International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1): 38-48
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

Detection and Protection Against Intrusions on Smart Grid Systems

Ata Arvani and Vittal S. Rao
Texas Tech University
Electrical and Computer Engineering Department
Box 43102, Lubbock, Texas 79409, USA
ata.arvani@ttu.edu, vittal.rao@ttu.edu

ABSTRACT

The wide area monitoring of power systems is implemented at a central control center to coordinate the actions of local controllers. Phasor measurement units (PMUs) are used for the collection of data in real time for the smart grid energy systems. Intrusion detection and cyber security of network are important requirements for maintaining the integrity of wide area monitoring systems. The intrusion detection methods analyze the measurement data to detect any possible cyber attacks on the operation of smart grid systems. In this paper, the model-based and signal-based intrusion detection methods are investigated to detect the presence of malicious data. The chi-square test and discrete wavelet transform (DWT) have been used for anomaly-based detection. The false data injection attack (FDIA) can be detected using measurement residual. If the measurement residual is larger than expected detection threshold, then an alarm is triggered and bad data can be identified. Avoiding such alarms in the residual test is referred to as stealth attack. There are two protection strategies for stealth attack: (1) Select a subset of meters to be protected from the attacker (2) Place secure phasor measurement units in the power grid. An IEEE 14-bus system is simulated using real time digital simulator (RTDS) hardware platform for implementing attack and detection schemes.

KEYWORDS

Cyber security, stealth attack, wide area monitoring, smart grid, anomaly-based detection methods, discrete wavelet transform.

1 INTRODUCTION

The generation, transmission, and distribution of electric power systems embedded with real time measurements make the smart grid the most dependable critical infrastructure in the world. The present monitoring systems depends on state estimation, which is based on the supervisory control and data acquisition (SCADA) systems for the collection of data from field devices such as remote terminal units (RTUs) and sent up to the central control center [1]. In the future smart grid systems, the wide area monitoring will be accomplished by collecting system level information in real time by using phasor measurement units (PMUs) and phasor data concentrators (PDCs). The data obtained from PMUs will be used for the state estimation and implementation of control strategies for optimal control of smart grid systems [2-4]. The PMUs which are also called synchrophasors provide accurate measurements of active power, reactive power, voltage, current along with phasor angles in real-time. The data from various remote locations will be synchronized with a common time source using global positioning systems (GPS). In a typical smart grid energy network synchrophasors are used along with PDCs where the data is collected. The synchrophasors can increase the reliability of power systems embedded with renewable energy sources, like the solar and wind power by triggering the corrective actions for accounting the unpredictable power generation. The synchrophasors hold the key to the future power systems by increasing the reliability, operational efficiency and quality of power distribution [5]. Early power system networks used communication standards like DNP3 protocols. These protocols have limitations to handle real-time data and synchronization with the geographically dispersed synchrophasor devices. The current PMUs use IEEE C37.118 protocols for communication, which defines the message and communication standards for synchronized networks in real-time. In future electrical power systems, the wide use of PMUs is inevitable and thus raises the importance of cyber security [6]. There are different methods to detect the malicious data. The main objective of this paper is to investigate the model- and signal-based intrusion detection methods to detect any anomalies in measurement data. The main feature of model-based method lies in the development of dynamic models of the power system and using the chi-square test along with largest normalized residual to detect and identify the malicious data. The signal-based method exploits the statistical properties of the signal and discrete wavelet transform are used to detect and identify the malicious data at different levels [7].

2 MODELLING OF IEEE 14-BUS SYSTEM

The benchmark IEEE 14-bus system has been investigated by a number of researchers for the analysis of dynamic system stability, power flow analysis and state estimation problems [8]. The power system simulator for engineering (PSS/E) is a commercially available software package for simulating, analyzing, and optimizing of power systems. This package has been used to build the PSSE files for the IEEE 14-bus system shown in Figure 1.

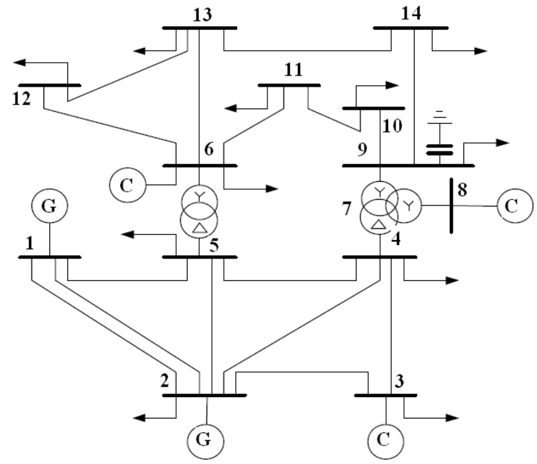

Figure 1. Schematic diagram of IEEE 14-bus system

These files are converted to RSCAD for implementation on RTDS system. An experimental smart grid test bed with hardware-in-the-loop (HIL) simulation capabilities is available at Texas Tech University and a schematic is shown in Figure 2. These facilities were used to implement attack and intrusion methods.

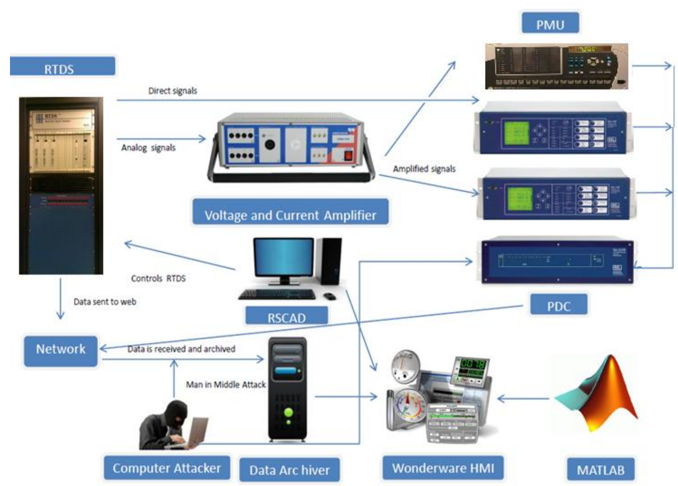

Figure 2. Schematic of smart grid test bed at Texas Tech University

3 MODEL-BASED INTRUSION DETECTION METHODS

Due to presence of malicious data in the power system measurements, the operation of power system will be compromised. Hence we need an intrusion detection method for the detection of malicious data in the measurements [10]. In this section we present an intrusion detection method using static state estimation algorithms. The chi-square distribution test and largest normalized residual tests are used to detect and identify the malicious data [11].

The linear measurement equation is given by:

$$\Delta z = H\Delta x + e \tag{1}$$

Where Δz is the measurement vector, H is the Jacobian coefficient matrix, and e is the error vector with:
$E(e) = 0$ and $cov(e) = R$. The weighted least square (WLS) estimator of the linear state vector can be obtained as follows:

$$\Delta\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} \Delta z \tag{2}$$

And the estimated value of Δz is:

$$\Delta\hat{z} = H\Delta\hat{x} \tag{3}$$

The intrusion detection method consists of two steps:
1) malicious data detection and 2) identification of bad data.
The chi-squares test is used to detect the malicious data and the largest normalized residual test is then used to identify the bad data.
The objective function can be obtained for corresponding measurements:

$$J(\hat{x}) = \sum_{i=1}^{m} \frac{\left(z_i - h_i(\hat{x})\right)^2}{\sigma_i^2} \tag{4}$$

Chi-square distribution table corresponding to a detection confidence with probability p and degree of freedom can be obtained as follows:

$$p = \Pr\left(J(\hat{x}) \leq \chi^2_{(m-n),p}\right) \tag{5}$$

If $J(\hat{x}) \geq \chi^2_{(m-n),p}$ the bad data will be suspected.
The largest normalized residual test can be used to identify bad data.
A gain matrix is defined as:

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

And the hat matrix is:

$$K = H G^{-1} H^T R^{-1} \tag{7}$$

The hat matrix, K, is used to find the residual sensitivity matrix, S, where I is the identity matrix:

$$S = I - K \tag{8}$$

S is multiplied by the error vector, e, to find the measurement residuals, r. The measurement residual vector is divided by the square root of the residual covariance matrix, Ω, which is defined as:

$$\Omega = SR \tag{9}$$

Thus, normalized value of the residual can be obtained as follows:

$$r^N = \frac{|r|}{\sqrt{diag(\Omega)}} \tag{10}$$

The largest normalized residual will be suspected as bad data. We have simulated the IEEE 14-bus system and its measurement configuration for the demonstration of intrusion detection methods [8]. The number of state variable, n, for this system is 27, made up of 14 bus voltage magnitudes and 13 bus voltage phase angles, slack bus phase angle being excluded from the state list. There are altogether $m = 41$ measurents, i.e., 1 voltage magnitude measurement, 8 pairs of real/reactive power injections, and 12 pairs of real/reactive flows. The degrees of freedom for the approximate chi-square distribution of the objective function $J(\hat{x})$ will be: $m - n = 41 - 27 = 14$
The real power injection at bus 2 is manipulated by the man-in-the-middle intentionally, to simulate bad data as shown in Table 1.

Table 1. Real power manipulation at bus 2

Measurement Type	No bad data	One bad data
P_2	0.183	0.483

Tables 2 and 3 illustrate the state estimation of IEEE 14-bus system without malicious data and with malicious data, respectively.

Table 2. IEEE 14-Bus system without malicious data

Bus Number	Estimated State (No Bad Data)	
	V	θ°
1	1	0.00
2	1.0068	0.00
3	0.9899	-5.5265
4	0.9518	-14.2039
5	0.9579	-11.4146
6	0.9615	-9.7583
7	1.0185	-16.0798
8	0.9919	-14.7510
9	1.0287	-14.7500
10	0.9763	-16.5125
11	0.9758	-16.7476
12	0.9932	-16.5397
13	1.0009	-17.0203
14	0.9940	-17.0583

Table 3. IEEE 14-Bus system with malicious data

Bus Number	Estimated State (One Bad Data)	
	V	θ°
1	1	0.00
2	0.9897	0.00
3	0.9731	-5.5304
4	0.9329	-14.9925
5	0.9370	-12.3482
6	0.9407	-10.6143
7	0.9992	-17.2033
8	0.9717	-15.8285
9	1.0094	-15.8269
10	0.9559	-17.6649
11	0.9554	-17.9071
12	0.9733	-17.6846
13	0.9812	-18.1813
14	0.9742	-18.2210

The test threshold at 0.95% confidence level is obtained by MATLAB function:
$y_{\text{threshold}} = \text{chi2inv}(0.95, 14) = 23.68$
For the first case (No malicious data), $J(\hat{x}) = 7.637 < 23.68$, bad data will not be suspected. For the second case (with malicious data in real power injection at bus 2), $J(\hat{x}) = 241.74 > 23.68$, bad data will be suspected.
Figure 3 shows the active power at bus number 2 for the IEEE 14-bus system.

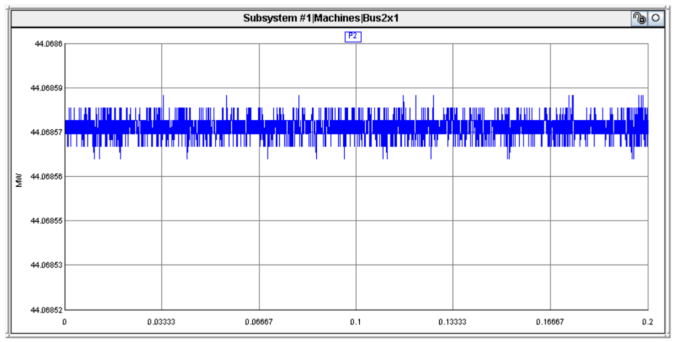

Figure 3. Active power at bus No 2

The normalized residual tests are used to detect and eliminate the bad data for this measurement set. The weighted least squares (WLS) state estimator results for the significant measurement residuals shows that the power injection at bus 2 is detected as bad data and ignored from the measurement set. We verified the efficiency of the model-based algorithm using chi-square test and largest normalized residual for detecting the malicious data.

4 STEALTH ATTACK

In this section, we investigate the stealthy false data injection attack (SFDIA) in the state estimation of power system. The bad data detection can be accomplished by calculating the measurement residual as follows:

$$r = \Delta z - \Delta\hat{z} \qquad (11)$$

if the measurement residual is larger than expected detection threshold, then an alarm is triggered and bad data can be identified. Avoiding such alarms in the residual test is referred to as stealth attack.

The basic principle of stealthy false data injection attack can be represented by:

$$\Delta z_a = \Delta z + \boldsymbol{a} \tag{12}$$

where Δz_a represents the malicious data measurements, and **a** is referred to as an attack vector. If the attack vector is a linear combination of the column vectors of H, that is $\mathbf{a} = \mathrm{Hc}$, the residual test can be bypassed by the attacker. The c is an arbitrary nonzero vector. The jth element attack vector being nonzero means that attacker manipulates the measurement. The new state estimation can be calculated as follows:

$$\Delta\hat{\mathrm{x}}_{\mathrm{bad}} = (\mathrm{H^T R^{-1} H})^{-1}\mathrm{H^T R^{-1}}\Delta \mathrm{z_a} \tag{13}$$

where

$$\Delta\hat{x}_{bad} = \Delta\hat{x} + (\mathrm{H^T R^{-1} H})^{-1}\mathrm{H^T R^{-1}}\mathbf{a} \tag{14}$$

considering $\mathbf{a} = \mathrm{Hc}$, the residual test can be computed as:

$$\begin{aligned}\mathrm{r_{bad}} = \Delta \mathrm{z_a} - \mathrm{H}\Delta\hat{\mathrm{x}}_{\mathrm{bad}} &= \Delta \mathrm{z} + \mathbf{a} \\ &- \mathrm{H}(\Delta\hat{\mathrm{x}} + (\mathrm{H^T R^{-1} H})^{-1}\mathrm{H^T R^{-1}}\mathbf{a}) \\ &= \Delta \mathrm{z} - \mathrm{H}\Delta\hat{\mathrm{x}} + \mathbf{a} - \mathrm{Hc} = \mathrm{r}\end{aligned} \tag{15}$$

Hence, the measurement residual of bad data is less than detection threshold and can bypass the residual test.

In general, there are three different scenarios:

(1) Protected meters (2) Verifiable states (3) Combined scenario

For protected meters we assume that the attacker can access to m particular meters and modify them. Let $\mathcal{F}_{\mathrm{meter}} = \{\mathrm{M_1}, \ldots, \mathrm{M_m}\}$ be the set of the m particular meters which can be accessed by the attacker. For the protected meters which cannot be accessed, the associated attack vector would be zero.

1) Targeted attack: In a targeted FDIA, the attacker aims to inject errors into state estimation of some particular state variables.

a) Constrained case:

The error injected into the state estimation can be calculated as follows:

$$\Delta\hat{x}_{bad} = \Delta\hat{x} + c \tag{16}$$

Let $\mathcal{F}_{\text{verified states}}$, represents the set of state variable which can be verified independently, i.e., $\mathrm{c_j} = 0$ for $j \in \mathcal{F}_{\text{verified states}}$. Therefore, the attacker can substitute c into $a = Hc$, and verify if $\mathrm{a_j} = 0$ for $j \notin \mathcal{F}_{\mathrm{meter}}$. If so, the attack vector can be generated.

b)unconstrained case:

For this case, the attack vector should meet these conditions:

1) $a = Hc$
2) $\mathrm{a_j} = 0$ for all $j \notin \mathcal{F}_{\mathrm{meter}}$
3) $\mathrm{c_j}$ is a particular value for $j \notin \mathcal{F}_{\text{verified states}}$

2) Random attack: In a random attack, the attacker aims to inject error into state estimation regardless of any particular state variables.

Theorem 1. $\mathrm{a} = \mathrm{Hc}$ if and only if $\mathrm{Ba} = 0$, where $\mathrm{B} = \mathrm{H(H^T H)^{-1} H^T} - \mathrm{I}$

Theorem 2. Let m be the number of particular meters which can be accessed. if $\mathrm{m} > \mathrm{l} - \mathrm{n}$, the attacker can always bypass the residual test which satisfies $\mathrm{a} = \mathrm{Hc}$ with $\mathrm{a_j} = 0$ for $j \notin \mathcal{F}_{\mathrm{meter}}$ where $\mathcal{F}_{\mathrm{meter}}$ represents the set of particular meters which can be accessed.

Demonstration of stealth attack using IEEE 14-bus system:

In this section, we investigate the targeted attack in IEEE 14-bus system for the first nineteen measurements. The linear measurement equation of IEEE 14-bus system can be expressed as follows:

$$\Delta \mathrm{z} = \mathrm{H}\Delta \mathrm{x} + \mathrm{e} \tag{17}$$

where Δz is a 41×1 measurement vector, H is 41×27 Jacobian coefficient matrix, and $\Delta\mathrm{x}$ is a 27×1 state vector.

The attack vector can be represented as follows:

$$\begin{bmatrix}\mathrm{a_{unprotected}} \\ \mathrm{a_{protected}}\end{bmatrix} = \begin{bmatrix}\mathrm{H_{11}} & \mathrm{H_{12}} \\ \mathrm{H_{21}} & \mathrm{H_{22}}\end{bmatrix}\begin{bmatrix}\mathrm{c_1} \\ \mathrm{c_2}\end{bmatrix} \tag{18}$$

where H_{11} is 19×5, H_{12} is 19×22, H_{21} is 22×5, and H_{22} is 22×22 square matrix.
As mentioned earlier, the attack vector for protected meters would be zero. Hence, the $\mathrm{a}_{\text{protected}} = 0$ and we have:

$$\mathrm{c}_2 = \mathrm{H}_{22}^{-1}\mathrm{H}_{21}\mathrm{c}_1 \tag{19}$$

and

$$\mathrm{a}_{\text{unprotected}} = \mathrm{a}_1 = [\mathrm{H}_{11} - \mathrm{H}_{12}\mathrm{H}_{22}^{-1}\mathrm{H}_{21}]\mathrm{c}_1$$
$$\mathrm{a}_{\text{protected}} = \mathrm{a}_2 = 0 \tag{20}$$

The numerical values are given in Appendix. Choosing c_1 arbitrary, the attack vector can be obtained as:

$$a = \begin{bmatrix} a_{unprotected} \\ 0 \end{bmatrix}$$
$$z_a = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} + \begin{bmatrix} a_1 \\ 0 \end{bmatrix} = \begin{bmatrix} z_1 + a_1 \\ z_2 \end{bmatrix} \tag{21}$$

There are two protection strategies for stealth attack.
(1) Select a subset of meters to be protected from the attacker
(2) Place secure phasor measurement units in the power grid
For the first strategy, let P be the minimum number of meters that the attacker needs to satisfies the detection evading condition as follows:

$$\mathrm{c} = (\mathrm{H}^{\mathrm{T}}\mathrm{H})^{-1}\mathrm{H}^{\mathrm{T}}\mathrm{a} \tag{22}$$

The injected error to the jth state can be expressed as:

$$\mathrm{a}_{\mathrm{j}} = \mathrm{H}_{\mathrm{j}}^{\mathcal{F}_{\text{meter}}}\bar{\mathrm{c}}_{\mathrm{j}} + \mathrm{h}_{\mathrm{j}}^{\mathcal{F}_{\text{meter}}} \tag{23}$$

where $\mathrm{H}_{\mathrm{j}}^{\mathcal{F}_{\text{meter}}}$ is $\mathrm{H}^{\mathcal{F}_{\text{meter}}}$ after deleting the jth column $\mathrm{h}_{\mathrm{j}}^{\mathcal{F}_{\text{meter}}}$ and $\bar{\mathrm{c}}_{\mathrm{j}}$ is the best possible attack vector modifying at least the jth state with the objective function and constraint as follows:

$$min \quad |\overline{\mathcal{F}_{\text{meter}}}|$$

such that: $$\min\|a_j\|_0 \geq P \tag{24}$$

which $\|\mathrm{a}_{\mathrm{j}}\|_0$ is the number of nonzero elements in a_j.
In the second strategy, by adding some other phasor measurement units into the power system, the Jacobian coefficient matrix would be modified. Consider H_{P} be the Jacobian associated matrix corresponding to a secure PMU at bus P.
The attacker should satisfies the following condition:

$$\begin{bmatrix} \mathrm{H}^{\mathcal{F}_{\text{meter}}} \\ \mathrm{H}_{\mathrm{P}} \end{bmatrix} \mathrm{c} = 0 \tag{25}$$

Given $\bar{c}_j$, the goal for grid designer is to find a bus to place a secure PMU such that:

$$\mathrm{H}_{\mathrm{P}}\bar{\mathrm{c}}_{\mathrm{j}} \neq 0 \tag{26}$$

As a result, the attacker should find another solution for c.

5 SIGNAL-BASED INTRUSION DETECTION METHODS

A brief review of discrete wavelet transform (DWT) is presented in this section [12]. DWT is a mathematical tool to decompose signals and is used to extract information in different resolution levels. Wavelet transform breaks the signal into its wavelets, which are scaled and shifted versions of a signal waveform known as the mother wavelet. Wavelet analysis is suitable for revealing scaling properties of the temporal and frequency dynamics simultaneously. The irregularity in shape and compactly supported nature of wavelets make wavelet analysis an ideal tool for analyzing signals of a non-stationary nature. Their fractional nature allows them to analyze signals with discontinuities or sharp changes, while their compactly supported nature enables temporal localization of a signal's features. A one-dimensional discrete wavelet transform is composed of decomposition (analysis) and reconstruction (synthesis). Discrete wavelet transform produces two sets of constants term as approximation and detail coefficients. The approximation coefficients are the high scale, low frequency components and the detail coefficients are the low scale, high frequency components. The signal is passed through a series of high pass and low pass filters to analyze respective functions at each level. Wavelet analysis starts by selecting basic wavelet function, called the mother wavelet, $\phi(t)$. Wavelet representaion of a function $f(t)$, defined for all $t \in \mathbb{R}$, can be given by:

$$f(t) = \sum_{k=-\infty}^{+\infty} a_{0,k}\, \phi(t-k)$$

$$+ \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{j-1} d_{j,k} \psi(2^j t - k) \qquad (27)$$

By considering Haar wavelet the scaling function $\phi(t)$ and wavelet function $\psi(t)$ are defined as:

$$\phi(t) = \begin{cases} \frac{1}{\sqrt{2}}, 0 \le t \le 1 \\ 0 \quad \text{otherwise} \end{cases} \qquad (28)$$

$$\psi(t) = \begin{cases} \frac{1}{\sqrt{2}}, 0 \le t \le \frac{1}{2} \\ \frac{-1}{\sqrt{2}}, \frac{1}{2} \le t \le 1 \\ 0 \quad \text{otherwise} \end{cases} \qquad (29)$$

For a given signal, approximation and detail coefficients can be obtained by convolving low-pass filter and high-pass filter followed by down sampler, respectively.

$$a_{j-1,i} = \sum_{k=0}^{2N-1} L_k c_{j,2i+k} \qquad (30)$$

$$d_{j-1,i} = \sum_{k=0}^{2N-1} H_k c_{j,2i+k} \qquad (31)$$

The low-pass filters are represented by L, and the high-pass filters are represented by H.

Anomaly detection of malicious data consists of three parts as shown in Figure 4. The first part is the PMU signal from the power system. The second part consists of discrete wavelet transformation to analyze the signal [13-15]. In the third part, the threshold values are compared for the determination of the anomalies in the signal.

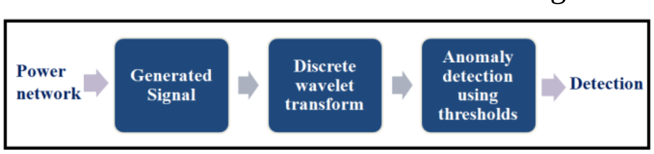

Figure 4. Anomaly-based intrusion detector

The benchmark and corrupted data of voltage and current are shown in Figures 5 and 6, respectively. Discrete wavelet transform is used to analyze the measured signal, by calculating the statistical properties of the signal.

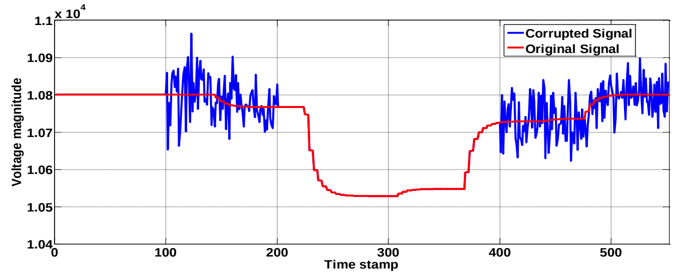

Figure 5. Original and corrupted data of voltage signal

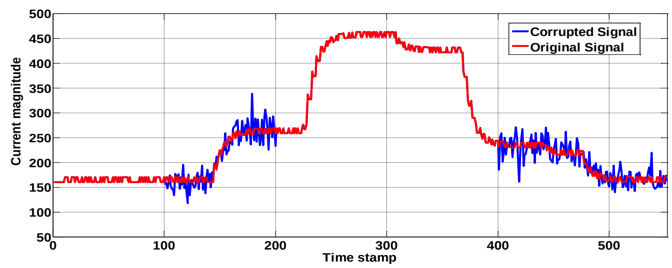

Figure 6. Original and corrupted data of current signal

We employ Haar filter and compute the one-dimensional discrete wavelet transform up to 5 levels. In order to obtain the thresholds for anomaly-based intrusion detection the distribution of the wavelet reconstructed signal without anomaly should be analyzed. Then, normality is verified by Lilliefors test for goodness of fit to normal distribution [16-18]. This has a normal distribution at 5% significance level. We can detect anomaly intrusion by choosing some of the levels through selective reconstruction. Table 4 and Table 5 show some statistical properties of original and corrupted data of voltage and current signal. It should be noted that the original data could be considered as Gaussian white noise, and anomaly could be considered as random signal. For any random variable, choosing $\pm 3\sigma$ confidence interval yields to:

$$P(\mu - 3\sigma < X \le \mu + 3\sigma) \approx 99.7\% \qquad (32)$$

This interval corresponds to 99.7% confidence level, which means that we can detect anomalies with 0.3% error rate.

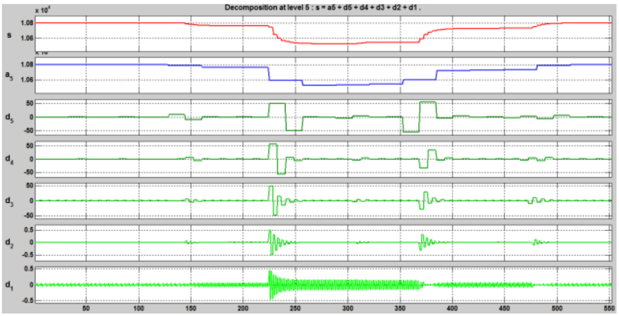

Figure 7. Wavelet decomposition of original voltage signal

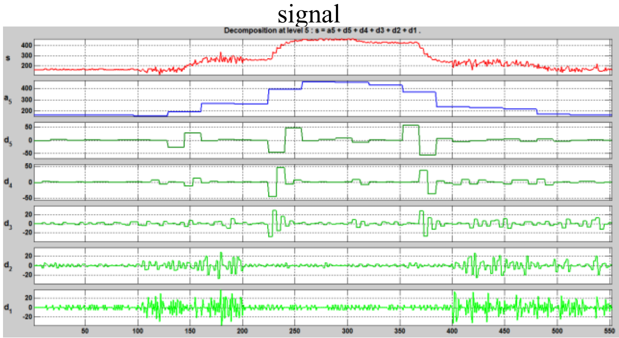

Figure 8. Wavelet decomposition of corrupted voltage signal

The PMU signals are analyzed at different resolution levels. Figures 7 and 8 show the approximation and detail coefficients of original and corrupted signal of voltage up to level 5. By comparing the analyzed information with thresholds it is possible to detect the anomalies and alert the operator regarding the presence of anomalies in the data. In order to detect shorter anomalies we have analyzed the signal at higher level such as 1 and 2. For example, by selecting the thresholds at level 1 to -0.2832 and 0.2832 respectively, which is equivalent to $\pm 3\sigma$ we can detect the anomalies with error rate of 0.3%. Table 4 shows the statistical parameters of voltage signal like standard deviation for original and corrupted data.

Table 4. Statistical properties of voltage signal

Original data of voltage magnitude			Corrupted data of voltage magnitude	
Level	Standard deviation	Threshold	Level	Standard deviation
1	0.0944	0.2832	1	5.121
2	0.1265	0.3795	2	4.854
3	20.67	62.01	3	21.64
4	47.13	141.39	4	48.11
5	102.2	306.60	5	101.4

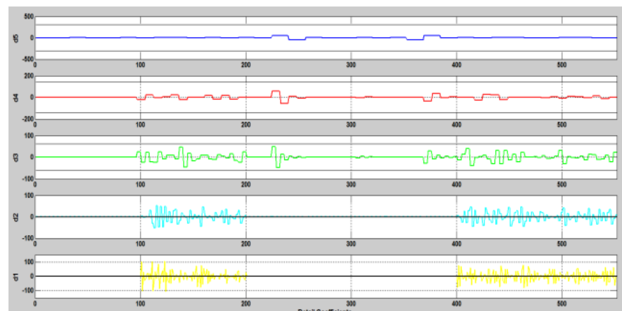

Figure 9. Thresholds values and detail coefficients at different levels of voltage signal

We can set the thresholds for each level, which are equivalent to $\pm 3\sigma$ confidence level to detect the anomalies. We have repeated the procedure for current signals. The detail and approximation coefficients of original current signal and corrupted current signals are shown in Figures 10 and 11, respectively.

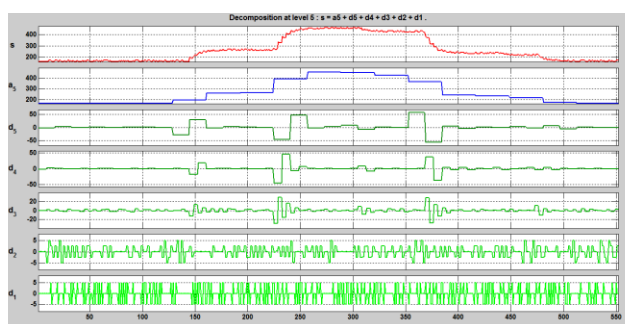

Figure 10. Wavelet decomposition of original current signal

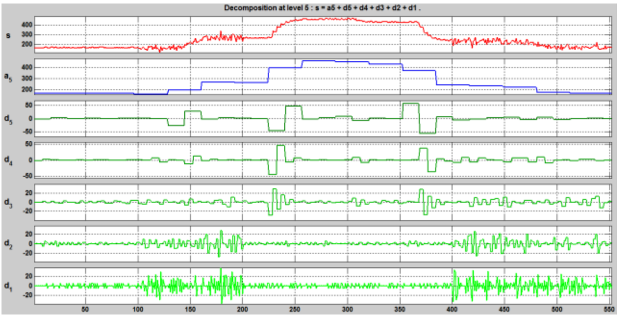

Figure 11. Wavelet decomposition of corrupted current signal

Table 5 shows the statistical parameters of current signal like standard deviation for original and corrupted data.

Table 5. Statistical properties of current signal

Original data of current magnitude			Corrupted data of current magnitude	
Level	Standard deviation	Threshold	Level	Standard deviation
1	5.122	15.36	1	13.57
2	4.84	14.52	2	14.94
3	17.86	53.58	3	19.47
4	42.86	128.58	4	43.44
5	111.4	334.2	5	110

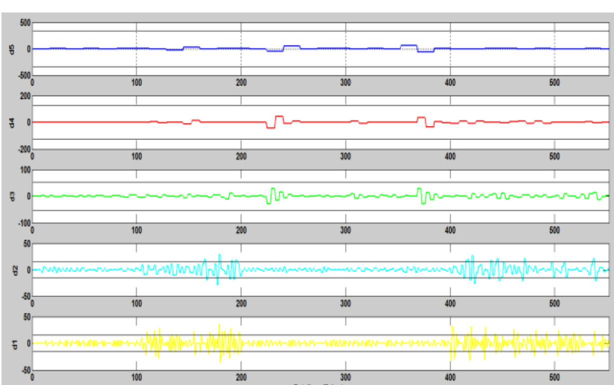

Figure 12. Thresholds values and detail coefficients at different levels of current signal

Figures 9 and 12 show the detail coefficients and corresponding thresholds for original and corrupted signal at different levels up to 5. The values located on the top and bottom of the thresholds indicate that intrusion has been occurred in the network. For the corrupted voltage and current signals, Figures 9 and 12, the detail coefficients at level 1, and level 2 are greater than the corresponding thresholds and the malicious data has been detected. The results show that the use of proposed method successfully detected the anomalies in the data.

6 CONCLUSIONS

Wide-area monitoring and control that coordinates the various devices of the power system to improve system-wide dynamic performance and stability is being implemented in the smart grids. These critical devices usually have the most significant impacts on power system oscillation, damping, performance and stability. The cyber security and the data integrity are very important for successful integration of phasor measurement units for automatic control of electric power systems. In this paper a cyber security tool is developed and presented for intrusion detection. We have simulated an IEEE benchmark 14-bus system using RTDS system. The bench mark and malicious data has been generated in our laboratory. The proposed cyber security tool for the detection of intrusion detection has been successfully employed on this data. The results are very satisfactory. The detection method depends on the selection of threshold values. In the future we will be comparing this method with the methods based on measurement residual detection methods.

7ACKNOWLEDGMENTS

The authors gratefully acknowledge support of the National Science Foundation through grant ECCS-

1040161 for acquiring the research instrumentation used in this research work.

8 APPENDIX

H_{11} =
[0 0 0 0 0; 29.3120 -4.6148 -4.9889 -5.0489 0; -4.2921 8.8195 -4.5274 0 0; 0 0 -4.6375 0 0; 0 0 0 0 0; 0 0 0 0 0; 0 0 0 0 -4.1249; 0 0 0 0 -3.2113; 0 0 0 0 0; -9.1431 0.3773 1.0925 1.2497 0; 1.7368 -3.7701 2.0333 0 0; 0 0 0.2704 0 0; 0 0 0 0 0; 0 0 0 0 0; 0 0 0 0 2.0106; 0 0 0 0 1.6083; 0 0 0 0 0; -15.6191 0 0 0 0; 4.6148 -4.6148 0 0 0];

H_{12} =
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 -6.3806 9.6128 -0.3964 -1.1406 -1.2999 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 -1.7546 1.9797 -2.1227 0 0 0 0 0 0 0 0 0;19.2277 -5.7921 -8.7981 0 0 0 0 0 0 0 0 -0.2823 0 0 0.0001 -0.0001 0.2772 0 0 0 0 0; -5.7921 5.7921 0 0 0 0 0 0 0 0 0 0 0 0.0001 0.0001 0 0 0 0 0 0; 0 0 -9.8589 14.1190 -4.2601 0 0 0 0 0 0 0 0 0 0 0 -3.8489 5.5507 -1.8509 0 0 0;0 0 0 -4.2733 8.3982 0 0 0 0 0 0 0 -1.9742 0 0 0 -1.8521 3.7749 0 0 0;0 0 0 0 5.4531 -2.2418 0 0 0 0 0 0 -1.5792 0 0 0 0 0 3.9574 -2.4896 0;0 0 -2.8194 0 0 0 -2.2033 5.0226 0 0 0 0 0 0 0 0 -1.4438 0 0 0 -1.1293 2.3159;0 0 0 0 0 0 0 -14.5614 30.3178 -4.8487 -5.2085 -5.2515 0 0 0 0 0 0 0 0 0 0;0 0 0 0 0 0 0 0 0 -4.3361 9.4306 -4.7266 0 0 0 0 0 0 0 0 0 0;0.0001 0.0001 -0.2706 0 0 0 0 0 0 0 0 -4.8415 0 0 19.3948 -5.6308 -9.0119 0 0 0 0 0; -0.0001 0.0001 0 0 0 0 0 0 0 0 0 0 0 -5.8395 6.0483 0 0 0 0 0 0;0 0 3.7577 -5.5958 1.8382 0 0 0 0 0 0 0 0 0 0 0 -10.0985 14.3511 -4.2895 0 0 0;0 0 0 1.8072 -3.8177 0 0 0 0 0 0 0 0 -4.0502 0 0 0 -4.3794 8.4210 0 0 0; 0 0 0 0 0 -4.0828 2.4745 0 0 0 0 0 0 -3.1532 0 0 0 0 0 5.4166 -2.2555 0;0 0 1.4096 0 0 0 1.1224 -2.5320 0 0 0 0 0 0 0 0 -2.8879 0 0 0 -2.2168 5.1031;0 0 0 0 0 0 0 6.5953 -3.5294 0 0 0 0 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 1.8658 -0.3964 0 0 0 0 0 0 0 0 0 0 0 0];

H_{21} =
[-4.6609 0 4.6609 0 0; 0 0 4.6375 0 0; 0 0 1.7283 0 0; -4.8100 0 0 4.8100 0; 0 0 -20.0455 20.0455 0; 0 0 0 4.1433 -4.1433; 0 0 0 0 6.2300; 0 0 0 0 0; 0 0 0 0 -4.1249; 0 0 0 0 0;3.4936 0 0 0 0; -0.3773 0.3773 0 0 0; 2.0878 0 -2.0878 0 0; 0 0 0.2704 0 0; 0 0 0.1542 0 0; 1.9793 0 0 -1.9793 0; 0 0 5.7228 -5.7228 0; 0 0 0 0.4591 -0.4591; 0 0 0 0 -3.0309; 0 0 0 0 0; 0 0 0 0 2.0106; 0 0 0 0 0];

H_{22} =
[0 0 0 0 0 0 0 0 0 -2.1092 0 1.0503 0 0 0 0 0 0 0 0 0 0;-4.6375 0 0 0 0 0 0 0 0 0 0 0 0.2823 0 0 0.2726 0 0 0 0 0 0; 0 0 -1.7283 0 0 0 0 0 0 0 0 0.1610 0 0 0 0 0.1579 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 -1.9996 0 0 1.2123 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0 0 -5.9746 7.2017 0 0 0 0 0 0 0 0 0;0 0 0 0 0 0 0 0 0 0 0 0 0.4775 0.4508 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 -6.2300 0 0 0 0 0 0 3.3361 0 0 0 0 0 -3.0495 0; 8.7981 0 -8.7981 0 0 0 0 0 0 0 0 0 0 0 0.2728 0 0.2772 0 0 0 0 0;0 0 0 0 4.1249 0 0 0 0 0 0 0 0 -1.9742 0 0 0 0 1.8587 0 0 0;0 0 0 0 0 2.2418 -2.2418 0 0 0 0 0 0 0 0 0 0 0 0 2.5099 -2.4896 0;0 0 0 0 0 0 0 15.1638 -15.7791 0 0 0 0 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 4.7613 -4.8487 0 0 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 -4.7087 0 4.9019 0 0 0 0 0 0 0 0 0 0; -0.2704 0 0 0 0 0 0 0 0 0 0 4.5253 0 0 -4.6755 0 0 0 0 0 0 0; 0 0 -0.1542 0 0 0 0 0 0 0 0 1.7503 0 0 0 0 -1.7703 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 -4.8592 0 0 4.9509 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0 -20.9276 20.6424 0 0 0 0 0 0 0 0 0; 0 0 0 0 0 0 0 0 0 0 0 3.8768 -4.0683 0 0 0 0 0 0 -6.2683 0;0 0 0 0 0 0 3.0309 0 0 0 0 0 0 6.3133 0 0 0 0 0 0 0 0; 0.2706 0 -0.2706 0 0 0 0 0 0 0 0 0 0 0 9.1621 0 -9.0119 0 0 0 0 0;0 0 0 0 -2.0106 0 0 0 0 0 0 0 0 -4.0502 0 0 0 0 3.9784 0 0 0;0 0 0 0 0 -2.4745 2.4745 0 0 0 0 0 0 0 0 0 0 0 0 2.2679 -2.2555 0];

$c_1 =$
[0.1; -2.5;3; 1;1.5];

$a_1 =$
[17.8938;-4.8379; -71.5305; 29.7217; -29.7013; -168.4239; 40.4534; -0.0244; -66.8719; -5.5095; 13.2331; 89.5476; -101.3154; -224.7588; 73.0451; -0.0801; -77.6946;55.6844;37.5025];

9 REFERENCES

[1] Leirbukt, A.; Breidablik, O.; Gjerde, J.O.; Korba, P.; Uhlen, K.; Vormedal, L.K., “Deployment of a SCADA integrated wide area monitoring system”, Transmission and Distribution Conference and Exposition: Latin America, 2008 IEEE/PES, pp. 1 – 6., Aug 2008.

[2] Hong Li; Weiguo Li, "A new method of power system state estimation based on wide-area measurement system," Industrial Electronics and Applications, 2009. ICIEA 2009. 4th IEEE Conference, pp.2065-2069, 25-27 May 2009.

[3] Monticelli, “Electric Power System State Estimation”, Proceedings of the IEEE, Vol. 88, No. 2, Feb. 2000 pp. 262-282.

[4] L. Zhao, A. Abur, “Multi Area State Estimation Using Synchronized Phasor Measurements,” IEEE Transactions on Power Systems, Vol. 20, No. 2, pp. 611-617, May 2005.

[5] XiaoYun Chen; DongMei Zhao; Xu Zhang, "A Novel Voltage Stability Prediction Index Based On Wide Area Measurement," Power and Energy Engineering Conference (APPEEC), 2010 Asia-Pacific ,Vol., No., pp.1-4, 28-31 March 2010.

[6] Luitel, B.; Venayagamoorthy, G.K.; Johnson, C.E., “Enhanced wide area monitoring systems”, Innovative Smart Grid Technologies, pp. 1-7, Jan. 2010.

[7] Seong Soo Kim; Reddy, A.L.N., "Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data," Networking, IEEE/ACM Transactions on, Vol.16, No.3, pp.562-575, June 2008.

[8] L.L. Freris, A.M. Sasson, “Investigation of the Load-Flow Problem,” Proceedings of IEE, Vol. 115, No. 10, pp. 1459-1470, 1968.

[9] Meikang Qiu; Wenzhong Gao; Min Chen; Jian-Wei Niu; Lei Zhang , “Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System”, IEEE Transactions on Smart Grid , Vol. 2, No. 4, pp. 715 – 723, Dec. 2011.

[10] Denning, D.E., "An Intrusion-Detection Model," Software Engineering, IEEE Transactions on, Vol.SE-13, No.2, pp. 222- 232, Feb. 1987.

[11] A. Abur and A. G. Expósito, "Power System State Estimation: Theory and Implementation." Boca Raton, FL: CRC, 2004.

[12] Mallat, A wavelet tour of signal processing. Academic Press, 1998.

[13] C. T. Huang, S. Thareja, and Y. J. Shin, “Wavelet based real time detection of network traffic anomalies,” in Securecomm and Workshops, 2006, pp. 1–7, 2006.

[14] J.Gao, G. Hu,X. Yao, and R. K. C. Chang, “Anomaly detection of network traffic based on wavelet packet,” in Proceedings of the Asia- Pacific Conference on Communications (APCC ’06), pp. 1–5, Busan, Korea, August 2006.

[15] Seong Soo Kim , A. L. Narasimha Reddy , Marina Vannucci, “Detecting traffic anomalies using discrete wavelet transforms“, Proceedings of International Conference on Information Networking (ICOIN), Busan, Korea.

[16] Kosut, O.; Liyan Jia; Thomas, R.J.; Lang Tong; , "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on , Vol., No., pp.220-225, 4-6 Oct. 2010.

[17] A. Monticelli, F. F. Wu, and M. Y. Multiple. Bad data identification for state estimation by combinatorial optimization. IEEE Transactions on Power Delivery, 1(3):361–369, July 1986.

[18] Y. Liu and P. Ning and M. K. Reiter, “False Data Injection Attacks against State Estimation in Electric Power Grids”, Proc. of the 16th ACM conference on Computer and communications security, Nov. 2009.