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. 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.

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:

$$\Delta z = H\Delta x + e$$  \hspace{1cm} (1)

Where $\Delta z$ is the measurement vector, $H$ is the Jacobian coefficient matrix, and $e$ is the error vector with:

$$E(e) = 0 \text{ and } \text{cov}(e) = R.$$ The weighted least square (WLS) estimator of the linear state vector can be obtained as follows:

$$\Delta \hat{x} = (H^TR^{-1}H)^{-1}H^TR^{-1}\Delta z$$  \hspace{1cm} (2)

And the estimated value of $\Delta z$ is:

$$\Delta \hat{z} = H\Delta \hat{x}$$  \hspace{1cm} (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:

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

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

$$p = \text{Pr} \left( J(\bar{x}) \leq \chi^2_{(m-n),p} \right)$$  \hspace{1cm} (5)

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

$$G = H^TR^{-1}H$$  \hspace{1cm} (6)

And the hat matrix is:

$$K = HG^{-1}H^TR^{-1}$$  \hspace{1cm} (7)

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

$$S = I - K$$  \hspace{1cm} (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, $\Omega$, which is defined as:

$$\Omega = SR$$  \hspace{1cm} (9)

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

$$r^N = \frac{|r|}{\sqrt{\text{diag}(\Omega)}}$$  \hspace{1cm} (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 $m = 41$ measurements, 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 $J(\bar{x})$ 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

<table>
<thead>
<tr>
<th>Measurement Type</th>
<th>No bad data</th>
<th>One bad data</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_2</td>
<td>0.183</td>
<td>0.483</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Bus Number</th>
<th>Estimated State (No Bad Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1.0068</td>
</tr>
<tr>
<td>3</td>
<td>0.9899</td>
</tr>
<tr>
<td>4</td>
<td>0.9518</td>
</tr>
<tr>
<td>5</td>
<td>0.9579</td>
</tr>
<tr>
<td>6</td>
<td>0.9615</td>
</tr>
<tr>
<td>7</td>
<td>1.0185</td>
</tr>
<tr>
<td>8</td>
<td>0.9919</td>
</tr>
<tr>
<td>9</td>
<td>1.0287</td>
</tr>
<tr>
<td>10</td>
<td>0.9763</td>
</tr>
<tr>
<td>11</td>
<td>0.9758</td>
</tr>
<tr>
<td>12</td>
<td>0.9932</td>
</tr>
<tr>
<td>13</td>
<td>1.0009</td>
</tr>
<tr>
<td>14</td>
<td>0.9940</td>
</tr>
</tbody>
</table>

Table 3. IEEE 14-Bus system with malicious data

<table>
<thead>
<tr>
<th>Bus Number</th>
<th>Estimated State (One Bad Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0.9897</td>
</tr>
<tr>
<td>3</td>
<td>0.9731</td>
</tr>
<tr>
<td>4</td>
<td>0.9329</td>
</tr>
<tr>
<td>5</td>
<td>0.9370</td>
</tr>
<tr>
<td>6</td>
<td>0.9407</td>
</tr>
<tr>
<td>7</td>
<td>0.9992</td>
</tr>
<tr>
<td>8</td>
<td>0.9717</td>
</tr>
<tr>
<td>9</td>
<td>1.0094</td>
</tr>
<tr>
<td>10</td>
<td>0.9559</td>
</tr>
<tr>
<td>11</td>
<td>0.9554</td>
</tr>
<tr>
<td>12</td>
<td>0.9733</td>
</tr>
<tr>
<td>13</td>
<td>0.9812</td>
</tr>
<tr>
<td>14</td>
<td>0.9742</td>
</tr>
</tbody>
</table>

The test threshold at 0.95% confidence level is obtained by MATLAB function:

$y_{threshold} = \text{chi2inv}(0.95, 14) = 23.68$

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:

$$r = \Delta z - \Delta \hat{z}$$  \hspace{1cm} (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:

\[ \Delta z_a = \Delta z + a \]  
(12)

where \( \Delta z_a \) 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 \( a = Hc \), the residual test can be bypassed by the attacker. The \( c \) is an arbitrary nonzero vector. The \( j \)th element attack vector being nonzero means that attacker manipulates the measurement. The new state estimation can be calculated as follows:

\[ \Delta \hat{x}_{bad} = (H^T R^{-1} H)^{-1} H^T R^{-1} \Delta z_a \]  
(13)

\[ \Delta \hat{x}_{bad} = \Delta \hat{x} + (H^T R^{-1} H)^{-1} H^T R^{-1} a \]  
(14)

considering \( a = Hc \), the residual test can be computed as:

\[ r_{bad} = \Delta z_a - H \Delta \hat{x}_{bad} \]

\[ = \Delta z + a \]
\[ - H(\Delta \hat{x} + (H^T R^{-1} H)^{-1} H^T R^{-1} a) \]
\[ = \Delta z - H \Delta \hat{x} + a - Hc = r \]  
(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 particular meters and modify them. Let \( F_{\text{meter}} = \{ M_1, ..., M_m \} \) be the set of the 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:

\[ \Delta \hat{x}_{bad} = \Delta \hat{x} + c \]  
(16)

Let \( F_{\text{verified states}} \) represents the set of state variable which can be verified independently, i.e., \( c_j = 0 \) for \( j \in F_{\text{verified states}} \). Therefore, the attacker can substitute \( c \) into \( a = Hc \), and verify if \( a_j = 0 \) for \( j \notin F_{\text{meter}} \). 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) \( a_j = 0 \) for all \( j \notin F_{\text{meter}} \)
3) \( c_j \) is a particular value for \( j \notin F_{\text{verified states}} \)

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

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

**Theorem 2.** Let \( m \) be the number of particular meters which can be accessed. if \( m > 1 - n \), the attacker can always bypass the residual test which satisfies \( a = Hc \) with \( a_j = 0 \) for \( j \notin F_{\text{meter}} \) where \( F_{\text{meter}} \) 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:

\[ \Delta z = H \Delta x + e \]  
(17)

where \( \Delta z \) is a \( 41 \times 1 \) measurement vector, \( H \) is \( 41 \times 27 \) Jacobian coefficient matrix, and \( \Delta x \) is a \( 27 \times 1 \) state vector.

The attack vector can be represented as follows:

\[ \begin{bmatrix} \alpha_{\text{unprotected}} \\ \alpha_{\text{protected}} \end{bmatrix} = \begin{bmatrix} H_{11} & H_{12} \\ H_{21} & H_{22} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \]  
(18)
where $H_{11}$ is $19 \times 5$, $H_{12}$ is $19 \times 22$, $H_{21}$ is $22 \times 5$, and $H_{22}$ is $22 \times 22$ square matrix.

As mentioned earlier, the attack vector for protected meters would be zero. Hence, the $a_{\text{protected}} = 0$ and we have:

$$c_2 = H_{22}^{-1}H_{21}c_1 \quad (19)$$

and

$$a_{\text{unprotected}} = a_1 = [H_{11} - H_{12}H_{22}^{-1}H_{21}]c_1$$

$$a_{\text{protected}} = a_2 = 0 \quad (20)$$

The numerical values are given in Appendix.

Choosing $c_1$ arbitrary, the attack vector can be obtained as:

$$a = \begin{bmatrix} a_{\text{unprotected}} \\ 0 \end{bmatrix}$$

$$z_a = \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ 0 \end{bmatrix} = \begin{bmatrix} z_1 + a_1 \\ z_2 \end{bmatrix} \quad (21)$$

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 satisfy the detection evading condition as follows:

$$c = (H^TH)^{-1}H^Ta \quad (22)$$

The injected error to the $j$th state can be expressed as:

$$a_j = H_{j\text{meter}}F\overline{c}_j + h_{j\text{meter}} \quad (23)$$

where $H_{j\text{meter}}$ is $H_{\text{meter}}$ after deleting the $j$th column $h_{j\text{meter}}$ and $\overline{c}_j$ is the best possible attack vector modifying at least the $j$th state with the objective function and constraint as follows:

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

such that:

$$\min \|a_j\|_0 \geq P \quad (24)$$

which $\|a_j\|_0$ 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:

$$\begin{bmatrix} H_{\text{meter}}^T \\ H_P \end{bmatrix} c = 0 \quad (25)$$

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

$$H_P\overline{c}_j \neq 0 \quad (26)$$

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 representation of a function $f(t)$, defined for all $t \in \mathbb{R}$, can be given by:

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

(27)

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

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

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

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.

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

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

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](image)

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](image)

![Figure 6. Original and corrupted data of current signal](image)

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:

$$P(\mu - 3\sigma < X \leq \mu + 3\sigma) \approx 99.7\% \quad (32)$$
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](image)

![Figure 8. Wavelet decomposition of corrupted voltage signal](image)

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

<table>
<thead>
<tr>
<th>Level</th>
<th>Standard deviation</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0944</td>
<td>0.2832</td>
</tr>
<tr>
<td>2</td>
<td>0.1265</td>
<td>0.3795</td>
</tr>
<tr>
<td>3</td>
<td>2.076</td>
<td>62.01</td>
</tr>
<tr>
<td>4</td>
<td>47.13</td>
<td>141.39</td>
</tr>
<tr>
<td>5</td>
<td>102.2</td>
<td>306.60</td>
</tr>
</tbody>
</table>

![Figure 9. Thresholds values and detail coefficients at different levels of voltage signal](image)

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](image)
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**

<table>
<thead>
<tr>
<th>Level</th>
<th>Original data of current magnitude</th>
<th>Corrupted data of current magnitude</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard deviation</td>
<td>Threshold</td>
</tr>
<tr>
<td>1</td>
<td>5.122</td>
<td>15.36</td>
</tr>
<tr>
<td>2</td>
<td>4.84</td>
<td>14.52</td>
</tr>
<tr>
<td>3</td>
<td>17.86</td>
<td>53.58</td>
</tr>
<tr>
<td>4</td>
<td>42.86</td>
<td>128.58</td>
</tr>
<tr>
<td>5</td>
<td>111.4</td>
<td>334.2</td>
</tr>
</tbody>
</table>

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.

7 ACKNOWLEDGMENTS

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

\[ H_{11} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ H_{12} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ H_{21} = \begin{bmatrix} -4.6375 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ H_{22} = \begin{bmatrix} -4.6375 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}^{-1} \begin{bmatrix} -0.2706 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]
9 REFERENCES


