2012 American Control Conference
Fairmont Queen Elizabeth, Montréal, Canada
June 27-June 29, 2012

Detection and Identification of Data Attacks in Power System

Kin Cheong Sou, Henrik Sandberg and Karl Henrik Johansson

Abstract— **In this paper a power system state estimator cyber-attack detection and identification scheme is presented. The proposed scheme considers the information from both the active power measurements and the reactive power measurements. Under the scenario that the network operator can take multiple different samples of measurements and the attackers can attack only once, the proposed scheme can detect the presence of what has been described as stealth (or unobservable) attacks. The detection is provably correct. Furthermore, if an attack is present, the proposed scheme can identify exactly the attacked transmission lines.**

I. Introduction

A. SCADA System and State Estimation

A modern society relies critically on the proper operation of the electric power distribution and transmission system, which is supervised and control through the *Supervisory Control And Data Acquisition* (SCADA) systems. SCADA systems measure data such as transmission line power flows, bus power injections and part of the bus voltages, and send them to the state estimator to estimate the power network states (e.g., the phase angles of bus voltages). The estimated states are used for vital power network operations such as optimal power flow calculation and contingency analysis [1], [2]. Any malfunctioning of these operations can lead to significant social and economical consequences (e.g. the northeast US blackout of 2003).

B. Stealth Data Attack on State Estimation

SCADA systems measure data through remote terminal units (RTUs) all over the grid and gather them at a control center, where computer processing takes place and control commands are sent back to the system. The vulnerabilities that are introduced could be exploited by malicious attackers. In [3] it was demonstrated that malicious attackers needed only to coherently corrupt relatively few measurements to achieve their attack objective, without being detected by standard bad data detection procedures such as the largest normalized residual test [1], [2]. Further, [4] verified with experiments that stealth attacks of significant implications could indeed be carried out in a realistic SCADA system testbed. Since [3], there have been significant amount literature studying various aspects of stealth attack and its countermeasures [5]–[10].

The authors are with the ACCESS Linnaeus Center and the Automatic Control Lab, the School of Electrical Engineering, KTH Royal Institute of Technology, Sweden. {sou,hsan,kallej}@kth.se
This work is supported by the European Commission through the VIKING project, the Swedish Foundation for Strategic Research (SSF) and the Knut and Alice Wallenberg Foundation.

C. Detection of Stealth Attack and Network Protection

Two types of countermeasures have been covered by the previous work. References [6], [7], [9] consider the scenario where certain measurement meters are protected (i.e., cannot be corrupted). Depending on the assignment of protection, stealth attack on the network can be impossible or very difficult. On the other hand, in [5], [8] the estimated states of the power network are assumed to follow some distribution or pattern. The presence of an attack is claimed (but not proved) when the estimated states deviate from the assumed normality. This paper also describes a scheme to detect the presence of an attack. However, there is no assumption on the distributions or the patterns of the states or the attack. In addition, the detection is deterministic and provably correct. Furthermore, for part of the measurements (i.e., transmission line measurements) the proposed scheme can correctly identify the attacked measurements in case an attack is present.

The proposed protection scheme is enabled by an extended state estimation framework considered in this paper. Power network state estimation typically involves two types of measurements - active power measurements and reactive power measurements [1], [2]. The estimated states also contain two groups - bus phase angles and bus voltages. Under normal operation conditions, the bus phase angles and bus voltages are estimated separately using active and reactive power measurements respectively because the two types of measurements are sensitive only to the corresponding states [1], [2]. Since the bus voltages typically do not vary too much during operation, the focus of state estimation and its stealth attack and protection has been on bus phase angles/active power measurements. This is the case for the previous work including [3]–[10]. However, if both active and reactive power measurements are taken into account, new counter stealth attack opportunities arise. For instance, if the reactive power measurements cannot be corrupted, they can be used to check the validity of the state estimate calculated based on possibly corrupted active power measurements. However, the above assumption might be too restrictive. In fact, it can be shown that a stealth attack on both active and reactive power measurements requires relatively little effort for the attackers. As a countermeasure, this paper proposes an attack detection and identification scheme in which the network operator considers ***multiple*** sets of reactive power measurements taken from different sampling time instances. It is assumed that these sets of measurements are different from each other because of the changing of the network states. If the attackers can attack the measurements only once, then with

978-1-4577-1094-0/12/$26.00 ©2012 AACC

enough sets of (even possibly corrupted) active and reactive power measurements the operator can detect the presence of an attack and partially identified the attacked meters. Finally, it should be emphasized that considering multiple sets of active power measurements would fail to detect stealth attack because the active power measurements are linear with respect to the states (i.e., bus phase angles) for any practical purposes. This will be elaborated later in this paper.

D. Organization of the Paper

The rest of the paper is organized as follows. In Section II notations and assumptions on power network state estimation and its stealth attack will be defined. Then Section III describes the main result, a stealth attack detection and identification scheme using reactive power measurements. In Section IV a numerical example is presented to demonstrate that the proposed attack detection and identification scheme can correctly identify the stealth attack, while the traditional active power measurement residuals cannot. Finally, Section V concludes the paper.

II. Background and Assumptions

A. Power Network Model and Power Measurements

The power network can be modeled as a directed graph with $n+1$ buses and m_a transmission lines. The transmission lines are directed to indicate the assumed directions of the (active) power flow on them. The (original) incidence matrix $A_o \in \mathbb{R}^{n\times m_a}$ describes the topology:

$$\forall j = 1,\dots,m_a \quad A_o(i,j) = \begin{cases} 1 & \text{if line } j \text{ starts at bus } i \\ -1 & \text{if line } j \text{ ends at bus } i \\ 0 & \text{otherwise} \end{cases}.$$

The transmission lines are assumed to have zero electrical resistance, and $B \in \mathbb{R}^{m_a\times m_a}$ is a nonsingular (typically negative definite) diagonal matrix describing the negative reciprocal of the reactance of the transmission lines.

The states of the power network can be partitioned into two groups: (a) bus phase angles $\theta_o \in [0,2\pi)^{n+1}$ and (b) bus voltages, which are assumed to be one (in the per unit system). Typically, an arbitrary bus is assigned as the reference, and its phase angle is set to zero. Hence, the phase angles for the rest of the buses, denoted as $\theta \in [0,2\pi)^n$, are the only states to be estimated. Correspondingly, the original incidence matrix A_0 has one row removed, and the resulted matrix is referred to as the incidence matrix denoted by A.

The vector of (uncorrupted) active power measurements [1], [2], denoted as P, is related to θ by

$$P = \begin{bmatrix} -ABA^T \\ -BA^T \end{bmatrix} \theta \triangleq H\theta. \tag{1}$$

Notice that the expression in (1) is a linearization of the true active power measurements (where $A^T\theta$ is replaced with $\sin(A^T\theta)$, and $\sin(\cdot)$ applies entry-wise). This is the standard approximation for active power related state estimation [1], [2] and power network state estimation cyber-security analysis [5]–[10]. The first n measurements in (1) are active power injections at the buses, and the rest are active power flows measured at the start end of the transmission lines. The expression in (1) represents the case where all possible active power measurements are considered. On the other hand, the (uncorrupted) reactive power measurement vector [1], [2], denoted as Q, is nonlinearly related to θ as

$$Q = \begin{bmatrix} |A|B\big(-\mathbf{1}+\cos(A^T\theta)\big) \\ B\big(-\mathbf{1}+\cos(A^T\theta)\big) \end{bmatrix}, \tag{2}$$

where $|A|$ is a matrix whose entries $|A|(i,j) = |A(i,j)|$ for all possible index pair (i,j). $\mathbf{1}$ is a vector of ones of appropriate dimension. $\cos(\cdot)$ applies entry-wise to its vector input argument. Again, the first n measurements in (2) are reactive power injections at the buses, and the rest are reactive power flows measured at one end of the transmission lines.

B. State Estimation and Stealth Attack

From (1) and (2) it can be seen that the active power measurement sensitivity $\frac{dP}{d\theta}$ is much more significant than the reactive power measurement sensitivity $\frac{dQ}{d\theta}$, when the network operates under normal conditions (i.e., $A^T\theta \approx 0$). Hence, conventional state estimation procedure estimates θ by solving (1) with active power measurements only. Specifically, denote $\tilde{P} \triangleq P + \Delta P$ where ΔP is the possible additive measurement noise or attack (to be defined) and $\tilde{P}$ is a vector of possibly corrupted active power measurements. Then the state estimate, denoted as $\hat{\theta}$, is

$$\hat{\theta} \triangleq (H^TH)^+H^T\tilde{P}. \tag{3}$$

In (3), $(H^TH)^+$ is the pseudo-inverse of H^TH. Also notice that in practice, the weighted variant of (3) is used instead. That is, $\hat{\theta} = (H^TR^{-1}H)^+H^TR^{-1}\tilde{P}$, where R is typically a positive definite diagonal matrix proportional to measurement noise variance. However, all results in this paper, derived based on (3), apply to the setup with the case when $R \neq I$ with slight modifications (see [11, Section III-F]).

To detect possible anomaly in the measurements, the measurement residual

$$R_P \triangleq \tilde{P} - H\hat{\theta} \tag{4}$$

is formed. In practice, a hypothesis testing of R_P based on measurement noise statistics is performed to see if $\tilde{P}$ contains any bad data [1], [2]. However, in this paper, the bad data detection criterion is simplified to whether $R_P = 0$ or not ($R_P = 0$ means no bad data or attack). Also, the same simplification applies to similar criteria (e.g., R_Q to be defined in (7)).

Reference [3] investigated an additive stealth attack ΔP on P of the form $\Delta P = Hc$, for some $c \in \mathbb{R}^n$. With this specific form of ΔP, the measurement residual R_P in (4) is zero, and hence ΔP is stealth. The details are as follows. The corrupted measurement vector becomes $\tilde{P} = P + Hc = H(\theta + c)$. Based upon $\tilde{P}$, the corrupted state estimate becomes $\hat{\theta} = (H^TH)^+H^T\tilde{P} = \theta + c$. The state estimator is unaware of the stealth attack, because the measurement residual fails to detect it:

$$R_P = \tilde{P} - H\hat{\theta} = P + Hc - H(\theta + c) = 0,$$

as the corrupted state estimate $\hat{\theta}$ is well explained by the corrupted measurements $\tilde{P}$. Also, [8] argued that, for the linearized model of P in (1), $\Delta P = Hc$ is also a necessary condition for ΔP to be a stealth attack.

Finally, notice that all angle related quantities in this paper such as θ, $\hat{\theta}$, c, $A^T\theta$, $A^T\hat{\theta}$ are considered in modulo 2π arithmetics. In particular, the entries of all the angle related vectors range from 0 to 2π (and 2π is not included).

III. Stealth Attack Detection and Identification with Reactive Power Measurements

A. Generalized Reactive Power Measurement Residual

To detect a stealth attack described in Section II-B, information in addition to the corrupted measurements $\tilde{P}$ is needed. In [5], [8] assumptions on the states θ are imposed. Whenever the corrupted state estimate $\hat{\theta}$ deviates too much from the assumption, an alarm is triggered. This paper, however, investigates an alternative approach based on the possibly corrupted ***reactive*** power measurements.

Before the proposed approach can be described, a preparatory statement should be made first. Let M be a matrix such that $\text{span}(M) = \text{Ker}(H^T)$, for H defined in (1). Any ΔP, not necessarily stealth, can be uniquely decomposed into

$$\Delta P = Hc + Mb, \tag{5}$$

for some vectors c and b of appropriate dimensions. The following statement specifies the consequences of ΔP.

Lemma 1: Let ΔP be any active power measurement attack with its decomposition in (5). Then the corrupted state estimate is $\hat{\theta} = \theta + c$. In addition, the active power measurement residual in (4) is $R_P = Mb$.

Proof: The state estimate $\hat{\theta}$ is

$$\begin{aligned} \hat{\theta} &= (H^TH)^+H^T\tilde{P} \\ &= (H^TH)^+H^T\big(H(\theta+c)+Mb\big) \\ &= \theta + c, \end{aligned}$$

where the first equality is due to (5) and $\tilde{P} = P + \Delta P = H\theta + \Delta P$, and the last equality is true because $H^TM = 0$. On the other hand, the active power measurement residual R_P is

$$\begin{aligned} R_P &= \tilde{P} - H\hat{\theta} \\ &= H\theta + Hc + Mb - H(\theta + c) \\ &= Mb. \end{aligned}$$

■

In other words, any attack ΔP can be decomposed into its "unobservable" part Hc which affects $\hat{\theta}$ and the "observable" part Mb which is revealed by the measurement residual R_P. In particular, a stealth attack ΔP consists entirely of its unobservable part.

Now the proposed attack detection scheme can be described. Denote Q in (2) as the uncorrupted reactive power measurement vector. ΔQ as a possible additive attack on Q, and the possibly corrupted reactive power measurement $\tilde{Q}$ as

$$\tilde{Q} \triangleq Q + \Delta Q. \tag{6}$$

Also denote $I_{\text{tl}} = \{n+1, \ldots, n+m_a\}$ as the row index set containing the transmission line measurements of $\tilde{Q}$ in (6). With $\tilde{P}$ and $\tilde{Q}$ measured and network information such as B, H and A available, this paper investigates the following generalized reactive power measurement residual, for transmission line measurements only:

$$\begin{aligned} R_Q &\triangleq \tilde{Q}(I_{\text{tl}}) - B\Big(-\mathbf{1} + \cos\big(A^T\hat{\theta} - B^{-1}R_P(I_{\text{tl}})\big)\Big) \\ &= B\cos\big(A^T\theta\big) + \Delta Q(I_{\text{tl}}) \\ &\quad -B\cos\big(A^T\hat{\theta} - B^{-1}R_P(I_{\text{tl}})\big), \end{aligned} \tag{7}$$

where the second equality is due to (6) and (2). In (7), $\hat{\theta}$ is the state estimate based on $\tilde{P}$. R_P is calculated using $\tilde{P}$ (cf. (4)). Symbols such as $\tilde{Q}(I_{\text{tl}})$ denote the sub-vector of $\tilde{Q}$, with only the entries from the index set I_{tl}. Notice that in the special case of a (active power) stealth attack $\Delta P = Hc$, it holds that $R_P = 0$ and R_Q becomes the reactive power analog of the standard measurement residual. That is, $R_Q = B\cos\big(A^T\theta\big) + \Delta Q(I_{\text{tl}}) - B\cos\big(A^T\hat{\theta}\big)\big)$. The motivation for considering R_Q as in (7) will be given in Section III-E.

The proposed state estimation, bad data detection and identification procedure includes the following three steps:

1) Estimate $\hat{\theta}$ as in (3).
2) Perform standard bad data test [1], [2] using R_P in (4).
3) Calculate R_Q as in (7), and perform the tests to be elaborated in Sections III-B or III-D.

With the additional information of R_Q, the fundamental questions of bad data detection and identification include:

(a) Is it possible to ***detect*** the presence of any arbitrary attack $(\Delta P, \Delta Q)$?
(b) In case $(\Delta P, \Delta Q)$ is present, is it possible to ***identify*** which measurements are attacked?
(c) Is it possible to recover the true state θ even if the measurements are attacked?

This paper attempts to answer question (a), and partially (b). However, how useful the information R_Q can be depends on the attackers' knowledge and control over the power network.

B. Stealth Attack Detection and Identification Using Uncorrupted Reactive Power Measurements

In this part of the discussion the conventional attack scenario in [5]–[10] is considered. In particular, the attackers have only the knowledge of matrix H in (1). The attackers can stage an attack ΔP on P. However, Q cannot be attacked (i.e., $\Delta Q = 0$). Under the above attack scenario, with R_Q in (7) the network operator can identify which transmission line measurements are attacked. The following statement establishes this fact.

Proposition 1: Let $k \in \{1, 2, \ldots, m_a\}$. Assume that $\Delta Q = 0$ in (7) and the attackers know only H. Then with probability one, for any active power measurement attack ΔP, stealth or not, it holds that $\Delta P(n+k) \neq 0$ if and only if $R_Q(k) \neq 0$.

Proof: Let $\Delta P = Hc + Mb$ as in (5). Then Lemma 1 states that $\hat{\theta} = \theta + c$ and $R_P = Mb$. In addition, with $\Delta Q = 0$,

$R_Q(k)$ in (7) becomes

$$\begin{aligned} R_Q(k) &= B(k,k)\Big(\cos\big((A^T\theta)(k)\big) - \cos\big((A^T\theta)(k) \\ &\quad +(A^Tc)(k) - \tfrac{1}{B(k,k)}(Mb)(n+k)\big)\Big) \\ &= B(k,k)\Big(\cos\big((A^T\theta)(k)\big) \\ &\quad -\cos\big((A^T\theta)(k) - \tfrac{1}{B(k,k)}\Delta P(n+k)\big)\Big), \end{aligned}$$

where $(A^Tc)(k) - \frac{1}{B(k,k)}(Mb)(n+k) = -\frac{1}{B(k,k)}\Delta P(n+k)$ is due to (5) and the definition of H in (1). Since $B(k,k) \neq 0$ as B is nonsingular, if $\Delta P(n+k) = 0$ then $R_Q(k) = 0$. On the other hand, since $(A^T\theta)(k)$ is not known to the attackers, with probability one $R_Q(k) \neq 0$ if $\Delta P(n+k) \neq 0$. ■

Remark 1: As indicated in the proof, if the attackers know P and B and A (and hence $A^T\theta$), then by setting $R_Q(k) = 0$ it is possible to calculate the corresponding $\Delta P(n+k)$. However, the the choice of $\Delta P(n+k)$ would be limited to only two points, and ΔP is unlikely to make $R_P = 0$. □

Combining the information of R_P and R_Q, the network operator can detect the presence of any active power attack ΔP, as indicated by the following statement.

Corollary 1: Under the assumptions in Proposition 1, with probability one $\Delta P = 0$ if and only if both $R_P = 0$ and $R_Q = 0$.

Proof: If $\Delta P \neq 0$ and $\Delta P \neq Hc$ for any $c \in \mathbb{R}^n$, then $R_P \neq 0$ as indicated by Lemma 1. If $\Delta P \neq 0$ and $\Delta P = Hc$ for some c, then by the definition of H in (1) there exists an index $k \in \{1,2,\ldots,m_a\}$ such that $\Delta P(n+k) \neq 0$. Then Proposition 1 implies that with probability one $R_Q \neq 0$. Finally, if $\Delta P = 0$, then the definitions in (4) and (7) imply that both $R_P = 0$ and $R_Q = 0$. ■

While Proposition 1 provides the answer to identify the attacked transmission line measurements, R_P and R_Q is not sufficient to identify the attacked bus measurements. Nevertheless, if $R_P = 0$ then ΔP must be of the form $\Delta P = Hc$. Consequently bus and transmission line attacks are related by H in (1). In particular, if any transmission line measurement is attacked, then the buses connected to this line should also be checked for possible attacks.

C. Stealth Attack on Reactive Power Measurements

The assumption that the reactive power measurements Q cannot be attacked might be too restrictive, especially for the transmission lines where the attackers can already attack the corresponding entries of P. Therefore, the attackers might contemplate devising an attack $(\Delta P, \Delta Q)$ which is defined to be stealth if both $R_P = 0$ and $R_Q = 0$. Lemma 1 requires that $\Delta P = Hc$ for some c. In this case, Mb in (5) is zero and $\hat{\theta} = \theta + c$. For $R_Q = 0$, ΔQ must satisfy

$$B\cos(A^T\theta) + \Delta Q(I_{\text{tl}}) = B\cos(A^T(\theta + c)) \tag{8}$$

To stage a stealth attack $(\Delta P, \Delta Q)$, the attackers need to have the following leverages over the power network. The attackers need to be able to attack both P and Q. In addition to knowing matrix H in (1), as in the standard attacking scenario in [3], the attackers also need to know A, B (at least locally) and θ (deducible from P if the attackers also know P). This is a substantial amount of extra information, and it is required because of the nonlinearity in (8).

Finally, let $S_{\Delta P}$ be the support of ΔP (i.e., $\Delta P(j) = 0$, $\forall j \notin S_{\Delta P}$). To reduce risk and effort, the attackers would prefer an attack ΔP such that $S_{\Delta P}$ is sparse [5], [6], [8], [10]. It turns out, unfortunately, that the support of the reactive power measurement attack ΔQ, denoted as $S_{\Delta Q}$, can also be sparse. From (8) it can be seen that for all $j > n$, $j \in S_{\Delta Q}$ if and only if $j \in S_{\Delta P}$. Also, since R_Q does not check the bus attack of ΔQ, this part of ΔQ can be set to zero.

D. Stealth Attack Detection and Identification with Multiple Samples of Reactive Power Measurements

The attackers can stage a stealth attack $(\Delta P, \Delta Q)$ with relatively little effort if they have enough information and control over the power network. To counter this, it is proposed in this paper that the network operator should take into account ***multiple*** sets of active and reactive power measurements from different sampling time instances. If the measurement sets are rich enough (to be made precise), a stealth attack $(\Delta P, \Delta Q)$ described in Section III-C can still be detected and partially identified, if the attackers can attack ***only once***. Note that with enough information and the freedom to stage multiple attacks, the situation returns to the one in Section III-C, where stealth attack is possible.

Denote θ^i, $i = 1,2,\ldots,N$ as the network states from different time instances. Corresponding to θ^i denote P^i as the uncorrupted active power measurements according to (1). Similarly, corresponding to θ^i denote Q^i as the uncorrupted reactive power measurements according to (2). As the attackers can attack only once, the corrupted power measurements are $\tilde{P}^i = P^i + \Delta P$ and $\tilde{Q}^i = Q^i + \Delta Q$. Based on $\tilde{P}^i$, the state estimates are calculated and denoted as $\hat{\theta}^i$. Analogous to (4) and (7), the following active and reactive power measurement residuals can be formed to detect possible anomaly:

$$\begin{aligned} R_P^i &\triangleq \tilde{P}^i - H\hat{\theta}^i \\ R_Q^i &\triangleq \tilde{Q}^i(I_{\text{tl}}) - B\Big(-\mathbf{1} + \cos\big(A^T\hat{\theta}^i - B^{-1}R_P^i(I_{\text{tl}})\big)\Big) \\ &\text{for } i = 1,2,\ldots,N. \end{aligned} \tag{9}$$

For the attackers, in order to avoid any possible alarm triggering, a stealth attack $(\Delta P, \Delta Q)$ means that $R_P^i = 0$ and $R_Q^i = 0$ for all $i = 1,2,\ldots,N$. These define a system of nonlinear equations with unknown $(\Delta P, \Delta Q)$. The hope for the network operator is that, with N increasing, the system of equations eventually becomes insolvable. This is indeed the case, as the following statement states that with enough "independent" equations, attacks on transmission lines will be identified.

Proposition 2: Let θ^i, $i = 1,2,\ldots,N$ be any network states at different sampling instances, and let $k \in \{1,\ldots,m_a\}$. If $(A^T\theta^s)(k) \neq (A^T\theta^t)(k)$ for all $s \neq t$ and $N \geq 3$, then for any attack $(\Delta P, \Delta Q)$, stealth or not, the following holds:

$$\begin{aligned} & R_Q^i(k) = 0 \quad \forall\, i = 1,\ldots,N \\ \iff \quad & \Delta P(n+k) = 0 \quad \text{and} \quad \Delta Q(n+k) = 0. \end{aligned}$$

Proof: Let $\Delta P = Hc + Mb$. Repeated applications of Lemma 1 yields that $\hat{\theta}^i = \theta^i + c$ and $R_P^i = Mb$ for all i. Together with (6) and (2), $R_Q^i(k)$ becomes

$$\begin{aligned} R_Q^i(k) &= B(k,k)\Big(\cos\big((A^T\theta^i)\big)(k) - \cos\big((A^T\theta^i)(k) \\ &\quad + (A^Tc)(k) - \tfrac{1}{B(k,k)}(Mb)(n+k)\big)\Big) + \Delta Q(n+k) \\ &= B(k,k)\Big(\cos\big((A^T\theta^i)\big)(k) - \cos\big((A^T\theta^i)(k) \\ &\quad - \tfrac{1}{B(k,k)}\Delta P(n+k)\big)\Big) + \Delta Q(n+k), \end{aligned} \tag{10}$$

where $(A^Tc)(k) - \frac{1}{B(k,k)}(Mb)(n+k) = -\frac{1}{B(k,k)}\Delta P(n+k)$ is due to (5) and the definition of H in (1). Introduce notations $\alpha^i \triangleq (A^T\theta^i)(k)$, $\Delta p \triangleq \frac{1}{B(k,k)}\Delta P(n+k)$ and $\Delta q \triangleq \frac{1}{B(k,k)}\Delta Q(n+k)$, the condition that $R_Q^i(k) = 0$ for all i simplifies to

$$\cos(\alpha^i) - \cos(\alpha^i - \Delta p) + \Delta q = 0, \quad \forall\, i = 1,\ldots,N, \tag{11}$$

where Δp and Δq are the unknowns. Obviously, $\Delta p = 0$ and $\Delta q = 0$ satisfy (11). To complete the "$\Rightarrow$" part, it remains to show that $\Delta p = 0$ and $\Delta q = 0$ is the only solution to (11). This is equivalent to the condition that for all $\Delta p \neq 0$, the scalar-valued 2π-periodic function $g_{\Delta p}(x) \triangleq \cos(x) - \cos(x - \Delta p)$ intersects the functions of the form $h(x) = d$ at most at two ($< N$) different points, for all $d \in \mathbb{R}$. The above condition, in turn, is equivalent to the condition that the number of stationary points of $g_{\Delta p}$ (i.e., x_0 such that $\frac{dg_{\Delta p}}{dx}(x_0) = 0$) is at most two. It can be verified that the stationary points x_0 of $g_{\Delta p}$ satisfies $\tan(x_0) = \frac{\sin(\Delta p)}{\cos(\Delta p) - 1}$, as $\Delta p \neq 0$. Since the inverse image of $\tan(x)$ contains exactly two points for any x in its image, the number of stationary points of $g_{\Delta p}$ is at most two. Therefore, (11) cannot have any solution $(\Delta p, \Delta q)$ such that $\Delta p \neq 0$ (and hence $\Delta q \neq 0$). This completes the proof of the "$\Rightarrow$" part. The "$\Leftarrow$" part is a consequence of (10). This concludes the proof. ■

Remark 2: Precisely, independent equations means that $(A^T\theta^s)(k) \neq (A^T\theta^t)(k)$ for all $s \neq t$ and all $k \in \{1,\ldots,m_a\}$. That is, for every transmission line the phase angle difference at different sampling instances are different. □

Remark 3: While enough independent samples of R_Q^i enables the detection of transmission line attacks, this is not the case for R_P^i. If $\Delta P = Hc$ for some c, then the repeated applications of Lemma 1 implies that $R_P^i = 0$ for all i. Thus, one-shot stealth attack is possible even under varying states, given the "old" bad data detection scheme monitoring only $\tilde{P}$. □

In order to detect the presence of attack $(\Delta P, \Delta Q)$, an extra piece of information regarding possible attacks on the reactive power bus injection measurements (i.e., $Q(k)$ for $k \leq n$) is needed, in addition to R_P^i and R_Q^i defined in (9). Define $I_{\text{inj}} = \{1,\ldots,n\}$ as the index set containing the bus power injection measurements of $\tilde{Q}$ in (6). Then define

$$\begin{aligned} R_{Q\text{inj}}^i &\triangleq \tilde{Q}^i(I_{\text{inj}}) - |A|B\big(-\mathbf{1} + \cos(A^T\hat{\theta}^i)\big) \\ &= |A|B\big(\cos(A^T\theta^i) - \cos(A^T\hat{\theta}^i)\big) + \Delta Q(I_{\text{inj}}). \end{aligned} \tag{12}$$

Using R_P^i, R_Q^i in (9) and $R_{Q\text{inj}}^i$ in (12) for $i = 1,\ldots,N$ with $N \geq 3$, the presence of any possible attack $(\Delta P, \Delta Q)$ can be detected.

Corollary 2: If $N \geq 3$ and θ^i for $i = 1,2,\ldots,N$ are such that $(A^T\theta^s)(k) \neq (A^T\theta^t)(k)$ for all $s \neq t$ and all $k \in \{1,\ldots,m_a\}$, then $(\Delta P, \Delta Q) = 0$ if and only if $R_P^i = 0$, $R_Q^i = 0$ and $R_{Q\text{inj}}^i = 0$ for all $i = 1,2,\ldots,N$.

Proof: If $(\Delta P, \Delta Q) \neq 0$, then either $\Delta P \neq 0$ or $\Delta Q \neq 0$. First consider the case when $\Delta P \neq 0$. If $\Delta P \neq Hc$ for any c, then Lemma 1 implies that $R_P^i \neq 0$ for all i. On the other hand, if $\Delta P = Hc$ for some c, then the structure of H in (1) implies that $\Delta P(n+k) \neq 0$ for some $k \in \{1,\ldots,m_a\}$. Proposition 2 then implies that $R_Q^i \neq 0$ for some i.

Next, consider the case when $\Delta Q \neq 0$. If $\Delta Q(n+k) \neq 0$ for some $k \in \{1,\ldots,m_a\}$, then Proposition 2 implies that $R_Q^i \neq 0$ for some i. For the last piece of "if" part only two scenarios are left to consider: (a) $\Delta Q(k) \neq 0$ for some $k \leq n$ and $\Delta P \neq 0$, and (b) $\Delta Q(k) \neq 0$ for some $k \leq n$ and $\Delta P = 0$. In case (a), $\Delta P \neq 0$ is detected as argued above. In case (b), $\Delta P = 0$ implies that $\hat{\theta}^i = \theta^i$ for all i (cf. Lemma 1). Then (12) implies that $R_{Q\text{inj}}^i \neq 0$ for some i. This completes the proof of the "if" part. The proof of the "only if" part is a direct consequence of the definitions of R_P^i, R_Q^i and $R_{Q\text{inj}}^i$. ■

While Corollary 2 can be used to detect the presence of $(\Delta P, \Delta Q)$, Proposition 2 can identify where the transmission line measurements are attacked. However, the identification of attacked bus measurements remains not fully solved. In particular, only when $R_P^i = 0$ for all i can the presented result be useful. In this case, if a bus is not connected by any attacked transmission line(s), then the bus active power measurement is not attacked.

E. Motivation for Generalized Reactive Power Measurement Residual

Instead of R_Q^i, it is possible to define an alternative (and perhaps more intuitive) reactive power measurement residual $\bar{R}_Q^i$ as

$$\begin{aligned} \bar{R}_Q^i &\triangleq \tilde{Q}^i(I_{\text{tl}}) - B\big(-\mathbf{1} + \cos(A^T\hat{\theta}^i)\big) \\ &= \Delta Q(I_{\text{tl}}) + B\big(\cos(A^T\theta^i) - \cos(A^T\theta^i + A^Tc)\big). \end{aligned}$$

This is the exact analog of R_P^i. Under the assumptions of Proposition 2 (for all k), it is possible to derive that

$$\begin{aligned} &\big(\Delta Q(n+k), (A^Tc)(k)\big) = 0 \\ \iff\quad & R_P^i(n+k) = 0, \quad \bar{R}_Q^i(k) = 0 \quad \forall\, i,\, \forall\, k \in \{1,\ldots,m_a\}. \end{aligned} \tag{13}$$

The expression $\Delta P = Hc + Mb$ in (5) and the definition of H in (1) imply that $\Delta P(n+k) = -B(k,k)(A^Tc)(k) + (Mb)(n+k)$. Therefore, the statement in (13) in fact identifies whether the unobservable part of $\Delta P(I_{\text{tl}})$ is zero or not, without providing the exact value. In general, unless $\Delta P = Hc$ for some c, the unobservable part of $\Delta P(I_{\text{tl}})$ is not sparse even if ΔP is sparse. Consequently, (13) does not provide much information as to which entries of ΔP is nonzero. This is in contrast with Proposition 2 where the nonzero entries of $\Delta P(I_{\text{tl}})$ are identified directly. This is the motivation for the generalized reactive power measurement residual.

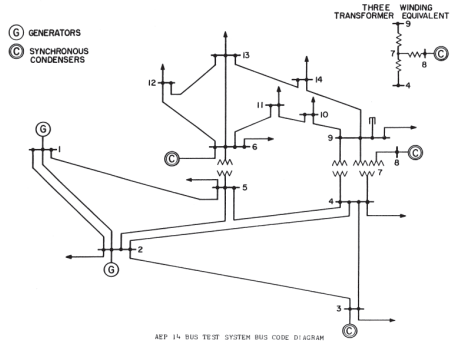

Fig. 1. IEEE 14-bus benchmark system.

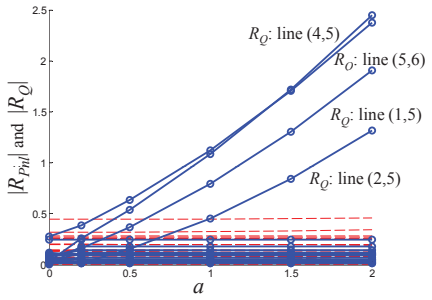

Fig. 2. Active and reactive power measurement residuals (R_{Pnl} and R_Q respectively) in the IEEE 14-bus benchmark system example. Red dashed line: R_{Pnl}. Blue solid line with circle markers: R_Q.

IV. Illustrative Numerical Example

In this section the attack identification in the IEEE 14-bus benchmark system in Fig. 1 is demonstrated. In this example, for each transmission line there is one pair of active and reactive power flow measurements. However, there is no power injection measurements. All active power measurements are corrupted by iid Gaussian noise whose standard derivation is 10% of the average of the magnitudes of the active power measurements. Similar iid Gaussian noise also corrupts the reactive power measurements.

A minimum cardinality stealth attack, as calculated using the method in [10], [12], targets the active power flow measurement between bus 2 and bus 5. Three other active power measurements incident to bus 5 are also attacked in order for the attack to be stealth. The stealth attack is of the form $\Delta P = \big(a|P(5)|\big)Hc$, where $a \geq 0$ is a scaling factor determining the magnitude of $\Delta P(5)$ relative to the absolute value of the true measurement $P(5)$ (when $a = 1/|P(5)|$, $\Delta P(5) = 1$). In this example, a takes the values of 0.2, 0.5, 1, 1.5 and 2 (i.e., attack magnitude up to 200% of $|P(5)|$). For each value of a, the noise and attack corrupted active power measurements $\tilde{P}$ are used to calculate the state estimate $\hat{\theta}$, then the nonlinear active power measurement residual $R_{Pnl} \triangleq \tilde{P} + B\sin(A^T\hat{\theta})$ are calculated. This is the the residual used by the bad data detection scheme in SCADA systems in practice. Also, the generalized reactive power measurement residuals R_Q, as defined in (7), are computed using R_{Pnl}. The residuals are plotted in Fig. 2. Relative to the vertical scale of Fig. 2, the entries of R_{Pnl} do not change too much for all values of a (i.e., the relative attack strength). On the other hand, four of the entries of R_Q are clearly increasing. Indeed, they correspond to the four measurements corrupted by the stealth attack.

V. Conclusions

The additional information provided by the reactive power measurements enables new possibilities to detect and identify cyber-attacks which are previously classified as stealth or unobservable. In particular, if the reactive power measurements cannot be corrupted, then arbitrary attack on the active power measurements can be detected by a test combining the standard active power measurement residual and the proposed generalized reactive power measurement residual in (7). In addition, attacks on transmission lines can be identified exactly. This is verified by a numerical example, even when the measurements are corrupted by noise of substantial strength. Even if the reactive power measurements can be corrupted, with enough (i.e., greater than two) independent samples of active and reactive power measurements, arbitrary one-shot attack on both active and reactive power measurements can still be detected and partially identified. Furthermore, the presented result also helps resolve the traditional problem of identifying multiple interacting bad data. However, open questions remain. For example, the identification of attacked buses is not fully understood.

References

[1] A. Abur and A. Expósito, *Power System State Estimation*. Marcel Dekker, Inc., 2004.

[2] A. Monticelli, *State Estimation in Electric Power Systems A Generalized Approach*. Kluwer Academic Publishers, 1999.

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

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

[5] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, 2011.

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

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

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

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

[10] K. Sou, H. Sandberg, and K. Johansson, "Electric power network security analysis via minimum cut relaxation," in *IEEE Conference on Decision and Control*, December 2011.

[11] ——, "Detection and identification of data attacks in power system," in *American Control Conference*, June 2012, [Online]. Available: http://www.ee.kth.se/~sou/papers/ssj+acc12.pdf, report version.

[12] J. Hendrickx, K. Johansson, R. Jungers, H. Sandberg, and K. Sou, "An exact solution to the power networks security index problem and its generalized min cut formulation," in *IEEE Conference on Decision and Control*, December 2012, submitted.