Data Attack Isolation in Power Networks Using Secure Voltage Magnitude Measurements

Kin Cheong Sou, Henrik Sandberg, and Karl Henrik Johansson

***Abstract*—In this paper a procedure to detect and isolate data attacks on power network power flow measurements is proposed. This method can be used in conjunction with available bad data detection (BDD) methods to isolate multiple bad data which are otherwise difficult to handle. The proposed procedure relies on secure measurements of bus voltage magnitudes to define a measurement residual using potentially compromised active and reactive power flow measurements on transmission lines. The proposed residual can be calculated in real-time. In addition, the component of the proposed residual on any particular line depends only locally on the component of the data attack on the same line. This makes the proposed residual well-suited for distributed data attack isolation in large-scale power networks. Furthermore, it can be shown that the proposed procedure becomes more effective when measurements from multiple time instances can be utilized. A detailed numerical case study on the IEEE 14-bus benchmark system demonstrates the effectiveness of the proposed procedure.**

***Index Terms*—Fault location, power network state estimation, security, wide-area protection.**

I. Introduction

THE PROPER operation of the electric power distribution and transmission systems is vital for our society. To supervise and control these systems the *Supervisory Control And Data Acquisition* (SCADA) systems are indispensable. Through remote terminal units (RTUs), SCADA systems measure data such as transmission line power flows, bus power injections, and part of the bus voltages. These measurements are then sent to the state estimator to estimate the power network states (e.g., the bus voltage phase angles and bus voltage magnitudes). The estimated states are used for important power network operations such as optimal power flow (OPF) dispatch and contingency analysis (CA) [1], [2]. Any malfunctioning of these operations can delay proper reactions in the control center, and lead to significant social and economical consequences such as the northeast US blackout of 2003 [3].

The SCADA systems of today are interconnected to office LANs, and through the LANs they are connected to the Internet. Hence, there are more access points to the SCADA systems, and also more functionalities to tamper with [4]. For example, the RTUs can be subjected to denial-of-service attacks. The communicated data can also be subjected to false data attacks. Furthermore, the SCADA master itself can be attacked. This paper focuses on the cyber security issues related to false data attacks, where the communicated measurements are subjected to additive data attacks. The motive of the data attack varies—the attacker might want to cause damage to the system, or he simply attacks for economic reasons (e.g., trying to mislead the utilities about his electricity usage). False data attacks have been the subject of considerable literature (e.g., [5]–[12]). Reference [5] was the first to point out that a coordinated intentional data attack can be staged without being detected by state estimation bad data detection (BDD) algorithm, which is a standard part of today's SCADA/EMS system [1], [2], [13]. References [5]–[7], [9]–[12] investigate the construction and impact assessment problem for such "unobservable" data attack, especially the sparse ones requiring relatively few meters to compromise.

Countermeasures against unobservable data attack have been studied. References [7], [8], [11], [12] consider the scenario where certain measurements are protected (i.e., cannot be corrupted). Procedures are proposed to plan the protection so that data attack can always be detected. Reference [9] considers data attack detection using extra information such as state statistical distribution. A generalized likelihood ratio test for attack detection is derived in [9]. In this paper, the goal is *data attack isolation*. This is one step beyond data attack detection, since it requires also that the exact location(s) of the compromised measurement(s) be identified. The proposed data attack isolation algorithm relies on some secure measurements, an assumption also made in [7], [8], [11], [12]. In particular, this paper assumes that the voltage magnitudes on the end buses of monitored transmission lines are securely measured and received by the network operator. Under this assumption, it is possible to define a *reactive power measurement residual vector*, one entry for each monitored line. Unlike the standard measurement residuals [1], [2], the proposed reactive power measurement residual vector has the advantage that each entry corresponding to a particular transmission line is a function of the data attack on the *same* line only, making it suitable to detect and isolate the data attack. In addition, the local nature of the proposed procedure means that it can be independently carried out in different parts of the network in a *distributed* fashion, enabling large-scale implementation. Furthermore, the computation requirement for the proposed data attack isolation procedure is similar to that of the standard BDD algorithm. It can be carried out in *real-time* without expensive computation. As shall be seen, the idea of the proposed procedure can be based on any measurement relationship. This means that the proposed procedure can be extended to

Manuscript received August 22, 2012; revised February 07, 2013, June 21, 2013; accepted August 21, 2013. Date of current version December 24, 2013. This work is supported by the European Commission through the HYCON2 project, the Swedish Research Council (VR) under Grant 2007-6350 and Grant 2009-4565, and the Knut and Alice Wallenberg Foundation. Paper no. TSG-00519-2012.

K. C. Sou was with KTH Royal Institute of Technology, 100 44 Stockholm, Sweden. He is now with the Department of Mathematical Sciences, Chalmers University of Technology, 412 96 Gothenberg, Sweden (e-mail: kincheong.sou@chalmers.se).

H. Sandberg and K. H. Johansson are with the ACCESS Linnaeus Center and the Automatic Control Lab, the School of Electrical Engineering, KTH Royal Institute of Technology, 100 44 Stockholm, Sweden (e-mail: hsan@kth.se; kallej@kth.se).

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

Digital Object Identifier 10.1109/TSG.2013.2280658

take advantage of emerging equipment such as phasor measurement unit (PMU) [14]. With advanced knowledge of the power network (i.e., full state information) the attacker can still stage an unobservable data attack, even if the proposed reactive power measurement residuals are examined. However, if the network operator can make use of *multiple* sets of reactive power measurements taken from different sampling time instances and the attacker can attack only once, then it becomes much more difficult to stage unobservable attacks as we will show in the paper.

The proposed procedure can detect and isolate measurement bad data (e.g., random gross error due to meter failure), as if it were data attack. Standard techniques for detecting and isolating bad data include the χ^2 test and the largest normalized residual test [1]. These methods utilize the system-wide measurement information (i.e., all available power flow and injection measurements), and in practice the largest normalized residual test performs well in isolating some random bad data (especially single bad data). However, the reliance on system-wide information can be a drawback, because the procedure can be subject to simultaneous bad data or data attacks as demonstrated in [5]–[7], [9]–[12]. In addition, it is well-known that the largest normalized residual test cannot isolate multiple interacting conforming bad data ([1, Ch. 5]. The proposed procedure, on the other hand, is opposite to the existing methods regarding the scale of information use. It utilizes only local transmission line and bus measurements, and attempts to isolate the bad data locally. As shall be seen, this strategy can be complementary to the existing methods in that it can isolate part of the multiple bad data that are otherwise not detectable by the existing methods. Among the more recent work, of particular relevance are methods for isolating multiple interacting conforming bad data (e.g., [15]–[20]). However, the current work is different. It aims at an easy-to-implement procedure that isolates part of the bad data (i.e., only the bad data on transmission lines). For each transmission line, the online computation requirement for the proposed scheme includes only the evaluation of a simple scalar trigonometric function and a comparison of two scalars. On the other hand, the previous work attempts to isolate general bad data with more expensive centralized computations. For instance, [15], [16] require solving integer programming problems and [17], [18], [20] involve solving linear programming problems. Furthermore, even in the case without measurement noise (a typical situation considered in BDD analysis), the previous methods can result in bad data vector estimates which are not the true ones. Contrary to this, even though the proposed method is not expected to find all bad data, the ones isolated are guaranteed to be bad data in the noiseless case.

Outline: Section II describes the model for BDD and states the key assumptions of this paper. The problem considered is also described. In Section III the proposed solution is described in detail. Section IV describes an extension to improve the effectiveness of the proposed solution. Section V demonstrates the proposed solution with a case study.

II. Model, Assumption, and Problem Statement

A. Standard BDD and Its Limitations

Let us briefly describe the basics of BDD. The states of a power network contain two groups: a) bus voltage phase angles denoted by a vector θ and b) bus voltage magnitudes denoted by a vector v. It is assumed that one of the buses is a reference, and the corresponding voltage phase angle is zero. To estimate the states two types of power measurements are available: a) active power measurements (flows on transmission lines and injections at buses) denoted by a vector $\tilde{P}$ and b) reactive power measurements (flows on transmission lines and injections at buses) denoted by a vector $\tilde{Q}$. In general, a linearized model relating the states and the measurements is sufficient to analyze state estimation and the subsequent BDD. Let x denote the state deviation from the linearization expansion point. The vector of linearized measurement deviations, denoted z, can be expressed in

$$z = Hx + \Delta z, \tag{1}$$

where H is the Jacobian of the measurement function, and Δz is a vector of bad data or data attack. From (1), a weighted least squares problem [1, (5.2)] is solved to obtain the state estimate as $\hat{x} = \left(H^T W H\right)^{-1} H^T W z$, where W is a positive definite diagonal weighting matrix, whose entries are typically the reciprocals of the variance of the measurement noise. To detect possible anomaly in the measurements, the following measurement residual vector is formed

$$R_z = z - H\hat{x} = (I - H(H^T W H)^{-1} H^T W)\Delta z. \tag{2}$$

In a typical BDD algorithm, if $\|R_z\|$ (vector 2-norm for instance) is too large then an alarm is sounded. This standard BDD algorithm performs reasonably well when detecting single random measurement errors. However, it can fail in face of a malicious coordinated data attack on multiple measurements. This observation was first reported in [5]. In particular, [5] investigated additive data attack of the form $\Delta z = Hc$, for some vector c. Then (2) implies that $R_z = 0$. Hence, data attack of the form $\Delta z = Hc$ can pass BDD test, and is referred to as *unobservable data attack* [9], [11] (also known as false data injection attack [5], stealth attack [6], [21], etc.).

B. Measurement Model With Known Voltage Magnitudes

The unobservable data attack poses a fundamental limitation to the standard BDD algorithm. To overcome this limitation a change of the standard BDD practice is proposed in this paper. As the level of penetration of distributed power generation increases, local control of voltage magnitudes [e.g., automatic voltage regulator (AVR)] becomes more common [22]–[25]. This makes it difficult to tamper with the voltage magnitude measurements because they are closely monitored. In addition, end-to-end authentication [26] can provide measurement communication security so that the communicated measurements cannot be compromised. In this paper, we follow these trends and make the assumption that the voltage magnitudes on some buses are known to the network operator. This paper focuses on the transmission lines where the voltage magnitudes at the two end buses are known. In the sequel, let k and m denote the two end buses of such a transmission line, and let v_k and v_m denote their bus voltage magnitudes, respectively. In fact, to simplify the presentation it is further assumed that

$$v_k = v_m = 1. \tag{3}$$

This coincides with the well-established DC power flow assumption [1], [2]. Furthermore, in Section III-H it will be seen that the assumption in (3) is not more restrictive than the one that both v_k and v_m are known (but not necessarily fixed at unity). The immediate consequence of (3) is that the phase angle θ_{km} is the only unknown state related quantity in the expression of transmission line power flow. The active power flow measurement can be well approximated by a linear function:

$$\tilde{P}_{km} = -b_{km}\theta_{km} + \Delta P_{km}, \tag{4}$$

where b_{km} is the series susceptance of the transmission line and assumed to be nonzero. ΔP_{km} is the active power measurement error. The symbol θ_{km} denotes $\theta_k - \theta_m$, and $\theta_{km} \in \Theta_{km} \subset [-\pi, \pi)$. The expression in (4) is an approximation of the true nonlinear relation

$$\tilde{P}_{km,\text{true}} = g_{km}(1 - \cos(\theta_{km})) - b_{km}\sin(\theta_{km}) + \Delta P_{km}, \tag{5}$$

where g_{km} is the series conductance of the transmission line. In this paper, the reactive power flow measurement (as a function of phase angle difference θ_{km}) is considered to be nonlinear, as the linearization is inaccurate:

$$\tilde{Q}_{km} = b_{km}(-1 + \cos(\theta_{km})) - g_{km}\sin(\theta_{km}) + \Delta Q_{km}, \tag{6}$$

where ΔQ_{km} is the reactive power measurement error. In (6), the shunt elements of the transmission line are ignored. The exact expressions for the power injection measurements are omitted as they are not relevant to the discussion in this paper.

C. Problem Statement

The measurement errors ΔP_{km} and ΔQ_{km} typically contain two parts: a) a gross error due to data attack or bad data, and b) a random measurement noise. The data attack isolation problem in this paper aims to determine whether or not the data gross error parts of ΔP_{km} and ΔQ_{km} are zero in the power flow measurements in (4) and (6), for each transmission line km where v_k and v_m satisfy (3) (or simply that both v_k and v_m are known). The required information for the proposed procedure includes power flow measurements $\tilde{P}_{km}$ and $\tilde{Q}_{km}$, the measurement models (4) and (6) and the assumed knowledge of voltage magnitudes in (3).

III. Data Attack Isolation Using Reactive Power Measurement Residual

A. Reactive Power Measurement Residual

The proposed data attack isolation procedure is similar to the standard residual-based BDD check, except that the residual is defined differently. In particular, the following reactive power measurement residual is proposed:

$$R_{Q_{km}} \triangleq \tilde{Q}_{km} - b_{km}\left(-1 + \cos\left(-b_{km}^{-1}\tilde{P}_{km}\right)\right) + g_{km}\sin\left(-b_{km}^{-1}\tilde{P}_{km}\right). \tag{7}$$

$R_{Q_{km}}$ is calculated based on known information: active power measurement $\tilde{P}_{km}$, reactive power measurement $\tilde{Q}_{km}$ and line physical properties b_{km} and g_{km}. To motivate the definition in (7), substitute (4) and (6) into (7) and this yields

$$\begin{aligned} R_{Q_{km}} = {} & b_{km}\left(\cos(\theta_{km}) - \cos\left(\theta_{km} - b_{km}^{-1}\Delta P_{km}\right)\right) \\ & - g_{km}\left(\sin(\theta_{km}) - \sin\left(\theta_{km} - b_{km}^{-1}\Delta P_{km}\right)\right) \\ & + \Delta Q_{km}. \end{aligned} \tag{8}$$

This means that for the proposed residual the measurement error dependency is *local* since $R_{Q_{km}}$ depends on ΔP_{km} and ΔQ_{km} but not on the data attack on any other measurements. This enables data attack isolation. In contrast, for the standard measurement residual R_z in (2) data attack dependency is not local, as the residual sensitivity matrix $I - H(H^T W H)^{-1} H^T W$ is typically full. $R_{Q_{km}}$ also depends on the phase angle difference θ_{km}, and this dependency will be explained subsequently. The line properties b_{km} and g_{km} are given throughout this paper. To simplify the notion, in the subsequent discussions the expressions for (7) and (8) will be simplified: The subscripts "km" will be dropped and the phase angle difference will be denoted α. That is, (7) simplifies to

$$R_Q = \tilde{Q} - b(-1 + \cos(-b^{-1}\tilde{P})) + g\sin(-b^{-1}\tilde{P}), \tag{9}$$

and (8) simplifies to

$$\begin{aligned} R_Q = {} & b(\cos(\alpha) - \cos(\alpha - b^{-1}\Delta P)) \\ & - g(\sin(\alpha) - \sin(\alpha - b^{-1}\Delta P)) + \Delta Q. \end{aligned} \tag{10}$$

Regardless of the value of α, R_Q is zero when both ΔP and ΔQ are zero. Conversely, R_Q is with probability one nonzero if ΔP and ΔQ are random with continuous probability distributions. Fig. 1 shows the absolute value of R_Q as a function of ΔP, for some typical settings with $b = -60$ p.u., $g = 2$ p.u., and α taking values of 0, 10, and 20 degrees (about 0, 0.17, 0.35 in radians, respectively). In Fig. 1 the attack strength is presented in "equivalent phase angle" $b^{-1}\Delta P$, whose unit is degrees (or radians). The dependency of R_Q on ΔQ is linear and it is not shown. Fig. 1 demonstrates that R_Q is a reasonable indicator of ΔP (R_Q is also a good indicator of ΔQ because of the linear dependency). However, R_Q is not perfect. Certain nonzero values of ΔP and ΔQ can make R_Q zero or very small. Nevertheless, the quality of R_Q as a data attack indicator can be improved if more samples of the line power flow measurements are available. This will be explained in Section IV.

B. Data Attack Isolation Using Reactive Power Residual R_Q

If the purpose of data attack isolation is simply to determine whether $\Delta P = 0$ and $\Delta Q = 0$ or not, the data attack alarm should be sounded for transmission line km whenever $|R_Q| > 0$. However, in practice both ΔP and ΔQ are corrupted by noise. Therefore, the data attack alarm should be sounded whenever $|R_Q| > r$ for some appropriately chosen threshold r. The choice of r and the associated analysis are studied in sequel. In general, the active power measurement error is the sum of two parts:

$$\Delta P = a_P + e_P, \tag{11}$$

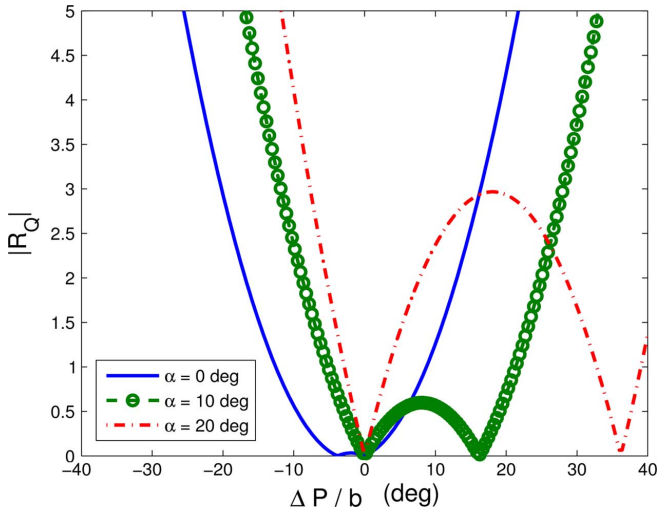

Fig. 1. Reactive power measurement residual in absolute value $|R_Q|$ as a function of active power measurement error ΔP.

where a_P represents gross error due to data attack or bad data, and e_P represents measurement noise which is assumed to be a Gaussian random variable with zero mean and known variance (i.e., $e_P \sim \mathcal{N}(0, \sigma_P^2)$). Similarly, the reactive power measurement error ΔQ is

$$\Delta Q = a_Q + e_Q \tag{12}$$

with $e_Q \sim \mathcal{N}(0, \sigma_Q^2)$. Substituting (11) and (12) into (10) implies that R_Q is a random variable whose distribution is a nonlinear function of a_P, a_Q and α. Therefore, a statistical approach should be used to determine the decision threshold r for sounding the alarm. This paper investigates the use of hypothesis testing (e.g., [27]). In the hypothesis testing, the test statistics is the residual R_Q. The null hypothesis is that there is no data attack (i.e., $a_P = 0$, $a_Q = 0$, and α is between its allowable limits). The decision threshold r is a function of the significance level β. β is defined to be the maximum probability, over all possible distributions under the null hypothesis, such that $|R_Q| > r$. This is the worst case false alarm probability. Once r is determined, it is also necessary to compute the probability that $|R_Q| > r$ when the null hypothesis is not true. It is the probability of correctly sounding the alarm when there is an attack, and this probability is known as the power of the test associated with r. In summary, it is important to calculate the probability $\Pr(|R_Q| > r)$.

C. Bounding the Probability $\Pr(|R_Q| > r)$

Because of the trigonometric terms in (10), $\Pr(|R_Q| > r)$ is difficult to characterize exactly. However, it can be bounded:

Proposition 3.1: For any given a_P, a_Q and α, define B as

$$B = b(\cos(\alpha) - \cos(\alpha - b^{-1}a_P)) - g(\sin(\alpha) - \sin(\alpha - b^{-1}a_P)) + a_Q. \tag{13}$$

Let X be a random variable such that

$$X = -(b\sin(\alpha - b^{-1}a_P) + g\cos(\alpha - b^{-1}a_P)) \times (b^{-1}e_P) + e_Q + B. \tag{14}$$

Let Y be a random variable such that

$$\begin{aligned} Y = {} & (b\sin(\alpha - b^{-1}a_P) + g\cos(\alpha - b^{-1}a_P)) \\ & \times \left(\frac{1}{3!}(b^{-1}e_P)^3 - \frac{1}{5!}(b^{-1}e_P)^5 + \dots\right) \\ & + \left(b\cos(\alpha - b^{-1}a_P) - g\sin(\alpha - b^{-1}a_P)\right) \\ & \times \left(\frac{1}{2!}(b^{-1}e_P)^2 - \frac{1}{4!}(b^{-1}e_P)^4 + \dots\right), \end{aligned} \tag{15}$$

where "..." above means the pattens follow indefinitely. Denote m_Y and σ_Y as the expected value and standard deviation (i.e., the square root of variance) of Y, respectively. Then for all $s \geq 0$ and $k > 0$, it holds that

$$\Pr(|R_Q| > s) \leq \Pr(|X| > s - |m_Y| - k\sigma_Y) + \frac{1}{k^2}, \tag{16a}$$

$$\Pr(|R_Q| > s) \geq \Pr(|X| > s + |m_Y| + k\sigma_Y) - \frac{1}{k^2}. \tag{16b}$$

Proof: See Appendix. ∎

Proposition 3.1 provides the lower and upper bounds for the difficult-to-compute probability $\Pr(|R_Q| > r)$ (with r substituting s in the statement). In fact, R_Q is expanded into the sum of X and Y which respectively correspond to the linear and higher order terms of a Taylor series expansion of R_Q with respect to e_P. The bounds make use of the probability distribution of X which is Gaussian (because e_P is), but only the first and second order statistics of Y are used. Intuitively, some information of the higher order terms Y can be ignored because the measurement noise e_P is typically "small" (i.e., having small variance).

B defined in (13) can be regarded as a version of the reactive power measurement residual which is due to gross error a_P and a_Q. Comparing (10) and (13), B is simply R_Q when ΔP and ΔQ contain only their respective gross error components a_P and a_Q.

D. Computing Decision Threshold r

The probability upper bound in (16a) can be used to compute an upper bound for the decision threshold r, for any given significance level $\beta \in [0, 1]$. The following statement provides the basis.

Proposition 3.2: Let a_P, a_Q, α be given. Let X be defined in (14). Then $X \sim \mathcal{N}(B, \sigma_X^2)$ with B defined in (13) and σ_X^2 defined as

$$\sigma_X^2 = (b\sin(\alpha - b^{-1}a_P) + g\cos(\alpha - b^{-1}a_P))^2 b^{-2}\sigma_P^2 + \sigma_Q^2. \tag{17}$$

Also, let m_Y and σ_Y be the expected value and standard deviation of Y in (15), respectively. Let $\Phi^{-1}(\cdot)$ denote the inverse of the cumulative distribution function of the standard Gaussian distribution. For any given $\beta \in [0, 1]$ and $k > 0$ such that $\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right) \leq 1$, if s satisfies

$$s > \sigma_X \Phi^{-1}\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right) + |B| + |m_Y| + k\sigma_Y, \tag{18}$$

then $\Pr(|R_Q| > s) < \beta$.

Proof: See Appendix. ∎

To find the hypothesis testing decision threshold r, (18) is applied to the case of the null hypothesis (i.e., $a_P = 0$, $a_Q = 0$, but α can vary in its range denoted as Θ_{km}). Under the null hypothesis, B is always zero regardless of the value of α. To ensure that a given significance level β is observed (i.e., worst case false alarm probability over all $\alpha \in \Theta_{km}$ is less than β), r can be chosen, for any $k > 0$ such that $\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right) \leq 1$, as

$$r = \bar{\sigma}_X \Phi^{-1}\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right) + \max_{\substack{\alpha \in \Theta_{km}, \\ a_P = 0, a_Q = 0}} \{|m_Y| + k\sigma_Y\}, \tag{19}$$

where

$$\bar{\sigma}_X \triangleq \max_{\substack{\alpha \in \Theta_{km}, \\ a_P = 0, a_Q = 0}} \sigma_X \tag{20}$$

was defined for notational convenience. The threshold r defined in (19) is a function of β and k, when the network properties b, g and Θ_{km} are given. In principle, the expression for r in (19) can be minimized with respect to k. However, in typical situations the term $\Phi^{-1}\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right)$ in (19) is on the order of unity. For instance, when $\beta = 0.05$ and $k = 20$, then $\Phi^{-1}\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right) \approx 1.98$. If in addition

$$\bar{\sigma}_X \gg \max_{\substack{\alpha \in \Theta_{km}, \\ a_P = 0, a_Q = 0}} \{|m_Y| + k\sigma_Y\}, \tag{21}$$

then the decision threshold r can be well approximated as

$$r \approx \bar{\sigma}_X \Phi^{-1}\left(1 - \frac{\beta}{2} + \frac{1}{2k^2}\right), \tag{22}$$

where k is as large as possible (so that r is least conservative), provided that (21) is still valid. The following statement provides a simple criterion to check whether (21) is justified, based on $|b|^{-1}\sigma_P$ and $|b|^{-1}\sigma_Q$:

Proposition 3.3: Let $\bar{\sigma}_X$ be defined by (20) and (17). Then with $c \triangleq \max_{\alpha \in \Theta_{km}} |\sin(\alpha) + (g/b)\cos(\alpha)|$, it holds that

$$\bar{\sigma}_X = \sqrt{c^2\sigma_P^2 + \sigma_Q^2}. \tag{23}$$

In addition, assume that $|b| > |g|$ and $|b|^{-1}\sigma_P < 1$. Define $\epsilon > 0$ by $\frac{1}{1 - b^{-2}\sigma_P^2} = 1 + \epsilon$. Then

$$\begin{aligned} |m_Y| &\leq (1+\epsilon)(|b|^{-1}\sigma_P^2), \\ \sigma_Y &\leq 2(1+\epsilon)\left(|b|^{-1}\sigma_P^2\right). \end{aligned} \tag{24}$$

Consequently, the following inequalities hold:

$$\begin{aligned} \frac{\bar{\sigma}_X}{|m_Y|} &\geq \frac{1}{(1+\epsilon)}\sqrt{c^2\frac{1}{\left(|b|^{-1}\sigma_P\right)^2} + \frac{\left(|b|^{-1}\sigma_Q\right)^2}{\left(|b|^{-1}\sigma_P\right)^4}}, \\ \frac{\bar{\sigma}_X}{\sigma_Y} &\geq \frac{1}{2(1+\epsilon)}\sqrt{c^2\frac{1}{\left(|b|^{-1}\sigma_P\right)^2} + \frac{\left(|b|^{-1}\sigma_Q\right)^2}{\left(|b|^{-1}\sigma_P\right)^4}}. \end{aligned} \tag{25}$$

Proof: See Appendix. ∎

A consequence of Proposition 3.3 is that if $|b|^{-1}\sigma_P \ll 1$ and $|b|^{-1}\sigma_Q \ll 1$, then (25) implies that (21) holds for relatively large k. This in turn implies that the decision threshold r can be approximately found by (22). In a typical setting, $b = -60$ p.u., $g = 2$ p.u., Θ_{km} range between -20 and $+20$ degrees, $\sigma_P^2 \leq |b|/1000$ p.u. and $\sigma_Q^2 \leq |b|/1000$ p.u. ([2, Ch. 8] examples). Then both $|b|^{-1}\sigma_P$ and $|b|^{-1}\sigma_Q$ are less than 0.042, and according to (25) the ratios $\bar{\sigma}_X/|m_Y|$ and $\bar{\sigma}_X/\sigma_Y$ are at least 100.

E. Simplified Analysis of the Probability $\Pr(|R_Q| > r)$

Assume that $k \gg 1$ and $r \gg |m_Y| + k\sigma_Y$. This can be the case, for instance, resulting from the fact that (21) holds and r is defined through (19) or (22). Then applying the probability bounds in (16a) and (16b) with r replacing s yields

$$\Pr(|R_Q| > r) \approx \Pr(|X| > r). \tag{26}$$

It is more convenient to characterize the probability $\Pr(|X| > r)$ because $X \sim \mathcal{N}(B, \sigma_X^2)$. Indeed,

$$\begin{aligned} &\Pr(|X| > r) \\ &\quad = \Pr\left(\sigma_X^{-1}\left|(X - B) + B\right| > \sigma_X^{-1} r\right) \\ &\quad = \Phi\left(-\sigma_X^{-1}(r - B)\right) + \Phi\left(-\sigma_X^{-1}(r + B)\right). \end{aligned} \tag{27}$$

For a given r, $\Pr(|X| > r)$ is a function of B and σ_X, which in turn are functions of a_P, a_Q and α. $|B|$ indicates the strength of the data attack. When $B = 0$ (e.g., when $a_P = 0$ and $a_Q = 0$), $\Pr(|R_Q| > r) \approx 2\Phi(-\sigma_X^{-1} r) \leq \beta$. This corresponds to the significance level β, the false alarm probability under the null hypothesis. When $|B|$ increases (as $|a_P|$ and $|a_Q|$ increase), $\Pr(|R_Q| > r)$ increases as well. This agrees with the intuition that a more aggressive data attack (as measured by $|B|$) leads to a higher probability for alarm. On the other hand, when σ_X decreases, the decision becomes more sensitive to $|B|$ and r. This also agrees with the intuition. With more accurate measurements, it becomes less ambiguous to decide whether or not to sound the alarm.

For a numerical illustration, consider the example situation in the end of Section III-D. Let (22) be used to determine r with $\beta = 0.05$ and $k = 20$. Also, let $\sigma_P^2 = \frac{1}{1000}|b|$ and $\sigma_Q^2 = \frac{1}{1000}|b|$. Fig. 2 (blue dashed line) shows the probability $\Pr(|X| > r)$ as a function of a_P when $a_Q = 0$ and $\alpha = 10$ degrees. The green solid line shows the value of B indicating that $\Pr(|X| > r)$ correlates with $|B|$. Another scenario with less significant noise is also considered ($\sigma_P^2 = \frac{1}{10\,000}|b|$ and $\sigma_Q^2 = \frac{1}{10\,000}|b|$). The corresponding $\Pr(|X| > r)$ value is plotted as the blue solid line with square markers. This indicates a more sensitive decision rule, demonstrating the effect of σ_X. Finally, in Fig. 2 the red circles correspond to empirical values of $\Pr(|R_Q| > r)$ (red circles) obtained through Monte Carlo simulation with 10^6 samples for each selected value of a_P, for the large σ_X case. Note that in Fig. 2 the theoretical model is close to the empirical results.

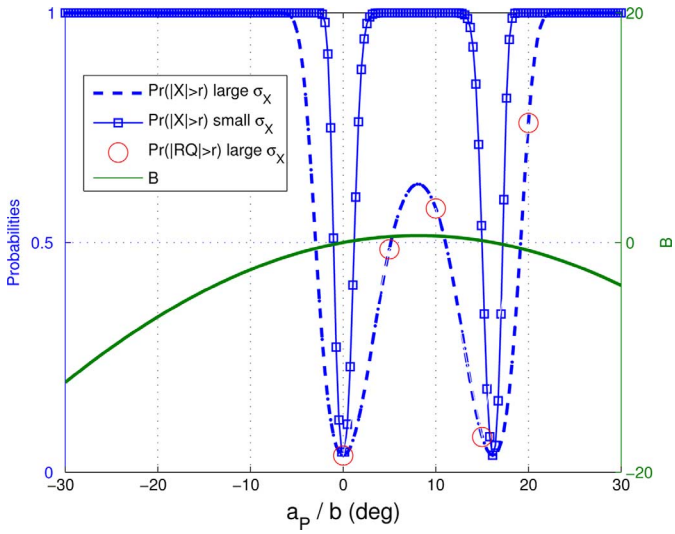

Fig. 2. The probability $\Pr(|X| > r)$ for two cases with different intensity of the measurement noise σ_X. Also plotted is the data attack indicator B and some empirical values of $\Pr(|R_Q| > r)$ based on Monte Carlo simulation.

F. Summary of Data Attack Isolation Procedure

When $|b|^{-1}\sigma_P \ll 1$ and $|b|^{-1}\sigma_Q \ll 1$, the proposed hypothesis testing based data attack isolation approach for any particular transmission line satisfying (3) is as follows:

1) Calculate $\bar{\sigma}_X$ according to (20) and (17).
2) Choose significance level β (e.g., $\beta = 0.05$). Use (25) to determine the largest possible k such that (21) holds.
3) Define decision threshold r based on (22).
4) Form reactive power measurement residual R_Q according to (9).
5) Hypothesis testing: sound BDD alarm if and only if $|R_Q| > r$.

G. Data Attack Isolation Using Secure PMU Measurements

The data attack isolation procedure presented in this section is one of the many ways to utilize the power flow equations

$$\begin{aligned}\tilde{P}_{km,v\theta} &= -v_k v_m b_{km}\theta_{km} + \Delta P_{km},\\ \tilde{Q}_{km,v\theta} &= -v_k^2 b_{km} - v_k v_m (g_{km}\sin(\theta_{km})\\ &\quad - b_{km}\cos(\theta_{km})) + \Delta Q_{km}\end{aligned} \tag{28}$$

and locally available secure information. Specifically, the previous discussions assume that $v_k = v_m = 1$. From (28) the unknown θ_{km} is eliminated and a statistics containing ΔP_{km} and ΔQ_{km} is obtained and analyzed. Now suppose θ_{km} is also available from secure PMU then more options for error statistics are possible. For example, the assumption that both v_k and v_m are known can be relaxed. Alternatively, two statistics, each linearly depending only on ΔP_{km} or ΔQ_{km}, can be formed from (28). This provides a framework to incorporate emerging equipment such as PMU into the legacy measurement system to improve its data attack isolation capability.

H. Discussion on the Voltage Magnitude Assumption in (3)

The assumption in (3) (i.e., $v_k = v_m = 1$) is not more restrictive than the assumption that both v_k and v_m are known. Indeed, the procedure to eliminate the unknown variable in (28) can be proceeded as long as v_k and v_m are known—they do not need to be fixed at unity.

In practice voltage magnitude sensors have finite precision. Therefore, it is necessary to analyze the reactive power measurement residual when $v_k = 1+\varepsilon_k$ and $v_m = 1+\varepsilon_m$, where ε_k and ε_m represent small but nonzero measurement mismatches. For simplicity, consider the noiseless case where $\Delta P = a_P$ in (11) and $\Delta Q = a_Q$ in (12). Then, with the imperfect v_k and v_m substituted in (28), the expression for the reactive power measurement residual R_Q becomes

$$R_Q = B + E(\varepsilon_k, \varepsilon_m, \alpha) + O((\max\{\varepsilon_k, \varepsilon_m\})^2 b), \tag{29}$$

where B is defined in (13) and the dominating part of the error term, denoted $E = E(\varepsilon_k, \varepsilon_m, \alpha)$, can be expressed in

$$E = (\varepsilon_k + \varepsilon_m)(b(-1+\cos(\alpha)) - g\sin(\alpha)) + b(\varepsilon_m - \varepsilon_k).$$

For normal network operation the phase angle difference is small (i.e., $\alpha \approx 0$). Hence,

$$E \approx b(\varepsilon_m - \varepsilon_k). \tag{30}$$

The expression in (29) means that there is a component E in R_Q unrelated to the data attack (the data attack is represented in B). E represents the inaccuracy due to imperfect voltage magnitude information. In addition, to maintain the desired false alarm rate in face of E, the decision threshold r defined in Section III-D should be increased. The amount of increase should be comparable to the value in (30). The increase in the decision threshold decreases the power (i.e., the probability for data attack detection) of the proposed procedure. For example, consider the previous numerical illustration with the additional condition that v_k and v_m are not precisely known. Let $\varepsilon_m - \varepsilon_k = 0.01$ (i.e., 1% of nominal voltage magnitude). The residuals with imperfect voltage magnitudes and the increased threshold are illustrated in Fig. 3. In summary, the imperfect information of voltage magnitudes results in inaccuracy of R_Q and increased decision threshold r, both undesirable from the viewpoint of the proposed bad data isolation scheme. This motivates the assumption in (3) to have very accurate voltage magnitude measurements. On the other hand, for attacks with larger magnitudes $|B|$ is typically larger (see Fig. 3) and the effect due to E becomes less significant. In another situation, if ε_k and ε_m appear as unknown but uniform biases, then the effect of the voltage magnitude mismatch is expected to be insignificant since $E = 0$. Finally, notice that the effect of the mismatch is local since the residual is based entirely on local measurement information.

IV. Improved Data Attack Isolation Using Residuals at Multiple Time Instances

The analysis in Section III-E [particularly (27)] indicates that if $|B|$ is small, then the probability of alarm $\Pr(|R_Q| > r) \approx \Pr(|X| > r)$ would be small. Therefore, to avoid detection the attacker could manipulate a_P and a_Q so that B is set to zero (i.e., minimizing $\Pr(|X| > r)$ with respect to B). To counter this, it is proposed in this paper that the network operator should utilize reactive power measurement residuals due to independent measurements from *multiple time instances*. In particular, let N be the number of time instances when the measurements are available. For time instance index $t = 1, 2, \ldots, N$, let $\tilde{P}^t$ be the

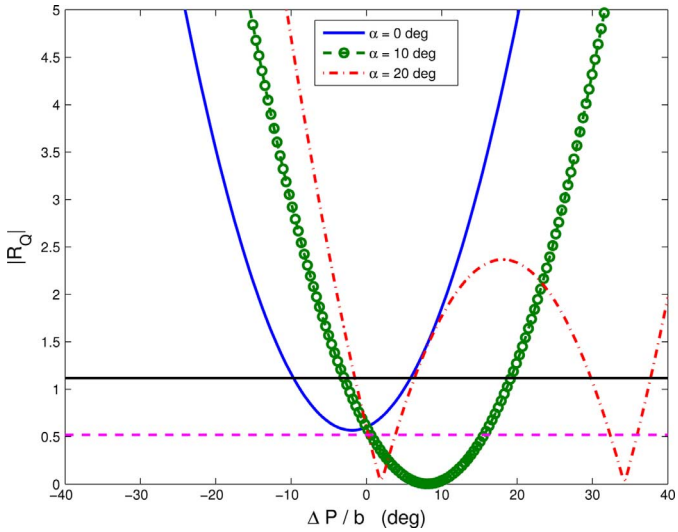

Fig. 3. Reactive power measurement residuals calculated with imperfect voltage magnitudes (i.e., through (29)). Magenta dashed line is the decision threshold with perfect voltage magnitudes. Black solid line is the increased decision threshold taking into account the imperfect voltage magnitudes.

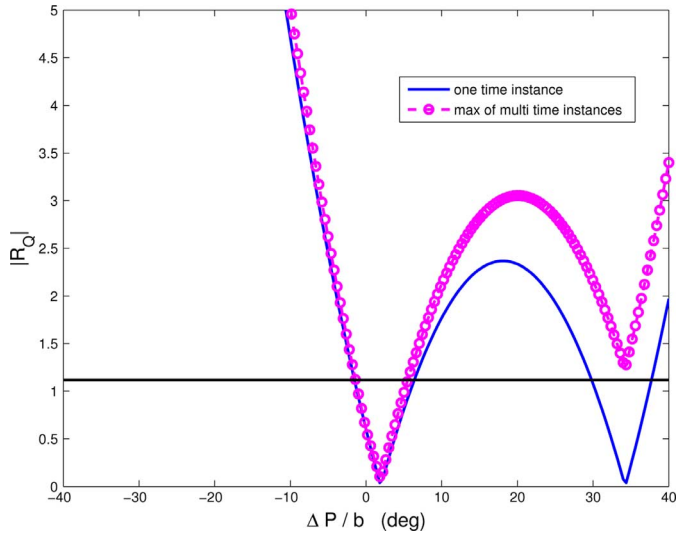

Fig. 4. Reactive power measurement residuals calculated with the measurement at one time instance and the maximum residual calculated with measurements at multiple time instances.

vectors of available active power measurements for the corresponding time instances. Similarly, for the considered transmission line, let α^t and $\tilde{Q}^t$ be the quantities defined in Section III for time instance index t. The improved data attack isolation scheme basically follows the procedure in Section III-F with the exception in step 4) and 5): Multiple reactive power measurement residuals are formed

$$R_Q^t \triangleq \tilde{Q}^t - b(-1+\cos(-b^{-1}\tilde{P}^t)) + g\sin(-b^{-1}\tilde{P}^t), \quad \forall t = 1,2,\ldots,N.$$

The alarm is sounded if

$$\max_{t=1,2,\ldots,N} \{|R_Q^t|\} > r. \tag{31}$$

As discussed earlier, the attackers' goal is to make a nontrivial choice of a_P and a_Q (i.e., $(a_P, a_Q) \neq 0$ and $|a_P|$ and $|a_Q|$ are reasonably small) to satisfy

$$B(\alpha^t, a_P, a_Q) = 0 \quad \forall t = 1,2,\ldots,N, \tag{32}$$

where B (defined in (13)) is treated as a function of α and a_P and a_Q. The network operator's hope is that if N is large enough it becomes impossible to satisfy (32) for any reasonable choice of (a_P, a_Q). This is indeed true, as formalized by the following statement:

Proposition 4.1: If $N \geq 3$, then for any $(\alpha^1, \alpha^2, \ldots, \alpha^N) \in [-\pi, \pi)^N$ such that $\alpha^t \neq \alpha^s$ for $t \neq s$, there does not exist $(a_P, a_Q) \neq 0$ with $|b^{-1}a_P| \leq \pi$ such that (32) is satisfied.

Proof: See Appendix. ■

To demonstrate the benefit offered by utilizing the measurements from multiple time instances, the residual corresponding to $\alpha = 20$ degrees in Fig. 3 is revisited. Here it is assumed that in addition to having the measurement for $\alpha = 20$ degrees, four measurements corresponding to 90%, 95%, 105%, and 110% of this value of α are available. Fig. 4 shows the proposed residual calculated using one measurement and the time-maximum residual in (31). While the data attack can still be missed if ΔP is too small in amplitude, the improved time-maximum residual consistently detects the presence of ΔP when it becomes larger. In particular, it no longer misses the alarm when $\Delta P/b$ is about 35 degrees, as in the original case.

V. Numerical Case Study

In this section the data attack isolation in the IEEE 14-bus benchmark system [28] in Fig. 5 is demonstrated. In this example, the values of the series susceptance and conductance of the transmission lines, the generator supplies, bus loads, and bus voltages (both magnitude and phase angle) are from [28], [29]. However, the line charging and tap ratio of the lines and the shunt susceptance of the buses are removed. This is to ensure that the power measurement expressions in (28) and (33) are sufficiently accurate. Nevertheless, as noted in Section III-G, the idea of the proposed method can be applied to handle the case where the power flow measurements are not truly represented by (28) or (33).

In this example, the active and reactive power injections at the following seven buses are measured: 1, 4, 5, 7, 8, 10, and 13. In addition, the active and reactive power flows are measured on the following thirteen lines: (1,2), (3,2), (2,4), (2,5), (7,4), (9,4), (5,6), (6,11), (6,12), (6,13), (11,10), (12,13), and (14,13). For instance, (3,2) corresponds to the power flow measurements from bus 3 to bus 2. The meters of the measurement system are indicated by black squares in Fig. 5 and the system is verified to be observable. In total there are 40 measurements. The non-corrupted measurements are computed using the following nonlinear expressions for power flows [1], [2]:

$$\begin{aligned} P_{km} &= {v_k}^2 g_{km} - v_k v_m(g_{km}\cos(\theta_{km}) + b_{km}\sin(\theta_{km})), \\ Q_{km} &= -{v_k}^2 b_{km} - v_k v_m(g_{km}\sin(\theta_{km}) - b_{km}\cos(\theta_{km})). \end{aligned} \tag{33}$$

Each measurement is corrupted by independent additive Gaussian noise whose variance is 0.1% of the absolute value of the corresponding non-corrupted measurement.

The data attack is unobservable according to [5], [9], [11], [21]. The attacker has the information of the Jacobian matrix

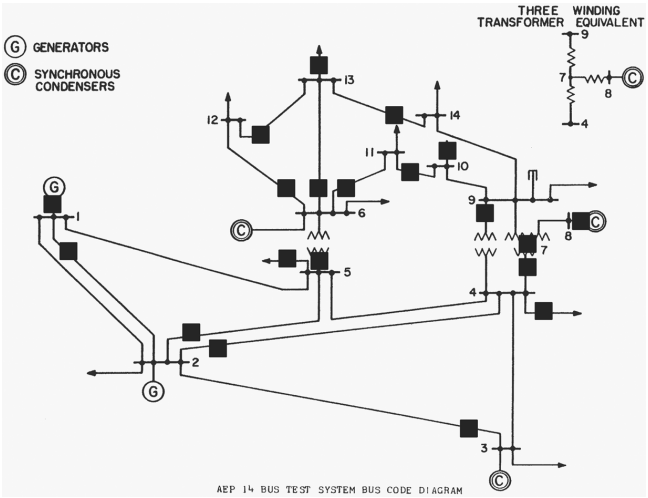

Fig. 5. IEEE 14-bus benchmark system. The meters are indicated by black squares. The figure is adapted from [28].

of the measurement function, evaluated at the operating point provided by [28]. The attacker uses the algorithm in [10], [30] to compute the unobservable data attack on the measurements. The attacker typically needs to attack, in addition to the target measurement, several other measurements which are required to make the attack unobservable. For example, the attacker aims to compromise the active power injection measurement at bus 1, which is referred to as the *target measurement* in the attack. However, to ensure that the attack is unobservable, the attacker needs to compromise additionally the following measurements: the reactive power injection at bus 1, the active power injection at bus 5 and the active and reactive power flows on line (1,2). In total, the data attack compromises five measurements, and it can be described by the vector

$$a = \rho |z_0| Hc, \tag{34}$$

where, for our example, Hc is the normalized attack vector having forty entries with five being nonzero corresponding to the five compromised measurements. Hc is normalized in the sense that the entry corresponding to the target measurement is unity (in the example, the target measurement is the active power injection at bus 1). $|z_0|$ is the absolute value of the target measurement. ρ can take the following values: $\{-200\%, -100\%, 100\%, 200\%\}$, indicating the relative strength of the data attack.

In addition to the mentioned example attack scenarios, in this section we consider other attack scenarios including all target measurement/attack strength pairs (in total 40×4 pairs). For each attack scenario, the network operator first estimates the states by solving a nonlinear weighted least squares problem [1, (2.10)] using the Gauss-Newton method with Armijo step-size rule [31]. Upon convergence of the Gauss-Newton method, the network operator computes the vector of measurement residuals R_z for all 40 active and reactive injection and line power flow measurements. These residuals are used to calculate the normalized residuals [1], [2] for each measurement. Measurement i is declared attacked if

$$\frac{|R_z(i)|}{\sigma_{R_z(i)}} > c_{\mathrm{LNR}}, \tag{35}$$

where $\sigma_{R_z(i)}$ is the standard deviation of the ith entry of R_z and the threshold c_{LNR} is chosen so that the false alarm probability is no more than 0.5%. It turns out that $c_{\mathrm{LNR}} \approx 2.58$.

Next, the proposed data attack isolation procedure described in Section III-F is applied to detect whether each of the 13 measured transmission lines is compromised or not (though the procedure would not distinguish between whether the compromised measurement is active power or reactive power or both). For each measured transmission line, the decision threshold r_{km} (for line km, for example) is found with the relevant parameters being $-20^\circ \leq \theta_{km} \leq +20^\circ$, $\sigma_P^2 = \sigma_Q^2 = |b|/1000$, $\beta = 0.005$ and $k = 20$. These thresholds are further increased by an amount specified in (30) for $\varepsilon_m - \varepsilon_k = 0.01$ to account for the imperfect knowledge of the voltage magnitudes. For instance, the threshold for line (1,2) is about 0.598. This corresponds to step 3) in the procedure in Section III-F. Then, the residual $R_{Q_{km}}$ for each measured transmission line is computed with two modifications to the procedure in Section III-F: a) the measurement expressions in (28) are used, and b) the voltage magnitudes v_k and v_m are perturbed from their nominal values (perturbation is random and uniformly distributed up to $\pm 0.5\%$). The modifications are introduced to simulate the effect of the lack of the assumption in (3). That is, instead of (9) the following expression is used to form the residual $R_{Q_{km}}$ for line km:

$$R_{Q_{km}} = \tilde{Q}_{km} - v_k v_m (g_{km} \sin((b_{km} v_k v_m)^{-1} \tilde{P}_{km}) + b_{km} \cos((b_{km} v_k v_m)^{-1} \tilde{P}_{km})) + b_{km} {v_k}^2,$$

where v_k and v_m are perturbed from nominal values. Computing the residuals $R_{Q_{km}}$ for all transmission lines finishes step 4) in the procedure in Section III-F. After that, the criterion $|R_{Q_{km}}| > r_{km}$ is checked to determine whether or not each of the 13 measured transmission lines is compromised.

The above descriptions correspond to one sample of a random experiment, since measurement noise is random. In total 1000 samples of the above random experiment are obtained in this case study, for each attack scenario with a particular pair of target measurement and attack strength. For each data attack scenario, the number of attacked transmission lines varies between 0 to 13 (in total there are 13 lines measured in the measurement system). Also, in some of the 1000 random samples the Gauss-Newton algorithm for state estimation fails to converge. For each convergent sample in each data attack scenario, a transmission line km is declared attacked by the normalized residual test if

$$\max\left\{ \frac{|R_z(p_{km})|}{\sigma_{R_z(p_{km})}}, \frac{|R_z(q_{km})|}{\sigma_{R_z(q_{km})}} \right\} > c_{\mathrm{LNR}}, \tag{36}$$

where p_{km} and q_{km} are the measurement indices of the active and reactive power flows on transmission line km, respectively. The numbers of misses (i.e., the transmission lines which are attacked but not declared attacked) and the number of false alarms (i.e., the transmission lines which are not attacked but declared attacked) can be counted. Note that in this part of the study we only consider the miss and false alarm for line flows but not for bus injections because the proposed method does not handle the injection case. We define the following relative average number of miss and relative average number of false alarm (FA in short),

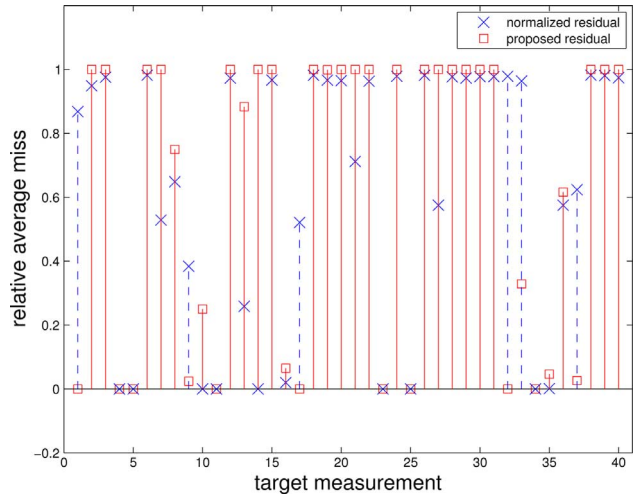

Fig. 6. Relative average number of miss for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = -200\%$. Blue dashed lines indicate the data attack scenarios where the normalized residual test performs worse, whereas red solid lines indicate the contrary.

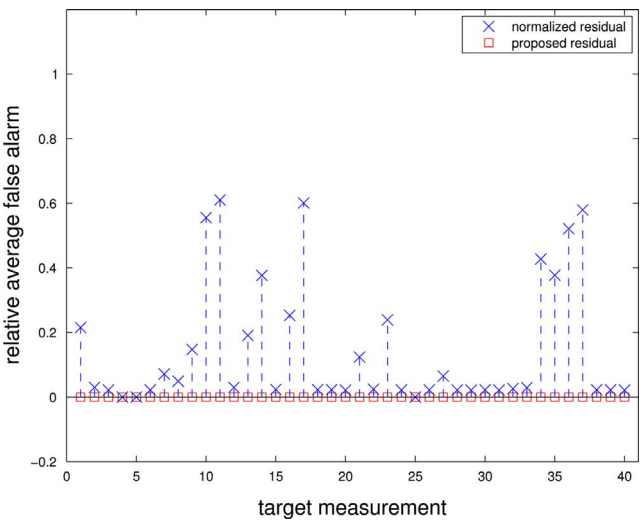

Fig. 7. Relative average number of false alarm for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = -200\%$. The proposed method is uniformly no worse than the normalized residual test.

for a data attack scenario with a particular pair of target and attack strength:

$$\begin{aligned}&\text{relative average \# of miss}\\&\quad=\frac{\text{total \# of miss over all convergent samples}}{\text{\# of convergent samples} \times \text{\# of attacked lines}}.\\&\text{relative average \# of FA}\\&\quad=\frac{\text{total \#of FA over all convergent samples}}{\text{\# of convergent samples} \times \text{\# of unattacked lines}}.\end{aligned} \tag{37}$$

Similarly, we can define the corresponding relative average miss and false alarm for the proposed test based on reactive power measurement residuals. In this case, instead of (36) transmission line km is declared attacked if $|R_{Q_{km}}| > r_{km}$, where r_{km} is the alarm decision threshold for line km. Fig. 6 shows the relative average number of miss for the normalized residual test and the proposed test, for all attack scenarios

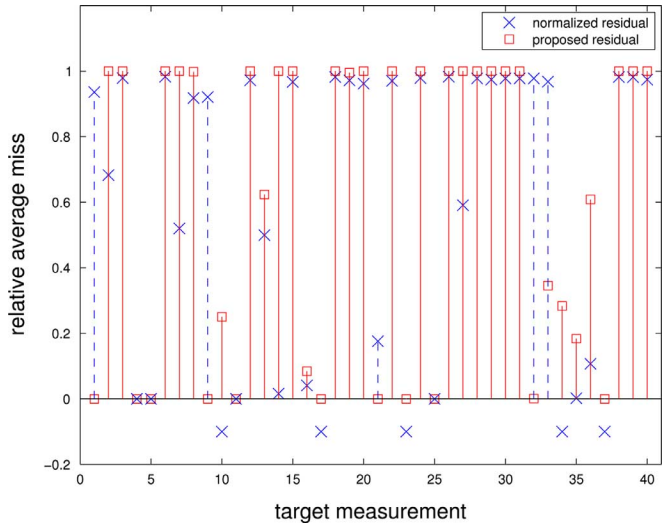

Fig. 8. Relative average number of miss for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = 200\%$. The negative crosses indicate the data attack scenarios where all 1000 random samples fail to converge.

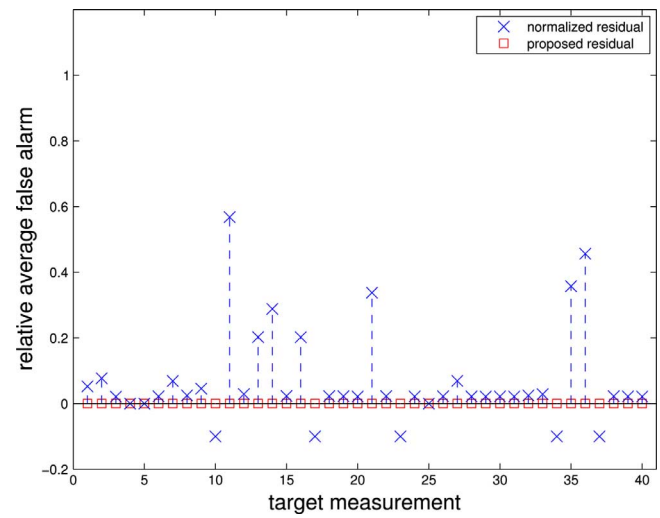

Fig. 9. Relative average number of false alarm for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = 200\%$. The negative crosses indicate the data attack scenarios where all 1000 random samples fail to converge.

with different attack targets and the data attack strength being $\rho = -200\%$. Fig. 7 shows the corresponding relative average number of false alarm. It can be seen that even though the proposed method has worse miss performance than the normalized residual test in some scenarios (i.e., the cases with red solid lines in Fig. 6), it detects the attacks in certain cases where the normalized residual test fails (i.e., the cases with blue dashed lines in Fig. 6). In addition, Fig. 7 indicates that the proposed method does not incur any false alarm while this can be a serious problem for the normalized residual test. These detection and false alarm properties, coupled with the computation efficiency, make the proposed data attack isolation method a promising complement to standard methods such as the normalized residual test.

For the data attack scenario with attack strength being $\rho = 200\%$, the corresponding error indicators are shown in Figs. 8 and 9. For the scenarios with $\rho = -100\%$ and $\rho = 100\%$, the

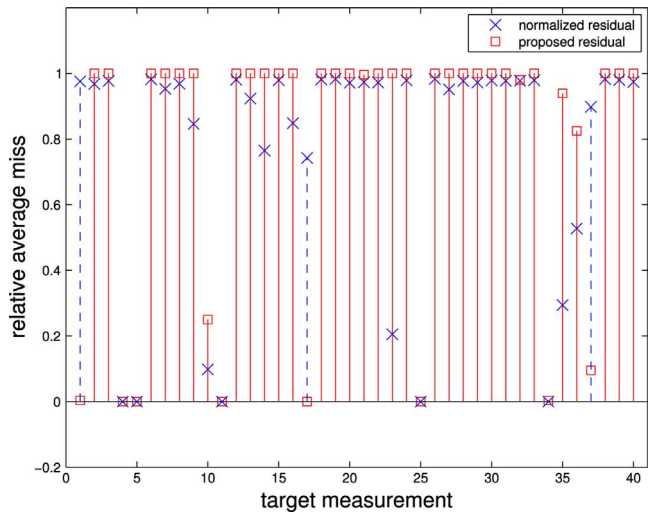

Fig. 10. Relative average number of miss for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = -100\%$.

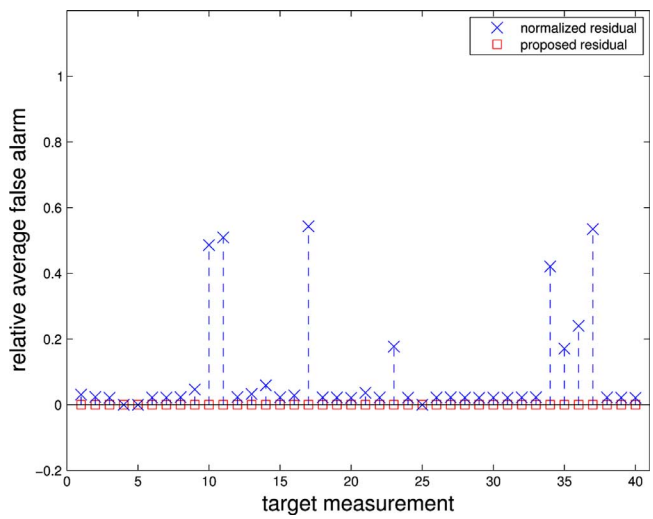

Fig. 11. Relative average number of false alarm for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = -100\%$.

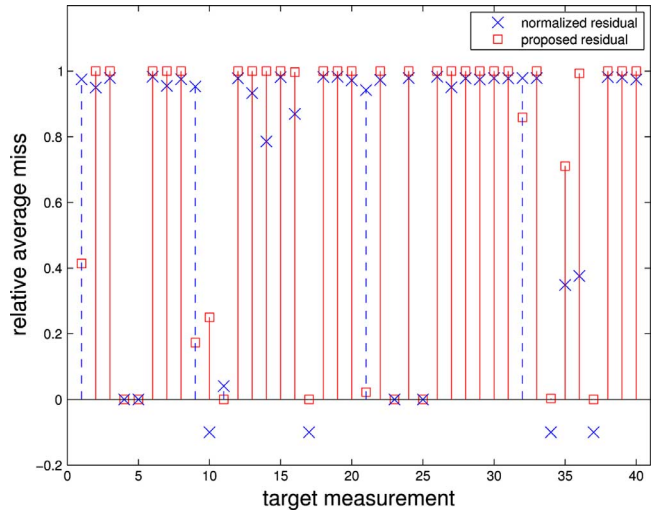

Fig. 12. Relative average number of miss for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = 100\%$. The negative crosses indicate the data attack scenarios where all 1000 random samples fail to converge.

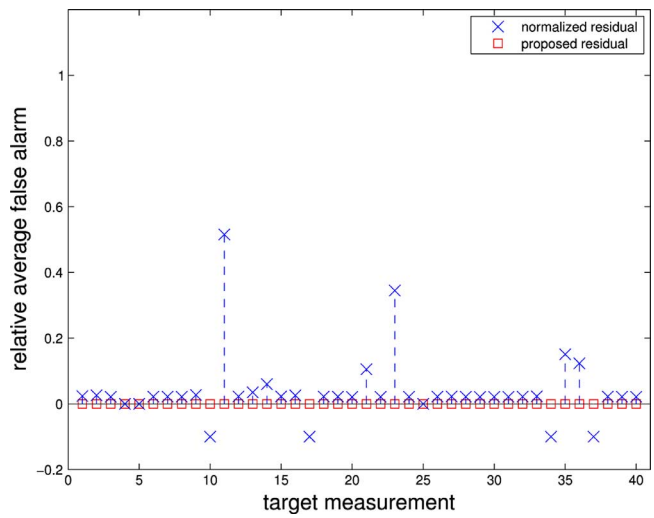

Fig. 13. Relative average number of false alarm for the normalized residual test and the proposed reactive power measurement residual test. The attack strength is $\rho = 100\%$. The negative crosses indicate the data attack scenarios where all 1000 random samples fail to converge.

results are shown in Figs. 10–13. These figures again demonstrate that the proposed method has much better false alarm performance while the miss performance is complementary to that of the normalized residual test.

A. Detailed Study for the Case Targeting Active Power Injection at Bus 1

For the rest of the case study the scenarios with target measurement being the active power injection at bus 1 are focused for more detailed examination. These scenarios correspond to the cases related to measurement 1 in Figs. 6–13. These attack scenarios involve five compromised measurements: the active power injection at bus 1 (i.e., the target measurement), the reactive power injection at bus 1, the active power injection at bus 5 and the active and reactive power flows on line (1,2). The range of attack strength is slightly larger in this part, with $\rho \in \{-200\%, -100\%, -50\%, -25\%, 0, 25\%, 50\%, 100\%, 200\%\}$.

Data attack detection (i.e., detecting the presence of any attack) is first considered. Standard methods include the measurement residual based χ^2 test and the largest normalized residual test [1], [2]. In the χ^2 test, an alarm is sounded if and only if

$$J(R_z) = {R_z}^T R^{-1} R_z > c_{\chi^2}, \tag{38}$$

where R is the covariance matrix of the measurement noise, and c_{χ^2} is chosen so that the probability of false alarm when there is no data attack is no more than 0.5%. The actual value of c_{χ^2} is about 28.3. In the largest normalized residual test, an alarm is sounded if and only if

$$|\mathrm{LNR}| = \max_i \left\{ \frac{|R_z(i)|}{\sigma_{R_z(i)}} \right\} > c_{\mathrm{LNR}}, \tag{39}$$

where c_{LNR} is chosen, again, so that the false alarm probability is no more than 0.5%. The actual value of c_{LNR} is about 2.58.

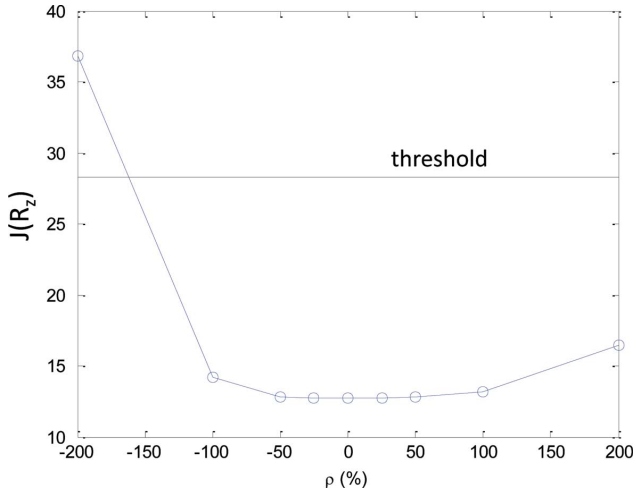

Fig. 14. The ensemble average of the weighted sum of measurement residuals $J(R_z)$ in (38) for the χ^2 test. On average only when $\rho = -200\%$ is the weighted sum large enough to warrant the BDD alarm.

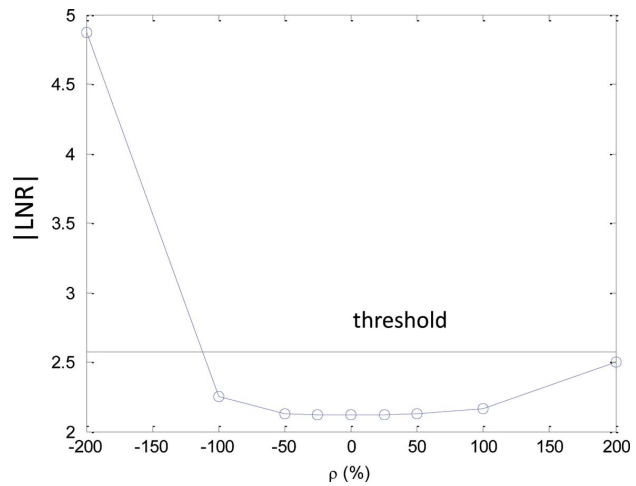

Fig. 15. The ensemble average of the largest normalized residuals in (39) for the largest normalized residual test. On average only when $\rho = -200\%$ is the residual large enough to warrant the BDD alarm.

For the χ^2 test and the largest normalized residual test, the detection considers all possible attacks (i.e., both line power flows and bus injections). On the other hand, to detect the attacks on the lines the proposed reactive power measurement residuals can be used. Fig. 14 shows the ensemble average (over 1000 samples) of the weighted sum of the measurement residuals $J(R_z)$ in (38). Fig. 15 shows the ensemble average of the largest normalized residuals in (39). Fig. 16 shows the ensemble average of the proposed reactive power measurement residuals for all 13 measured transmission lines. Figs. 14 and 15 indicate that the standard methods such as the χ^2 test and the largest normalized residual test are not sufficient to detect the data attack. On the contrary, the proposed reactive power measurement residual test can complement the standard methods to detect the data attack much earlier. In addition, Fig. 16 verifies that the proposed procedure correctly isolates the attacked transmission line [i.e., line (1,2)]. The residuals for the rest of the lines remain small, and they are below the smallest threshold for the alarm.

Next, data attack isolation is considered. For this the comparison is between the normalized residual test as in (35) (can be used for both line and bus measurements) and the proposed

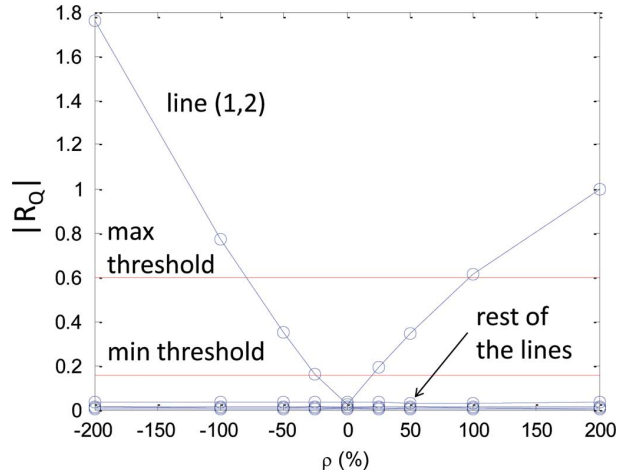

Fig. 16. The ensemble average of the proposed reactive power measurement residuals in absolute value for all transmission lines. The residuals associated with line (1,2) increase rapidly in absolute value with the attack strength $|\rho|$. On average the data attack is detected when $|\rho| \geq 100\%$. On the other hand, the residuals associated with the rest of the lines do not increase significantly to lead to any false alarm.

residual test (for lines only). To demonstrate the attack isolation capability of the normalized residuals the following empirical relative frequencies are defined: a random experiment sample belongs to "miss-all" event if and only if

$$\max_{i \in M_{\text{att}}} \left\{ \frac{|R_z(i)|}{\sigma_{R_z(i)}} \right\} \leq c_{\text{LNR}}, \tag{40}$$

where M_{att} is the index set of all measurements which are attacked. This event means that the normalized residual test fails to detect any attack on the attacked measurements. The relative frequency (over all 1000 samples) of samples in the miss-all event is denoted Pr_{MA}. In addition, the random sample belongs to "miss-partial" event if and only if

$$\min_{i \in M_{\text{att}}} \left\{ \frac{|R_z(i)|}{\sigma_{R_z(i)}} \right\} \leq c_{\text{LNR}}. \tag{41}$$

This event means that the normalized residual test fails to detect some attacks on the attacked measurements. The relative frequency of samples in the miss-partial event is denoted Pr_{MP}. Further, the random sample belongs to "false-alarm" event if and only if

$$\max_{i \notin M_{\text{att}}} \left\{ \frac{|R_z(i)|}{\sigma_{R_z(i)}} \right\} > c_{\text{LNR}}. \tag{42}$$

This event means that the normalized residual test wrongly declares some measurements to be attacked when they are in fact not attacked. The relative frequency of samples in the false-alarm event is denoted Pr_{FA}. Table I shows these empirical relative frequencies. In order to compare with the proposed data attack isolation method which only works for line power flow measurements, in Table II the above empirical relative frequencies are modified where the index set M_{att} in (40) and (41) are replaced by L_{att} where L_{att} is a subset of M_{att} containing only the indices of the transmission lines whose active or reactive power flows are measured. In addition, in (42) the index i chooses from the complement of L_{att}, relative to the index set of all line measurements. To compare against

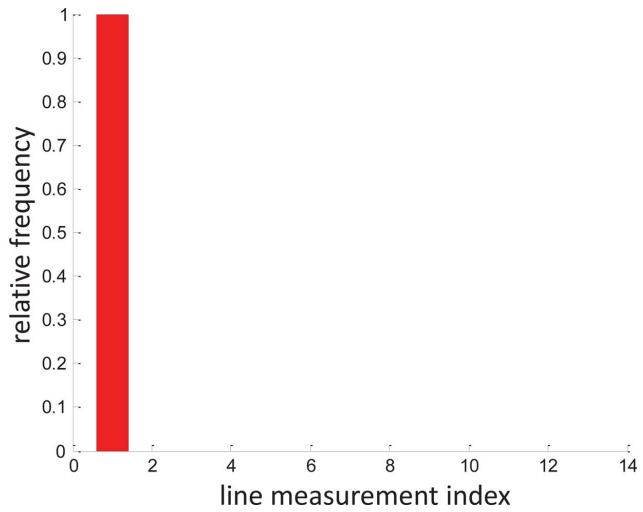

Fig. 17. Relative frequency of attack declaration for different lines. The detection is based on the reactive power measurement residuals. $\rho = -200\%$. Red bars correspond to the lines which are indeed attacked. The other lines are not attacked and are never mistakenly declared attacked by the proposed data attack isolation scheme.

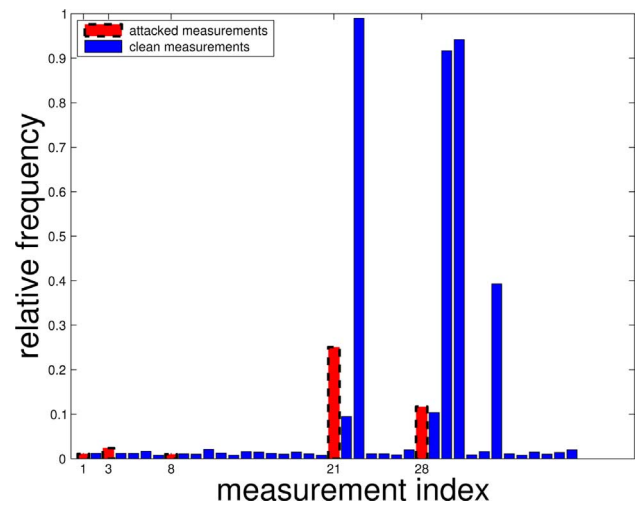

Fig. 18. Relative frequency of attack declaration for different measurements. The detection is based on the normalized residuals. $\rho = -200\%$. Red and dashed bars correspond to the measurements which are indeed attacked (1, 3, 8, 21, 28). Blue bars correspond to the measurements which are in fact not attacked. In addition to failing to identify the attacked measurements, the normalized residual test leads to significant false alarms.

the proposed method, the corresponding empirical error probabilities are shown in Table III. The comparison by Tables II and III further suggests that the proposed method exhibits much better attack isolation capabilities especially for attack with significant strength (e.g., $|\rho| = 100\%, 200\%$). To examine more closely a specific scenario of significant attack strength (i.e., $\rho = -200\%$), Fig. 17 shows the relative frequency out of the 1000 samples, for each measured line (in total 13 lines), of the sample instances where the reactive power measurement residual is larger than its respective threshold in absolute value (i.e., declared attacked). On the contrary, Fig. 18 shows the corresponding relative frequencies of attack declaration for all 40 measurements, for the normalized residual test. Fig. 18 indicates that even if the BDD alarm is sounded, the normalized

TABLE I
EMPIRICAL ERROR RELATIVE FREQUENCIES CHARACTERIZING THE DATA ATTACK ISOLATION CAPABILITY OF THE NORMALIZED RESIDUAL TEST. ALL ATTACKED MEASUREMENTS (INJECTION AND LINE FLOW) ARE INCLUDED IN THE CALCULATION

ρ (%)	-200	-100	-50	50	100	200
$\Pr_{MA}$	0.72	0.96	0.97	0.96	0.96	0.94
$\Pr_{MP}$	1	1	1	1	1	1
$\Pr_{FA}$	0.99	0.24	0.20	0.18	0.20	0.40

TABLE II
EMPIRICAL ERROR RELATIVE FREQUENCIES CHARACTERIZING THE DATA ATTACK ISOLATION CAPABILITY OF THE NORMALIZED RESIDUAL TEST. ONLY MEASURED TRANSMISSION LINES ARE INCLUDED IN THE CALCULATION

ρ (%)	-200	-100	-50	50	100	200
$\Pr_{MA}$	0.87	0.98	0.98	0.98	0.98	0.96
$\Pr_{MP}$	0.87	0.98	0.98	0.98	0.98	0.96
$\Pr_{FA}$	0.97	0.22	0.18	0.17	0.19	0.36

TABLE III
EMPIRICAL ERROR RELATIVE FREQUENCIES CHARACTERIZING THE DATA ATTACK ISOLATION CAPABILITY OF THE PROPOSED REACTIVE POWER MEASUREMENT RESIDUAL TEST. ONLY MEASURED TRANSMISSION LINES ARE INCLUDED IN THE CALCULATION

ρ (%)	-200	-100	-50	50	100	200
$\Pr_{MA}$	0	0	1	1	0.4	0
$\Pr_{MP}$	0	0	1	1	0.4	0
$\Pr_{FA}$	0	0	0	0	0	0

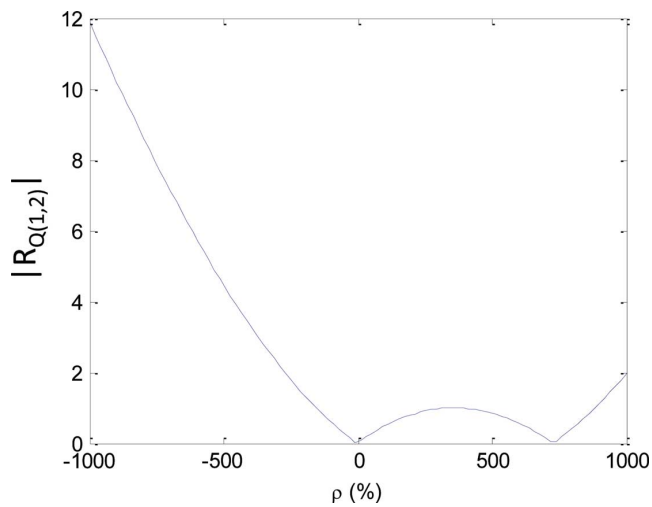

Fig. 19. Absolute value of the reactive power residual on line (1,2) in the noiseless setup for a larger range of ρ.

residual information is not helpful in isolating the measurements which are under attack. This explains the relatively large miss and false alarm relative frequencies displayed in the first column of Table I.

While in this example the attack strength is limited to $\pm 200\%$, Fig. 19 shows the reactive power measurement residual on line (1,2) for ρ up to $\pm 1000\%$ in the noiseless setup. The result indicates that with an appropriate nonzero value of ρ (about 700%) the data attack might remain undetected even if the proposed detection procedure is employed. Nevertheless, it should be emphasized that such large values of ρ might not be realizable, as the Gauss-Newton iterations might not even converge.

B. Summary of the Numerical Case Study and Discussions

From the case study it can be concluded that the proposed reactive power measurement residuals can be used to complement the detection and isolation of data attack or bad data as indicated by Figs. 6, 8, 10, and 12. The proposed method does not detect the presence of all attacks on the lines because of the limited information available for the distributed localized test. As indicated by (8), the proposed residual is affected jointly by the physical properties of the line, the actual phase angle difference, and the strength of the active and reactive power attack/bad data. Nevertheless, the case study suggests that the proposed method has excellent false alarm performance as it incurs no false alarm in Figs. 7, 9, 11, and 13. Combined with the fact that the proposed residuals can be computed efficiently in a distributed fashion, this makes the proposed data attack isolation method an attractive complement to standard data attack detection/BDD methods such as the χ^2 test and the normalized residual test.

The numerical case study also suggests that improving the miss performance of the proposed residual test is a worthwhile research effort. Improving the quality of the estimate phase angle difference can be a step forwards this direction. For instance, instead of utilizing the linearized active power measurement equation in (28), the following nonlinear one can be utilized [cf. (33)]:

$$\begin{aligned}\tilde{P}_{km} &= {v_k}^2 g_{km} - v_k v_m (g_{km}\cos(\theta_{km}) \\ &\quad + b_{km}\sin(\theta_{km})) + \Delta P_{km}, \\ \tilde{Q}_{km} &= -{v_k}^2 b_{km} - v_k v_m (g_{km}\sin(\theta_{km}) \\ &\quad - b_{km}\cos(\theta_{km})) + \Delta Q_{km}. \end{aligned} \tag{43}$$

In particular, if $g_{km} \neq 0$, then it is possible to form

$$-\frac{b_{km}\tilde{P}_{km} + g_{km}\tilde{Q}_{km}}{2v_k v_m b_{km} g_{km}} = \sin(\theta_{km}) - \frac{b_{km}\Delta P_{km} + g_{km}\Delta Q_{km}}{2v_k v_m b_{km} g_{km}}$$

as a corrupted estimate of the phase angle difference θ_{km}. This estimate can be more accurate than the linear one studied in this paper, and it can be used in (43) to form measurement residuals for data attack isolation. Its analysis can be a potential research topic of great interest.

VI. Conclusion

It is well-known that secure measurements can help contribute to the defense against data attack by enabling the network operator to detect "unobservable" type attack. By combining the knowledge of secure measurements and power system specific measurement model, an unconventional measurement residual can be obtained to achieve data attack isolation in addition to the standard BDD. Also, if utilized appropriately the increased amount of available information (a main feature of smart grid) can indeed lead to additional benefits in data security. This is demonstrated by using measurements from multiple time instances.

Appendix A

A. Proof of Proposition 3.1

Substituting the expressions $\Delta P = a_P + e_P$ and $\Delta Q = a_Q + e_Q$ into (10) yields

$$\begin{aligned} R_Q = a_Q + e_Q + b\cos(\alpha) - g\sin(\alpha) \\ - (b\sin(\alpha - b^{-1}a_P) + g\cos(\alpha - b^{-1}a_P))\sin(b^{-1}e_P) \\ - (b\cos(\alpha - b^{-1}a_P) - g\sin(\alpha - b^{-1}a_P))\cos(b^{-1}e_P). \end{aligned}$$

Expanding the terms as $\sin(b^{-1}e_P) = (b^{-1}e_P) - (1/3!)(b^{-1}e_P)^3 + (1/5!)(b^{-1}e_P)^5 - \ldots$ and $\cos(b^{-1}e_P) = 1 - (1/2!)(b^{-1}e_P)^2 + (1/4!)(b^{-1}e_P)^4 - \ldots$ and applying the definitions of B, X and Y in (13), (14) and (15) yields $R_Q = X + Y$. Therefore,

$$\begin{aligned}\Pr(|R_Q| > s) &= \Pr(|X + (Y - m_Y) + m_Y| > s) \\ &\leq \Pr(|X| + |Y - m_Y| + |m_Y| > s) \\ &\leq \Pr(|X| > s - |m_Y| - k\sigma_Y) \\ &\quad + \Pr(|Y - m_Y| > k\sigma_Y) \\ &\leq \Pr(|X| > s - |m_Y| - k\sigma_Y) + \frac{1}{k^2}. \end{aligned} \tag{44}$$

This shows (6a). In (44), the first inequality is true since $|X + (Y - m_Y) + m_Y| \leq |X| + |Y - m_Y| + |m_Y|$. The second one is true since $\{(x, y) \in \mathbb{R}^2 \,|\, |x| + |y - m_Y| > s - |m_Y|\}$ is in the union of $\{(x, y) \in \mathbb{R}^2 \,|\, |x| > s - |m_Y| - k\sigma_Y\}$ and $\{(x, y) \in \mathbb{R}^2 \,|\, |y - m_Y| > k\sigma_Y\}$. The third one is a consequence of the Chebyshev's inequality. Similarly, for (16b):

$$\begin{aligned}\Pr(|R_Q| > s) &\geq \Pr(|X| - |Y - m_Y| - |m_Y| > s) \\ &\geq \Pr(|X| > s + |m_Y| + k\sigma_Y) \\ &\quad - \Pr(|Y - m_Y| > k\sigma_Y) \\ &\geq \Pr(|X| > s + |m_Y| + k\sigma_Y) - \frac{1}{k^2}. \end{aligned}$$

B. Proof of Proposition 3.2

The definition of X in (14) implies that $X \sim \mathcal{N}(B, \sigma_X^2)$. (16a) states that if s satisfies

$$\Pr(|X| > s - |m_Y| - k\sigma_Y) + \frac{1}{k^2} < \beta, \tag{45}$$

then $\Pr(|R_Q| > s) < \beta$. The inequality in (45) is implied by

$$\Pr\left(|\sigma_X^{-1}(X - B)| > \sigma_X^{-1}(s - |B| - |m_Y| - k\sigma_Y)\right) + \frac{1}{k^2} < \beta. \tag{46}$$

Since $\sigma_X^{-1}(X - B) \sim \mathcal{N}(0, 1)$, (46) is the same as

$$2\left(1 - \Phi(\sigma_X^{-1}(s - |B| - |m_Y| - k\sigma_Y)\right) < \beta - \frac{1}{k^2},$$

where $\Phi(\,\cdot\,)$ is the cumulative distribution function of a standard Gaussian random variable. Rearranging terms and inverting Φ in above yields (18).

C. Proof of Proposition 3.3

Equation (23) is a restatement of (20) and (17).

For the first statement in (24), denote $M_2 = (b\cos(\alpha - b^{-1}a_P) - g\sin(\alpha - b^{-1}a_P))$. Since $b^{-1}e_P$ is a zero mean Gaussian random variable, $E[(b^{-1}e_P)^{2i+1}] = 0$ for all positive integer i. Therefore,

$$\begin{aligned}|m_Y| = |E[Y]| &= |M_2|\sum_{i\geq 1}(-1)^{i+1}\frac{(2i-1)!!}{(2i)!}b^{-2i}\sigma_P^{2i}\\ &\leq \frac{1}{2}|M_2|\sum_{i\geq 1}b^{-2i}\sigma_P^{2i}\\ &= \frac{1}{2}|M_2|\frac{b^{-2}\sigma_P^2}{1-b^{-2}\sigma_P^2}\\ &= (1+\epsilon)\left(|b|^{-1}\sigma_P^2\right).\end{aligned}$$

In above, the symbol $(2i-1)!!$ denotes the product $1\times 3\times\ldots\times(2i-1)$. Hence, $((2i-1)!!)/((2i)!) \leq 1/2$ for all i and the inequality holds. The convergence of the series follows from the assumption that $|b|^{-1}\sigma_P < 1$. Finally, in the last equality the fact that $|M_2| \leq |b| + |g| \leq 2|b|$ is used.

For the second statement in (24), denote $M_1 = (b\sin(\alpha - b^{-1}a_P) + g\cos(\alpha - b^{-1}a_P))$. Note that both M_1 and M_2 satisfy $|M_1| \leq 2|b|$ and $|M_2| \leq 2|b|$. Then

$$\begin{aligned}\sigma_Y^2 &= E[Y^2] - (E[Y])^2\\ &\leq E[Y^2]\\ &= M_2^2\frac{3!!}{(2!)^2}b^{-4}\sigma_P^4 + \left(\frac{5!!}{(3!)^2}M_1^2 - 2\frac{5!!}{(2!)(4!)}M_2^2\right)b^{-6}\sigma_P^6\\ &\quad + \left(\frac{7!!}{(4!)^2}M_2^2 - 2\frac{7!!}{(3!)(5!)}M_1^2\right)b^{-8}\sigma_P^8 + \ldots\\ &\leq 24b^2\left(\frac{3}{4}b^{-4}\sigma_P^4\right.\\ &\quad \left.+\sum_{i\geq 3}\left|\frac{1}{(i!)^2} - \frac{2}{((i-1)!)((i+1)!)}\right|(2i-1)!!b^{-2i}\sigma_P^{2i}\right)\\ &\leq 4b^2\sum_{i\geq 2}b^{-2i}\sigma_P^{2i}\\ &= 4b^2\frac{b^{-4}\sigma_P^4}{1-b^{-2}\sigma_P^2}\\ &= \left(2(1+\epsilon)|b|^{-1}\sigma_P^2\right)^2 \qquad (47)\end{aligned}$$

The third and fourth inequalities in (47) hold because of the following facts: For all $i \geq 3$,

$$\begin{aligned}&\text{Fact 1}: \quad (i!)^2 < ((i-1)!)((i+1)!) < 2(i!)^2\\ &\text{Fact 2}: \quad \left|\frac{1}{(i!)^2} - \frac{2}{((i-1)!)((i+1)!)}\right|\\ &\qquad\qquad < \frac{1}{((i-1)!)((i+1)!)} < \frac{1}{(i!)^2}\\ &\text{Fact 3}: \quad \frac{(2i-1)!!}{(i!)^2} = \frac{\prod_{j=1}^{i}(2j-1)}{\prod_{j=1}^{i}j^2} < 1.\end{aligned}$$

Finally, (25) is a direct consequence of (23) and (24).

D. Proof of Proposition 4.1

For given a_P define the function $B_{a_P}(\gamma) : [-\pi,\pi) \mapsto \mathbb{R}$ as

$$\begin{aligned}B_{a_P}(\gamma) &\triangleq b(\cos(\gamma) - \cos(\gamma - b^{-1}a_P))\\ &\quad - g(\sin(\gamma) - \sin(\gamma - b^{-1}a_P))\\ &= (-g + g\cos(b^{-1}a_P) - b\sin(b^{-1}a_P))\sin(\gamma)\\ &\quad + (b - b\cos(b^{-1}a_P) - g\sin(b^{-1}a_P))\cos(\gamma)\\ &\triangleq A_s\sin(\gamma) + A_c\cos(\gamma). \qquad (48)\end{aligned}$$

The statement of the proposition is equivalent to: ($\star$) If $N \geq 3$, then for any $(a_P, a_Q) \neq 0$ with $|b^{-1}a_P| \leq \pi$, there does not exist $(\alpha^1, \alpha^2, \ldots, \alpha^N) \in [-\pi,\pi)^N$ such that $\alpha_i \neq \alpha_j$ for $i \neq j$ that satisfies $B_{a_P}(\alpha^1) = B_{a_P}(\alpha^2) = \ldots = B_{a_P}(\alpha^N)$.

Now the proof begins: If $(a_P, a_Q) \neq 0$ then $a_P \neq 0$, since $a_P = 0$ and $B = 0$ implies $a_Q = 0$. It is claimed that $a_P \neq 0$ implies that A_s and A_c in (48) cannot both be zero. Under the claim, $B_{a_P}(\gamma) = M\sin(\gamma + \varphi)$ with $M = \sqrt{A_s^2 + A_c^2} > 0$. For such $B_{a_P}(\gamma)$ statement ($\star$) can be verified by inspection. Finally, to see the claim note that if $A_s = 0$ and $A_c = 0$, then

$$\begin{aligned}-bg + bg\cos(b^{-1}a_P) - b^2\sin(b^{-1}a_P) &= 0\\ bg - bg\cos(b^{-1}a_P) - g^2\sin(b^{-1}a_P) &= 0. \qquad (49)\end{aligned}$$

This implies that $(b^2+g^2)\sin(b^{-1}a_P) = 0$. Since $b^2 + g^2 > 0$, $|b^{-1}a_P|$ is either 0 or π (as $|b^{-1}a_P| \leq \pi$). The choice of $|b^{-1}a_P| = \pi$ is not allowed, since otherwise the assumption that $A_s = 0$ and $A_c = 0$ would imply that $b = 0$ and $g = 0$. Therefore, $A_s = 0$ and $A_c = 0$ imply that $a_P = 0$, and its contrapositive is the claim above.

REFERENCES

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

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

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

[4] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in *Proc. 2nd Int. Symp. Resilient Control Syst. (ISRCS'09)*, Aug. 2009, pp. 31–35.

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

[6] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. First Workshop Secure Control Syst. (CPSWEEK)*, 2010.

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

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

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

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

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

[12] 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.

[13] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. Power App. Syst.*, vol. PAS-94, no. 2, pp. 329–337, Mar. 1975.
[14] H. Wu and J. Giri, "Pmu impact on state estimation reliability for improved grid security," in *Proc. 2005/2006 IEEE PES Transm. Distrib. Conf. Exh.*, May 2006, pp. 1349–1351.
[15] A. Monticelli, F. F. Wu, and M. Yen, "Multiple bad data identification for state estimation by combinatorial optimization," *Power Engineering Review, IEEE*, vol. PER-6, no. 7, pp. 73–74, July 1986.
[16] E. Asada, A. Garcia, and R. Romero, "Identifying multiple interacting bad data in power system state estimation," in *Proc. IEEE Power Eng. Soc. Gen. Meet. 2005*, Jun. 2005, vol. 1, pp. 571–577.
[17] M. Irving, R. Owen, and M. Sterling, "Power-system state estimation using linear programming," *Proc. Inst. Electr. Eng.*, vol. 125, no. 9, pp. 879–885, Sep. 1978.
[18] W. Peterson and A. Girgis, "Multiple bad data detection in power system state estimation using linear programming," in *Proc. 20th Southeastern Symp. Syst. Theory 1988*, pp. 405–409.
[19] M. Cheniae, L. Mili, and P. Rousseeuw, "Identification of multiple interacting bad data via power system decomposition," *IEEE Trans. Power Syst.*, vol. 11, no. 3, pp. 1555–1563, Aug. 1996.
[20] D. Gorinevsky, S. Boyd, and S. Poll, "Estimation of faults in dc electrical power system," in *Proc. 2009 Conf. Amer. Control Conf.*, pp. 4334–4339.
[21] 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. 2010 49th IEEE Conf. Decision Control (CDC)*, Dec. 2010, pp. 5991–5998.
[22] P. Kundur, *Power System Stability and Control*. New York: McGraw-Hill, 1993.
[23] P. Vovos, A. Kiprakis, A. Wallace, and G. Harrison, "Centralized and distributed voltage control: Impact on distributed generation penetration," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 476–483, 2007.
[24] F. Viawan, "Voltage control and voltage stability of power distribution systems in the presence of distributed generation," Ph.D. dissertation, Chalmers Univ. Technology, Gothenburg, Sweden, 2008.
[25] H. Li, F. Li, Y. Xu, D. Rizy, and J. Kueck, "Adaptive voltage control with distributed energy resources: Algorithm, theoretical analysis, simulation, and field test verification," *IEEE Trans. Power Syst.*, vol. 25, no. 3, pp. 1638–1647, 2010.
[26] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. .
[27] G. Casella and R. Berger, *Statistical Inference*. Pacific Grove, CA, USA: Duxbury Press, 2001.
[28] R. Christie, "Power system test case archive," Univ. Washington. Seattle, WA, USA [Online]. Available: http://www.ee.washington.edu/research/pstca/pf14/pg_tca14bus.htm, 1993
[29] R. Zimmerman, C. Murillo-Sánchez, and R. Thomas, "MATPOWER steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, 2011.
[30] J. Hendrickx, K. H. Johansson, R. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Trans. Autom. Control*, Special Issue on Control of Cyber-Physical Systems, accepted for publication.
[31] D. Bertsekas, *Nonlinear Programming*. Belmont, MA, USA: Athena Scientific, 1999.

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

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

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

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

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

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

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

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