Ming Hsieh Department of Electrical Engineering

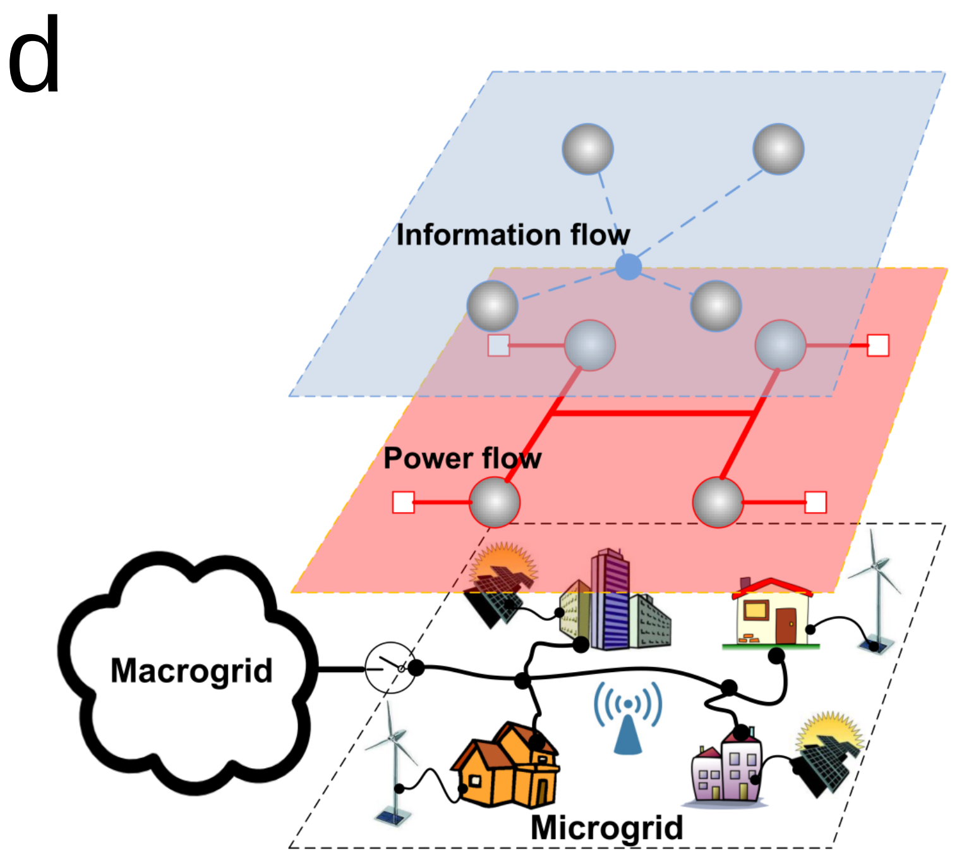
USC Viterbi School of Engineering

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

Hanie Sedghi and Edmond Jonckheere

Motivation and Introduction

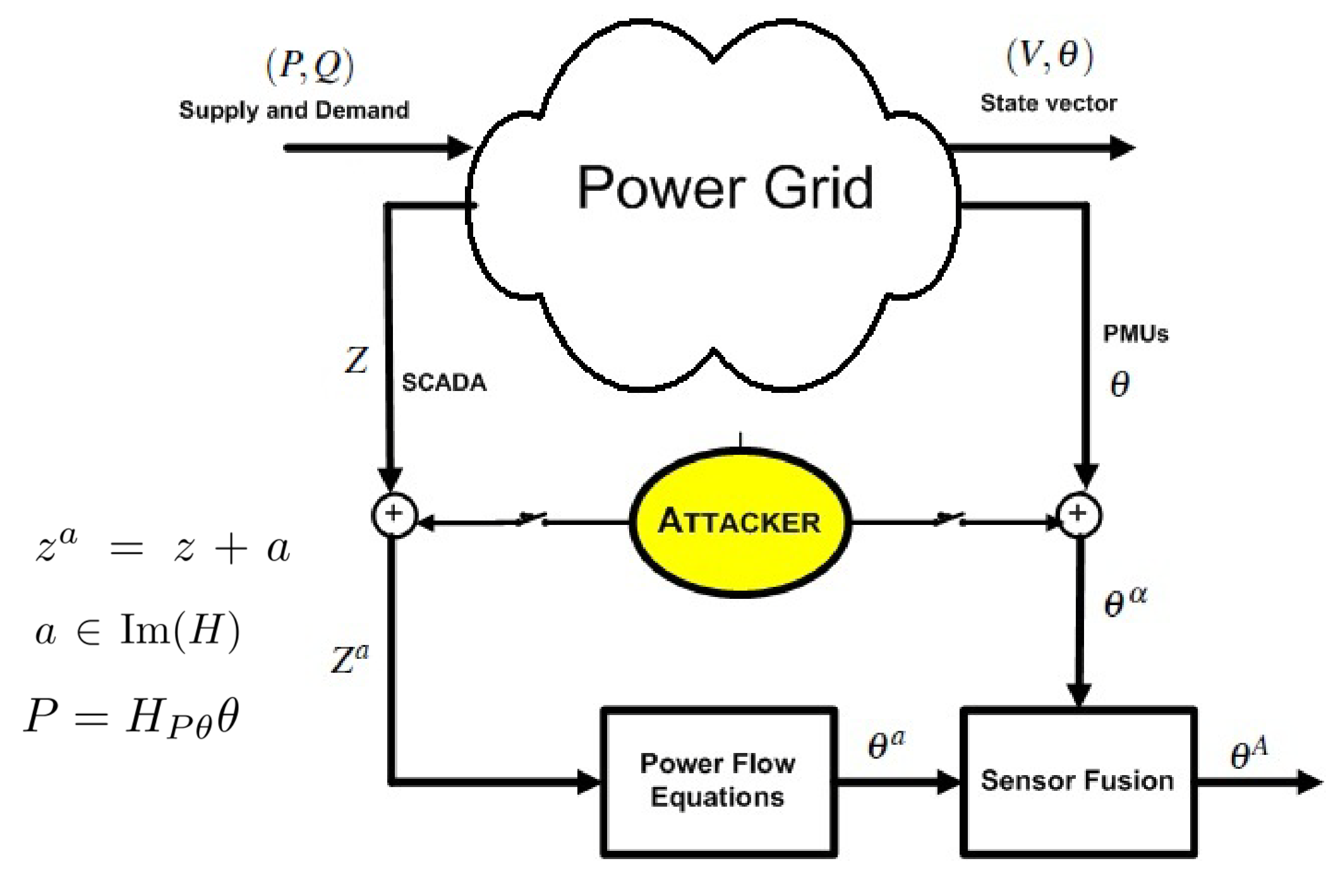
➢ Future grid vs. current grid



➢ Phasor Measurement Units (PMUs)

- Synchronous with GPS stamp
- Various applications
- Will be placed partially along with State Estimators

➢ False Data Injection



$$z^a = z + a$$
$$a \in \mathrm{Im}(H)$$
$$P = H_{P\theta}\theta$$

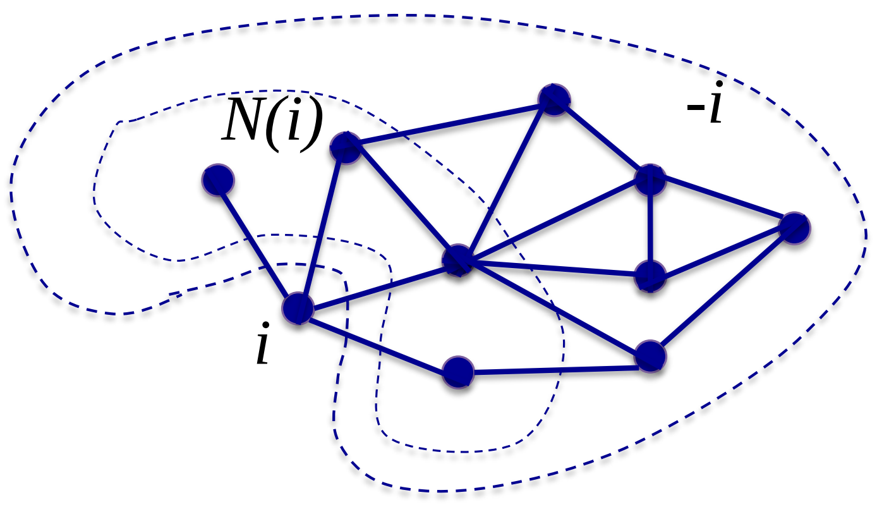
Problem Formulation

Gaussian Markov Random Field

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

$$J(i,j) = 0 \Longleftrightarrow (i,j) \notin E$$

$$E\left(X_i \mid X_{N(i)}\right) = E\left(X_i \mid X_{-i}\right)$$



DC power flow equations

$P_{ij} = b_{ij}(X_i - X_j)$ ⇒ $X_i = \sum_{j \neq i}\{\frac{b_{ij}}{\sum_{i \neq j} b_{ij}}\}X_j + \frac{1}{\sum_{j \neq i} b_{ij}}P_i$

Structure Learning

Conditional Covariance Test (Anandkumar et.al. 2012)

Estimates the structure of underlying graphical model given i.i.d. samples of the r.v.s

```
Algorithm 1 Algorithm CCT($\mathbf{x}^n; \xi_{n,p}, \eta$) for structure learning using samples $\mathbf{x}^n$.
    Initialize $\widehat{G}_p^n = (V, \emptyset)$.
    For each $i, j \in V$, if
        $\min_{S \subset V \setminus \{i,j\}, |S| \leq \eta} |\widehat{\Sigma}(i,j|S)| > \xi_{n,p}$,
    then add $(i,j)$ to $\widehat{G}_p^n$.
    Output: $\widehat{G}_p^n$.
```

Detection Scheme

➢ Decentralized scheme

➢ Online calculations

➢ Markov graph changes under attack

➢ Mismatch ⇒ alarm

$$z^a = z + a = H(X+d) = HX^a$$

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

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

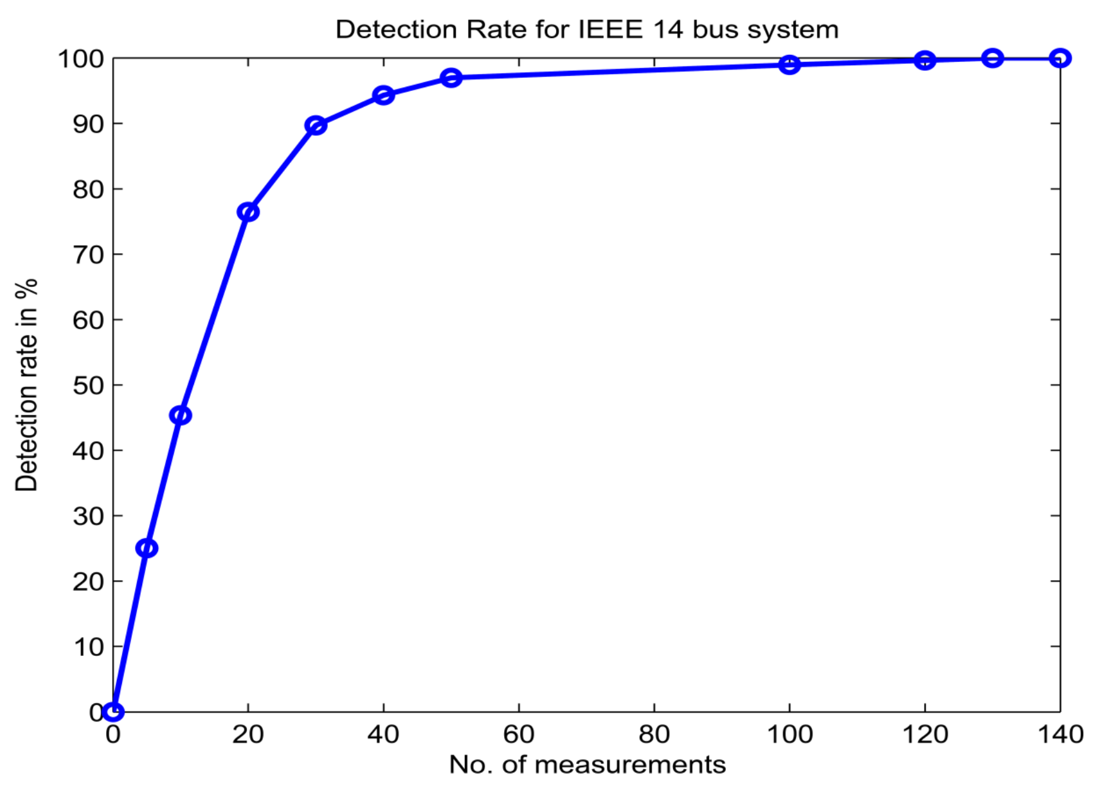
➢ All attack scenarios

➢ MATPOWER for running DC power flow

➢ IEEE 14-bus system & IEEE 30-bus system

➢ 100% detection rate, min corrupted samples = 130 for IEEE-14 and 50 for IEEE-30.

Reason: sparsity



Detection rate is 90% for just 30 corrupted samples

Considering current sampling rate these values are pretty good.

Discussion & Future Work

➢ The first detection scheme for this sophisticated attack

➢ Computational complexity $O(p^{\eta+2})$

➢ Sample complexity $\Omega(J_{min}^{-2} \log p)$

➢ Apply to bigger networks

➢ Readily detects other types of attack

➢ Causality approach with time series analysis

hsedghi@usc.edu

Ming Hsieh Institute

Ming Hsieh Department of Electrical Engineering