Bad Data Detection and Identification in Distribution Power Systems

Tim Streubel, Daniel Groß, Krzysztof Rudion
Institute of Power Transmission and High Voltage Technology, IEH
Stuttgart, Germany

Abstract—**Measurement values in power systems may include bad data, adversely affecting the accuracy of the state estimation algorithm. In order to detect and identify erroneous measurements, mathematical methods such as the Chi-Squared Distribution Test (CSDT), Largest Normalized Residual Test (LNRT) and Hypotheses Testing Identification (HTI) are embedded in state estimators. However, due to the increasing digitalization of distribution power systems new security threats, such as smart meter manipulation and bad data injection, are imposed on power system operators. In this paper, a bad data detection and identification monitoring system for distribution power systems is proposed. Aside from the conventional approaches for bad data detection, the monitoring system includes a new intelligent method for the detection of energy theft and meter manipulation scenarios. By utilizing a feed forward artificial neural network, irregularities within the measurement distributions can be recognized and specific cyber-attacks exposed. The implemented computational algorithms are coupled with a distribution system state estimator and the detection ability validated for various bad data injection scenarios.**

Keywords — Bad data detection; smart grid security; smart meter manipulation

I. INTRODUCTION

State estimation is utilized in power systems to maintain the operating conditions in a normal and secure state. In order to determine the operational state of a power system, the complex phasor voltages at every system bus are estimated by processing accessible and redundant measurements. Distribution system state estimation constitutes the core of the on-line security analysis function, providing a reliable real-time data base of the observed system [1]. The concept of power system state estimation and bad data detection was first introduced by Schweppe and Wilders [2] three decades ago and has not been significantly updated since.

The importance of robust state estimation, particularly regarding bad data detection and identification, was reflected during the North-east blackout of 2003 in the US and Canada. The critical error in the cascade of failures was an incorrect telemetry measurement data set causing the state estimator to malfunction. Measurement errors in power systems may appear due to incorrect installation or servicing, disorders in communication systems and auxiliary devices such as current transformers (CTs), potential transformers (PTs) or capacitive voltage transformers (CTVs) [3]. To ensure that the state estimator is provided with qualitative and adequate merits, bad data detection and identification is continuously carried out. Bad data detection describes the procedure of revealing the presence of bad data within a set of measurements, whereas bad data identification methods locate the erroneous measurements. The conventional approaches include the Chi-Squared Distribution Test (CSDT), the Largest Normalized Residuals Test (LNRT) and Hypotheses Testing Identification (HTI). The algorithms process the measurement residuals of the state estimator and classify measurements based on their statistical properties. The computational bad data monitoring system, proposed in this paper, focuses on distribution power systems. The main responsibilities of the system are the time-continuous detection, identification and removal of bad data. The detection ability of the implemented software is validated by integrating the monitoring system in a state estimator and inject bad data measurements.

Aside from the mathematical bad data detection and identification approaches, a new method is introduced, monitoring measurement distributions (MMD). The objective is to reduce the susceptibility of smart grids towards cyber-attack related threats, specifically smart meter manipulation. Since the data in smart grids can easily be monetized, bad data injection becomes increasingly attractive for hackers, with the predominant motivation of energy theft and energy market manipulation [4]. Furthermore, bad data injection could mislead the system operators to take incorrect actions.

The introduced method involves an artificial neural network (ANN) with the ability to distinguish between regularly occurring measurements and manipulated measurement by reviewing the distributions, respectively. This is achieved by training the ANN classifier with historical measurement data and predetermined data sets for various generic meter manipulation scenarios.

II. State Estimation

The relation between measurement model and state variables is described by the following expression (1):

$$z = h(x) + e \tag{1}$$

Where *z* is the measurement vector with size *m* and *x* the state vector with size *n*. The variable *h(x)* is a vector function relating measurements to state variables. The measurement error vector *e* is expected to follow the Gaussian distribution with a mean of zero. This is a generally accepted assumption in state estimation concept [5]. Based on the hypothesis of normal distributed errors, the objective is to determine a state vector *x* for a best fit to the corresponding measurement vector *z*. Thus, an optimization problem can be considered:

$$J(x) = [z - h(x)]^T \; R^{-1}[z - h(x)] \tag{2}$$

Where R^{-1} is the inverse matrix of variances. By applying the Weighted Least Squares (WLS) method the state estimation optimization problem (2) is solved by applying Newton's iterative solution scheme [6].

III. Bad data detection and Identification Monitoring System

The main components of the bad data detection and identification monitoring system involve a plausibility check (PC) for preprocessing raw measurement data, the CSDT for bad data detection and the LNRT as well as the HTI for bad data identification. The PC processes raw measurements prior to state estimation in order to eliminate obvious measurement errors, widely deviating from their expected values by several margins. Furthermore, the PC ensures data consistency and replaces previous identified faulty measurements. Subsequent to state estimation, bad data detection is carried out, analyzing the statistical properties of the measurement residuals. If the presence of erroneous measurements within a data set is suspected by the CSDT, the bad data identification methods are initialized with the objective to locate the faulty measurements.

A. Chi-Squared Distribution Test

The chi-squared distribution is a theoretical statistical distribution built by the sum of squares of a set of independent standard normal distributed variables. The distribution properties of the chi-squared distribution are commonly utilized to determine the probability of an observed error of an expected value. Assuming the measurement errors *e* are normally distributed random variables a function *f(x)* can be formulated:

$$f(e) = \sum_{i=1}^{m} \left(\frac{e_i}{\sqrt{R_{ii}}} \right)^2 \tag{3}$$

Where R_{ii} are the diagonal entries of the inverse covariance matrix of measurements. The function *f(x)* will have a chi-squared distribution with at most *k* degrees of freedom:

$$k = m - (2n - 1) \tag{4}$$

Where *m* is the number of measurements and *n* is the number of states within the observed system. The error square sum function *J(x)* (2) serves as an indicator in respect to the presence of bad data. Large measurement errors lead to an increasing difference between measurement vector *z* and state vector *x*. Thus, large measurement errors are raising the value for the objective error square sum function *J(x)*.

To decide whether bad data is present within a measurement data set, the test determines a critical threshold value *Jcrit*. For each *J(x)* a corresponding critical value *Jcrit* can be selected from the chi-square distribution table with the given significance level and *k* degrees of freedom. The critical threshold *Jcrit* is chosen based on a significance level, commonly *5%*, which represents the probability that the observed result for *J(x)* can be justified by normal distributed measurement errors. The presence of bad data is suspected, if the obtained state estimation result for *J(x)* exceeds the predetermined critical threshold, indicating that the measurement errors are not normally distributed.

B. Largest Normalized Resiudals Test

Noncritical erroneaous measurements within a data set can be identified utilizing the LNRT. The residue for the *ith* measurement can be written as:

$$r_i = z_i - h(x)_i \tag{5}$$

The residues r_i are normalized in order to calculate the residual covariance matrix. The measurement residual covariance matrix is Ω defined by the equation:

$$\Omega = R - HG^{-1} H^T \tag{6}$$

Where *H* is the jacobian matrix, *G* the gain matrix and *R* the measurement covariance matrix. The diagonal entries of the residual covariance matrix are processed to determine the normalized residual vector:

$$r^N = \frac{|r_i|}{\sqrt{\Omega_{ii}}} \tag{7}$$

Where Ω_{ii} are the diagonal entries of the measurement residual covariance matrix Ω. Gross measurement errors lead to an increased residue (5), yielding in a larger denominator in (7). Thus, bad data corresponds to a large element in r^N [7]. Admitting the hypothesis that measurement errors are normally distributed independent random variables, the elements of the normalized residues vector follow the Gaussian standard normal distribution.

With normalization of the residuals, the expected statistical properties of the vector elements can be expressed:

$$r_i^N \sim N(0,1) \tag{8}$$

In order to decide if bad data is existent, the normalized residual vector elements are compared against a statistical threshold, commonly assumed to be 3 [8]. If i.e. a normalized residual element r_i^N exceeds the threshold of three standard deviations, bad data is suspected in the *ith* measurement.

C. Hypotheses Testing Identification

The HTI method was first introduced in 1984 by L. Mili [9] and is substantiated by two hypotheses:

H_0: *Measurement does not contain bad data*

H_1: *Measurement does contain bad data*

In HTI two conceptual errors may occur; type I and type II errors. Classification of a bad data measurement as an error-free measurement is considered as a type I error, also known as *false positive*. A type II error, a so called *false negative*, occurs in case the HTI fails to identify bad data.

Following the assumption of normal distributed errors, the statistical properties of the null hypothesis H_0 can be expressed as:

$$\hat{e}_{si} \sim N(0, \sigma_i^2 S_{ii}^{-1}) \tag{9}$$

Where S_{ii}^{-1} are the diagonal entries of the inverted sensitivity matrix S^{-1} and σ_i is the diagonal entries of the measurement covariance matrix R. The sensitivity matrix S relates to the susceptibility of measurements towards bad data. The null hypothesis is accepted, if the observed measurement errors are distributed according to (9). In case the tested measurement error exceeds the given standard deviation $\sigma_i^2 S_{ii}^{-1}$, H_0 is rejected and consequently bad data suspected. Type I error probability is denoted with α and the type II error probability with β. The critical decision threshold λ is calculated for each measurement independently.

The type I and type II error probabilities for HTI are illustrated in Fig. 1. HTI can be either executed with a fixed type I error probability, determining the corresponding type II probability or vice versa. The implemented HTI for the monitoring system was carried out with a fixed type I error probability of α=*0.05*. Consequently, *5%* of processed measurements are assumed to be incorrectly classified as *false positives*. Thus, the type I error probability can be formulated as:

$$\alpha = \Pr(H_0 \ rejected \mid H_0 \ is \ true) = \Pr(|\hat{e}_{si}| > \lambda_i) \tag{10}$$

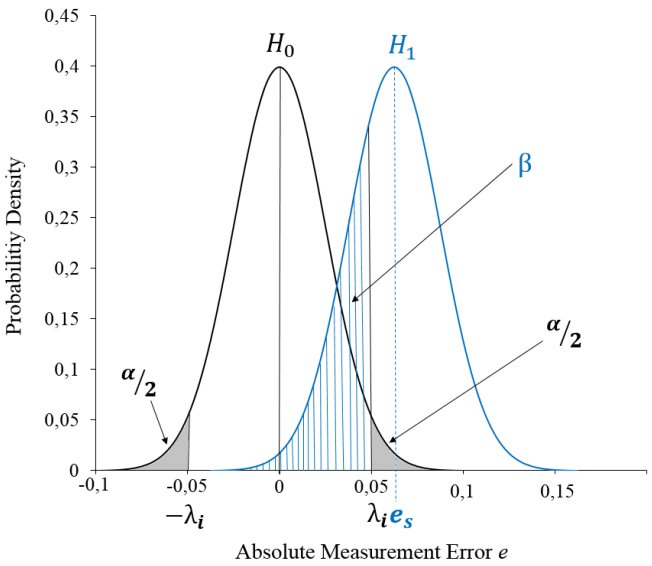

Figure 1. Type I and II errors in hypotheses testing

Where $\hat{e}_{si}$ is ideally distributed according to (9). By normalizing the absolute error of the estimated error, a corresponding cut-off value $N_{1-\alpha/2}$ can be determined from the standard normal distribution table. Hence, the type I error probability can be rewritten as:

$$\alpha = \Pr\left(\frac{|\hat{e}_{si}|}{\sigma_i^2 \sqrt{S_{ii}^{-1}}} > N_{1-\alpha/2}\right) \tag{11}$$

Utilizing (11), the critical decision threshold λ_i can be calculated:

$$\lambda_i = \sigma_i \sqrt{S_{ii}^{-1}} N_{1-\alpha/2} \tag{12}$$

The threshold value λ_i is determined for each tested measurement error. Errors satisfying the condition $|\hat{e}_{si}| > \lambda_i$ are suspected of accommodating bad data.

IV. Artificial Neural Network for Measurement Distribution Classification

The presented mathematical bad data detection and identification approaches, as well as the WLS state estimation, share the assumption of normal distributed measurement errors. Since non-normal error distributions may adversely affect the mentioned methods, as written in [10], the implemented bad data detection system was extended by the integration of algorithms, continuously monitoring the measurement and measurement residual distributions.

While measurement errors are expected to be distributed according to the Gaussian standard distribution, the assumption is not necessarily observed in field regarding measurements. Considering that bad data detection is solely based on processing measurement residuals, it is possible that the manipulation of measurement distributions may remain unnoticed by the conventional bad data detection concepts. Normal distributed measurements and estimates result in normal distributed residuals. However, the systems residual distribution, the decisive factor for bad data detection, may remain normally distributed, even if the measurement distribution parameters vary. In other terms, the measurement distribution shape can be manipulated to a certain extent without initializing the conventional bad data detection methods.

Figure 2 illustrates the distribution of 1000 synthetically generated standardized power measurements and the corresponding systems residual distribution. The generated measurement data was manipulated by applying a skew factor of -4. To confirm the normality of the residuals distribution, the Shapiro Wilk [12] test was carried out, returning a goodness of fit of 98.7% with a p-value of 83%. For normal distributed measurements, the statistical properties of the corresponding residuals did not significantly change. Consequently, depending on the size of the observed network and extent of manipulation, the CSDT nor the LNRT or HTI, are able to detect changes in measurement distribution shapes.

The measurement distribution shape may vary due to season, daytime, renewable energy supply and energy consumption. The properties of the measurement distributions are time dependent and may differ for each measurement within the observed power network. The primary objective of the implemented ANN is to distinguish between admissible measurement distributions and irregular measurement distributions based on historical data. The individuality of measurement distributions and its dependency on various influencing factors, increase the complexity of the classification problem.

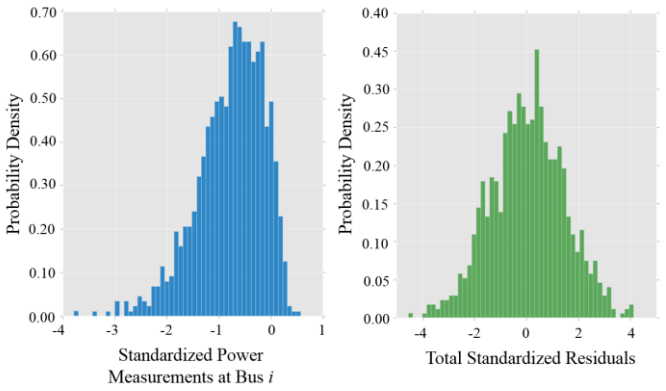

Figure 2. Probability density of manipulated standardized power measurements and residuals

Observed distributions for each measurement point respectively are labeled as acceptable distributions. Uncommon distribution related to energy theft or other manipulation scenarios, are specifically classified in distinctive extendable training sets. The classification accuracy of the ANN depends heavily on the provided data size, its inherent variety and declared labels.

V. Results

A. Bad Data Injection Scenario

In order to validate the implemented computational CSDT, LNRT and HTI algorithms, the bad data monitoring system was embedded into an 84-bus distribution network state estimator.

Collectively three measurement errors were injected with increasing percentage of error and processed by the state estimator. The affected measurements differ in respect to their measurement inverse covariance matrix diagonal entry σ. The voltage magnitude measurement V_{M1} has the largest susceptibility towards measurement errors, followed by the power flow measurement P_{T3} and power generation measurement P_{G0}. Both algorithms were able to identify the injected bad data. Table I verifies the linear relationship between normalized residual and error percentage. Furthermore, a higher detection sensibility of the HTI compared to the LNRT can be observed. The test sensitivity can be adjusted individually for each test by changing the corresponding critical thresholds respectively. The plausibility check was able to remove the identified erroneous measurements in the subsequent state estimation cycle, eliminating the bad data from the system.

B. Smart Meter Manipulation Scenarios

The ANN classifier was trained with 2000 observed standardized power measurement distributions, each with a sample size of 60, originating from a low voltage power system. In order to validate the classifier, two separate manipulation scenarios were reviewed.

TABLE I. Bad data injection of three measurements with different error susceptibility

Percentage of error	Normalized residuals[1]			Identified by HTI	Identified by LNRT
	P_{T3}	P_{G0}	V_{M1}		
2.5%	0.54	0.99	5.23	V_{M1}	-
5%	1.05	1.92	10.48	V_{M1}	V_{M1}
7.5%	1.60	2.85	15.74	P_{G0}, V_{M1}	V_{M1}
10%	2.08	3.78	21.00	P_{G0}, V_{M1}	P_{G0}, V_{M1}
15%	3.14	5.60	31.51	P_{G0}, V_{M1}, P_{T3}	P_{G0}, V_{M1}, P_{T3}

1. $\sigma_{P_T} = 0.2$; $\sigma_{P_G} = 0.15$; $\sigma_{V_M} = 0.10$

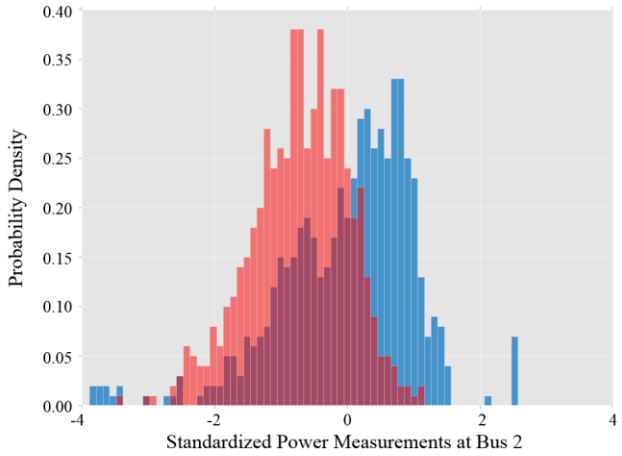

Figure 3. Scenario 1: Manipulated standardized power measurements in red and expected standardized power measurements in blue.

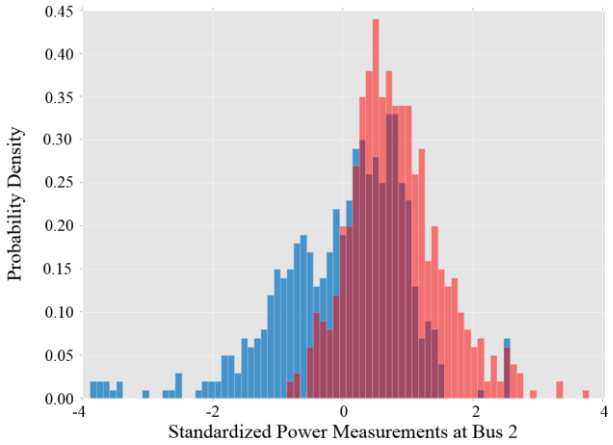

Figure 4. Scenario 2: Manipulated standardized power measurements in red and expected standardized power measurements in blue.

In the first scenario the attacker's motivation is energy theft by manipulating the power measurements at a single bus. In the attack scenario, also known as naive attack [11], the attacker manipulates the meter by pretending to consume less energy than typically observed. The blue distribution in figure 3 shows the historical standardized power measurements of a distribution network, representing the expected distribution. The red distribution shows the manipulated standardized power measurements in a possible attack scenario, where lower measurements occur more frequently.

In the second scenario the manipulated measurements (red) are shifted to the right, relative to the regular measurements (blue). A conceivable scenario for this uncommon distribution could be an attacker pretending to feed an incorrect elevated amount electrical energy with a renewable energy source for a monetary profit. For the validation scenario the ANN was trained with approximately 10000 datasets for each label, achieving a classification accuracy of 96.7%. The ANN was able to successfully distinguish the distributions and identify the manipulated data for both manipulation scenarios. The presented attack scenarios only serve as exemplary use cases since ANN may be trained with any set of distributions related to a manipulation scenario.

VI. Conclusions

In this paper a bad data detection monitoring system for distribution system networks was implemented. Its objectives are the detection, identification and removal of erroneous measurements. Bad data is detected by the CSDT and identified by the LNRT and the HTI respectively. The CSDT determines the presence of bad data within a measurement set based on the statistical properties of the observed measurement residuals. In case the CSDT suspects erroneous measurements within a data set, the bad data identification algorithms LNRT and HTI are initialized in order to locate bad measurements. Prior to state estimation a plausibility check is carried out, removing previous identified bad data and ensuring data consistency. The mathematical methods were validated by coupling the monitoring system with a state estimator observing an 84-bus distribution network and injecting measurements with increasing error percentages.

Aside from the conventional bad data identification methods an intelligent classifier was embedded into the monitoring system. The ANN is able to distinguish between admissible measurement distributions and measurement distributions related to a possible manipulation scenarios based on historical data. In the two exemplary use cases the classifier was able to distinguish expected distributions and hypothesized manipulated distributions.

The ANN can be trained with any set of distributions related to a measurement manipulation scenario and may be utilized for extending the network classification abilities. The ANN applications functionality may be expanded on system level, where the monitored distribution properties at a specific node is compared to observed distributions at nodes with similar specifications. If, for example, a temporarily unusual high load in the system is observed, this may favor an incorrect classification of the ANN on bus level. However, if the ANN observes similar abnormalities at other nodes on system level, an exception of the rule can be formulated. With further investigation, the ANN can be utilized to classify occurring measurement distributions on bus level relative to observations on system level.

REFERENCES

[1] A. Abur, A. Exposito, "Power System State Estimation," M. Dekker New York, vol. 1, pp. 21-35, 2004.

[2] F.C. Schweppe and J.Wilders, "Power System Static-state estimation, Part 1: Exact Model, "IEEE Transactions on Power apparatus and Systems," pp. 120-125, 1970.

[3] M. Hagh, S. Mahaei, M. Zare, "Improving Bad Detection in State Estimation of Power System," IJECE, vol. 1, pp. 85-92, December 2011.

[4] Y. GU, T. Liu, D. Wang, "Bad Data Detection Method for Smart Grid based on Distributen State Estimation," IEEE ICC, 2013.

[5] W. Xu, M. Wang, A. Tang, "On State Estimation with Bad Data Detection," Cornell University, May 2011.

[6] M. Pai, "State Estimation in Electrical Power Systems," Kluwer Boston, vol. 1, pp. 39-61, 1999.

[7] A. Abur, A. Exposito, "Power System State Estimation," M. Dekker New York, vol. 1, pp. 115-141, 2004.

[8] B. Carvalho, "Analysis of the Largest Normalized Residual Test Robustness for Measurement Gross Errors Processing in the WLS State Estimator," Systemics, Cybernetics and Informatics, vol. 11, 2013

[9] L. Mili, T. can Cutsem, M. Pavella, "Hypothesis Testing Identification: A New Method for Bad Data Analysis in Power System State Estimation," IEE Transaction on Power Apparatus and Systems, vol. 103, November 1984.

[10] R. Minguez, A. Conejo, A. Hadi "Non Gaussian State Estimation in Power Systems," International Conference on Mathematical and Statistical Modeling, June 2006

[11] G. Dan, O. Vukovic, H. Sandberg, "Cyber-physical Models of Power System State Estimation Security," KTH Stockholm, December 2012

[12] M. B. Wilk, "An analysis of variance test for nomality," Biometrika, vol. 4, pp. 591-611, 1965