Cyber Attack Detection in PMU Measurements via the Expectation-Maximization Algorithm

Dongchan Lee and Deepa Kundur
The Department of Electrical and Computer Engineering
University of Toronto
Toronto, ON, M5S3G4 Canada

***Abstract*—This paper presents the detection and identification of cyber attacks in phasor measurement unit (PMU) data using the expectation-maximization algorithm. Power systems today is prone to malicious cyber attack with its greater complexity and dependence on PMUs. While the conventional power system estimation is very advanced and robust, this paper will extend the power system estimation to inherently consider the possibility of malicious cyber attack. The detection is incorporated into the estimation problem in our approach, which will be solved by the EM algorithm. The proposed algorithm is applied on an IEEE 14-bus system to illustrate the performance of the algorithm.**

I. Introduction

The introduction of smart grid brings great opportunity in increasing the efficiency and reliability of the electric transmission system using information and communication systems (ICSs). As part of implementing the smart grid, the phasor measurement units (PMUs) are deployed in the electric grid to measure the bus voltage and phasor angle. The phasor angle plays a significant role in power systems studies, such as solving the optimal power flow and system estimation problem. The availability of PMU data real-time has provided opportunities for enhanced applications and has been studied for system estimation, dynamic security assessment, and system awareness [1], [2]. The use of PMU has become practical in the past decade, and the applications of PMUs are extended to protection, control and wide-area monitoring of electric grids [3]–[5]. As more applications of phasor measurement have emerged, the prominence of information has become greater.

Additionally, PMU data are realized to be useful for investigating blackouts and disturbances. A number of major North American blackouts are identified to be caused by a lack of system awareness, and a reliable measurement system is clearly essential [6]. PMU has unique capability to provide real time synchronized measurement, which provides not only insight into the grid operation, but also it promises improved reliability and efficiency of operation. However, the integration of PMUs brings new vulnerabilities in malicious cyber attack, which can result in physical consequences.

The control and operation of electricity system is based on real-time information acquisition and communication devices. The information is sent to the Supervisory Control and Data Acquisition (SCADA) system, which can host potential malicious cyber attacks or unintended failures in ICS [7]. PMUs are part of SCADA measurement and thus, the information is prone to cyber attack. The physical consequences have been studied for cyber attack [8], and there exist classical state estimation methods, which eliminate the contaminated data [9]–[11]. Although those methods are very well studied and robust, cyber attack is not well incorporated in the power system estimation. Our work will focus on the cyber attack of phasor measurements and propose a novel way to inherently model the malicious cyber attack inside the system estimation using the Expectation-Maximization (EM) algorithm. We approach the detection and estimation problem by solving them in parallel from sampled data. We assume Gaussian model to PMU data because of its known simplicity that makes solving the problem more tractable [12]. One of the relevent work that has similar problem formulation is [13], but we solve the problem with EM algorithm in our approach.

The EM algorithm is used to find missing data and to optimize intractable likelihood function [14]. It is a very efficient and powerful tool and has been applied to various applications including power systems [15]. For our application, the presence of malicious cyber attack is the hidden variable that we would like to estimate using the observed data. We illustrate the cyber attack detection algorithm in an IEEE standard 14-bus system.

II. Background

A. DC Power Flow

In this section, we present a common formulation of DC state estimation. In DC state estimation, the resistance is ignored since the line impedance between buses have high reactance relative to the resistance. The bus voltage is assumed to be constant in normal operation and the voltage phase difference between two buses is small. The transmission power is approximated with the following equation:

$$P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}, \tag{1}$$

where θ_i is the voltage phase angle at bus i, and X_{ij} is the reactance of the transmission line between bus i and bus j.

We assume that phasor measurements are available at every bus. We can represent the relationship between phasor angle and power injection at every bus as:

$$\mathbf{B}\mathbf{\Theta} = \mathbf{P}_{inj}, \tag{2}$$

978-1-4799-7088-9/14/$31.00 ©2014 IEEE

where $\mathbf{B} \in \mathbb{R}^{n \times n}$ represents the branch admittance, $\mathbf{\Theta} = [\theta_1, \theta_2, ..., \theta_n]^\intercal \in \mathbb{R}^n$ represents the system phasor, and $\mathbf{P}_{inj} \in \mathbb{R}^n$ represents the power injection at every bus in matrix form. We assume we have generation and load data so that P_{inj} is already known without any malicious bias. Our approach employs the DC power flow equation to design a prior potential function needed for the EM algorithm, which will be discussed in the later section.

B. PMU and False Data Injection Model

We assume that all PMU measurements are prone to Gaussian white noise with probability density function, $p(x) = \mathcal{N}(\theta, \sigma^2)$, where x is the PMU measurement, and σ is the variance of PMU data. We assume that the variance of the PMU data depends on the type of device and is already available. The false data is represented as a bias on true phasor angle:

$$p(\mathbf{x}) = \mathcal{N}(\mathbf{\Theta} + \mathcal{B}, \mathbf{\Sigma}^2), \tag{3}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the observed phasor measurement after the attack, $\mathcal{B} \in \mathbb{R}^n$ is a malicious bias injected into phasor measurement, and $\mathbf{\Sigma}$ is the variance of PMU data. We note that there is a cyber attack if $\mathcal{B} \neq 0$. Based on this Gaussian model of PMU data, we model the variance and uncertainty of the measurements.

C. EM algorithm

Expectation-Maximization (EM) is an iterative algorithm for parameter estimation and incomplete point estimation by maximum likelihood. Given a set of observable variables, x and latent variable z, we want to estimate the parameters γ in the model. The EM algorithm consists of two steps:
E step : $Q(\gamma|\gamma^{(t)}) = E[z|x, \gamma^{(t)}] \log p(x, z|\gamma)$
M step : $\gamma^{(t)} = \arg\max_\gamma E[z|x, \gamma^{(t)}] \log p(x, z|\gamma)$.

The missing data is estimated given the observed data and current estimate of the model parameter in the E step. In the M step, the likelihood function is maximized under assumption that the missing data is known. The likelihood increases every iteration, and the convergence of EM algorithm is guaranteed.

D. Problem Formulation

In this section, we will formulate our problem, which incorporates detection and identification of cyber attack in the power system estimation problem. We consider PMU data that are attacked by malicious users discussed in the previous section. We attempt to find the set of malicious data that attempts to attack the system. In order to solve this problem in real time, we need an algorithm that is efficient and easy to implement. The EM algorithm is a popular tool in statistical estimation problem that meets the requirements for this application.

Our goal is to find the true phasor, $\mathbf{\Theta}$, and to identify the attack set, $\mathbf{z} \in \binom{n}{k}$, where k is the number of attacked measurements. We let $p(z_i = 1) = \pi_i$, where π_i is the probability that measurement x_i is attacked. Figure 1 shows the Bayesian network of the formulated problem. In the next section, we will discuss the mathematical formulation of solving the described problem.

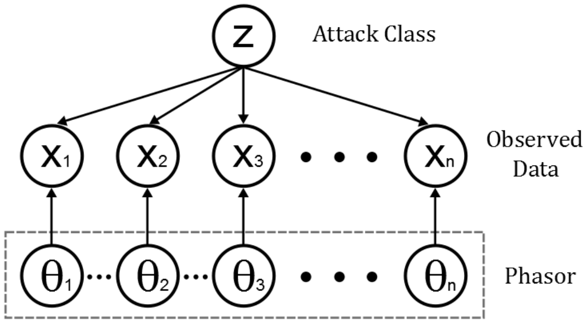

Fig. 1. Illustration of problem formulation using graph.

III. False Data Injection Detection Algorithm

The false data injection detection and identification algorithm is developed in this section. Firstly, the model is framed to be suitable for EM algorithm. Then, the potential function will be employed to find the true phase angle with cyber attack parameter estimation. The construction of the potential function is dominated by physical dynamics of the power systems, which in this case is the DC power flow approximation.

Let us define the parameter for the model, $\mathbf{\Gamma} = [\mathbf{\Pi}\ \mathbf{\Theta}]$, where $\mathbf{\Pi} = [\pi_1, \pi_2, ..., \pi_n]^\intercal$ is the vector that defines the probability of a cyber attack at every bus. $\mathbf{\Gamma}$ is what we want to estimate using the EM algorithm. Maximum likelihood (ML-EM) is applied to $\mathbf{\Pi}$, and maximum a posteriori (MAP-EM) is applied to $\mathbf{\Theta}$. The objective of our problem is to find the parameter,

$$\hat{\mathbf{\Gamma}} = \arg\max_{\mathbf{\Gamma}} \log p(\mathbf{x}, \mathbf{\Theta}|\mathbf{\Pi}, \mathbf{\Sigma}). \tag{4}$$

By maximizing the likelihood, we reveal the hidden cyber attack in phasor measurement. In the following section, we will model the system based on the background.

A. System Model

We assume the bias can be any value in the event of an attack. If there is no attack, we take the potential function to evaluate the probability. Thus, the following probability for observing data if formulated:

$$P(x_i|\theta_i, z_i) = \begin{cases} \frac{1}{\sigma_i\sqrt{2\pi}} e^{-(x_i - \theta_i)^2/2\sigma_i^2} & \text{if } z_i = 0 \\ \frac{1}{\theta_{i,max} - \theta_{i,min}} & \text{if } z_i = 1. \end{cases} \tag{5}$$

In our approach, we use the fact that the power should be balanced at every bus and we design a potential function that penalizes unbalanced power. From Equation 2, we define the potential function between phasor angles using the DC power flow equation:

$$\mathbf{\Phi}(\mathbf{\Theta}) = e^{-(\mathbf{B\Theta} - \mathbf{P}_{inj})^\intercal \mathbf{\Sigma}_\Phi^{-1} (\mathbf{B\Theta} - \mathbf{P}_{inj})}. \tag{6}$$

where Σ_Φ is the variance of the potential function. This potential function is used to compute the distribution of $\mathbf{\Theta}$, which is used to compute the probability of a cyber attack at each bus. We can rewrite the potential function equation as:

$$\Phi_i(\mathbf{\Theta}) = e^{\frac{a_i\theta_i^2 + b_i\theta_i + c_i}{\sigma_\Phi^2}}, \tag{7}$$

where

$$a_i = -\left(\sum_{c\in\mathcal{C}} \frac{1}{X_{ic}}\right)^2 - \sum_{c\in\mathcal{C}} \left(\frac{1}{X_{ic}}\right)^2, \tag{8}$$

$$\begin{aligned} b_i = {} & 2\left(\sum_{c\in\mathcal{C}} \frac{1}{X_{ic}}\right)\left(-\sum_{c\in\mathcal{C}} \frac{\theta_j}{X_{ic}} - P_{inj,i}\right) \\ & + 2\sum_{c\in\mathcal{C}}\left[\left(\frac{1}{X_{ic}}\right)\left(\sum_{k\in\mathcal{K}} \frac{\theta_c - \theta_k}{X_{ck}} + \frac{\theta_c}{X_{ci}} - P_{inj,c}\right)\right], \end{aligned} \tag{9}$$

$$\begin{aligned} c_i = {} & -\sum_{q\in\mathcal{Q}}\left(\sum_{m\in\mathcal{M}} \frac{\theta_q - \theta_m}{X_{qm}} - P_{inj,q}\right)^2 \\ & - \left(\sum_{c\in\mathcal{C}} \frac{\theta_c}{X_{ic}} - P_{inj,i}\right)^2 - \sum_{c\in\mathcal{C}}\left(\sum_{k\in\mathcal{K}} \frac{\theta_c - \theta_k}{X_{ck}} - P_{inj,c}\right)^2. \end{aligned} \tag{10}$$

Bus c is connected to bus i, and k is connected to bus c. Bus q is the bus other than bus i and c, and bus m is connected to bus q. In mathematical notation, $\mathcal{C} = \{c : X_{ic} \neq 0\}$, $\mathcal{K} = \{k : X_{ck} \neq 0\, k \neq i\}$, $\mathcal{Q} = \{q : q \neq i, c\}$, and $\mathcal{M} = \{m : X_{qm} \neq 0\}$. Based on the system model, we compute the parameters to maximize the likelihood in the next section.

B. Computation

We want to complete the data set $\{\mathbf{x}, \mathbf{\Theta}, \mathbf{z}\}$ using the observed data set $\mathbf{x}$ and the potential function Φ. Based on how the model is constructed, it is easy to apply EM algorithm to solve the problem. Firstly, the probability of observing data, given all the other parameters can be computed as below using equation 5:

$$p(x_i|\theta_i, z_i, \pi_i) = \left[\frac{1}{\theta_{i,max} - \theta_{i,min}}\right]^{z_i} [\mathcal{N}(x_i|\theta_i, \sigma_i^2)]^{(1-z_i)}. \tag{11}$$

We apply Baysian probability to compute the probability of the states and measurements given the parameter:

$$p(\mathbf{x}, \mathbf{\Theta}, \mathbf{z}|\mathbf{\Pi}) = \frac{1}{N}\prod_{i=1}^{n} \Phi_i(\mathbf{\Theta}) p(x_i|\theta_i, z_i, \pi_i) p(z_i), \tag{12}$$

where N is the normalizing constant to make the probability sum to one, $\Phi_i(\mathbf{\Theta})$ and $p(x_i|\theta_i, z_i, \pi_i)$ are defined in Equation 6 and 11 respectively, and $p(z_i)$ is π_i. The EM algorithm is used to maximize the following log likelihood expectation of sampled data:

$$Q(\mathbf{\Gamma}|\mathbf{\Gamma}^{(t)}) = E_{p(z|x,\theta^{(t)})}[\log \prod_{k=1}^{m} p(\mathbf{x}^k, \mathbf{\Theta}^k, \mathbf{z}^k|\mathbf{\Pi})], \tag{13}$$

where k is the index for sampled data and m is the total number of sampled data. Using Bayesian probability, we compute the expectation for the cyber attack:

$$\begin{aligned} E[z_i|x_i, \theta_i^{(t)}] &= p(z_i|x_i, \gamma_i) \\ &= \frac{p(x_i|\gamma_i, z_i)p(z_i)}{\sum_{z_i=0}^{1} p(x_i|\gamma_i, z_i)p(z_i)} \\ &= \frac{\pi_i(\theta_{i,max} - \theta_{i,min})^{-1}}{\pi_i(\theta_{i,max} - \theta_{i,min})^{-1} + (1-\pi_i)\mathcal{N}(x_i|\theta_i, \sigma_i^2)}. \end{aligned} \tag{14}$$

We take the derivative of Q to compute $\pi^{(t+1)}$ and $\theta^{(t+1)}$, increasing Q. We first find the optimal π and θ that maximizes Q:

$$\pi_i^* = \sum_{k=1}^{m} p(z_i|x_i, \gamma_i) \tag{15}$$

$$\theta_i^{k,*} = \frac{b_i^k + (1 - E[z_i^k|x_i^k, \theta_i^{k,(t)}])\frac{x_i^k}{\sigma_i^{k^2}}}{2a_i^k + \frac{(1 - E[z_i^k|x_i^k, \theta_i^{k,(t)}])}{\sigma_i^{k^2}}}. \tag{16}$$

We use the steepest descent to reach the maximum Q with learning rate η. Steepest descent will ensure that the algorithm does not diverge, and it can be implemented using equations:

$$\pi^{(t+1)} = \pi^{(t)} + \eta(\pi^* - \pi^{(t)}) \tag{17}$$

$$\theta^{k,(t+1)} = \theta^{k,(t)} + \eta(\theta^{k,*} - \theta^{k,(t)}). \tag{18}$$

To summarize the EM algorithm in our application, we take the following two steps:
E step : Evaluate the expectation, $E[z_i|x_i, \gamma_i^{(t)}]$ for every bus i using Equation 14.
M step : Update the parameters using Equation 17 and 18.

We expect that the EM algorithm will not converge to the right solution if the cyber attack is too big. In addition, if the attacker has much control over the measurements, then the algorithm could converge into a false solution. However, the classical power system estimation can address this issue since the attack is very obvious in these cases. Combining this tool with the classical state estimation method will provide strong tool for detecting malicious cyber attack.

IV. Case Study

We demonstrate the performance of the detection algorithm in the IEEE 14 bus system of Figure 2. The phasor measurement data were obtained from Matlab/PSAT, and the cyber attack was applied at bus 5 with magnitude of -0.5 rad and at bus 9 with magnitude of 1.0 rad. We obtained 10 sample data from the simulation. Details of the data and result can be seen in Table I. The EM algorithm was applied with a learning rate of 0.1 and an iteration of 10^6. The initial parameter for θ was

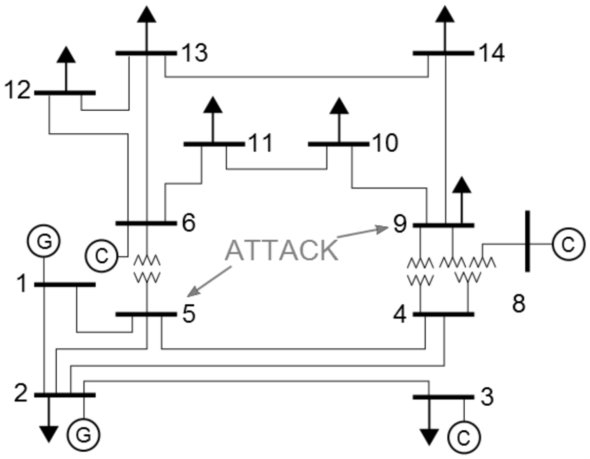

Fig. 2. IEEE 14 bus system under cyber attack at bus 4.

set to the observed data x and the probability of attack π was set to 0.1.

Figure 3 shows the phasor angle distribution of one of the sampled data using the potential function discussed in the previous section. The performance of EM algorithm is best when the portion of missing information is small. We note that the cyber attack detection could fail if too many data are corrupted, and the detection using internal data will not work. However, we consider malicious attacker with limited access to attack PMU measurements in this paper.

The performance of detection also depends on the sampled data. In the case of mixed data between attacked data and normal data, it will result in probability depending on how many attacked data is sampled. The data is sampled over attacked period, so we expect the malicious data is present for signficant amount of time in order to make desired impact.

The result shows that the EM algorithm correctly find the attacked bus while it estimate the state accurately. Figure 4 shows that the cyber attack detection converges to one for bus 5 and bus 9 where the cyber attack is applied, and zero for other buses. In addition, the actual state is estimated with error less than 3% at every bus. In addition, the probability of cyber atttack, π, can provide a unique information about the system. Since the value is probability instead of binary, it indicates our confidence on the measurement data. The algorithm will be able to detect high variance of the measurement as well as a cyber attack. It efficiently detects the maliciousness of the data by embedding the hidden cyber attack class into the state estimation model.

TABLE I
SUMMARY OF SIMULATION RESULT

Bus Number	Phasor Data (rad)	Attack (rad)	Detection	Identification (rad)
3	-0.22209	0	0	-0.0019
5	-0.15313	-0.5	1	-0.0459
9	-0.26073	0.1	1	0.0928
11	-0.2581	0	0	0.0004

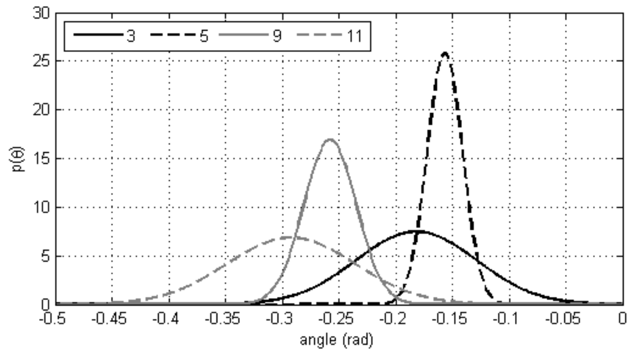

Fig. 3. Converged phasor measurement prior distribution

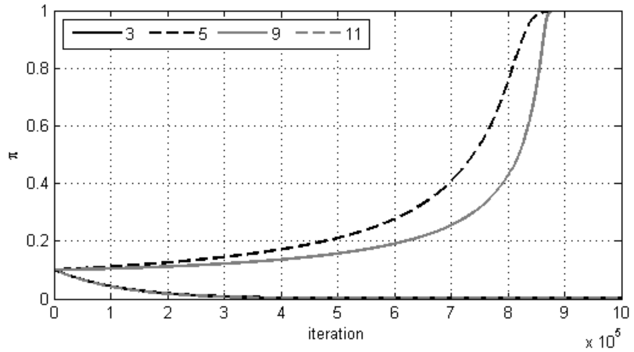

Fig. 4. Convergence of detection of cyber attack

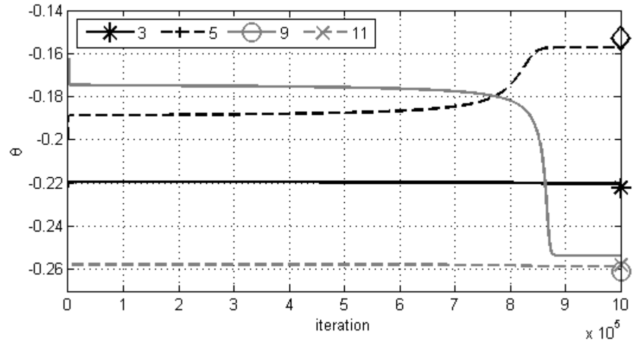

Fig. 5. Convergence of phasor measurement with actual phasor marked in the last iteration

V. CONCLUSION

We have proposed a novel approach for detecting cyber attacks in PMU phasor measurements using the EM algorithm. The advantage of an EM algorithm approach is that it embeds the possibility of cyber attack while estimating the state. While estimation is based on the physical model of the power system, the EM algorithm efficiently elimiates the maliciousness of the data. In addition, the detection of cyber attack in the probability form gives new insight to analyze the behaviour of the attacker. Coupling this method with conventional power system estimation will give better protection against cyber attack. The future work for the proposed algorithm includes incorporating non-linear power flow model into the system. Using more sophisticated model has potential to delivering more accurate result.

References

[1] A. Phadke, J. Thorp, and K. J. Karimi, "State estimlatjon with phasor measurements," *Power Systems, IEEE Transactions on*, vol. 1, no. 1, pp. 233–238, Feb 1986.

[2] K. Sun, S. Likhate, V. Vittal, V. Kolluri, and S. Mandal, "An online dynamic security assessment scheme using phasor measurements and decision trees," *Power Systems, IEEE Transactions on*, vol. 22, no. 4, pp. 1935–1943, Nov 2007.

[3] J.-A. Jiang, J.-Z. Yang, Y.-H. Lin, C.-W. Liu, and J.-C. Ma, "An adaptive pmu based fault detection/location technique for transmission lines. i. theory and algorithms," *Power Delivery, IEEE Transactions on*, vol. 15, no. 2, pp. 486–493, Apr 2000.

[4] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, "A flocking-based dynamical systems paradigm for smart power system analysis," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–8.

[5] D. Karlsson, M. Hemmingsson, and S. Lindahl, "Wide area system monitoring and control - terminology, phenomena, and solution implementation strategies," *Power and Energy Magazine, IEEE*, vol. 2, no. 5, pp. 68–76, Sept 2004.

[6] J. Dagle, "Postmortem analysis of power grid blackouts - the role of measurement systems," *Power and Energy Magazine, IEEE*, vol. 4, no. 5, pp. 30–35, Sept 2006.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[8] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 244–249.

[9] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC Press, 2004.

[10] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[11] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, vol. 2010, 2010.

[12] C. Wei, A. Wiesel, and R. Blum, "Distributed change detection in gaussian graphical models," in *Information Sciences and Systems (CISS), 2012 46th Annual Conference on*, March 2012, pp. 1–4.

[13] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 220–225.

[14] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the em algorithm," *J. R. Statist. Soc. Ser. B*, vol. 39, no. 1, pp. 1–38, 1977.

[15] R. Singh, B. Pal, and R. Jabr, "Statistical representation of distribution system loads using gaussian mixture model," *Power Systems, IEEE Transactions on*, vol. 25, no. 1, pp. 29–37, Feb 2010.