Local False Data Injection Attacks Against Power Grid

Xuan Liu
Ph.D. Student

Zuyi Li
Associate Professor

Galvin Center for Electricity Innovation
Illinois Institute of Technology

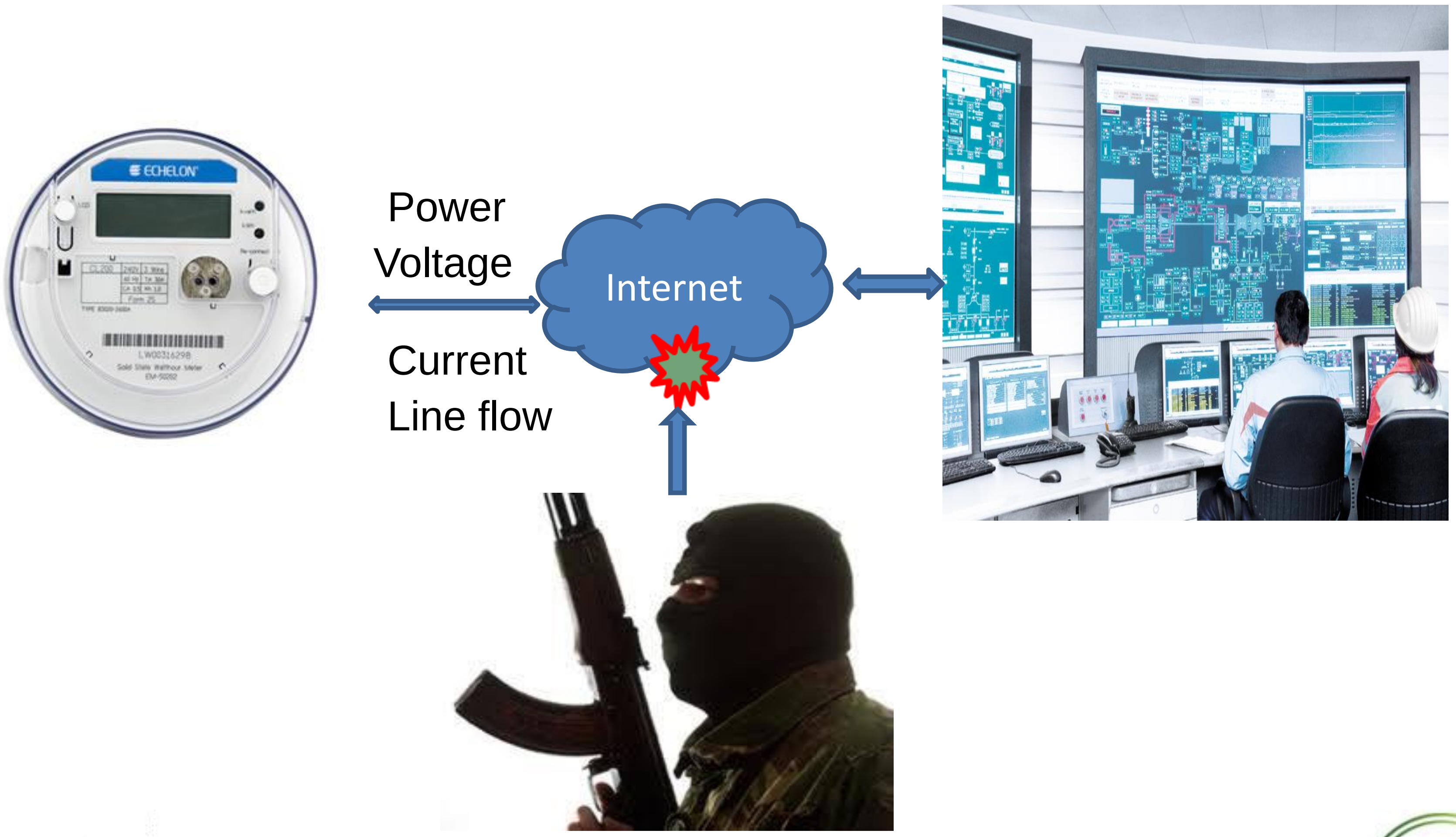
galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

Outline

- Background
- False Data Attacks
- Load Redistribution(LR) Attacks
- Local LR Attacks
- Feasibility Theorem
- Conclusion

Cyber Security Issue



State Estimation

$$\mathbf{z} = \mathbf{H}X + \mathbf{e}$$

$$\hat{\mathbf{x}}(\mathbf{z}) = (\mathbf{H}^T \mathbf{e}^{-1} \mathbf{H})^{-1} \mathbf{H}^T \mathbf{e}^{-1} \mathbf{z}$$

Z: Measurements

e: Measurement errors

H: Jacobian matrix

Bad Data Detection

- The residual r

$$\mathbf{r} = Z - H\hat{X}$$

- If

$$\|\mathbf{r}\| > \tau$$

Predetermined threshold

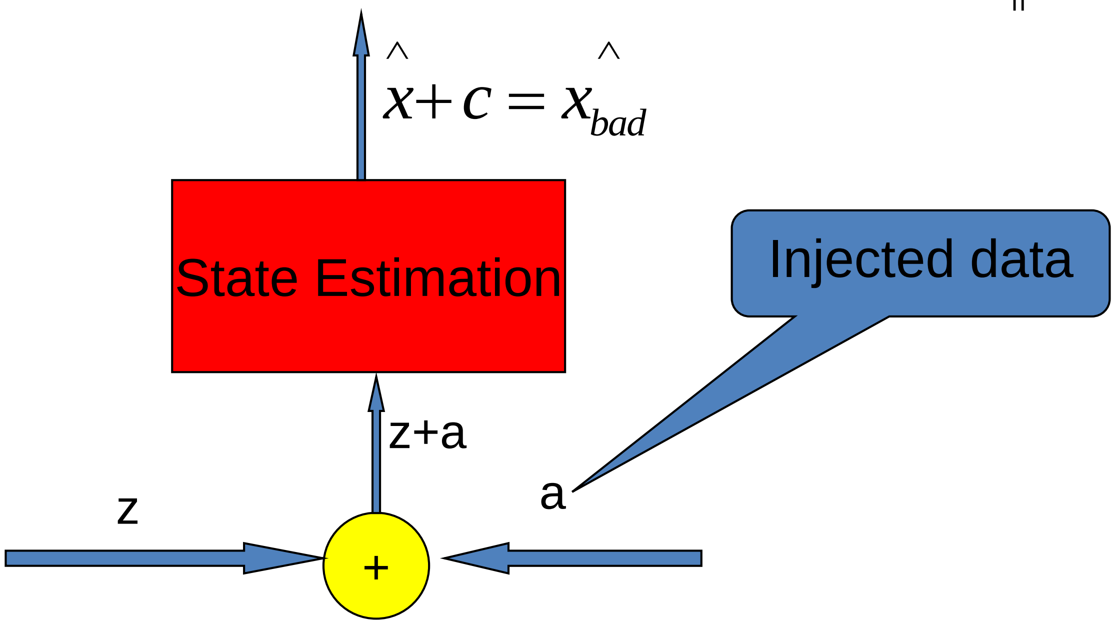
there is at least one faulty measurement.

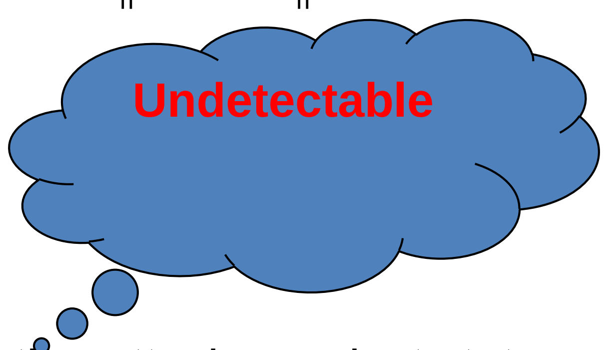
False Data Injection Attacks

$$a = Hc \Rightarrow \left\| z_a - H\hat{x}_{bad} \right\| = \left\| z + a - H(\hat{x} + c) \right\|$$

$$= \left\| z - H\hat{x} + (a - Hc) \right\|$$

$$= \left\| z - H\hat{x} \right\| \le \tau$$





Y. Liu, M. K. Reiter, and P. Ning,"False data injection attacks against state estimation in electric power grids," 2009.

Load Redistribution Attack

- Assumptions
  - Generator output measurements cannot be altered;
  - Bus injection measurements of zero-injection buses in the power grid cannot be altered;
  - Load measurements can be altered within certain ranges.

Problem Formulation for Load Redistribution Attack

Load redistribution attacking model is formulated as:

$$\sum_{d=1}^{ND} \Delta D_d = 0 \qquad (1)$$

$$-\tau D_d \le \Delta D_d \le \tau D_d \qquad (2)$$

S: shift factor matrix

$$\mathbf{\Delta F} = -\mathbf{S}.\mathbf{V}.\mathbf{\Delta D} \qquad (3)$$

V: Bus-load incidence matrix

Y. Yuan, Z. Li, and K. Ren, “Modeling load redistribution attacks in power systems,” *IEEE Transaction on Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

Issues for General False Data Injection Attack

$$a = Hc$$

To construct a, an attacker must know the topology and parameter information of the entire network;

It is impossible for an attacker to do so;

Does it mean that power systems are immune to false data injection attacks?

----------------No!!!!!!

galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

Local Load Redistribution Attack

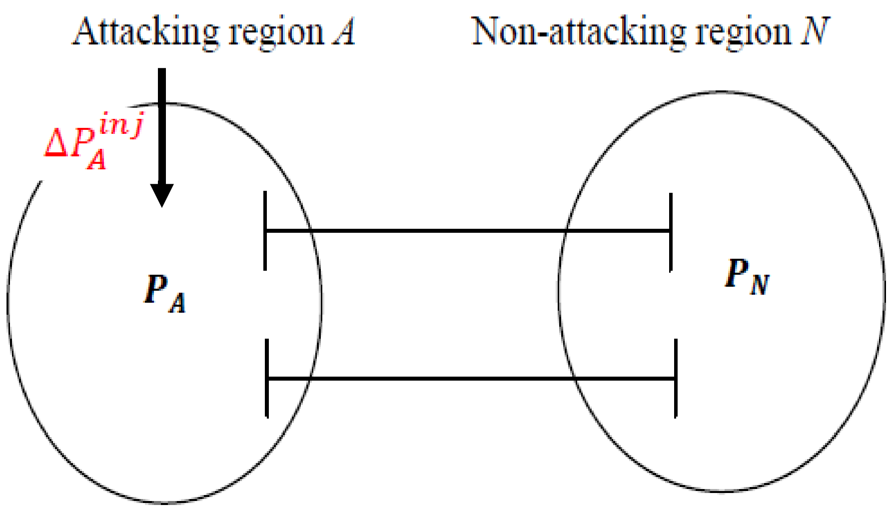


Fig. 1 Illustrative diagram for attacking region and non-attacking region

Theorem 1 indicates that $\Delta \mathbf{P}_{\mathbf{A}}^{\mathbf{inj}}$ can be constructed by an attacker who has only the information of the attacking region ($\boldsymbol{B}_{A'}$) and who does not have any information of the rest of the power grid.

Theorem 1: If an additional injected power into region A makes the phase angles of all its boundary buses increase or decrease the same

Then:

(1) All buses in region N have the same incremental phase angle

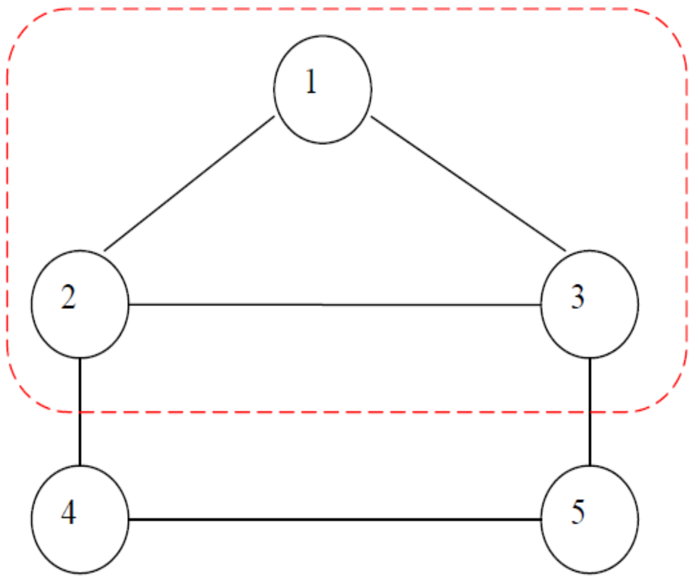
(2) The power flows in region N remain the same.

(3) The incremental bus power injection vector and the incremental phase angle vector in region A satisfy

$$\Delta \mathbf{P}_{\mathbf{A}}^{\mathbf{inj}} = \boldsymbol{B}_{A'} \Delta \boldsymbol{\theta}_{A}$$

$\boldsymbol{B}_{A'}$ is the bus susceptance matrix in region A excluding tie lines;

Example



- According to KCL, for the attacking region:

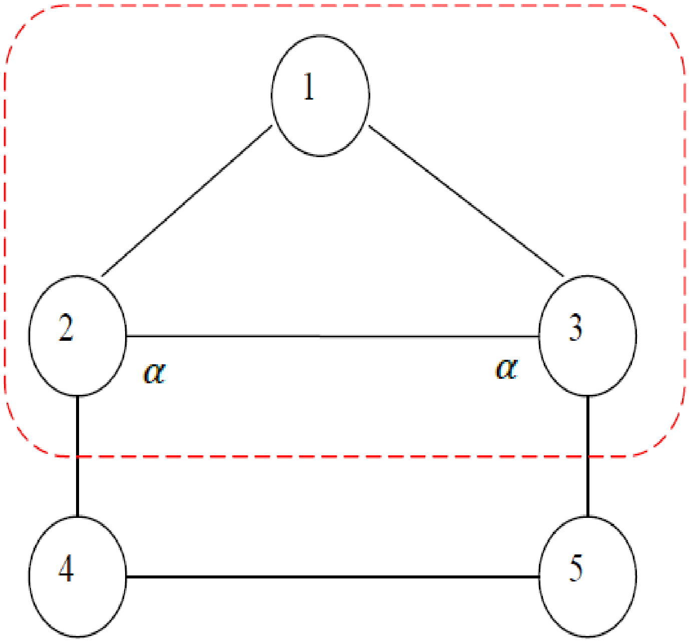
Line	Admittance
1-2	0.1
1-3	0.2
2-3	0.1
2-4	0.1
3-5	0.2
4-5	0.1

$$\Delta D_1 = -15\Delta\theta_1 + 10\Delta\theta_2 + 5\Delta\theta_3$$

$$\Delta D_2 = 10\Delta\theta_1 - 20\Delta\theta_2 + 10\Delta\theta_3$$

$$\Delta D_3 = 5\Delta\theta_1 + 10\Delta\theta_2 - 15\Delta\theta_3$$

Example



$$\Delta D_1 = -15\Delta\theta_1 + 10\Delta\theta_2 + 5\Delta\theta_3$$

$$\Delta D_2 = 10\Delta\theta_1 - 20\Delta\theta_2 + 10\Delta\theta_3$$

$$\Delta D_3 = 5\Delta\theta_1 + 10\Delta\theta_2 - 15\Delta\theta_3$$

Choose bus 1 as the reference bus, and set :

$$\Delta\theta_2 = \Delta\theta_3 = \alpha \qquad (3)$$

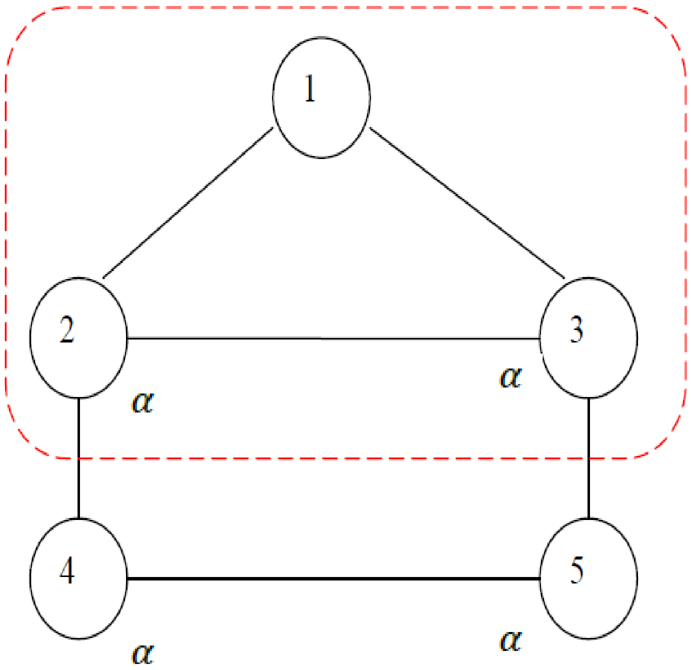
Substituting (3) into the KCL equations, we have the vector of false data injection of powers as follows:

$$\Delta D_1 = 15\alpha$$

$$\Delta D_2 = -10\alpha$$

$$\Delta D_3 = -5\alpha$$

Example



Since bus 4 and bus 5 is in the non-attacking region,

$$\Delta D_4 = 10\Delta\theta_2 - 20\Delta\theta_4 + 10\Delta\theta_5 = 0$$

$$\Delta D_5 = 5\Delta\theta_3 + 10\Delta\theta_4 - 15\Delta\theta_5 = 0$$

Substituting $\Delta\theta_2 = \Delta\theta_3 = \alpha$,

$$10\alpha - 20\Delta\theta_4 + 10\Delta\theta_5 = 0 \quad (4)$$

$$5\alpha + 10\Delta\theta_4 - 15\Delta\theta_5 = 0 \quad (5)$$

Solving (4) and (5), we have

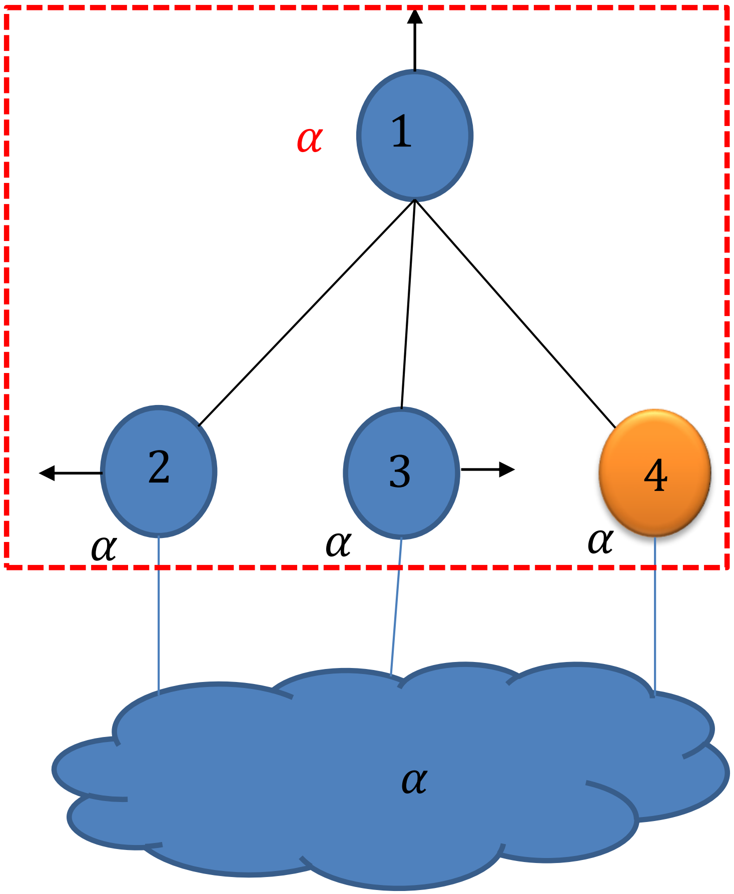
$$\Delta\theta_4 = \Delta\theta_5 = \alpha$$

Feasibility Theorem for Local Load Redistribution Attack

- How to guarantee the feasibility of the attacking vector?

- **Theorem 2**: Suppose the attacking region consists of ρ non-boundary buses. If there are at most $\rho - 1$ non-attackable buses, then a feasible attacking vector can be constructed.

Examples



There are $\rho = 1$ non-boundary buses, so

$$zm \leq \rho - 1 = 0$$

Assuming bus 4 is non-attackable, we can obtain

$$\Delta\theta_1 = \Delta\theta_2 = \Delta\theta_3 = \Delta\theta_4 = 0$$

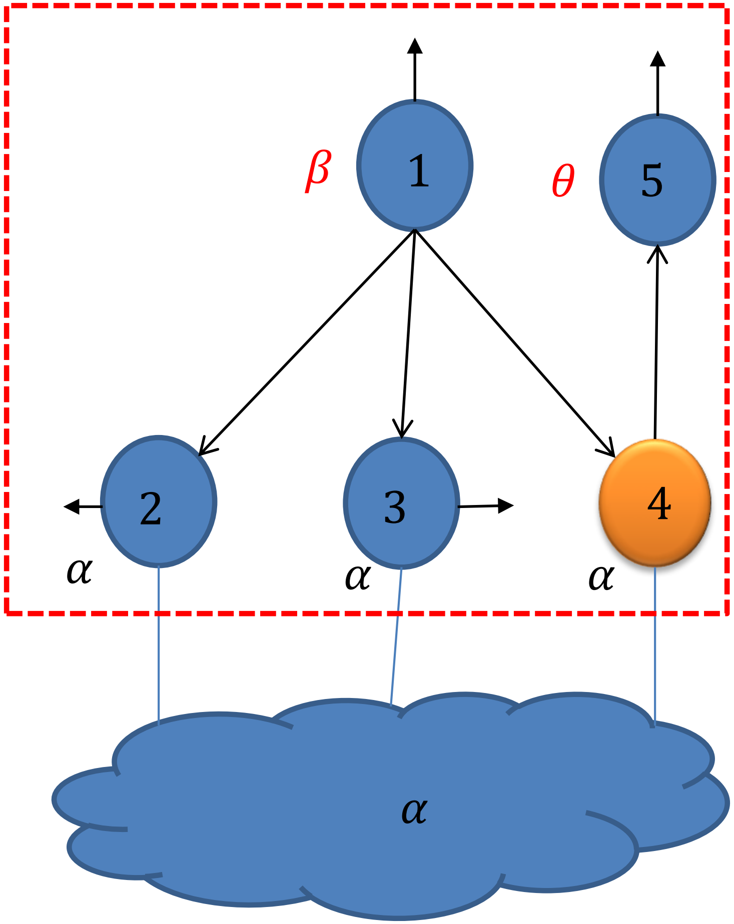
So,

$$\Delta D_1 = \Delta D_2 = \Delta D_3 = \Delta D_4 = 0$$

galvin center for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society

Examples



There are $\rho = 2$ non-boundary buses, so

$$zm \leq 2 - 1 = 1$$

The attacking vector is:

$$\Delta D_1 = 3(\alpha - \beta)$$

$$\Delta D_2 = \beta - \alpha$$

$$\Delta D_3 = \beta - \alpha$$

$$\Delta D_5 = \alpha - \theta$$

Conclusion

- An attacker can launch a successful false data attacks with local network information;
- Developing effective detecting methods becomes very important;
- Defending power grids against local false data attacks.

Thanks!