# OPTIMUM NODE SELECTION FOR PROTECTION UNDER POWER GRID STATE ESTIMATION

*Qian He*, Duo Bai*, and Rick S. Blum†*

*EE Department, Univ. of Electron. Sci. and Tech. of China, Chengdu, Sichuan 611731 China
†ECE Department, Lehigh University, Bethlehem, PA 18015 USA

## ABSTRACT

State estimation of a power grid under undetected power injection attacks is considered. With a known prior probabilistic description of the state variables, the maximum *a posteriori* probability (MAP) estimator is adopted. Undetected attacks lead to model mismatch, which may greatly degrade the estimation performance. The mean square error (MSE) of the MAP estimate under model mismatch is derived. Considering the case where we are able to protect a limited number of nodes under power injection attacks, we formulate and solve an optimization problem to select which nodes to protect to minimize the MSE degradation that the attacker can provide.

***Index Terms*—** Maximum *a posteriori* probability (MAP), mean square error (MSE), node selection for protection, state estimation.

## 1. INTRODUCTION

Our society relies heavily on critical large-scale power grids which connect electric power generators to consumers. Resiliency to attacks which inject bad data is of increased interest lately, based on studies which suggest such attacks are eminent. While current grids employ bad data detection methods, such as the energy conservation test, the Chi-squared test and the normalized residuals test [1] in state estimation procedures, these detectors lack the ability to identify highly structured bad data that conforms to the network topology and some particular physical laws governing the power grid operation [2]-[5].

While the majority of existing work [6, 7, 8, 9] seeks to prevent undetectable attacks, this paper considers the case where the attacks have been successfully launched and the power system is unfortunately unaware of the attacks. The one paper we saw [10] which did consider minimizing the impact of successfully launched attacks, did not consider state estimation, and employed a significantly different criterion on the impact than we consider here where we focus on state estimation. We consider power injection attacks, either stealth or not, and assume that they are undetected and thereby lead to a model mismatch. The mean square error (MSE) of the mismatched maximum *a posteriori* probability (MAP) estimation is derived and employed as the evaluation metric of the state estimation performance. Considering the case where we are able to protect a limited number of nodes under power injection attacks, we formulate and solve an optimization problem to select which nodes to protect to minimize the MSE degradation that the attacker can provide. It is shown that the optimum node selection strategy is determined by the description of the power grid network and the statistical description of the state, noise and attack. Numerical results for a 9-bus system and the IEEE 14-bus system are presented to verify the theoretical findings.

This work was supported by the National Nature Science Foundation of China under Grant 61102142, the International Science and Technology Cooperation and Exchange Research Program of Sichuan Province under Grant 2013HH0006, the Fundamental Research Funds for the Central Universities under Grant ZYGX2013J015, the U. S. Army Research Laboratory and the U. S. Army Research Office under Grants No. W911NF-14-1-0245 and W911NF-14-1-0261.

## 2. PROBLEM FORMULATION

Consider a power system consisting of $N$ buses (nodes) and $L$ transmission lines. Define the node set $\mathcal{N} \triangleq \{1, 2, ..., N\}$ and line set $\mathcal{E} \triangleq \{(i, j)\}$, where $(i, j)$ denotes a transmission line between nodes $i$ and $j$. Denote the admittance of the series branch connecting buses $i$ and $j$ by $g_{ij} + jb_{ij}$ with $g_{ij}$ the branch conductance and $b_{ij}$ the branch susceptance. Likewise [1], the admittance of the shunt branch from node $i$ to ground is $g_{io} + jb_{io}$ with $g_{io}$ the shunt conductance and $b_{io}$ the shunt susceptance. Thus, the real power flow from bus $i$ to bus $j$ can be described as [1]

$$\begin{aligned} P_{ij} =& v_i^2 (g_{io} + g_{ij}) - v_i v_j [g_{ij} \cos(\theta_i - \theta_j) \\ &+ b_{ij} \sin(\theta_i - \theta_j)] \end{aligned} \tag{1}$$

where $v_i$ and $\theta_i$ denote the voltage magnitude and phase corresponding to the $i$th node. Consider the DC power flow model, which assumes that the bus voltage amplitudes are close to unity. Neglecting all the shunt elements and branch resistances, the real power flow measured from bus $i$ to $j$ can be approximated by the first order Taylor expansion around

$\boldsymbol{\theta} = \mathbf{0}$, which reduces (1) to

$$P_{ij} = b_{ij}(\theta_i - \theta_j) \tag{2}$$

Therefore, the power injected at bus $i$, which is the sum of the power flows through the branches connected to bus $i$, can be expressed as

$$P_i = \sum_{j\in\mathcal{R}_i} P_{ij} = \sum_{j\in\mathcal{R}_i} b_{ij}(\theta_i - \theta_j) = \sum_{j\in\mathcal{R}_i} \mathbf{h}_{ij}^T\boldsymbol{\theta} \tag{3}$$

where $\mathcal{R}_i = \{j|(i,j) \in \mathcal{E}, j = 1, ..., N\}$ is the index set of the buses that are directly connected to bus $i$,

$$\mathbf{h}_{ij} = [0, ..., 0, \underbrace{b_{ij}}_{\text{column } i}, 0, ..., 0 \underbrace{-b_{ij}}_{\text{column } j}, 0, ..., 0]^T \tag{4}$$

and the state vector to estimate consists all the voltage phases

$$\boldsymbol{\theta} = [\theta_1, \theta_2, ...\theta_N]^T. \tag{5}$$

Thus, the measurement vector that contains the power injected at every bus is given by

$$\mathbf{z} = [P_1, P_2, ..., P_N]^T = \mathbf{H}\boldsymbol{\theta} + \mathbf{v} \tag{6}$$

where $\mathbf{v}$ represents the measurement noise vector and

$$\mathbf{H} = \left[\sum_{j\in\mathcal{R}_1} \mathbf{h}_{1j}^T, \sum_{j\in\mathcal{R}_2} \mathbf{h}_{2j}^T, ..., \sum_{j\in\mathcal{R}_N} \mathbf{h}_{Nj}^T\right]^T. \tag{7}$$

is the measurement matrix.

*Assumption 1:* The measurement noise vector $\mathbf{v}$ obeys a Gaussian distribution with mean zero and full-rank covariance matrix $\mathbf{R}_v$.

*Assumption 2:* The prior distribution of the state vector $\boldsymbol{\theta}$ is known to be zero-mean Gaussian with full-rank covariance matrix $\mathbf{R}_\theta$. The vectors $\boldsymbol{\theta}$ and $\mathbf{v}$ are independent.

Under Assumptions 1 and 2, based on the observation model in (6), the MAP estimate of $\boldsymbol{\theta}$ can be obtained as

$$\begin{aligned}
\hat{\boldsymbol{\theta}}_{\text{MAP}} &= \arg\max_{\boldsymbol{\theta}} \{p_{\boldsymbol{\theta}|\mathbf{z}}(\boldsymbol{\theta}|\mathbf{z})\} \\
&= \arg\max_{\boldsymbol{\theta}} \left\{\frac{p_{\mathbf{z}|\boldsymbol{\theta}}(\mathbf{z}|\boldsymbol{\theta})p_{\boldsymbol{\theta}}(\boldsymbol{\theta})}{p(\mathbf{z})}\right\} \\
&= \arg\max_{\boldsymbol{\theta}} \{p_{\mathbf{z}|\boldsymbol{\theta}}(\mathbf{z}|\boldsymbol{\theta})p_{\boldsymbol{\theta}}(\boldsymbol{\theta})\} \\
&= \arg\max_{\boldsymbol{\theta}} \{\ln p_{\mathbf{z}|\boldsymbol{\theta}}(\mathbf{z}|\boldsymbol{\theta}) + \ln p_{\boldsymbol{\theta}}(\boldsymbol{\theta})\}
\end{aligned} \tag{8}$$

where

$$p_{\boldsymbol{\theta}}(\boldsymbol{\theta}) = \frac{1}{(2\pi)^{\frac{N}{2}} \det(\mathbf{R}_\theta)|^{\frac{1}{2}}} \exp\left\{-\frac{1}{2}\boldsymbol{\theta}^T\mathbf{R}_\theta^{-1}\boldsymbol{\theta}\right\} \tag{9}$$

and

$$\begin{aligned}
p_{\mathbf{z}|\boldsymbol{\theta}}(\mathbf{z}|\boldsymbol{\theta}) =& \frac{1}{(2\pi)^{\frac{N}{2}} \det(\mathbf{R}_v)^{\frac{1}{2}}} \\
&\times \exp\left\{-\frac{1}{2}(\mathbf{z} - \mathbf{H}\boldsymbol{\theta})^T\mathbf{R}_v^{-1}(\mathbf{z} - \mathbf{H}\boldsymbol{\theta})\right\}
\end{aligned} \tag{10}$$

in which $\det(\mathbf{R})$ denotes the determinant of matrix $\mathbf{R}$. Taking the derivative of (8) with respect to $\boldsymbol{\theta}$ and setting it equal to zero yields

$$\left[\frac{\partial \ln p_{\mathbf{z}|\boldsymbol{\theta}}(\mathbf{z}|\boldsymbol{\theta})}{\partial\boldsymbol{\theta}} + \frac{\partial \ln p_{\boldsymbol{\theta}}(\boldsymbol{\theta})}{\partial\boldsymbol{\theta}}\right]\Bigg|_{\boldsymbol{\theta}=\hat{\boldsymbol{\theta}}_{\text{MAP}}} = 0, \tag{11}$$

which can be written as

$$\mathbf{H}^T\mathbf{R}_v^{-1}(\mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}_{\text{MAP}}) + \mathbf{R}_\theta\hat{\boldsymbol{\theta}}_{\text{MAP}} = 0. \tag{12}$$

Thus, one can solve equation (12) to obtain

$$\hat{\boldsymbol{\theta}}_{\text{MAP}} = \left(\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{H} + \mathbf{R}_\theta^{-1}\right)^{-1}\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{z}. \tag{13}$$

## 3. STATE ESTIMATION UNDER MODEL MISMATCH

When the observed data follows the DC model in (6), the estimate in (13) is optimal under the MAP criterion. In practice, however, the observed data may not follow the model in (6) exactly, possibly due to a failure or an attack. If the control center is unaware of the attack and continues using (6) to estimate the state, it will lead to a model mismatch. Denote the actual observation vector by $\mathbf{z}_a$, then the mismatched MAP estimation can be expressed as

$$\hat{\boldsymbol{\theta}}_{\text{MAP,a}} = \left(\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{H} + \mathbf{R}_\theta^{-1}\right)^{-1}\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{z}_a. \tag{14}$$

Note that due to the model mismatch, $\hat{\boldsymbol{\theta}}_{\text{MAP,a}}$ in (14) is no longer optimum under the MAP criterion.

Consider the scenario where additive attacks, denoted by a column vector $\mathbf{a}$, are injected covertly without the control center's knowledge. Assume that one can protect only $M$ of the $N$ nodes such that any node under protection is not faced with the power injection attack. Hence, the actual observation vector can be written as

$$\mathbf{z}_a = \mathbf{H}\boldsymbol{\theta} + \mathbf{Q}\mathbf{a} + \mathbf{v} \tag{15}$$

where

$$\mathbf{Q} = diag\{q_1, q_2, ..., q_N\} \tag{16}$$

and

$$q_i = \begin{cases} 0, & \text{bus } i \text{ is protected} \\ 1, & \text{bus } i \text{ is unprotected} \end{cases}. \tag{17}$$

In the special case when every bus is protected, then $\mathbf{Q} = \mathbf{0}$, the effect of the attacks can be neglected. If no protection is taken, then $\mathbf{Q} = \mathbf{I}$, which may cause serious model mismatch and severely degrade the estimation performance.

Next, we analyze how the model mismatch caused by the undetected additive attack affects the performance of the state estimation. Before proceeding, we make an assumption on the statistical distribution of the additive attack.

*Assumption 3:* The additive attack vector $\mathbf{a}$ is known to follow a Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\mathbf{R}$. The vector $\mathbf{a}$ is independent of $\mathbf{v}$.

*Lemma 1:* Consider a DC power system with protected nodes facing an undetected additive attack. Suppose the MAP estimator (13) designed for (6) is employed, while the actual observations follow the model in (15). Under Assumptions 1-3, the mean square error (MSE) matrix of the mismatched MAP estimation (14) is

$$\begin{aligned}\mathbf{R}_{\varepsilon_\theta} =&\mathbb{E}\{\boldsymbol{\varepsilon}_\theta \boldsymbol{\varepsilon}_\theta^T\} \\ =&\mathbf{B}^{-1} + (\mathbf{CQRQ}^T\mathbf{C}^T - \mathbf{D} - \mathbf{D}^T)\end{aligned} \tag{18}$$

where $\mathbb{E}\{\cdot\}$ is the expectation operator,

$$\boldsymbol{\varepsilon}_\theta \triangleq \boldsymbol{\theta} - \hat{\boldsymbol{\theta}}_{\text{MAP,a}} \tag{19}$$

$$\mathbf{B} = \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{H} + \mathbf{R}_\theta^{-1} \tag{20}$$

$$\mathbf{C} = \mathbf{B}^{-1}\mathbf{H}^T\mathbf{R}_v^{-1} \tag{21}$$

and

$$\mathbf{D} = \mathbf{B}^{-1}\mathbf{R}_\theta^{-1}\mathbb{E}\{\boldsymbol{\theta}\mathbf{a}^T\}\mathbf{Q}^T\mathbf{R}_v^{-1}\mathbf{H}\mathbf{B}^{-1}. \tag{22}$$

*Proof of Lemma 1:* Plugging (14) and (15) into (19) yields

$$\begin{aligned}\boldsymbol{\varepsilon}_\theta =&\boldsymbol{\theta} - \mathbf{B}^{-1}\mathbf{H}^T\mathbf{R}_v^{-1}\left(\mathbf{H}\boldsymbol{\theta} + \mathbf{Qa} + \mathbf{v}\right) \\ =&\mathbf{B}^{-1}\left[\left(\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{H} + \mathbf{R}_\theta^{-1}\right)\boldsymbol{\theta} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{H}\boldsymbol{\theta}\right. \\ &\left.-\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{Qa} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{v}\right] \\ =&\mathbf{B}^{-1}(\mathbf{R}_\theta^{-1}\boldsymbol{\theta} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{Qa} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{v})\end{aligned} \tag{23}$$

It is seen from (20) that both $\mathbf{B}$ and $\mathbf{B}^{-1}$ are symmetric. Recall that $\boldsymbol{\theta}$, $\mathbf{v}$ and $\mathbf{a}$ are mutually independent, and $\boldsymbol{\theta}$ and $\mathbf{v}$ both have zero mean. Thus, the MSE matrix can be computed as follows

$$\begin{aligned}&\mathbf{R}_{\varepsilon_\theta} = \mathbb{E}\{\boldsymbol{\varepsilon}_\theta\boldsymbol{\varepsilon}_\theta^T\} \\ =&\mathbb{E}\left\{\mathbf{B}^{-1}(\mathbf{R}_\theta^{-1}\boldsymbol{\theta} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{Qa} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{v})\right. \\ &\left.\times(\boldsymbol{\theta}^T\mathbf{R}_\theta^{-1} - \mathbf{a}^T\mathbf{Q}^T\mathbf{R}_v^{-1}\mathbf{H} - \mathbf{v}^T\mathbf{R}_v^{-1}\mathbf{H})\mathbf{B}^{-1}\right\} \\ =&\mathbf{B}^{-1}\left[\mathbf{R}_\theta^{-1}\mathbb{E}\{\boldsymbol{\theta}\boldsymbol{\theta}^T\}\mathbf{R}_\theta^{-1} + \mathbf{H}^T\mathbf{R}_v^{-1}\mathbb{E}\{\mathbf{v}\mathbf{v}^T\}\mathbf{R}_v^{-1}\mathbf{H}\right. \\ &- \mathbf{R}_\theta^{-1}\mathbb{E}\{\boldsymbol{\theta}\mathbf{a}^T\}\mathbf{Q}^T\mathbf{R}_v^{-1}\mathbf{H} - \mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{Q}\mathbb{E}\{\mathbf{a}\boldsymbol{\theta}^T\}\mathbf{R}_\theta^{-1} \\ &\left.+\mathbf{H}^T\mathbf{R}_v^{-1}\mathbf{Q}\mathbb{E}\{\mathbf{a}\mathbf{a}^T\}\mathbf{Q}^T\mathbf{R}_v^{-1}\mathbf{H}\right]\mathbf{B}^{-1} \\ =&\mathbf{B}^{-1} - \mathbf{D} - \mathbf{D}^T + \mathbf{CQRQ}^T\mathbf{C}^T\end{aligned} \tag{24}$$

which completes the proof. ∎

According to Lemma 1, the MSE performance of the mismatched MAP estimation is dependent on the prior information about the observation noise, the additive attack, and the states to be estimated. It also depends on the structure of the power system, the nodes selected to be protected, and on $\mathbb{E}\{\boldsymbol{\theta}\mathbf{a}^\mathbf{T}\}$. In the case of no attacks, it can be shown that the MSE matrix is reduced to $\mathbf{R}_{\varepsilon_\theta} = \mathbf{B}^{-1}$. Comparing this with (18), we see that the effect of the additive attack enters the MSE matrix through the second term of (18), $(\mathbf{CQRQ}^T\mathbf{C}^T - \mathbf{D} - \mathbf{D}^T)$.

## 4. OPTIMAL NODE PROTECTION

This section attempts to determine which nodes to protect to minimize the impact of undetected attacks on the MSE performance, assuming we are able to protect only a limited number of nodes. Denote the index set of the protected buses by

$$\mathcal{M} = \{i | q_i = 0, i = 1, ..., N\}. \tag{25}$$

The optimization problem is formulated as

$$\min_{\mathcal{M}} \quad tr(\mathbf{R}_{\varepsilon_\theta}) \tag{26}$$

$$s.t. \quad |\mathcal{M}| = M \tag{27}$$

where $|\mathcal{M}|$ denotes the cardinality of the set $\mathcal{M}$. Plugging (18) in (26) and recalling that $tr(\mathbf{AB}) = tr(\mathbf{BA})$ for square matrices $\mathbf{A}$ and $\mathbf{B}$, we have

$$\begin{aligned}tr(\mathbf{R}_{\varepsilon_\theta}) &= tr(\mathbf{B}^{-1} + \mathbf{CQRQ}^T\mathbf{C}^T - \mathbf{D} - \mathbf{D}^T) \\ &= tr(\mathbf{B}^{-1}) + tr(\mathbf{JQRQ}^T) - 2tr(\mathbf{D})\end{aligned} \tag{28}$$

where

$$\mathbf{J} = \mathbf{C}^T\mathbf{C}. \tag{29}$$

Since the first term in (28) is independent of the variables to be optimized, the objective function in (26) can be rewritten as

$$\min_{\mathcal{M}} \quad tr(\mathbf{JQRQ}^T - 2\mathbf{D}) \tag{30}$$

To solve this optimization problem, one could try all solutions or a greedy algorithm can be employed.

The analysis provided so far is very general. It allows a non-diagonal covariance matrix $\mathbf{R}$ of the attack vector $\mathbf{a}$, as well as possible correlation between $\mathbf{a}$ and the state vector $\boldsymbol{\theta}$. It is worth noting that any correlation between different components of $\mathbf{a}$ implies communication between agents at spatially separated physical locations which may be very costly to implement. The attack vector $\mathbf{a}$ being correlated with $\boldsymbol{\theta}$ implies that the attackers must have information about the states, which also requires high complexity. It also requires significant communication between the agents that are attacking at different nodes. In the sequel, we focus on a more practical class of attacks of much lower complexity.

*Definition 1: Uncoordinated and state-uninformed attacks* employ attack vectors $\mathbf{a}$ with uncorrelated components which satisfy $\mathbb{E}\{\boldsymbol{\theta}\mathbf{a}^T\} = \mathbf{0}$.

*Assumption 4:* We assume uncoordinated and state-uninformed attacks.

*Theorem 1:* Consider an $N$-bus DC power system with $M$ protected nodes facing additive attacks. Suppose the MAP estimator (13) designed for (6) is employed, while the actual observations follow the model in (15). Under Assumptions 1-4, in order to minimize the trace of the MSE matrix (18), an optimum solution is to protect the $M$ nodes with the $M$ largest value of $R_{ii}J_{ii}$, $i = 1, ..., N$.

*Proof of Theorem 1:* Substituting (16) in (30), after manipulation, and considering that $\mathbf{D} = \mathbf{0}$ since $\mathbb{E}\{\boldsymbol{\theta}\mathbf{a}^T\} = \mathbf{0}$ as per Assumption 4, we obtain

$$tr(\mathbf{JQRQ}^T) = \sum_{i=1}^{N}\sum_{j=1}^{N} J_{ij}R_{ji}q_i q_j \tag{31}$$

where $A_{ij}$ denotes the $ij$th entry of matrix $\mathbf{A}$. Since $\mathbf{R}$ is diagonal according to Assumption 4, (31) can be reduced to

$$tr(\mathbf{JQRQ}^T) = \sum_{i=1}^{N} J_{ii}R_{ii}q_i^2. \tag{32}$$

Further, based on the definition of $q_i$, minimizing the objective function in (32) is equivalent to

$$\max_{\mathcal{M}} \quad \sum_{i\in\mathcal{M}} J_{ii}R_{ii}. \tag{33}$$

Let

$$x_i = J_{ii}R_{ii} \tag{34}$$

and sort the values of $x_i$, $i = 1, ..., N$ in descending order, such that

$$x_{d_1} > x_{d_2} > ... > x_{d_N} \tag{35}$$

where the $d_n$ denotes the bus index associated with the $n$th largest $x_i$, $i = 1, ..., N$. Obviously, the solution to the optimization problem is

$$\mathcal{M}_{opt} = \{d_1, d_2, ..., d_M\}, \tag{36}$$

meaning that the nodes with the $M$ largest $x_i$ should be protected first, which completes the proof. ■

## 5. NUMERICAL RESULTS

In this section, we present some numerical examples to illustrate the MSE of the state estimation obtained using the optimum node protection method stated in Theorem 1. Assume that $\mathbf{R}_\theta = \sigma_\theta^2\mathbf{I}$, $\mathbf{R}_v = \sigma_v^2\mathbf{I}$, and the attacks have mean zero and are uncoordinated and state-uninformed such that $\mathbf{R}$ is diagonal. For convenience we define $\rho = \sigma_\theta^2/\sigma_v^2$.

Consider the 9-bus system from [11]. Assume that we are able to protect $M = 3$ nodes and $R_{ii} = 0.0002$ for $i = 1, 2, ..., 9$. Fig. 1 shows the trace of the MSE matrix for the MAP estimate of $\boldsymbol{\theta}$ under attack with the several sets of nodes protected, called protection plans, for the 9-bus system. For comparison purposes, the cases with a suboptimal protection plan (black dash-dot curve), the protection plan proposed in Theorem 1 (green solid curve), the optimal protection plan from a global enumeration (purple square marks), all nodes protected (blue dashed curve), and no nodes protected (red dotted curve) are presented. The suboptimal protection plan chooses protected nodes {2,4,9}. The protection plan presented in Theorem 1 was found to coincide with the optimal plan found by enumeration. It can be seen that if there is no protection, the MSE under attack is above the case with the suboptimal protection plan under attack at high SNR. This indicates that in power systems under attack, if arbitrary nodes are protected, the MSE will generally be smaller than if no nodes are protected. Note that the MSE under attack with the proposed protection plan is below the case with the suboptimal protection plan which further supports the claims of optimality. Similar results were obtained using the IEEE 14-bus system [11].

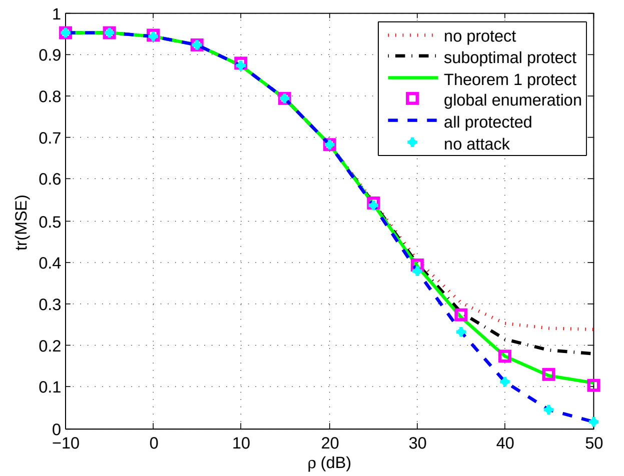


**Fig. 1**: The MSE for the MAP estimate of $\boldsymbol{\theta}$ for 9-bus system under various attacks. The number of protected nodes is 3. The covariance of attack is $R_{ii} = 0.0002$, $i = 1, 2, ..., 9$.

## 6. CONCLUSION

This paper studied the performance of MAP estimation for a power grid under a DC model which is attacked. The after attack MSE for MAP estimation was computed. Then by assuming there are $M$ protected nodes, we developed a method to select the protected nodes to attain the minimum possible MSE under attack for the MAP estimate. For uncoordinated and state uninformed attacks, it is shown that the optimal nodes to protect can be found by rank ordering the values of a set of coefficients in descending order. Numerical results for a 9-bus system and the IEEE 14-bus system demonstrated the optimal solution for a specific example.

## 7. REFERENCES

[1] Ali Abur and A. Gomez-Exposito, "Power System State Estimation: Theory and Implementation," New York:

Marcel Dekker, 2004.

[2] O. Kosut, Liyan Jia, R. J. Thomas and Lang Tong, "Malicious data attacks on the smart grid," *IEEE Trans. on Smart Grid*, vol. 2, no. 4, pp. 645-658, December 2011.

[3] E. Handschin F. C. Schweppe J. Kohlas and A Fiechter, "Bad data analysis for power system state estimation," *IEEE Trans. on Power Apparatus and Systems*, vol. PAS-94, no. 2, pp. 329-337, March 1975.

[4] Yao Liu, Peng Ning and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. on Information and System Security*, vol. 14, no. 1, article 13, May 2011.

[5] Yi Huang, M. Esmalifalak, Huy Nguyen, Rong Zheng, Zhu Han, Husheng Li and Lingyang Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, vol. 6, no. 2, pp. 10-15, January 2013.

[6] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. on Smart Grid*, vol. 2, no. 2, pp. 326-333, Jun 2011.

[7] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," *Proceedings of the 1st IEEE International Conference on Smart Grid Communications*, pp. 214-219, 2010.

[8] Suzhi Bi and Ying Jun Zhang, "Graphical Methods for Defense Against False-Data Injection Attacks on Power System State Estimation," *IEEE Trans. on Smart Grid*, vol. 5, no. 3, pp. 1216 - 1227, May 2014.

[9] O. Vukovic, Kin Cheong Sou, G. Dan, and H. Sandberg, "Network-layer protection schemes against stealth attacks on state estimators in power systems," *Proceedings of the IEEE International Conference on Smart Grid Communications*, pp. 184 - 189, 2011.

[10] Zhengrui Qin, Qun Li, and Mooi-Choo Chuah, "Defending against Unidentifiable Attacks in Electric Power Grids," *IEEE Trans. on Parallel and Distributed Systems*, vol. 22, no. 10, pp. 1961 - 1971, Oct 2013.

[11] R. D. Zimmerman and C. Murillo-Snchez, "MATPOWER User's Manual" [Online]. Available: http://www.pserc.cornell.edu/matpower/.