Statistical Structure Learning of Smart Grid for Detection of False Data Injection

Hanie Sedghi and Edmond Jonckheere

Department of Electrical Engineering
University of Southern California
Los Angeles, California 90089-2563
Email: {hsedghi,jonckhee}@usc.edu

***Abstract*—Although synchronous PMUs are being deployed across the grid, it is not economical to place them at every node. Therefore, at some nodes in the system state estimators will be used. Both PMUs and state estimators are prone to false data injection attacks. Thus, it is crucial to have a mechanism for fast and accurate detection of malicious tampering; both for preventing the attacks that may lead to blackouts, and for routine monitoring and control tasks of smart grid.**

We propose a decentralized false data injection detection scheme based on Markov graph of bus phase angles. We utilize Conditional Covariance Test (CCT) to learn the structure of smart grid. Using the DC power flow model, we show that under normal circumstances, and because of walk-summability of the grid graph, the Markov graph of voltage angles matches the power grid graph; otherwise, a discrepancy should trigger the alarm. Local grid topology is available online from the protection system and we exploit it to check for mismatch.

Our method can detect the most recent stealthy deception attack on power grid that assumes knowledge of bus-branch model of the system and is capable of deceiving the state estimator. Specifically, under the stealthy deception attack, the Markov graph of phase angles changes. To the best of our knowledge, our remedy is the first to comprehensively detect this sophisticated attack and it does not need additional hardware. Moreover, our detection scheme is successful no matter the size of the attacked subset. Simulation of various power networks confirms our claims.

***Index Terms*—Bus phase angles, structure learning, Conditional Covariance Test, false data injection detection**

I. Introduction

Synchronous Phasor Measurement Units are being massively deployed throughout the grid and provide us with synchronized measurements relevant to the state of grid health. Currently, PMU's provide the fastest measurements of grid status. As a result, recent monitoring and control schemes rely primarily on PMU measurements. For example, [1] tries to increase voltage resilience to avoid voltage collapse by using synchronized PMU measurements and decision trees. In addition, [2]–[4] rely on phase angle measurements for fault detection and localization. Nevertheless, we need to consider that it is not economical to place PMUs in every node. Therefore, in some nodes in the system, State Estimators will still be used. PMUs are prone to false data injection attack and even if we do not consider that, part of the grid using the state estimators is the window to false data injection attacks. Therefore, aforementioned methods can be deluded by false data injection attack. Thus, it is crucial to have a mechanism for fast and accurate discovery of malicious tampering; both for preventing the attacks that may lead to blackouts, and for routine monitoring and control tasks of smart grid.

We have designed a decentralized false data injection attack detection mechanism that utilizes bus phase angles Markov graph. We utilize Conditional Covariance Test (CCT) [5] to learn the structure of smart grid. We show that, under normal circumstances, and because of the grid graph structure, the Markov graph of voltage angles matches the power grid graph; otherwise, a discrepancy should trigger the alarm. Because of the connection we have made between Markov graph of bus angle measurements and the grid topology, our method can be performed in a decentralized manner, i.e. at each subnetwork. Currently, sub-network topology is available online and global network structure is available hourly [2]. Not only by decentralization can we increase the speed and get closer to online detection, but also we increase accuracy and stability by avoiding communication delays and synchronization problems when trying to send measurement data between locations far apart. We noticeably decrease the amount of exchanged data to address privacy concerns as much as possible.

We show that our method can detect the most recently designed attack on power grid that can fool the State Estimator [6]. The attack assumes the knowledge of bus-branch model of the grid. To the best of our knowledge, our method is the first to detect such a sophisticated attack comprehensively and efficiently with any number of attacked nodes.

Although in [7] the authors suggest an algorithm for PMU placement such that this attack is observable, they only claim an algorithm for 2-node attack and empirical approaches for 3,4,5 node attacks. According to [7], for cases where more than two nodes are under the attack the complexity of the approach is *disheartening*. Considering the fact that finding the number of needed PMUs is NP hard and [7] gives an upper bound and use a heuristic method for PMU placement; we need to mention that our algorithm has no hardware requirements, the complexity does not depend on number of nodes under attack and it works for any number of attacked nodes. It is worth mentioning that even in the original paper presenting the attack for a relatively small network (IEEE-30) seven measurements

from five nodes are manipulated. So it seems that the 2-node attack is not the most probable one.

Dependency graph approach is used in [4] for topology fault detection in grid. However, since attacks on state estimators are not considered, such methods can be deceived by false data injection. Furthermore, [4] uses a constrained maximum likelihood optimization for finding the information matrix while here an advanced structure learning method is used that captures power grid structure better. This is because in power grid the edges are distributed over the network. This is discussed in section $3.A$

The rest of this paper is organized as follows: In section II we show that bus phase angles form a Gaussian Markov Random Field (GMRF) and discuss that their Markov graph follows the grid structure. In section III we explain Conditional Covariance Test (CCT) [5] which we use for obtaining the Markov graph between bus phase angles and discuss how we leverage it to perform optimally for power grid. The stealthy deception attack on the state estimator is introduced in section IV. We elaborate on our detection scheme in section V. Simulations are presented in section VI and section VII concludes the paper.

II. Preliminaries and problem formulation

A. Preliminaries

A Gaussian Markov Random Field (GMRF) is a family of jointly Gaussian distributions, which factor according to a given graph. Given a graph $G = (V, E)$, with $V = \{1, ..., p\}$, consider a vector of Gaussian random variables $X = [X_1, X_2, ..., X_p]^T$, where each node $i \in V$ is associated with a scalar Gaussian random variable X_i. A Gaussian Markov Random Field on G has a probability density function (pdf) that may be parametrized as

$$f_X(x) \propto exp[-\frac{1}{2}x^T Jx + h^T x]; \tag{1}$$

where J is a positive-definite symmetric matrix whose sparsity pattern corresponds to that of the graph G. More precisely,

$$J(i, j) = 0 \Longleftrightarrow (i, j) \notin E. \tag{2}$$

The matrix $J = \Sigma^{-1}$ is known as the *potential* or *information* matrix, the non-zero entries $J(i, j)$ as the edge potentials, and the vector h as the vertex potential vector. In general, Graph $G = (V, E)$ is called the Markov graph(graphical model) underlying the joint probability distribution $f_X(x)$ where the node set V represents each random variable X_i and the edge set E is defined in order to satisfy local Markov property. For a Markov Random Field, local Markov property states that $X_i \perp X_{-\{i,N(i)\}}|X_{N(i)}$, where $X_{N(i)}$ represents all random variables associated with the neighbors of i in graph G and $X_{-\{i,N(i)\}}$ denotes all variables except for X_i and $X_{N(i)}$.

B. Bus phase angles as GMRF

We now apply the preceding to bus phase angles. The DC power flow model [8] is often used for analysis of power systems in normal steady-state operations. When system is stable, the phase angle differences are small, so $\sin(\theta_i - \theta_j) \sim \theta_i - \theta_j$. By the DC power flow model, system state X can be described using bus phase angles. The power flow on the transmission line connecting bus i to bus j is given by

$$P_{ij} = b_{ij}(X_i - X_j), \tag{3}$$

where X_i and X_j denote the phasor angles at bus i and j respectively, and b_{ij} denotes the inverse of the line inductive reactance. The power injected at bus i equals the algebraic sum of the powers flowing away from bus i:

$$P_i = \sum_{j \neq i} P_{ij} = \sum_{j \neq i} b_{ij}(X_i - X_j). \tag{4}$$

whenever bus i and j are not connected $b_{ij} = 0$. Thus, it follows that the phasor angle at bus i could be represented as:

$$X_i = \sum_{j \neq i} \{\frac{b_{ij}}{\sum_{i \neq j} b_{ij}}\} X_j + \frac{1}{\sum_{j \neq i} b_{ij}} P_i. \tag{5}$$

Because of load uncertainty injected power can be modelled as a random variable [9] and since injected power models the superposition of many independent factors (e.g. loads), it can be modelled as a Gaussian random variable. Thus, the linear relationship in (3) implies that the difference of phasor angles across a bus could be approximated by a Gaussian random variable truncated within $[0, 2\pi)$. Considering the fixed phasor at the slack bus, it is assumed that under steady-state, phasor angle measurements can be considered as Gaussian variables [4].

The next step is to find the correct neighboring relationship between X_i's. From (5), we can see the relationship between X_i's and the nodes connected to them electrically. Thorough analysis of the second term of (5) shows that this term causes some second-neighbor relationships between X_i's which are weaker than the relationship between immediate neighbors. This approximation falls under the generic fact of the tapering off of Fourier coefficients. So, we can approximate the neighboring relationship to be only that of immediate neighbors in grid graph. The proofs are omitted due to page limits. We explain shortly why CCT best describes this approximation and why this approximation is in fact true for a grid graph, meaning local local Markov property holds for $N(i)$, where $N(i)$ denotes the nodes that are electrically connected to node i in the power grid.

III. Structure Learning

A. Conditional Covariance Test

In order to learn the structure of the power grid, we utilize the new Gaussian Graphical Model Selection method called *Conditional Covariance Test (CCT)* [5]. CCT method estimates the structure of underlying graphical model given i.i.d. samples of the random variables. CCT method is shown in Algorithm 1.

In Algorithm 1, the output is an edge set corresponding to graph G given n i.i.d. samples x^n, each of which has p variables, a threshold $\xi_{n,p}$ (that depends on both p and n) and a constant $\eta \in \mathbb{N}$, which is related to the local vertex separation

Algorithm 1 $CCT(x^n; \xi_{n,p}, \eta)$ for structure learning using samples x^n [5]

Initialize $\widehat{G}_p^n = (V, \emptyset)$

For each $(i,j) \in V^2$,
if $\min_{\substack{S \subset V \setminus \{i,j\} \\ |S| \leq \eta}} \widehat{\Sigma}(i,j|S) > \xi_{n,p}$,
then
add (i,j) to the edge set of $\widehat{G}_p^n$.

end if
Output:$\widehat{G}_p^n$

property (described later). In our case, each bus phase angle represents one of the p variables.

The sufficient condition for output of CCT to have structural consistency with underlying Markov graph between variables is that the graph has to satisfy local separation property and walk-summability [5]. An ensemble of graphs has the (η, γ)-local separation property if for any $(i,j) \notin E(G)$, the maximum number of paths between i,j of length at most γ does not exceed η. A Gaussian model is said to be α-walk summable if $||\bar{\mathbf{R}}|| \leq \alpha < 1$ where $\bar{\mathbf{R}} = [|r_{ij}|]$ and $||.||$ denotes the spectral or 2-norm of matrix, which for symmetric matrices is given by the maximum absolute eigenvalue [5]. $\mathbf{R}$ is the matrix consisting of partial correlation coefficients. It is zero on diagonal entries and for non-diagonal entries we have:

$$\begin{aligned} r_{ij} \triangleq & \quad \frac{\Sigma(i,j|V \setminus \{i,j\})}{\sqrt{\Sigma(i,i|V \setminus \{i,j\})\Sigma(j,j|V \setminus \{i,j\})}} \\ = & \quad -\frac{J(i,j)}{\sqrt{J(i,i)J(j,j)}} \end{aligned} \tag{6}$$

r_{ij}, the *partial correlation coefficient* between variables X_i and X_j for $i \neq j$, measures their conditional covariance given all other variables [10].

Power grid structure (which coincides with Markov graph of bus phase angles) is an example of bounded local path graphs which satisfies local separation property. We also checked the analyzed networks for walk-summability condition. It is shown in [5] that under walk summability, the effect of faraway nodes on covariance decays exponentially with distance and the error in approximating the covariance by local neighboring decays exponentially with distance. So by correct tuning of the threshold $\xi_{n,p}$ and enough number of samples, we expect the output of CCT method to follow the grid structure.

CCT distributes the edges fairly uniformly across the nodes while ℓ_1 method tends to cluster all the edges together between the "dominant" variables leading to a densely connected component and several isolated points [5]. Therefore, CCT is more suitable for detecting the structure of the power grid where the edges are distributed over the network. It should be noted that the computational complexity of CCT is $O(p^{\eta+2})$, which is efficient for small η [5]. η is the parameter associated with local separation property described above.

The sample complexity associated with CCT method is $n = \Omega(J_{min}^{-2} \log p)$ where J_{min} is the minimum absolute edge potential in the model [5].

B. Decentralization

We want to find the Markov graph of our bus phasor measurements. Since we have made the connection between electrical connectivity and correlation, this helps us to decentralize our method to a great extent. We consider the power network in its normal condition. It consists of different areas connected together via border nodes. So we decompose our network into these sub-areas. Our method can be performed locally in sub-networks. The sub-network connection graph is available online from protection system at each sub-network and can be readily compared with bus phase angles Markov graph. In addition, only for border nodes, we need to consider their out-of-area neighbors as well. This can be done either by receiving measurements from neighbor sub-networks or by solving the power flow equations for that border link. Therefore we run CCT for each sub-graph to figure out the Markov graph. Then we compare it with online network graph information to detect false data injection attack.

This decentralization reduces complexity and increases speed. Our decentralized method is a substitute for considering all measurement throughout the power grid,which requires a huge amount of data exchange and computation. In addition to having less nodes to analyse, this decentralization leads us to a smaller η and greatly reduces computational complexity, which makes our method capable of being executed in huge networks. Moreover, utility companies are not willing to expose their information for economical competition purposes and there has been several attempts to make them do that [11]. So it is desired to reduce the amount of data exchange between different areas and our method adequately fulfils this requirement.

C. Online calculations

For monitoring the power grid, we need an on-line algorithm. Therefore, we need to have an iterative method to make use of new data without the need to recalculate. Here, we derive an iterative formulation for sample covariance matrix. Then it can be used for calculating the conditional covariance using

$$\widehat{\Sigma}(i,j|S) := \widehat{\Sigma}(i,j) - \widehat{\Sigma}(i,S)\widehat{\Sigma}^{-1}(S,S)\widehat{\Sigma}(S,j). \tag{7}$$

As we know, in general

$$\Sigma = E[(X-\mu)(X-\mu)^T] = E[XX^T] - \mu\mu^T. \tag{8}$$

Let $\widehat{\Sigma}^{(n)}(X)$ denote the sample covariance matrix for a vector X of p elements from n samples and $\widehat{\mu}^{(n)}(X)$ be the sample mean for that. In addition, let $X^{(i)}$ be the ith sample of our vector. Then we have

$$\widehat{\Sigma}^{(n)}(X) = \frac{1}{n-1}\sum_{i=1}^{n} X^{(i)}X^{(i)^T} - \widehat{\mu}^{(n)}\widehat{\mu}^{(n)^T}. \tag{9}$$

Therefore,

$$\widehat{\Sigma}^{(n+1)}(X) = \frac{1}{n}[\sum_{i=1}^{n} X^{(i)}X^{(i)^T} + X^{(n+1)}X^{(n+1)^T}] - \widehat{\mu}^{(n+1)}\widehat{\mu}^{(n+1)^T}; \quad (10)$$

where

$$\widehat{\mu}^{(n+1)} = \frac{1}{n+1}[n\widehat{\mu}^{(n)} + X^{(n+1)}]. \quad (11)$$

By keeping first term in (9) and sample mean, our updating rule is (10). Thus, we revise the sample covariance as soon as any bus phasor measurements changes and leverage it to reach conditional covariances needed for CCT.

IV. Stealthy Deception Attack

The most recent and most realistically dreaded false data injection attack on the power grid is introduced in [6]. For a p-bus electric power network, the $l = 2p - 1$ dimensional state vector x is $(\theta^T, V^T)^T$, where $V = (V_1, ..., V_p)$ is the vector of voltage bus magnitudes and $\theta = (\theta_2, ..., \theta_p)$ vector of phase angles. It is assumed that the nonlinear measurement model for state estimation is defined by $z = h(x) + \epsilon$, where $h(.)$ is the measurement function, $z = (z_P, z_Q)$ is the measurement vector consisting of active and reactive power flow measurements and ϵ is the measurement error. $H(x^k) := \frac{dh(x)}{dx}|_{x=x^k}$ denotes the Jacobian matrix of the measurement model $h(x)$ at x^k.

The goal of the stealthy deception attacker is to compromise the measurements available to the State Estimator (SE) such that $z^a = z + a$, where z^a is the corrupted measurement and a is the attack vector. Vector a is designed such that the SE algorithm converges and the attack a is undetected by the Bad Data Detection scheme. Then it is shown that, assuming the DC power flow model, such an attack can only be performed locally with $a \in \mathrm{Im}(H)$, where $H = H_{P\theta}$ is the matrix connecting the vector of bus injected powers to the vector of bus phase angles, i.e., $P = H_{P\theta}\theta$.

V. Stealthy Deception Attack Detection

The fundamental idea behind our detection scheme is that of structure learning. Our learner, CCT method, is tuned with correct data representing the data structure, which corresponds to grid graph. Therefore, any attack that changes the structure alters the output of CCT method and this triggers the alarm. Let us consider the aforementioned attack more specifically. As we are considering the DC power flow model the state vector introduced in [6] reduces to the vector of voltage angles, X. Since $a \in Im(H)$, $\exists d; a = Hd$.

$$z^a = z + a = H(X + d) = HX^a, \quad (12)$$

where X^a represents the vector of angles when the system is under attack, z^a is the attacked measurement vector and X is the phasor angle vector. Considering (4), we have $H_{ij} = -b_{ij}$ for $i \neq j$ and $H_{ii} = \sum_{i \neq j} b_{ij}$, where b_{ij} denotes the inverse of the line inductive reactance. We have

$$X^a = X + d = H^{-1}P + H^{-1}a = H^{-1}(P + a), \quad (13)$$

As definition of H matrix shows, it is of rank $p-1$. Therefore the above H^{-1} means pseudo inverse of H matrix. Another way to address this singularity is to remove the row and column associated with slack bus.

From (13),

$$\Sigma(X^a, X^a) = H^{-1}[\Sigma(P + a, P + a)]H^{-1^T} = H^{-1}[\Sigma(P, P) + \Sigma(a, a)]H^{-1^T}. \quad (14)$$

The above calculation assumes the attack vector being independent of current values in the network as demonstrated in [6].

An attack is considered successful if it causes the operator to make a wrong decision. For that matter, the attacker would not insert just one wrong sample. In addition, if the attack vector remains constant, it does not cause any reaction. Therefore, the attacker is expected to insert random vectors a during some samples. Thus $\Sigma(a, a) \neq 0$ and

$$\Sigma(X^a, X^a) \neq \Sigma(X, X) \quad (15)$$

It is not difficult to show that if we remove the assumption on independence of attack vector and injected power, (15) still holds.

Considering (15) and the fact that matrix inversion enjoys uniqueness property, this means that in case of an attack, the new Σ^{-1} will not be the same as network's J matrix in normal condition, i.e. $\Sigma^{-1}(X^a, X^a) \neq J_{normal}$, and as a result, the output of CCT method will not follow the grid structure. We use this mismatch to trigger the alarm. In order to find all the buses whose measurements are ruined, we notice that if at least one measurement is ruined in a pair (i, j), the sample covariance between i,j changes. We utilize this to trace back to all attacked nodes as soon as alarm is triggered. The attack is performed locally and because of local Markov property, we are certain that no nodes from other sub-graphs contributes to the attack.

We should emphasize that the considered attack assumes the knowledge of the system's bus-branch model. So the attacker is equipped with very critical information. Yet, we can mitigate such an intelligent attack. Next, we show that simulation of various power networks including IEEE 14-bus system and IEEE 30-bus system confirms our claims.

VI. Simulation

We consider IEEE 14-bus system as well as IEEE-30 bus system. First, we feed the system with Gaussian demand and simulate the power grid. We use MATPOWER [12] for solving the DC power flow for various demand and use the resulting angle measurements as the input for CCT algorithm. We leverage YALMIP [13] and SDPT3 [14] to perform CCT method in MATLAB.

With right choice of parameters and threshold, and enough

measurements, the Markov graph follows the grid structure. We use edit distance metric for tuning the threshold value.

After the threshold is set, our detection algorithm works in the following manner. Each time the procedure is initiated, i.e. any PMU angle measurement or state estimator output changes, it updates the conditional covariances based on new data, runs CCT and checks the edit distance between Markov graph of phasor data and grid structure. A discrepancy triggers the alarm and then the system uses the information matrix to reach correlation matrix and trace the changes to find all the buses under the attack.

Next we introduce the stealthy deception attack to the system. The attack is claimed to be successful only if performed locally on connected nodes. Having this constraint in mind, for IEEE-14 test case the maximum number of attacked nodes is 6 and for IEEE 30-bus system this number is 8. For IEEE-14 network, we consider the cases where 2 to 6 nodes are under attack. For IEEE-30 network, we consider the cases where 2 to 8 nodes are under attack. For each case and for each network, we simulate all possible attack combinations. This is to make sure we have checked our detection scheme against all possible stealthy deception attacks. Each case is repeated 1000 times for different attack vector values.

With enough number of samples, our algorithm is 100% successful in detecting all cases and types of attacks discussed above, both for IEEE-14 and IEEE-30 bus systems. The minimum number of samples for having 100% detection rate for IEEE 14-bus system is 130 and it is 50 for IEEE 30-bus system. Since IEEE-30 is more sparse compared to IEEE 14-bus system, our method performs better in the former case.Yet, for a 60 Hz system, detection speed for IEEE 14-bus system is quite astonishing as well.

Another interesting fact is detection rate's trend as the number of measurements increases. This is shown in Fig.1 for IEEE 14-bus system. Detection rate is averaged over all possible attack scenarios. It can be seen that even for small number of measurements our method presents a good performance. The detection rate is 90% with 30 samples.

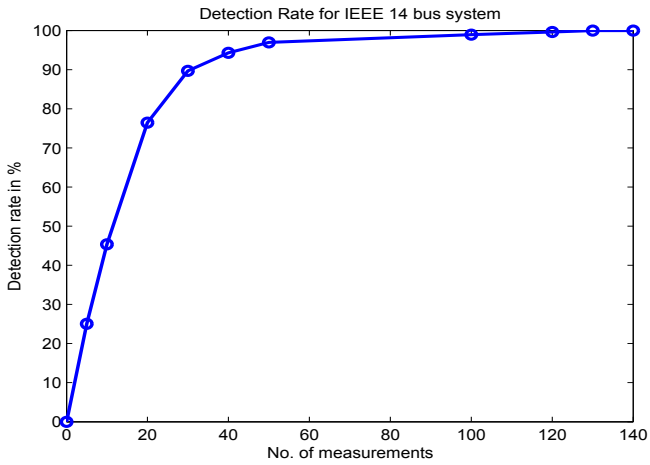

Fig. 1: Detection rate for IEEE 14-bus system

VII. Discussion and Conclusion

We proposed a decentralized false data injection attack detection scheme that is capable of detecting the most recent stealthy deception attack on smart grid SCADA. To the best of our knowledge, our remedy is the first to comprehensively detect this sophisticated attack. As stated before, computational complexity of our method is polynomial and the decentralized property makes our scheme suitable for huge networks with bearable complexity and run time. Consequently, our approach can be extended to bigger networks, namely IEEE-118 and IEEE 300-bus systems.

It is worth mentioning that, with similar calculations, we can consider the case where the attacker manipulates reactive power data to lead the state estimator to wrong estimates of voltage. Such an attack can be designed to fake a voltage collapse or tricking the operator to cause a voltage collapse. The detection can be done by linearisation of AC power flow and considering the fluctuations around steady state. Then following the algorithm we introduced here, it readily follows that such an attack can also be detected following the similar approach as we did here for bus phase angles and active power.

References

[1] R. Diao, K. Sun, V. Vittal, R. OKeefe, M. Richardson, N. Bhatt, D. Stradford, and S. Sarawgi, "Decision tree-based online voltage security assesment using pmu measurements," *IEEE Transactions on Power Systems*, vol. 24, pp. 832–839, May 2009.

[2] H. Zhu and G. B. Giannakis, "Sparse Overcomplete Representations for Efficient Identification of Power Line Outages," to appear in *IEEE Tran. on Power Systems*, 2012.

[3] R. B. C. Wei, A. Wiesel, "Change detection in smart grids using errors in variables models," in *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2012 IEEE 7th*, June 17-20 2012, pp. 16–20.

[4] M. He and J. Zhang, "A dependency graph approach for fault detection and localization towards secure smart grid," *IEEE Transactions on Smart Grid*, vol. 2, pp. 342–351, June 2011.

[5] A. Anandkumar, V. Tan, F. Huang, and A. Willsky, "High-dimensional gaussian graphical model selection:walk summability and local separation criterion," *Journal of Machine Learning*, June 2012, accepted.

[6] A. Teixeira, G. Dan, H. Sandberg, and K. H. Johansson, "A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator," in *IFAC World Congress*, September 2011.

[7] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, January 2012.

[8] A. Abur and A. Exposito, *Power System State Estimation, Theory and Implementation*. Marcel Dekker, 2004.

[9] M. Luettgen, W. Karl, A. Willsky, and R. Tenney, "Multiscale representations of markov random fields," *IEEE Transaction on Signal Processing*, vol. 41, p. 33773396, Dec 1993.

[10] S. Lauritzen, *Graphical models: Clarendon Press*. Clarendon Press, 1996.

[11] S. M. S. R. Rajagopalan, L. Sankar and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *2nd Annual IEEE Conference on Smart Grid Communications*, Brussels, Belgium, Oct 17-20 2011.

[12] C. E. M.-S. R. D. Zimmerman and R. J. Thomas, "Matpower steady-state operations, planning and analysis tools for power systems research and education," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[13] J. Lofberg, "YALMIP: A Toolbox for Modeling and Optimization in MATLAB." in *IEEE international symposium on Computer Aided Control Systems Design (CACSD)*, September 2004, available from http://users.isy.liu.se/johanl/yalmip/.

[14] K. C. Toh, M. Todd, and R. H. Tutuncu, "SDPT3 - a MATLAB software package for semidefinite programming," *Optimization Methods and Software*, vol. 11, pp. 545–581, 1999.