Malicious data injection attack against power system state estimation based on orthogonal matching pursuit

Chao Zhang
School of Electrical Engineering
Xi'an Jiaotong University, Xi'an, China
gumingsiyizhc@stu.xjtu.edu.cn

Aimin Zhang
School of Electronics and information Engineering
Xi'an Jiaotong University, Xi'an, China
zhangam@mail.xjtu.edu.cn

Zhigang Ren*
School of Electronics and information Engineering,
Xi'an Jiaotong University, Xi'an, China
renzg@mail.xjtu.edu.cn

Yuanxin Zhang
School of Electronics and information Engineering
Xi'an Jiaotong University, Xi'an, China
walnutmilk0116@gmail.com

Yingsan Geng
School of Electrical Engineering
Xi'an Jiaotong University, Xi'an, China
ysgeng@mail.xjtu.edu.cn

***Abstract*—State estimation is a critical power system component that estimates the state of the power network and deals with bad data, depending in general on a redundant set of meter measurements and network topology configuration. Recently, some researchers have constructed a new class of attack which can successfully bypass the existing power system state estimation and inject bad data to the state variables, causing enormous threats to the power system. This paper investigates the methods to identifying the minimum number of meter measurements to compromise in launching such an attack, which is named least-effort malicious data injection attack. A modified orthogonal matching pursuit (OMP) algorithm is introduced here for identifying the meters, since traditional matching pursuit (MP) algorithm requires a large number of iterations to reach convergence. Comparison of the two methods in the simulation on standard IEEE test system indicates that the OMP algorithm compromises fewer meters than the MP algorithm in the same number of iterations.**

Keywords—Malicious Data Injection; MP; OMP; Power System State Estimate

I. INTRODUCTION

The power system is a complex network interconnecting electric power generation, transmission, distribution, and consumption across usually a large geographical area. It is a typical cyber-physical system [1] that we depend on, and needs to be monitored and controlled effectively to guarantee its security and reliability. Supervisory control and data acquisition (SCADA) systems have been used to monitor the meter measurements, status information and other signals in the power system, and transmit the detected information to the control center. There exist a number of disturbances in the process of meter-reading collection, including measurement noise, meter errors, inappropriate operation and malicious data injection. These disturbances, if not eliminated, may affect the judgment of the control center as well as its contingency regulation, and further result in catastrophic consequences.

State estimator is used to estimate the power system state based on analysis of meter measurement data and power network models. It estimates the state variables and filters the disturbances, ensuring that the power system is running in the desired states. A number of techniques have been developed to process the disturbances in meter-reading collection [2], [3]. Most of these techniques remove the bad meter measurements and network topology configuration to remove the bad meter measurements effectively based on a redundant set of meter measurements and network topology configuration. However, a recent study on the bug of state estimator reported a set of deliberately conceived malicious data which could bypass the bad data detector and attack the power system state estimation successfully [4]. This is named false data injection attack. Inspired by the report, a volume of studies have been performed [5-9] on this issue. One of the heated topics is to determine the minimum number of meter measurements that need to be changed to successfully form a malicious data injection attack. Liu *et al.* [4] gave an approximate range according to different types of busses in the IEEE test system. Sandberg et al. [5] introduced two security indices to quantify the least effort needed to achieve the attack. Kosut. O *et al.* [6], using a graph theoretic approach, obtained an efficient algorithm with polynomial-time complexity for the design of unobservable malicious data attack with least number of meters to compromise. In the defensive aspect, Bobba et al. [7] explored the detection of the attack proposed in [4], pointing out that it can be defended by protecting a selected set of meter measurements and by having a way in addition to the state estimation to independently measure the value of a selected set of state variables.

This work was supported by National Natural Science Foundation of China (51177126, 61105126) and Major Technological Innovation Project Special Fund of Shaanxi Province (2008ZKC01-09).

*Corresponding author

978-1-4673-5769-2/13/$31.00 ©2013 IEEE

To avoid the data injection attack being detected, the attacker needs to know the network topological configuration as much as possible and guarantee that the data contain as few number of attack vectors as possible. This is called least-effort attack, which is a non-deterministic polynomial (NP) complete problem. Given an $\mathrm{Ax}=\mathrm{b}$, where A represents a matrix, b represents a vector, and x represents a vector containing at most k non-zero elements. The NP-complete problem is to obtain the minimum k. A number of efficient heuristic approaches have been used to deal with the problem, among which matching pursuit (MP) algorithm is the most popular for computing the sparse signal representation [1, 8-10, 12].

Though being widely utilized, the MP algorithm needs involves a large number of iterations to guarantee its convergence. The calculation is very complicated. The purpose of this paper attempts is to find an alternative algorithm that reaches convergence in less iterations. The least-effort attack problem is usually formalized by identifying the minimum set of meters to be compromised using the least topological configuration possible. It was has been reported that orthogonal matching pursuit (OMP) algorithm [13], a modified method based on the MP algorithm, was able to converge fasters in fewer iterations. Therefore, we conduct the present study to see whether the OMP algorithm can better solve the NP-complete problem in the bad malicious data injection attack against the power system state estimation. In our scheme, we firstly set a number of selected state variables that have been changed are set first, and the MP and OMP algorithms are used to obtain the minimum set of meters to be compromised, respectively. Comparison of the results indicates that the OMP algorithm can reach convergence in fewer iterations, and the number of meters to be compromised in the OMP algorithm is are comparatively smaller fewer in the same number of iterations. Simulation of the two algorithms is performed using the standard IEEE test system, including the IEEE 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus systems. The results testify the feasibility and efficiency of the OMP algorithm.

The organization of this paper is as follows: Section II gives the background information of state estimation and malicious data injection attack. Section III introduces the MP algorithm and the problems in it. The OMP algorithm is then presented to solve the problems. Section IV presents the simulation of the two algorithms, and the data are compared. Section V gives a brief conclusion of this study.

II. PRELIMINARIES

A. State estimation and bad data detection

1) State estimation

In the energy management system (EMS), the state estimators obtain the real-time SCADA signals, including the transmission line loadings and all voltage magnitudes of buses. These data are called meter measurements, which are used for the estimation of the state variables of the power network. Generally speaking, the number of state variables is less than the number of meter measurements. In DC-state estimation, the state variables are related to the meter measurements in the form below:

$$\mathrm{z}=\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{\mathrm{m}} \end{bmatrix}=\begin{bmatrix} h_1(x_1,x_2,\ldots,x_n) \\ h_2(x_1,x_2,\ldots,x_n) \\ \vdots \\ h_{\mathrm{m}}(x_1,x_2,\ldots,x_n) \end{bmatrix}+\begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_m \end{bmatrix}=\mathrm{h(x)+e}, \quad (1)$$

where z_i represents the meter measurements which include the bus active power flow and branch active power flow, x_{i} represents the state variables including the voltage phase angles and voltage magnitudes, and e represents the error in the meter measurement. $\mathrm{h(x)}$ is a nonlinear function related to the state variable x and is derived from the power network topology.

In DC-state estimation, all shunt elements and branches of reactive power flow are neglected. The linearization of (1) can be realized as

$$\mathrm{z=Hx+e}, \quad (2)$$

where e denotes the meter measurement error and H is a Jacobian matrix which represents the power network topology. Weighted least square (WLS) criterion is usually used in DC-state estimation to identify the optimal state variable $\hat{\mathrm{x}}$ according to the meter measurement z. When the meter error e is assumed to be Gaussian distributed with zero mean, the WLS criterion leads to an estimator with the following matrix solution:

$$\hat{\mathrm{x}}=(\mathrm{H^T R^{-1} H})^{-1}\mathrm{H^T R^{-1} z}. \quad (3)$$

R is a diagonal matrix of the variances of meter errors, which is expressed as $\mathrm{R}=diag(\sigma_1^2,\sigma_2^2,\ldots,\sigma_m^2)$.

2) Bad data detection

The state estimation outcome can be changed by the bad data derived from device misconfiguration, random errors and faulty manipulation. Techniques for bad data detection have been developed to protect state estimation outcome. Intuitively, the estimates of state variables based on normal meter measurements are close to the actual variable values. Abnormal meter measurements may cause big difference between the estimates and the true variable values. To detect the presence of the abnormal measurements, the measurement residual $\mathrm{z}-\mathrm{H}\hat{\mathrm{x}}$, the difference between the observed and the estimated measurements, is calculated. A threshold τ is determined through a hypothesis test with a significance level a. The presence of bad measurements is confirmed if L_2-norm $\|\mathrm{z}-\mathrm{H}\hat{\mathrm{x}}\|>\tau$. Otherwise, the bad data cannot be detected.

B. Malicious data injection attack

There are attackers attempting to manipulate the state variables by injecting malicious data to meter measurements. This is called malicious data injection attack. The key point in this attack is to have the injected data bypass the state estimator and bad data detector. For this, the attackers must have as much knowledge of the power system topology as possible.

The malicious data injection attack is basically to add a non-zero attack vector $\mathrm{a}=(a_1,a_2,\cdots a_m)^{\mathrm{T}}$ to the original meter measurement vector z, and the observed meter measurement is

then $z_a = z + a$. The state estimator receives z_a and obtains the bad state estimate $\hat{x}_{bad}$ following the WLS criterion. Let $\hat{x}_{bad} = \hat{x} + c$, in which $\hat{x}$ is the original state variable estimate and c is the malicious error added to the original estimate.

In [4], the malicious data injection is expressed as $a = Hc$, where a is a linear combination of the column vectors of H. Substituting a into $z_a = z + a$ and then z_a into the L_2-norm $\|z - H\hat{x}\|$, we get

$$\begin{aligned} \|z_a - H\hat{x}_{bad}\|^2 &= \|z + a - H(\hat{x} + c)\|^2 \\ &= \|z - H\hat{x} + (a - Hc)\|^2 \\ &= \|z - H\hat{x}\|^2 \le \tau \end{aligned} \tag{4}$$

As a result, the meter measurement z_a can pass the bad data detection.

Suppose that an attacker has access to k specific meters. Assume $I_v = \{i_1, \cdots i_k\}$ is the set of indices of r target state variables chosen by the attacker. Note that $a = Hc = \sum_{i \in I_v} h_i c_i + \sum_{i \notin I_v} h_j c_j$. Let $H_s = (h_{j_1}, h_{j_2} \cdots h_{j_{n-r}})$ and $c_s = (c_{j_1}, c_{j_2} \cdots c_{j_{n-r}})$, where $j_k \notin I_v$ for $1 \le k \le n - r$. Let $b = \sum_{i \in I_v} h_i c_i$, $P_s = H_s (H_s^T H_s)^{-1} H_s^T$, $B_s = P_s - I$ and $y = B_s b$. Thus, $a = Hc$ can be transformed into the following equivalent forms:

$$\begin{aligned} & a = Hc \\ \Leftrightarrow\ & a = \sum_{i \in I_v} h_i c_i + \sum_{i \notin I_v} h_j c_j = H_s c_s + b \\ \Leftrightarrow\ & P_s a = P_s H_s c_s + P_s b \\ \Leftrightarrow\ & P_s a = a - b + P_s b \\ \Leftrightarrow\ & (P_s - I)a = (P_s - I)b \\ \Leftrightarrow\ & B_s a = B_s b \Leftrightarrow B_s a = y. \end{aligned} \tag{5}$$

Equation (5) implies that the attack vector a satisfies the relation $a = Hc$ if and only if a satisfies $B_s a = y$. Therefore, the attacker needs to find the vector a which satisfies $B_s a = y$ where $a = (a_1, a_2, \cdots a_m)^T$ and $a_i = 0$ for $i \notin I_v$.

Usually, attackers may hope to manipulate the state variables arbitrarily by changing as few meter measurements as possible. This is called a least-effort malicious data injection attack, which is an NP-complete problem.

III. Two Different Arolgrithms for Least-effort Malicious Data Injection Attack

To solve the NP-complete problem in the least-effort malicious data injection attack, most attackers select the MP algorithm to determine the minimum number of meter measurements to compromise.

A. MP algorithm

The MP algorithm is a reiterative censoring by means of projecting the original signal f to the column of matrix D. Let $D = \{x_1, x_2, \cdots x_n\}$ be a dictionary in Hilbert space, where x_i for $1 \le i \le n$ is normalized as $\|x_n\| = 1$. The original signal f can be calculated as

$$f = \sum_n a_n x_n, \tag{6}$$

and the result of each iterative step is represented as

$$f = \sum_{i=1}^{k} a_i x_i + R_k f, \tag{7}$$

where $R_k f$ is the current residual.

The MP algorithm is comprised of the following steps. First, compute the inner-products $\left\{\left\langle R_k f, x_{n_{k+1}} \right\rangle\right\}_n$ and judge whether $x_{n_{k+1}}$ satisfies $\left|\left\langle R_k f, x_{n_{k+1}} \right\rangle\right| \ge \alpha \sup_j \left|\left\langle R_k f, x_j \right\rangle\right|$, where $0 \le \alpha \le 1$. Second, set $f_{k+1} = f_k + \left\langle R_k, x_{n_{k+1}} \right\rangle$ and $R_{k+1} = R_k f - \left\langle R_k f, x_{n_{k+1}} \right\rangle x_{n_{k+1}}$, where k is the number of iterations and k, ($k \leftarrow k+1$). Third, repeat the above two steps until certain convergence criteria are satisfied.

To realize convergence, the MP algorithm should satisfy $\left\langle R_{k+1} f, x_{n+1} \right\rangle = 0$, i.e., the residual is orthogonal to the last vector in the dictionary $D = \{x_1, x_2, \cdots x_n\}$. Consequently, we can get

$$\|R_k f\|^2 = \|R_{k+1} f\|^2 + \left|\left\langle R_k f, x_{n_{k+1}} \right\rangle\right|^2 \tag{8}$$

The residual value gets smaller and smaller, and convergence criteria are satisfied.

The MP algorithm seems to be a good method for the NP-complete problem in the least-effort malicious data injection attack. However, let us consider a simple case. In Hilbert space, the signal y can be denoted by the selected vector dictionary $\{x_1, x_2\}$. With the MP algorithm, the iteration will be repeated between x_1 and x_2, as shown below:

$$y = a_1 x_1 + a_2 x_2 + a_3 x_1 + a_4 x_2 + \ldots \tag{9}$$

This is because the residual is only perpendicular to the last vector rather than the linear combination of the previously selected vectors. In this way, the number of iterations involved will be infinite. In another word, an asymptotic convergence can be reached through a huge number of iterations.

B. OMP algorithm

A refinement of the MP algorithm, which is referred to as OMP, is adopted to solve the above mentioned problem. Define $V_N = \overline{\text{Span}\{x_{n_1}, \cdots, x_{n_N}\}}$, where N denotes the number of iterations. The best approximation we can construct.

Assume that we have the following k[th]-order model for $f_N = \sum_{n=1}^{k} a_n^k x_n + \mathrm{R}_k f$, with $\langle \mathrm{R}_k f, x_n \rangle = 0, n = 1, \ldots k$.

Update it to k+1[th]-order model, $f_N = \sum_{n=1}^{k+1} a_n^{k+1} x_n + \mathrm{R}_{k+1} f$ with $\langle \mathrm{R}_{k+1} f, x_n \rangle = 0, n = 1, \ldots k+1$.

f_N is the N-iteration approximation. The convergence will be faster only if each iteration satisfies $\mathrm{R}_k f \in V_N^{\perp}$.

The OMP algorithm is comprised of the following steps.

First, compute the inner-products $\{\langle \mathrm{R}_k f, x_{n_k} \rangle\}$ ($x_n \in \mathrm{D}$) and judge whether $x_{n_{k+1}}$ satisfies $|\langle \mathrm{R}_k f, x_{n_{k+1}} \rangle| \geq \alpha \sup_j |\langle \mathrm{R}_k f, x_j \rangle|$, where $0 \leq \alpha \leq 1$. Reorder the dictionary D by applying the permutation $k+1 \leftrightarrow n_{k+1}$. The calculation will cease when $|\langle \mathrm{R}_k f, x_{n_{k+1}} \rangle| < \delta$ ($\delta > 0$). Second, compute $\{b_n^k\}_{n=1}^{k}$ to get the auxiliary model $x_{k+1} = \sum_{n=1}^{k} b_n^k x_n + \gamma_k$, where $\langle \gamma_k, x_n \rangle = 0, n = 1, \ldots, k$, $\sum_{n=1}^{k} b_n^k x_n = P_{V_k} x_{k+1}$ and $\gamma_k = P_{V_k^{\perp} x_{k+1}}$. Update $f_{k+1} = \sum_{n=1}^{k+1} a_n^{k+1} x_n$, $\mathrm{R}_{k+1} f = f - f_{k+1}$ and $\mathrm{D}_{k+1} = \mathrm{D}_k \cup \{x_{k+1}\}$. a_n^k denotes the coefficients. Finally, set k, $(k \leftarrow k+1)$, and repeat the above steps.

Since the auxiliary model $x_{k+1} = \sum_{n=1}^{k} b_n^k x_n + \gamma_k$ satisfies $\langle \gamma_k, x_n \rangle = 0$, the model of order k can be updated to the model of order $k+1$ in the following way:

$$\mathrm{R}_k f = \mathrm{R}_{k+1} f + \alpha_k \gamma_k$$
$$\|\mathrm{R}_k f\|^2 = \|\mathrm{R}_{k+1} f\|^2 + \frac{|\langle \mathrm{R}_k f, x_{k+1} \rangle|^2}{\|\gamma_k\|^2} \qquad (10)$$

The residual $\mathrm{R}_{k+1} f$ satisfies (10), which means $\mathrm{R}_N f \in \mathrm{V}_N^{\perp}$ in each iteration. This suggests that the OMP algorithm, compared with the MP algorithm, requires much fewer iterations. Consider the example shown in (9). The convergence can be ensured with only two iterations using the OMP algorithm.

IV. Simulation

The performances of the MP and the OPMP algorithms are evaluated through simulation on the standard IEEE standard test system including 9-bus, 14-bus, 30-bus, 118-bus and 300-bus systems. The relationship between the number of meter measurements and the number of state variables for each IEEE bus system is given in Table 1. The information used in the simulation is from the package of MATPOWER of the MATLAB 7.2.0. [14], which includes the configuration of measurement matrix H, real meter measurements and state variables.

TABLE I. The Number of State Variables and Meter Measurements in IEEE Test System

System type	State variables	Meter measurements
IEEE 9-bus	8	27
IEEE 14-bus	13	54
IEEE 30-bus	29	112
IEEE 118-bus	117	490
IEEE 300-bus	299	1122

The DC-state estimator and the bad data detector are constructed on the small IEEE test systems including 9-bus, 14-bus and 30-bus systems, and the malicious data injection attack against the systems is simulated. The results indicate that the malicious data in meter measurements can bypass the state estimator and the bad data detector if the data is a linear combination of the column vectors of H (a = Hc).

The least-effort malicious data injection attack is also simulated, and the MP and the OMP algorithms are used separately to determine the minimum number of meters to compromise in the same number of iterations. In the simulation against IEEE 118-bus system, a number of $k (1 \leq k \leq 10)$ target state variables are randomly selected and the malicious data are produced to attack the variables. The malicious error added to each original variable estimate is set to be 100 times of the original estimate. The iterations are set to be 490 times. The simulation is performed 1,000 times for each of the selected variables. The relationships between the number of meter measurements and that of the state variables in the two algorithms are shown in Fig. 1 and Fig. 2.

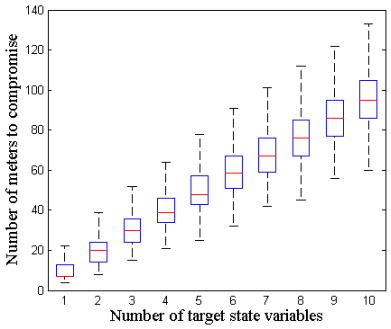

Fig. 1. MP algorithm case: number of meters to compromise to inject malicious data into *k* state variables in IEEE 118-bus system

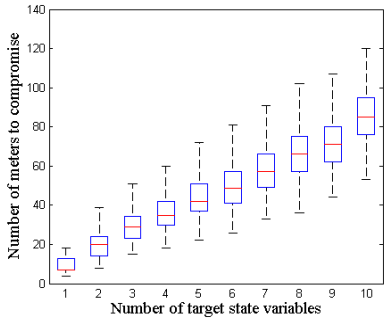

Fig. 2. OMP algorithm case: number of meters to compromise to inject malicious data into k state variables in IEEE 118-bus system

As shown in Figure 1, the attacker needs to compromise 5 to 22 meters in the best case (k=1) and 60 to 140 meters in the worst case (k=10) in the MP algorithm. Whereas, the attacker using the OMP algorithm needs to compromise 4 to 18 meters in the best case (k=1) and 50 to 120 meters in the worst case (k=10). It is clearly seen that more meter measurements need to be compromised using the MP algorithm than the OMP algorithm to launch malicious data injection attack on the same number of state variables.

Figures 3 and 4 show the number of meters to compromise for the attack on one state variable in each IEEE bus test system using the two algorithms, respectively. It is obviously shown that less number of meters need to be compromised in the MP algorithm compared with that in the OMP algorithm in all the test systems.

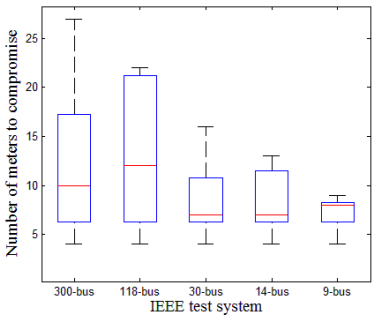

Fig. 3. MP algorithm: number of meters to compromise to attack one state variable

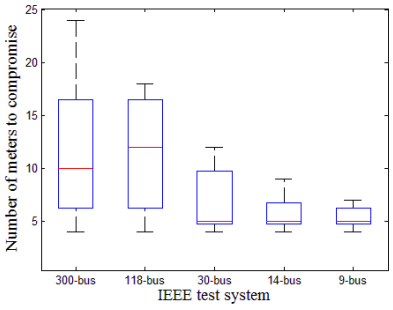

Fig. 4. OMP algorithm: number of meters to compromise to attack one state variable

V. CONCLUSION

This paper investigates the least-effort malicious data injection attack against power system state estimation, which is a NP-complete problem. The traditional solution to the problem, the MP algorithm, requires a large number of iterations to reach convergence. With a hope to find a better alternative, we adopt the OMP algorithm, a modified method based on MP. Simulation of malicious data injection attack on the IEEE standard bus test system using the two algorithms shows that the modified method needs to compromise a comparatively smaller number of meter measurements to attack the state variables in the same number of iterations. This indicates that the OMP algorithm may be an effective approach to launching the least-effort malicious data injection attack against power system state estimation. In our future work, we would like to extent the OMP algorithm from the test system to realistic settings.

REFERENCES

[1] Siddharth Sridhar, Adam Hahn, and Manimaran Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, January 2012.

[2] A. Monticelli, F. F. Wu, and M. Y. Multiple, "Bad data identification for state estimation by combinatorial optimization," IEEE Transactions on Power Delivery, vol. 1, no. 3, pp. 361–369, July 1986

[3] M. M. G.P. Granelli, "Identification of interacting bad data in the framework of the weighted least square method," Electric Power System Research, vol. 78, no. 5, pp. 806–814, May 2008.

[4] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM conference on Computer and communications security, pp.21-32, 2009.

[5] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.

[6] Kosut O, Jia L, Thomas R J, et al. "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures", Proceedings of 1st IEEE International Conference on Smart Grid Communications. MD USA: IEEE, 2010.

[7] 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," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.

[8] Monticelli, F. F. Wu, and M. Y. Multiple, "Bad data identification for state estimation by combinatorial optimization," IEEE Transactions on Power Delivery, vol. 1, no. 3, pp. 361–369, July 1986.

[9] M.G. P. Granelli, "Identification of interacting bad data in the framework of the weighted least square method," Electric Power System Research, vol. 78, no. 5, pp. 806–814, May 2008.

[10] Harald Nautsch, Jorn Ostermann, "Transform Coding of Compound Images Using Matching Pursuit," 2012 Picture Coding Symposium, May 7-9, 2012.

[11] L. Lovisolo, E. A. B. da Silva, M. A. M. Rodrigues, and P. S. R. Diniz, "Efficient coherent adaptive representations of monitored electric signals in power systems using damped sinusoids," IEEE Transactions on Signal, Processing, vol. 53, no. 10, pp. 3831–3846, October 2005.

[12] P. S. Huggins and S. W. Zucker, "Greedy basis pursuit," IEEE Transactions on Signal Processing, vol. 55, no. 7, pp. 3760–3772, July 2007.

[13] Y. C. Pati, R. Rezaiifar, and P. S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," in the 27th Asilomar Conference on Signals, Systems and Computers, 1993.

[14] R. D. Zimmerman, C. E. Murillo-Sanchez, and D. Gan. (2007) Matpower, a matlab power system simulation package, [Online]. Available: http://www.pserc.cornell.edu/matpower/manul.pdf