Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems

Ognjen Vuković, Kin Cheong Sou, György Dán, Henrik Sandberg
School of Electrical Engineering, KTH, Royal Institute of Technology, Stockholm, Sweden
Email: {vukovic,sou,gyuri,hsan}@ee.kth.se

***Abstract*—The power system state estimator is an important application used to calculate optimal power flows, to maintain the system in a secure state, and to detect faulty equipment. Its importance in the operation of the smart grid is expected to increase, and therefore its security is an important concern. Based on a realistic model 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 provide efficient algorithms to calculate these metrics, and use the metrics to show how various network layer and application layer mitigation strategies 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.**

I. Introduction

Large-scale power networks are operated by means of complex supervisory control and data acquisition (SCADA) systems, which transmit information through wide area networks to a control center. The SCADA system collects measurement data from remote terminal units (RTUs) installed in various substations in the grid, and relay aggregated measurements to the control center. The SCADA systems for power networks are complemented by a set of application specific software, usually called energy management systems (EMS). Modern EMS provide information support in the command center for a variety of applications related to power network monitoring and control. The power network state estimator (SE) is an on-line application which uses redundant measurements and a network model to provide the EMS with an accurate state estimate at all times, see [1], [2]. The SE is, for example, an integral tool for optimal routing of power flows in the network, so-called optimal power flow (OPF). EMS and SE, and derivatives thereof, are also expected to be integral parts in future SmartGrid solutions, and hence their proper operation is of critical importance, see also [3], [4].

It has been pointed out in, for example, [5], [6], that the SCADA system is potentially vulnerable to cyber attacks. A cyber attacker can gain access to the communication network, and can inject crafted packets or can corrupt measurement data destined for the SE and EMS. As was first pointed out in [7], measurements can be corrupted so that they do not trigger the built-in bad data detection (BDD) system, even though the measurements are erroneous. We term such corruptions *stealth attacks* on the SE. Recent experiments on real SCADA/EMS software [8] indeed verify that large stealth attacks can be made without triggering alarms. Several works aimed to quantify the difficulty of performing stealth attacks against some measurements [7], [9], [10], [11], [12], [13]. These works assume that each measurement is delivered individually to the control center [7], [9], [10], [11], [13], or that measurements taken at the same substation are delivered to the control center over a communication channel independent of the measurements from other substations [12]. These assumptions do not hold, however, for most SCADA systems.

In this paper we use a realistic model of the communication infrastructure used in modern power transmission systems. The model accounts for the fact that measurement data are usually delivered to the SE via other substations, and consequently an attacker that gains access to a substation can in fact access and modify all data that traverses the substation. Our contribution in this paper is that we develop a methodology for SCADA system operators to assess the vulnerability of their systems and to protect their systems against stealth attacks taking into account the characteristics of the SCADA communication infrastructure. We develop quantitative metrics to assess the importance of substations with respect to the SE, and use these metrics to decrease the SE's vulnerability through the use of various protective measures. As protective measures we consider both network layer solutions, such as routing, and application layer solutions such as data authentication. To our knowledge this paper provides the most realistic treatment of stealth attacks and protection schemes for power system SE.

The structure of the paper is as follows. In Section II we outline power system SE and stealth attacks, and describe modern SCADA communication infrastructures. In Section III, we introduce two system security metrics and show how they can be efficiently computed even for large power systems. In Section IV, we use the proposed metrics to evaluate the potential of various routing algorithms and protection schemes to improve security. In Section V we conclude the paper.

II. 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. 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. One has to fix one (arbitrary) bus phase angle as reference angle, for example $\delta_1 := 0$, and therefore only n angles have to be estimated. The active power flow measurements are denoted by $z = (z_1, \ldots, z_M)$, 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 $R := \mathbf{E} e e^T$ 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. $\delta \in \mathbb{R}^n$ is a vector of the unknown phase angles δ_i. 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

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

where K is the so-called "hat matrix" [2]. 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.

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 [7], 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 [8] it was verified that despite the simplifying assumptions, stealth attacks indeed can be made large in real (nonlinear) SE software: in the example considered in [8], a power flow measurement was corrupted by 150 MW (57% of the nominal power flow) without triggering alarms.

B. Power System Communication Infrastructure

The measurement data collected by meters in the same substation are multiplexed by a Remote Terminal Unit (RTU) before they are sent to SE at the control center. To detect bit errors, the RTUs calculate an error detection code and send it along with the data. The error detection code can be based on, for example, 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 in the substation in one of two ways. (i) First, by installing a bump-in-the-wire (BITW) device adjacent to a legacy RTU. 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 tha data between the BITW device and the control center. (ii) 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.

Because electric power transmission systems extend over large geographical areas, typically entire countries, wide-area networks (WANs) are used to deliver the multiplexed measurement data from the RTUs, together with voice, video and other data traffic from the substations to the control center of the transmission system operator (TSO). The control center is often located at or near an important substation. For reliability the WAN communication infrastructure is usually owned by the TSO, and is 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. Typically, 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.

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 $S(m) \in \mathcal{S}$. We model the communication system by an undirected graph $\mathcal{G} = (\mathcal{S}, E)$. The vertices of the graph are the substations, and there is an edge between two substations if they are connected by a transmission line. The graph $\mathcal{G}$ is connected but is typically sparse. We denote the substation at which the control center is located by $s_c \in \mathcal{S}$. For each substation $s \in \mathcal{S}$ there is a set of established routes $\mathcal{R}_s = \{r_s^1, \ldots, r_s^{R(s)}\}$ from s to s_c through $\mathcal{G}$. $\mathcal{R}$ denotes the collection of all $\mathcal{R}_s$. We represent a route by the set of substations it traverses including s itself and the control center s_c, i.e., $r_s^i \subseteq \mathcal{S}$. The order in which the substations appear in the route is not relevant to the considered problem. 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 data is split equally among the routes such that if the data sent

over any route gets corrupted the control center can detect the data corruption using the error detection code.

We denote the set of substations that use a BITW device to *authenticate* the data sent to the control center by $\mathcal{E} \subseteq \mathcal{S}$. For a route r_s^i we denote by $\sigma_{\mathcal{E}}(r_s^i)$ the set of substations in which the data is *susceptible* to attack despite BITW authentication. By definition $\sigma_{\mathcal{E}}(r_s^i) = \{s\}$ if $s \in \mathcal{E}$ and $\sigma_{\mathcal{E}}(r_s^i) = r_s^i$ otherwise, that is, BITW authenticated data can only be modified at the substation where it originates from, if physical access is possible. To avoid physical access a substation can be protected, e.g., by guards or video surveillance. We denote the set of protected substations by $\mathcal{P} \subseteq \mathcal{S}$. Protected substations are not susceptible to attacks. We assume that the substation where the control center is located is protected, that is, $s_c \in \mathcal{P}$.

III. 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 m. To perform the 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 switching 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, physical protection or data authentication 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 protection measures implemented by the operator, and we use the metrics in Section IV to quantify how various protection measures can decrease the system's vulnerability.

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 unencrypted parts of all routes from $S(m)$ to the control center pass through substation s. Let us denote by $\mathcal{M}_s \subset \{1,\ldots,M\}$ the index set of all such attackable measurements. Then measurement $m \in \mathcal{M}_s$ can be *stealthy* attacked if and only if the following system of equations has a solution with respect to unknowns $a \in \mathbb{R}^M$ and $c \in \mathbb{R}^{n+1}$

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

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 encrypted substations $\mathcal{E}$, and the protected substations $\mathcal{P}$.

1) Calculating I_s: By a linear algebra fact [14], $a = Hc$ 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

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

can be solved, where e_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.

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

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.

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

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 is encrypted ($S(m) \in \mathcal{P} \cap \mathcal{E}$) 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 the unencrypted part of every route of the substations $S(m')$ involved in the stealth attack passes through at least one substation in ω

$$\Gamma_m = \min_{\omega \subseteq \mathcal{S}; \omega \bigcap \mathcal{P} = \emptyset} |\omega| \;\; s.t. \;\; \exists\, a, c \;\; s.t. \;\; a = Hc, \;\; a(m) = 1 \text{ and}$$
$$a(m') \neq 0 \implies \omega \bigcap \sigma_{\mathcal{E}}(r^i_{S(m')}) \neq \emptyset, \quad \forall\, r^i_{S(m')} \in \mathcal{R}_{S(m')} \tag{9}$$

The attack cost of a measurement depends on the routing $\mathcal{R}$, the encrypted substations $\mathcal{E}$, and the protected substations $\mathcal{P}$.

1) Calculating Γ_m: We can obtain Γ_m by solving a mixed integer linear programming problem as follows. Define decision vectors $a \in \mathbb{R}^M$ and $c \in \mathbb{R}^{n+1}$. 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

$$a(m) = 1 \quad \text{and (4) is satisfied.} \tag{10}$$

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., $s \in \mathcal{P}$)

$$x(s) = 0 \quad \forall\, s \in \mathcal{P}. \tag{11}$$

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

$$a \leq Ky \quad \text{and} \quad -a \leq Ky, \tag{12}$$

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 unencrypted part of every route between $S(m)$ and s_c goes through at least one of the attacked substations. This is captured by the following constraints

$$y(m) \leq \sum_{s \in \sigma_{\mathcal{E}}(r^i_{S(m)})} x(s), \qquad \forall\, r^i_{S(m)} \in \mathcal{R}_{S(m)},\ \forall\, m = 1,\ldots,M \tag{13}$$

Note that by (13) 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 calculation of Γ_m is NP-hard, but moderate instances of the problem are feasible to solve offline using off-the-shelf mixed integer linear program (MILP) solvers. The following summarizes the calculation.

Proposition 2. *The mixed integer linear program for finding the attack scheme on measurement m with the minimum number of substation attacks is as follows:*

$$\begin{aligned} \underset{a,c,x,y}{\text{minimize}} \quad & \sum_{s \in \mathcal{S}} x(s) \\ \textit{subject to} \quad & \textit{constraints (10) through (13)} \\ & x(s) \in \{0,1\} \quad \forall\, s \\ & y(m) \in \{0,1\} \quad \forall\, m \end{aligned} \tag{14}$$

If (14) is infeasible, then the measurement attack cost is defined to be $\Gamma_m = \infty$. Otherwise, Γ_m is the optimal objective function value in (14).

C. Numerical results

We used the algorithms to calculate the attack impact and the measurement attack cost for two IEEE benchmark power systems: the IEEE 118 and 300 bus power systems. As a baseline we considered that all substations use a single shortest path ($|\mathcal{R}_s| = 1$) to the control center s_c, which is located at the substation with highest degree. Measurements are taken at every power injection and power flow, and $\mathcal{E} = \mathcal{P} = \emptyset$.

Fig 1 shows the attack impact I_s for the substations for which $I_s > 0$ for the two power systems. The results show

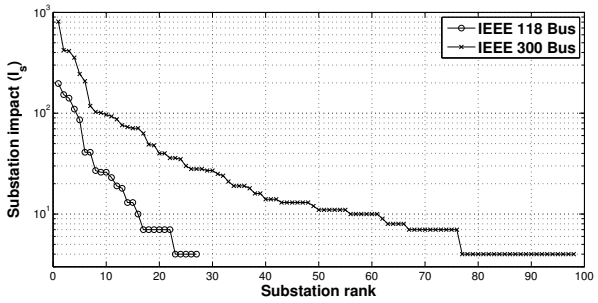

Fig. 1. Attack impact I_s of the substations in the IEEE 118 and 300 bus systems in decreasing order of attack impact. The case of shortest path routing.

that there are several substations that would enable an attacker to perform a *stealth* attack on a significant fraction of the measurements in the power system, e.g., on about 1000 measurements for the 300 bus system (approx. 90% of all measurements). The attack impact decreases slower than exponentially with the rank of the substation, and almost 50 percent of the substations have non-zero attack impact. The measurement attack costs are low, in the 118 bus (300 bus) system the number of measurements with attack cost 1, 2, 3 and 4 is 374, 78, 11 and 0 (975, 89, 3 and 6), respectively.

IV. Protection against attacks

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, data authentication and physical protection.

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 $\min_{m \in \mathcal{M}} \Gamma_m$. 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 [12]. Nevertheless, due to the structure of the graph $\mathcal{G}$ it might happen that $\max_s I_s$ can not be decreased, but the second highest attack impact can. Similarly, it might not be possible to increase $\min_m \Gamma_m$, even though the second lowest attack cost can be increased (cf. Fig. 4 and Fig. 5).

Hence, we formulate the operator's goal as a multi-objective optimization problem. Objective γ is to minimize 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 vector $w \in \mathbb{N}^{S-1}$ whose γ^{th} component is $w_\gamma = |\{m|\Gamma_m = \gamma\}|$. The goal of the operator is then

$$\underset{\mathcal{P},\mathcal{E},\mathcal{R}}{\textit{lexmin}}\, w(\mathcal{P},\mathcal{E},\mathcal{R}), \tag{15}$$

where l*exmin* stands for lexicographical minimization [15]. w attains its minimum $w_\gamma = 0$ $(1 \leq \gamma \leq S-1)$ when no measurement can be attacked, i.e., $\Gamma_m = \infty$ for all $m \in \mathcal{M}$. Due to the definition of w the solution to (15) is a solution to $\max_{\mathcal{P},\mathcal{E},\mathcal{R}} \min_{m \in \mathcal{M}} \Gamma_m$. Furthermore, since I_s and Γ_m are

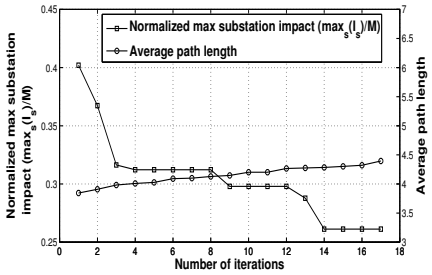

Fig. 2. Maximum normalized attack impact and average path length vs. the number of single-path routes changed in the IEEE 118 bus system.

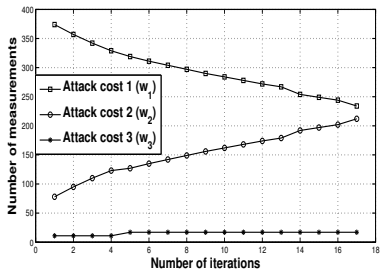

Fig. 3. Number of measurements for various attack costs vs. the number of routes changed in the IEEE 118 bus system.

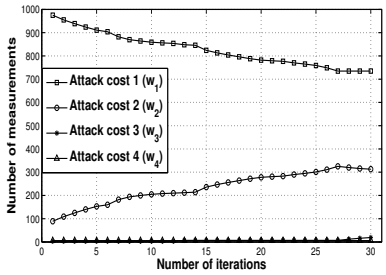

Fig. 4. Number of measurements for various attack costs vs. the number of routes changed in the IEEE 300 bus system.

related, $I_s = 0\ \forall s \in \mathcal{S} \iff \min_m \Gamma_m > 1$, it is also a solution to $\min_{\mathcal{P},\mathcal{E},\mathcal{R}} \max_{s\in\mathcal{S}} I_s$ if $\max_{\mathcal{P},\mathcal{E},\mathcal{R}} \min_{m\in\mathcal{M}} \Gamma_m > 1$.

We solve the lexicographical minimization in (15) in an iterative way [15]. Consider given $\mathcal{P},\mathcal{E},\mathcal{R}$ and let $\gamma^* = \min\{\gamma | w_\gamma > 0\}$. If $\gamma^* = \infty$ the system is not vulnerable. Otherwise, we use the following algorithm to decrease w_γ for some $\gamma \geq \gamma^*$.

Critical First Algorithm:

(i) For every measurement m with $\Gamma_m = \gamma^*$ calculate the set of RTU stealth attacks using the algorithm in [12]. Every such stealth attack is a set of substations including $S(m)$. Consider only the stealth attacks that can be performed by attacking some set of substations ω with cardinality γ^* as defined in (9). For every measurement m with $\Gamma_m = \gamma^*$ there is at least one such stealth attack.

(ii) For every measurement m find the substations that appear in all of the corresponding stealth attacks. Call these *critical* substations for measurement m. There is always at least one *critical* substation $\hat{s}$ for every measurement m, $S(m)$.

(iii) For every *critical* substation $\hat{s}$ create alternate protection schemes $\mathcal{P}'$, $\mathcal{E}'$, and $\mathcal{R}'$ as described in the following subsections.

(iv) Calculate Γ'_m using Theorem 2 for every measurement assuming $\mathcal{P}'$, $\mathcal{E}'$, and $\mathcal{R}'$. Among all $\mathcal{P}'$, $\mathcal{E}'$ and $\mathcal{R}'$ discard the ones that result in $w'_\gamma > w_\gamma$ for some $\gamma \leq \gamma^*$. If an alternate protection scheme remains then pick the alternate protection scheme for which w'_{γ^*} is minimal. Otherwise, if $\gamma^* \geq \max\{\gamma | w_\gamma > 0\}$ terminate. If not, set $\gamma^* = \gamma^* + 1$ and restart from (i).

In the following we describe how to calculate the alternate protection schemes $\mathcal{P}'$, $\mathcal{E}'$, or $\mathcal{R}'$, and illustrate their potential with numerical results.

A. The case of single-path routing

Modifying single-path routes has the smallest complexity among the protection schemes we consider, hence we start with evaluating its potential to decrease the vulnerability of the system. For single-path routing the alternate protection schemes differ only in terms of routing. Consequently, $\mathcal{P}' = \mathcal{P}$ and $\mathcal{E}' = \mathcal{E}$. To obtain $\mathcal{R}'$ 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. 2 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. 3 shows the number of measurements that have attack cost 1, 2 and 3 (i.e., w_1, w_2 and w_3) as a function of the number of routes changed in the 118 bus system. By changing single-path routes the algorithm could increase the attack cost for about 200 measurements from $\Gamma_m = 1$ to $\Gamma_m = 2$, and for some measurements to $\Gamma_m = 3$ (e.g., at iteration 5). Fig. 4 shows the corresponding results for the 300 bus system. Note that after 27 iterations w_1 does not decrease, but instead w_2 does. After 17 resp. 30 iterations the algorithm could not find any single-path route that would lead to increased attack cost for any measurement. Hence, we turn to multi-path routing.

B. The case of multi-path routing

In the case of multi-path routing the alternate protection schemes differ only in terms of routing, as for single-path routing. Consequently, $\mathcal{P}' = \mathcal{P}$ and $\mathcal{E}' = \mathcal{E}$. To obtain $\mathcal{R}'$ 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. 5 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 system. 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, about 80 measurements have

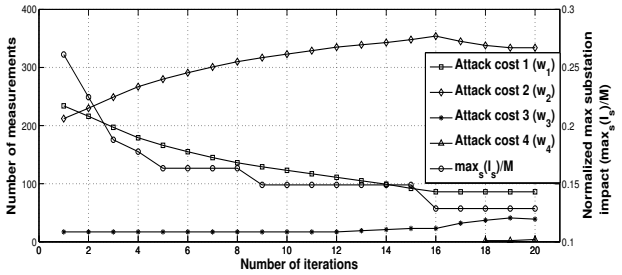

Fig. 5. Maximum attack impact and number of measurements for various attack costs vs. the number of multi-path routes. IEEE 118 bus system.

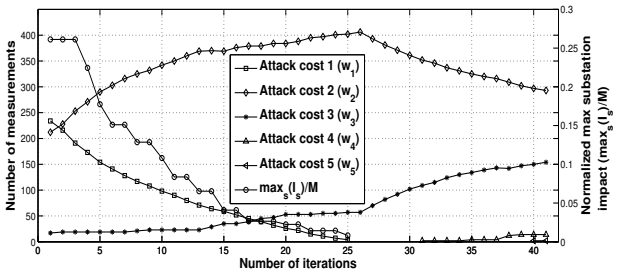

Fig. 6. Maximum attack impact and number of measurements for various attack costs vs. the number of authenticated RTUs ($|\mathcal{E}|$). IEEE 118 bus system.

attack cost 1 when the algorithm terminates.

C. Data authentication and Protection

In the case of authentication the alternate protection schemes differ in terms of the set of authenticated substations $\mathcal{E}$. Consequently, $\mathcal{P}' = \mathcal{P}$ and $\mathcal{R}' = \mathcal{R}$. To obtain $\mathcal{E}'$ from $\mathcal{E}$ for a critical substation $\hat{s}$ we add substation $\hat{s}$ to the set of substations using authentication, i.e., $\mathcal{E}' = \mathcal{E} \cup \hat{s}$.

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 multipath routing.

Fig. 6 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 authenticated RTUs in the system. Authentication eliminates measurements with attack cost $\Gamma_m = 1$ after 25 substations are authenticated. Upon termination, more measurements have attacks cost $\Gamma_m \geq 3$, than using multi-path routing.

Protection can be considered in a similar way, i.e., $\mathcal{P}' = \mathcal{P} \cup \hat{s}$, but we omit the results for brevity. Instead we establish a relationship between the RTU attack model considered in [12] and authentication combined with protection.

Proposition 3. *If $\mathcal{E} = \mathcal{P}$ then it is possible to achieve $\Gamma_m = \infty$ $\forall m$ by letting $\mathcal{E} = \mathcal{P}$ be an appropriate dominating set of $\mathcal{G}$.*

Proof: If $\mathcal{E} = \mathcal{P}$ then $\sigma_{\mathcal{E}}(r_i(s)) = \emptyset \ \ \forall s \in \mathcal{E}$, that is, the measurements in substations $s \in \mathcal{E}$ are not susceptible to attacks. This is equivalent to the RTU cost model considered in [12]. The result then follows from Proposition 1 in [12]. ■

V. Conclusion

We considered the problem of finding and mitigating stealth attacks against the power system state estimator. We described a model of state-of-the-art SCADA communication infrastructure, 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 an algorithm to improve system security by deploying various mitigation solutions, such as modified routing and 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 network layer when analyzing the security of the state estimator against stealth attacks.

VI. Acknowledgement

This work was financed by the EU FP7 project Viking and by the ACCESS Linnaeus Centre at KTH.

References

[1] A. Monticelli, "Electric power system state estimation," *Proc. of the 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] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Proc. of IEEE SmartGridComm*, Oct. 2010.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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*, 2010.

[10] 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. of IEEE Conf. on Decision and Control (CDC)*, Dec. 2010.

[11] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. of IEEE SmartGridComm*, Oct. 2010.

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

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

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

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