ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 138-143
doi: 10.18178/wcse.2017.06.024

False Data Injection Attacks Using Matrix Recovery and PARAFAC in Smart Grid

Jiwei Tian[+] and Buhong Wang

Information and Navigation College' Air Force Engineering University, Xi'an 710077

Abstract. Existing researches demonstrate that state estimation result could be compromised by malicious attacks. However, to construct the attack vectors, a usual assumption in most works is that the attacker has perfect information regarding the topology even such information is difficult to acquire in practice. Recent research shows that Parallel Factor Analysis (PARAFAC) can be used to drive the linear structure matrix of the smart grid which can be used to carry out undetectable attacks. However, we found that the above PARAFAC based blind attack strategy is only feasible in the environment with Gaussian noises. If there are outliers (device malfunction or communication errors), the Bad Data Detector will easily detect the attack. Hence, we propose a robust PARAFAC based blind attack strategy that one can use matrix recovery to circumvent the outlier problem and construct stealthy attack vectors. The proposed attack strategies are tested with IEEE 14-bus system. Simulations verify the feasibility of the proposed method.

Keywords: false data injection; parallel factor analysis; matrix recovery; augmented lagrange multiplier

1. Introduction

With the rapid development of smart grid, security threat has been on the rise in both physical and cyber spaces [1], [2]. Recently, the cyber security has been identified as a dominating component in the development of power grid. In smart grid, state estimation is a vital important module which is pregnable to cyber-attacks, for example, false data injection (FDI) attacks.

FDI attacks were first named in 2009 by Liu et al [3]. [3] shows that such attacks can bypass traditional bad data detector [4] based on residual testing with the knowledge of power network, which makes the claimed attacks undetectable to the power grid system. Furthermore, the false data injection attacks can mislead systems into the unsecure operations, e.g., line overloading [5], power outage [6] [7].

Although the attack strategy is deeply studied where different researchers have investigated different sides of attack construction, in most works it is assumed that the attacker has perfect information regarding the topology and so on even such information is difficult to acquire in practice. Recently, several groups concentrate on the attacks under the presumption that attackers don't have system information. In [8], an attacking strategy is proposed using parallel factor analysis. In the work, it was assumed that the attacker has no prior knowledge of the system information and the stealthy attack was constructed only based on measurement matrix. And the experiment results in [8] show that the PARAFAC based method achieves a higher accuracy performance than the independent component analysis (ICA) based method in [9]. In this paper, at first we demonstrate that the above claimed attack strategy is feasible if the measurements only include Gaussian noises. If there are outliers, bad data detector will detect the attacks. Next, we propose a robust PARAFAC based blind attack strategy that the attacker use matrix recovery to solve the outlier problem, and construct stealthy attack vectors. The equivalent information of the original measurement matrix is recovered using augmented lagrange multiplier (ALM) method. The proposed attack strategies are tested with IEEE 14-bus system. Simulations verify the feasibility of the proposed method.

[+] Corresponding author. Tel.: +15339152689.
E-mail address: tianjiwei2016@163.com.

2. State Estimation and Conventional Bad Data Detection

In power grid, transmission lines deliver power to consumers [10]. In theory, the transferred power is depended on the difference of voltage between the two buses, and that it's also the line's impendence's function. Generally, the impedance can be approximated with reactance of a transmission line on account of the high reactance over resistance ratio. Active transferred power from bus i to j can be expressed as [11]

$$\mathrm{P}_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_{\mathrm{i}} - \theta_j) \tag{1}$$

where V_i, V_j are the voltage magnitudes, $\theta_{\mathrm{i}}, \theta_j$ are the voltage phase angels, and X_{ij} is the reactance of the transmission line. In DC power flow, the phase differences are assumed small and the voltage magnitudes are close to unity. Therefore, transmitted active power can be expressed as [12]:

$$\mathrm{P}_{ij} = \frac{\theta_{\mathrm{i}} - \theta_j}{X_{ij}} \tag{2}$$

Now assume that m measurements measure injected or transmitted power in the buses or lines. In this case, voltage angles can be estimated except one reference bus $(\theta_1 = 0)$ and the measurement vector z can be written as follows:

$$z = P(\theta) + e \tag{3}$$

where $P(\theta)$ represents the nonlinear relation between measurement vector $z = [z_1, \cdots, z_m]^T$ and state vector $\theta = [\theta_1, \cdots, \theta_n]^T$, and that $e = [e_1, \cdots, e_m]^T$ represents the Gaussian measurement noise with covariant matrix Σ_e .If the phase angle differences are small, the linear approximation of (3) can be written as

$$\mathrm{z} = Hx + e \tag{4}$$

where H is Jacobian matrix, and it is known to the System Operator, but usually unknown to the attackers.

Using the weighted least squares method [13], the system state vector of (4) can be estimated by

$$\hat{\theta} = (H^T \Sigma_e^{-1} H)^{-1} H^T \Sigma_e^{-1} z \tag{5}$$

Due to the topological error or faulty sensors, the residual testing is generally used to compare the difference between real measurements and estimated measurements:

$$r = z - H\hat{\theta} \tag{6}$$

Therefore, the expected value and the covariance of the residual are:

$$E(r) = 0 \quad and \quad \mathrm{cov}(r) = (I - M)\Sigma_e \tag{7}$$

where $M = H(H^T \Sigma_e^{-1} H)^{-1} H^T \Sigma_e^{-1}$.

The chi-square testing is generally used to detect bad data[14].If $\|r\| \geq \chi^2_{(m-n),p}$ (p represents desired significance level), then there exists at least one bad data.

If an attacker obtains the topology matrix, the undetectable attack compromises the measurements as follows:

$$\mathrm{z}_a = H\theta + a + e \tag{8}$$

where

$$a = Hc \tag{9}$$

In this case，the measurement residual has the following result:

$$r_a = z_a - H\hat{\theta}_a = z + a - H(\hat{\theta} + c) = z - H\hat{\theta} = r \tag{10}$$

The bad data detector can't detect the attack as there is no difference between r_a and r .It means that the attack is undetectable to the operator.

3. False Data Injection Based on Matrix Recovery and PARAFAC

The main idea of PARAFAC-based false data injection is when power loads vary slightly, structural information will be implicit among the power flow measurements.

Usually, state vector is a nonlinear function of the topology H and the power loads s, $\theta = f(H,s)$.While the topology is static over the time, loads can be modelled as random variables. If the system dynamics are sufficiently small, $f(H,s)$ can be approximated by $\theta \approx \Phi s$, then

$$z = H\Phi s + e = Gs + e \tag{11}$$

In [8], the authors use the PARAFAC technique to infer $H\Phi$ and s. The authors adopt Alternative Least Square (ALS) [15] method in the research. The algorithm converges quickly and doesn't rely on the user-defined parameters.

Although the above attack strategy can construct a stealthy attack with low detection rate, it is merely feasible for the measurement matrix with Gaussian noises only. If there are outliers, the traditional bad data detector will detect the attacks. Hence, we propose a robust PARAFAC based blind attack strategy that the attacker use matrix recovery to solve the outlier problem and construct stealthy attack vectors.

Suppose, the measurement matrix containing outliers is written as:

$$Zoutlier = Z + E \tag{12}$$

where Z represents the original low rank matrix, it is needs to be recovered, E is a sparse matrix, it represents outliers. Now, before constructing attack vectors, the attacker needs to separate Z and E from the measurement matrix containing outliers $Zoutlier$. It is a matrix recovery problem and the recovery of Z and E can be represented as below:

$$\min \|Z\|_* + \lambda \|E\|_1 \quad s.t.\ \ Zoutlier = Z + E \tag{13}$$

In the above convex optimization problem, $\|\bullet\|_*$ denotes the nuclear norm of a matrix, $\|\bullet\|_1$ denotes l_1 norm of a matrix, and λ represents a positive weighting parameter[16].In order to figure out this problem, the augmented lagrange multiplier (ALM) [17] approach is adopted as discussed below:

The ALM approach can be exploited for usual constraint optimization problems as follows:

$$\min \quad f(x) \qquad s.t. \quad h(x) = 0 \tag{14}$$

With the ALM approach, the objective function can be expressed as a lagrangian function:

$$L(x, Y, \mu) = f(x) + \langle \gamma, h(x) \rangle + \frac{\mu}{2} \|h(x)\|_F^2 \tag{15}$$

where γ is the lagrange multiplier and μ is a positive scalar. Considering $x = (Z, E)$, $f(x) = \|Z\|_* + \lambda \|E\|_1$ and $h(x) = Zoutlier - Z - E$, the Lagrangian function can be written as:

$$L(A, E, \gamma, \mu) = f(x) = \|Z\|_* + \lambda \|E\|_1 + \langle \gamma, (Z_{\text{outlier}} - Z - E) \rangle + \frac{\mu}{2} \|Z_{\text{outlier}} - Z - E\|_F^2 \tag{16}$$

The optimization process is solved by two update steps,

$$Z_{K+1} = \arg\min L(Z, E_k, \gamma_k, \mu_k) \tag{17}$$

$$E_{K+1} = \arg\min L(Z_{k+1}, E, \gamma_k, \mu_k) \tag{18}$$

Eq(18) can be solved from the soft shrinkage formula[18], using an iterative method which uses the singular value decomposition of the matrix $(Z_{outlier} - E_k + \mu_k^{-1}\gamma_k)$. After that, we can get the unitary matrix U, V and rectangular diagonal matrix S. Then, update Z:

$$Z_{k+1} = U\xi_{\mu_k^{-1}}[S]V^T \tag{19}$$

and update E:

$$E_{k+q} = \xi_{\lambda\mu_k^{-1}}[Z_{outlier} - Z_{k+1} + \mu_k^{-1}\gamma_k] \tag{20}$$

here $\lambda = \frac{1}{\sqrt{\max(m,t)}}$ and ξ is a soft-thresholding operator, it is defined as[18]:

$$\xi_{\varepsilon}[x]=\begin{cases} x-\varepsilon, & if\ x>\varepsilon \\ x+\varepsilon, & if\ x<-\varepsilon \\ 0, & otherwise \end{cases} \tag{21}$$

γ and μ are updated during each iteration as follows:

$$\gamma_{k+1}=\gamma_k+\mu_k(Z_{outlier}-Z_{k+1}-E_{k+1}) \tag{22}$$

$$\mu_{k+1}=\Psi\mu_k \tag{23}$$

where Ψ is a positive constant. The optimization process continues till the criteria is satisfied. And the convergence is examined based on the relative error using (25) against a tolerance, τ.

$$c_k^{ite}=\frac{\left\|Z_{outlier}-Z_{k+1}-E_{k+1}\right\|}{\left\|Z_{outlier}\right\|_F} \tag{24}$$

Once the algorithm has converged, the original measurement matrix Z is recovered. Then, we can construct stealthy attack vector based on original measurement matrix using PARAFAC. The algorithm is expressed in Algorithm 1.

Algorithm 1: False data injection attack using matrix recovery and PARAFAC

Input: $Z_{outlier}$,measurement matrix containing outliers

1 [Z , E]=ALM($Z_{outlier}$) %%use ALM based approach to generate true measurement matrix Z ;

2 [G and s]=ALS(Z);

3 if $\max(Z-Gs)>\varepsilon$ then exit;

4 Generate $\delta s\sim N(0,\sigma^2)$;

5 $z_a=z+G(s+\delta s)$

Output: false data z_a

4. Results and Discussion

First of all, we show the case when attack strategy is generated using PARAFAC. Next we demonstrate that independent component analysis based attacks fail to maintain unobservable in the bad data detection in the presence of outliers. In the end, we separate the sparse outlier matrix and the real measurement matrix using ALM based approach. The real measurement matrix is then used for attack construction. We use Matpower[19] for analysis purposes.

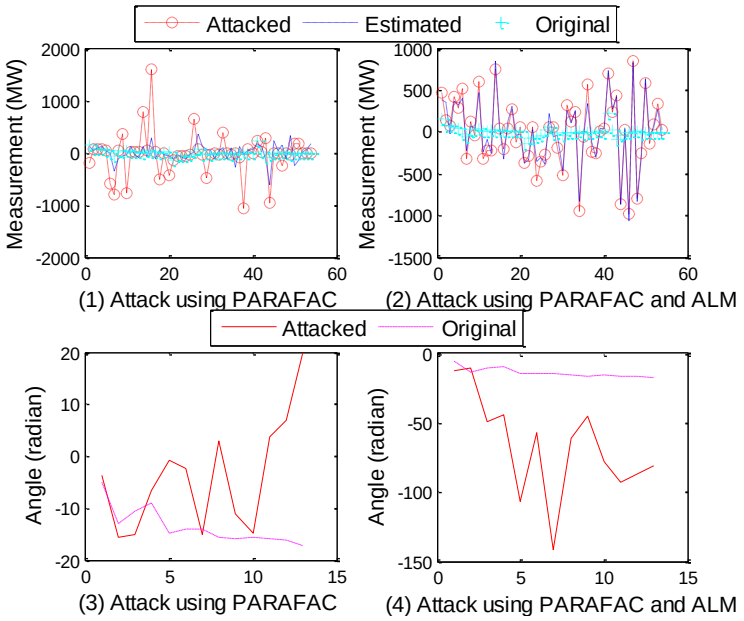
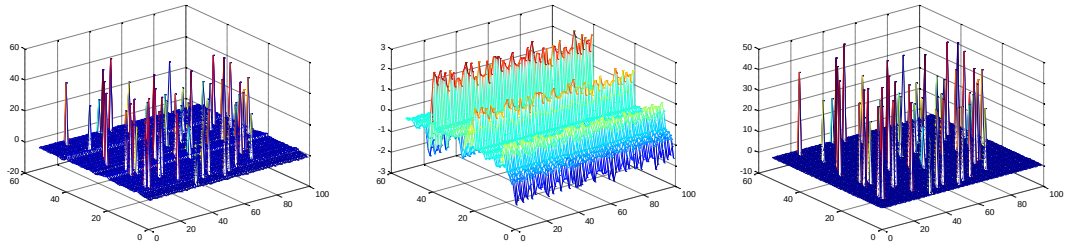


Fig. 1: Sensor measurements and State variables in different attack schemes (with outliers)

IEEE 14 bus system is used in the experiment. The system is fully measured so that there are totally 54 sensors. As the system has 13 states and 54 measurements, the degree of freedom is 41. Following a chi-square test considering 97.5% confidence interval, the threshold for BDD is $\chi^2_{0.025}(54-13)=60.65$. Under Gaussian noise cases, i.e., the signal-to-noise (SNR) is between 15~30 db. And we consider there are 1% outliers of the measurement matrix. Then, if PARAFAC based attack construction is followed when the measurement matrix containing outliers, a high residual value $3.5e^5$ is observed. From fig.1(1), we can see that the estimated measurement doesn't follow neither the attacked measurement or original measurement. This experiment validates the fragility of the PARAFAC approach when there are outliers. Here, we carry out the attack strategy using ALM and PARAFAC above and acquire original measurement matrix as show in Fig.2. We can observe from Fig.1 (3) that the estimated signal follows the attacked signals. The residual is also below the threshold which makes the attack undetectable in the bad data detector. In Fig.3, we find that the proposed attack strategy follows the nearly same probability as the real (no attack) case and thus remain unobservable.



$Z_{outlier}$ Z E

Fig. 2: The ALM method recovers the true measurement matrix

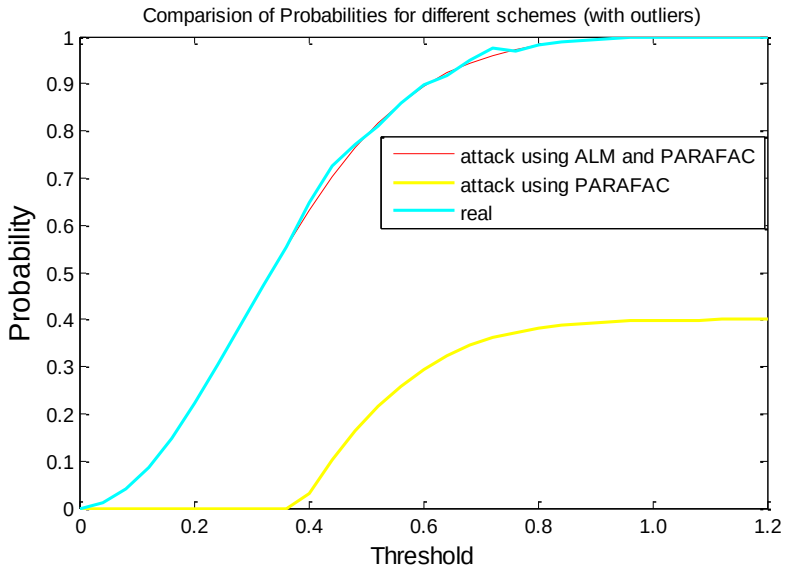


Fig. 3: Comparison of Probabilities for different schemes (with outliers)

5. Conclusion

This paper found that the original PARAFAC-based attack tactic is merely feasible for the measurement matrix with Gaussian noises. When there are outliers, the traditional Bad Data Detector will detect the attacks. Hence, we propose a robust PARAFAC based blind attack strategy that the attacker use matrix recovery to solve the outlier problem and construct stealthy attack vectors. The proposed attack strategies are tested with IEEE 14-bus system. The simulated results confirm that our attack strategy is undetectable.

6. Acknowledgements

This work was supported by Project Supported by the National Natural Science Fund of China (61671465).

7. References

[1] Bertsch, J., Carnal, C., Karlson, D., et al. Wide-area protection and power system utilization, Proc. IEEE, 2005, 93, (5), pp. 997–1003

[2] Mo, Y., Kim, T.H.J., Brancik, K., et al. Cyber–physical security of a smart grid infrastructure, Proc. IEEE, 2012, 100, (1), pp. 195–209

[3] Y. Liu, P. Ning, and M. K. Reiter, False data injection attacks against state estimation in electric power grids, in ACM Conf. Comput. Commun. Security, 2009, pp. 21-32

[4] D. Gorinevsky, S. Boyd, and S. Poll, Estimation of faults in dc electrical power system, in IEEE Conf. Decision and Control, 2009, pp. 4334-4339

[5] Y.Yuan, Z. Li, and K. Ren, Quantitative analysis of load redistribution attacks in electric grid, IEEE Trans. Parallel Distrib. Syst., vol. 23, no.9, pp. 1731–1738, Sep. 2012

[6] J. Zhang and L. Sankar, Physical system consequences of unobservable state-and-topology cyber-physical attacks, IEEE Transactions on Smart Grid, vol. PP, no. 99, pp. 1–10, 2016

[7] J. Liang, L. Sankar, and O. Kosut, Vulnerability analysis and consequences of false data injection attack on power system state estimation, IEEE Transactions on Power Systems, vol. PP, no. 99, pp. 1–9, 2016

[8] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, Bad data injection in smart grid: attack and defense mechanisms, IEEE Commun. Mag., vol. 51, no. 1, pp. 27-33, Jan. 2013.

[9] Yang J, Yu R, Liu Y, et al. A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid[C]//IEEE International Conference on Communications. IEEE, 2015:7210-7215.

[10] J. Casazza and F. Delea, Understanding Electric Power Systems, IEEE Press Understanding Science and Technology Series, Wiley, 2010

[11] J. J. Grainger and W. D. Stevenson Jr., Power System Analysis, vol. 621. New York, NY, USA: IEEE Press, 1994

[12] A. J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control. New York, NY. USA: IEEE Press, 1996

[13] G. P. Granelli and M. Montagna, Identification of interacting bad data in the framework of the weighted least square method, Electric Power Syst. Research, vol. 78, no. 5, pp. 806-814, May 2008

[14] A. Abur and A. Exp ́osito, Power System State Estimation: Theory and Implementation, ser. Power Engineering (Willis). CRC Press, 2004

[15] L. D. Lathauwer and J. Castaing, Blind identification of underdetermined mixtures by simultaneous matrix diagonalization, IEEE Transactions on Signal Process, vol.56, no.3, pp.1096-1105, Mar.2008.

[16] Z. Lin, M. Chen, and Y. Ma, Fast convex optimization algorithms for exact recovery of a corrupted low-rank matrix, UIUC Technical Report UILU-ENG-09-2214, Tech. Rep., 2009

[17] Z. Lin, M. Chen, Y. Ma, The augmented Lagrange multiplier method for exact recovery of corrupted low-rank matrices, UIUC Technical Report UILU-ENG-09-2214, Tech. Rep., 2009.

[18] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, Z. Han, Detecting false data injection attacks on power grid by sparse optimization, IEEE Trans. Smart Grid 5(2) (March 2014) 612–621

[19] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education, IEEE Transactions on Power Systems, vol. 26, no. 1, pp. 12–19, Feb 2011