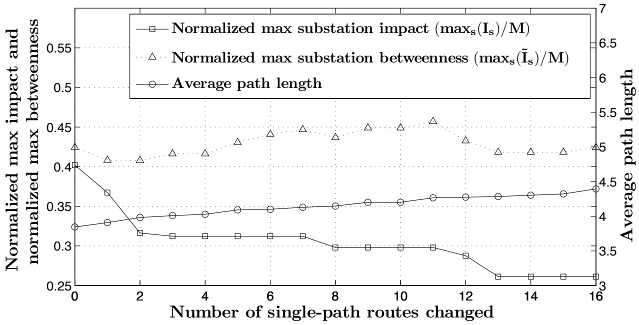


Fig. 3. Maximum normalized attack impact, substation betweenness, and average path length vs. the number of single-path routes changed in the IEEE 118 bus system and mesh topology.

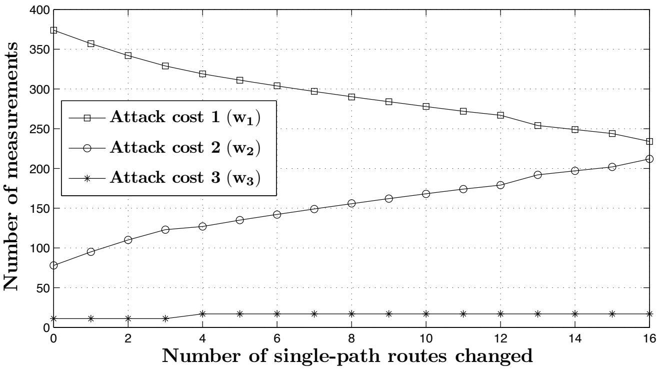


Fig. 4. Number of measurements for various attack costs vs. the number of single-path routes changed in the IEEE 118 bus system and mesh topology.

Motivated by the large substation attack impacts and low measurement attack costs in the case of shortest path routing, in the following we investigate how the operator can improve the system security by changing single-path routes, using multi-path routing, authentication and protection.

B. The Case of Single-path Routing

Modifying single-path routes has the smallest complexity among the mitigation schemes we consider, hence we start with evaluating its potential to decrease the vulnerability of the system. For single-path routing the alternate mitigation schemes differ only in terms of routing. Consequently, $\mathcal{P}'(\hat{s}) = \mathcal{P}$, $\mathcal{E}^{P\prime}(\hat{s}) = \mathcal{E}^P$ and $\mathcal{E}^{N\prime}(\hat{s}) = \mathcal{E}^N$.

In the star topology, substations are directly connected to the control center. Hence, modifying single-path routes is not feasible. For the case of the mesh topology, in order to obtain $\mathcal{R}'(\hat{s})$ from $\mathcal{R}$ for a critical substation $\hat{s}$ we modify the only route $r_1^{\hat{s}}$ in $\mathcal{R}_{\hat{s}}$. For a route $r_1^{\hat{s}}$ we create the shortest alternate route $r_1^{\hat{s}\prime}$ that avoids the substation $s \in r_1^{\hat{s}}$ that appears in most substation attacks ω with cardinality γ^*.

Fig. 3 shows the maximum normalized substation attack impact, i.e., $\max_s I_s/M$, as a function of the number of single-path routes changed in the 118 bus system. The maximum attack impact shows a very fast decay, and decreases by almost a factor of two. At the same time the average path length to the control center increases by only 10%.

Fig. 4 shows the number of measurements that have atta cost 1, 2 and 3 (i.e., w_1, w_2 and w_3) as a function of tl number of routes changed in the 118 bus system for the me topology. By changing single-path routes the algorithm cou increase the attack cost for about 200 measurements fro $\Gamma_m = 1$ to $\Gamma_m = 2$, and for some measurements to $\Gamma_m =$ (e.g., at iteration 5). Fig. 5 shows the corresponding resul for the 300 bus system. Note that after 27 iterations w_1 do not decrease, but instead w_2 does. After 16 resp. 29 iteratio the algorithm could not find any single-path route that wou lead to increased attack cost for any measurement. Hence, v turn to multi-path routing.

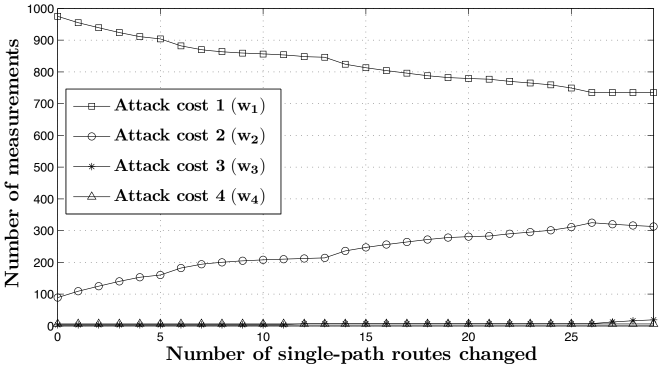


Fig. 5. Number of measurements for various attack costs vs. the number of single-path routes changed in the IEEE 300 bus system and mesh topology.

C. The Case of Multi-path Routing

In the case of multi-path routing the alternate mitigation schemes differ only in terms of routing, as for single-path routing. Consequently, $\mathcal{P}'(\hat{s}) = \mathcal{P}$, $\mathcal{E}^{P\prime}(\hat{s}) = \mathcal{E}^P$ and $\mathcal{E}^{N\prime}(\hat{s}) = \mathcal{E}^N$.

Since in the star topology substations are directly connected to the control center, multi-path routing can not decrease the vulnerability of the system. For the mesh topology, to obtain $\mathcal{R}'(\hat{s})$ from $\mathcal{R}$ for a critical substation $\hat{s}$, we consider the single route $r_1^{\hat{s}}$ in $\mathcal{R}_{\hat{s}}$, and construct the shortest route $r_2^{\hat{s}\prime}$ such that $r_2^{\hat{s}\prime}$ and $r_1^{\hat{s}}$ are node-disjoint. The routes in $\mathcal{R}_{\hat{s}}'$ are then $r_1^{\hat{s}\prime} = r_1^{\hat{s}}$ and $r_2^{\hat{s}\prime}$.

Multi-path routing introduces complexity in the management of the communication infrastructure. In the case of SDH at the link layer several virtual circuits have to be configured and maintained. In the case of Ethernet some form of traffic engineering is required (e.g., using MPLS). Hence the cost of establishing a multi-path route from a substation to the control center has a higher cost than changing a single-path route, considered in the previous subsection. We therefore take the set of routes $\mathcal{R}$ obtained in the last iteration of the algorithm in the previous subsection as the starting point for deploying multi-path routing.

Fig. 6 shows the maximum normalized substation attack impact and the number of measurements with attack costs 1 to 4 vs. the number of multi-path routes in the 118 bus system and the mesh topology. Multi-path routing could decrease the maximum attack impact by 50% through increasing the number of measurements with attack cost $\Gamma_m = 2$ and $\Gamma_m = 3$. Still, 86 measurements have attack cost 1 when the algorithm terminates. The achieved attack costs are much closer to the measurement connectivity $\tilde{\Gamma}_m$ than in the case of single-path routing. However, the measurement connectivity still overestimates the attack costs. This is because we only consider two node-disjoint paths to the control center. By considering all node-disjoint paths the attack costs would approach and potentially exceed the measurement connectivity.

D. The Case of Authentication

In the case of (non) tamper-proof authentication the alternate mitigation schemes differ in terms of the set of (non) tamper-proof authenticated substations $\mathcal{E}^P$ ($\mathcal{E}^N$). Consequently, $\mathcal{P}'(\hat{s}) = \mathcal{P}$ and $\mathcal{R}'(\hat{s}) = \mathcal{R}$.

To obtain $\mathcal{E}^{N\prime}(\hat{s})$ from $\mathcal{E}^N$ for a critical substation $\hat{s}$ we add substation $\hat{s}$ to the set of substations using non tamper-proof authentication, i.e., $\mathcal{E}^{N\prime}(\hat{s}) = \mathcal{E}^N \cup \hat{s}$. We follow a similar procedure to augment the set $\mathcal{E}^P$ of substations with tamper-proof authentication.

Apart from the deployment costs (e.g., new equipment), authentication requires that secret keys be protected and managed, which results in costs for the operator. The cost of introducing authentication is certainly higher than that of reconfiguring single-path routing, but it is difficult to compare its cost to that of introducing multi-path routing. We therefore take the set of routes $\mathcal{R}$ obtained in the last iteration of the algorithm for single-path routing as the starting point for deploying authentication.

Fig. 7 shows the number of measurements with attack cost 1 to 9 as a function of the number of tamper-proof authenticated RTUs in the 118 bus system for the star topology. Note that there are no measurements with attack cost 1. With 31 substations using tamper-proof authentication stealth attacks are impossible to perform. The 31 substations form a dominating set of the power system graph, in accordance with Proposition 5. Note that this number is less than one third of the number of substations in the system, which is $S = 109$.

Fig. 8 shows the maximum normalized substation attack impact and the number of measurements with attack cost 1 to 5 as a function of the number of non tamper-proof authenticated RTUs in the 118 bus system for the mesh topology. Authentication eliminates measurements with attack cost $\Gamma_m = 1$ after 25 substations are authenticated. Furthermore, upon termination more measurements have attacks cost $\Gamma_m \geq 3$, than using multi-path routing.

Fig. 9 shows the maximum normalized substation attack impact and the number of measurements with attack cost 1 to 3 as a function of the number of tamper-proof authenticated RTUs in the 118 bus system for the mesh topology. Authentication eliminates measurements with attack cost $\Gamma_m = 1$ ($\Gamma_m = 2$, $\Gamma_m = 3$) after 19 (31,32) substations are authenticated. With 32 using tamper-proof authentication stealth attacks are impossible to perform. These 32 substations also form a dominating set of the power system graph, in accordance with Proposition 5. We note that authenticating the 31 substations found to make stealth attacks impossible for the star topology

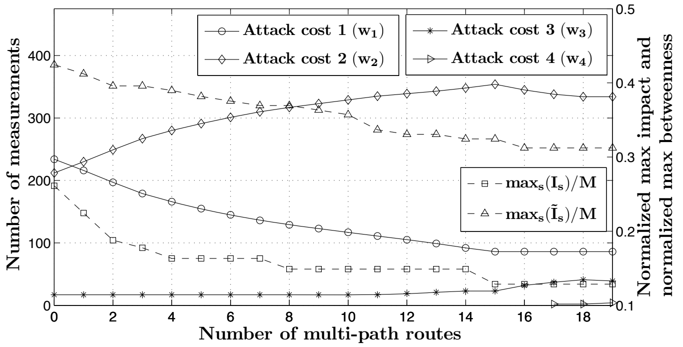


Fig. 6. Maximum attack impact, substation betweenness, and number of measurements for various attack costs vs. the number of multi-path routes. IEEE 118 bus system, mesh topology.

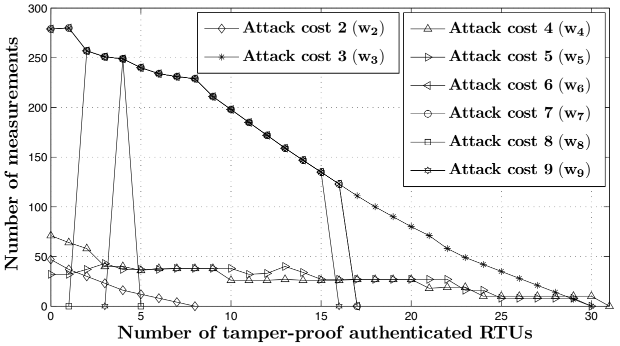


Fig. 7. Maximum attack impact and number of measurements for various attack costs vs. the number of tamper-proof authenticated RTUs ($|\mathcal{E}^P|$). IEEE 118 bus system, star topology.

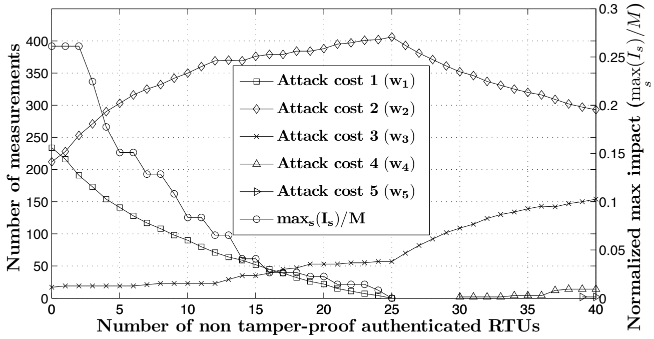


Fig. 8. Maximum attack impact and number of measurements for various attack costs vs. the number of non tamper-proof authenticated RTUs ($|\mathcal{E}^N|$). IEEE 118 bus system, mesh topology.

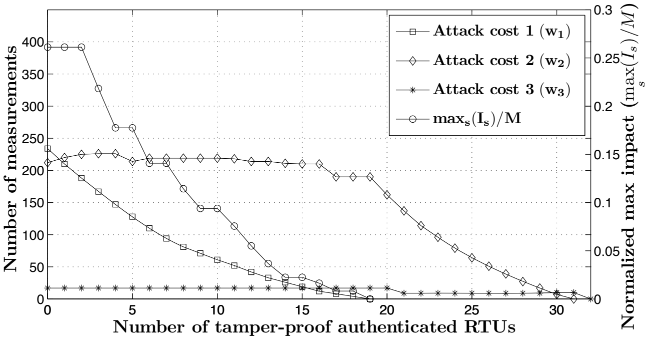


Fig. 9. Maximum attack impact and number of measurements for various attack costs vs. the number of non tamper-proof authenticated RTUs ($|\mathcal{E}^N|$). IEEE 118 bus system, mesh topology.

would also make stealth attacks impossible for the mesh topology.

VII. Conclusion

We considered the problem of mitigating data integrity attacks against the power system state estimator. By combining a power flow model with a model of the SCADA communication infrastructure, we developed a framework and proposed security metrics to quantify the importance of substations and the cost of stealthy attacks against measurements. We provided efficient algorithms to calculate the security metrics. We proposed easy to calculate approximations of the security metrics based on the communication network topology only. We proposed an algorithm to improve the system security by using various mitigation measures, such as modified routing and data authentication. We illustrated the potential of the solutions through numerical examples on large IEEE benchmark power systems. Our results show the importance of considering the physical system and the network topology jointly when analyzing the security of the state estimator against attacks. It is subject of our future work to analyze the robustness of our metrics to changes in the power system topology and to random failures.

References

[1] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, 2000.

[2] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation.* Marcel Dekker, Inc., 2004.

[3] National Energy Technology Laboratory, "Smart grid principal characteristics: Operates resiliently against attack and natural disasters," U.S. Department of Energy, Tech. Rep., September 2009.

[4] A. Giani, S. S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in *Proc. of the 2nd International Symposium on Resilient Control Systems*, 2009.

[5] A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *Proc. of 3rd USENIX Workshop on Hot topics in security*, July 2008.

[6] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM conference on Computer and Communications Security (CCS)*, 2009, pp. 21–32.

[7] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," in *Proc. IFAC World Congress*, Aug. 2011.

[8] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. of IEEE SmartGridComm*, Oct. 2010.

[9] L. Mili, T. Cutsem, and M. Ribbens-Pavella, "Bad data identification methods in power system state estimation: A comparative study," *IEEE Trans. Power App. Syst.*, vol. 104, no. 11, pp. 3037–3049, Nov. 1985.

[10] F. F. Wu and W. H. E. Liu, "Detection of topology errors by state estimation," *IEEE Trans. Power Syst.*, vol. 4, no. 1, pp. 176–183, Feb. 1989.

[11] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, Stockholm, Sweden, April 2010.

[12] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber-security analysis of state estimators in electric power systems," in *Proc. IEEE Conf. on Decision and Control (CDC)*, Dec. 2010.

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

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

[15] 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.

[16] L. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, vol. 40, pp. 35–41, 1977.

[17] R. Diestel, *Graph Theory*, S. Axler and K. A. Ribet, Eds. Springer-Verlag, 2006.

[18] M. Bigrigg, K. Carley, K. Manousakis, and A. McAuley, "Routing through an integrated communication and social network," in *Proc. IEEE Military Communications Conference (MILCOM)*, 2009.

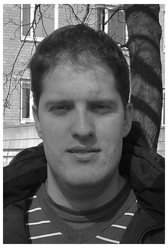
[19] Y. W. Law, L. Yen, R. Di Pietro, and M. Palaniswami, "Secure k-connectivity properties of wireless sensor networks," in *Proc. IEEE Conference on Mobile Adhoc and Sensor Systems (MASS)*, Oct. 2007.

[20] P. Tsang and S. Smith, "YASIR: A low-latency, high-integrity security retrofit for legacy scada systems," in *Proc. IFIP/TC11 International Information Security Conference*, 2008.

[21] G. Strang, *Introduction to Applied Mathematics*. Wellesley-Cambridge Press, 1986.

[22] A. L. R. Oded Goldreich and A. L. Selman, Eds., *Dinitz' Algorithm: The Original Version and Even's Version*, ser. LNCS Festschrift. Springer-Verlag, 2006, vol. 3895, pp. 218–240.

[23] J. Ignizio and T. Cavalier, *Linear Programming*. Prentice Hall, Englewood Cliffs, NJ, 1994.



Ognjen Vuković is a PhD student in the Laboratory of Communication Networks at the KTH Royal Institute of Technology in Stockholm, Sweden. In 2010, he received his M.Sc. degree in Telecommunications, System engineering and Radio Communications, from the Faculty of Electrical Engineering, University of Belgrade.

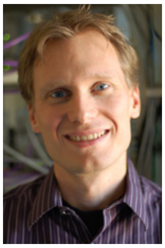
His research interests include power system communication technologies, communication security and availability, and resource management for networked systems.

Kin Cheong Sou received a Ph.D. degree in Electrical Engineering and Computer Science at Massachusetts Institute of Technology in 2008. In 2008-2010 he was a postdoctoral researcher at Lund University, Lund, Sweden, and since September 2010 he has been a postdoctoral researcher at KTH Royal Institute of Technology, Stockholm, 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.

György Dán received the M.Sc. degree in computer engineering from the Budapest University of Technology and Economics, Hungary in 1999 and the M.Sc. degree in business administration from the Corvinus University of Budapest, Hungary in 2003. He worked as a consultant in the field of access networks, streaming media and videoconferencing 1999-2001. He received his Ph.D. in Telecommunications in 2006 from KTH Royal Institute of Technology, Stockholm, Sweden, where he currently works as an assistant professor. He was a visiting researcher at the Swedish Institute of Computer Science in 2008.

His research interests include cyber-physical systems security and the design and analysis of distributed and peer-to-peer systems.



Henrik Sandberg received the M.Sc. degree in Engineering Physics in 1999 and the Ph.D. degree in Automatic Control in 2004, both from the Lund University, Sweden. In 2005-2007, he was a postdoctoral scholar at the California Institute of Technology in Pasadena, USA. Since 2008, he is an Assistant Professor in the Automatic Control Laboratory at the KTH Royal Institute of Technology in Stockholm, Sweden. He has also held visiting appointments at the Australian National University and the University of Melbourne, Australia.

His research interests include secure networked control, power systems, model reduction, and fundamental limitations in control. Henrik Sandberg was the winner of the Best Student-Paper Award at the IEEE Conference on Decision and Control in 2004, and is an associate editor of Automatica.