Load Redistribution Attacks and Protection Strategy in Electric Power Systems

Dr. Yanling Yuan

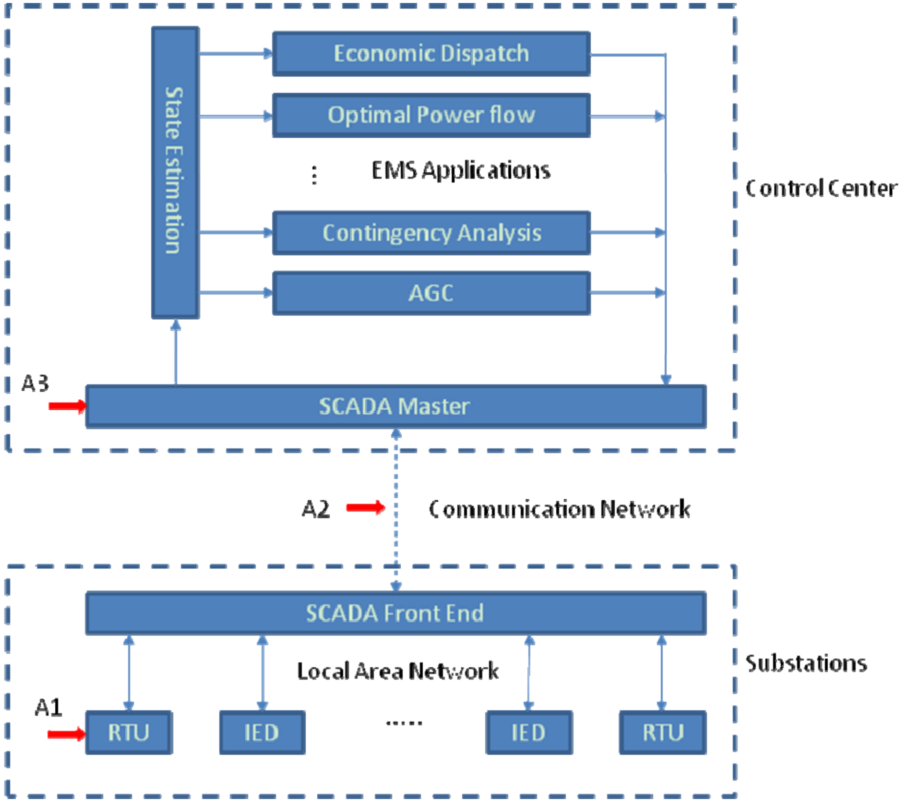
Illinois Institute of Technology

galvincenter for electricity innovation at ILLINOIS INSTITUTE OF TECHNOLOGY

IEEE PES Power & Energy Society®

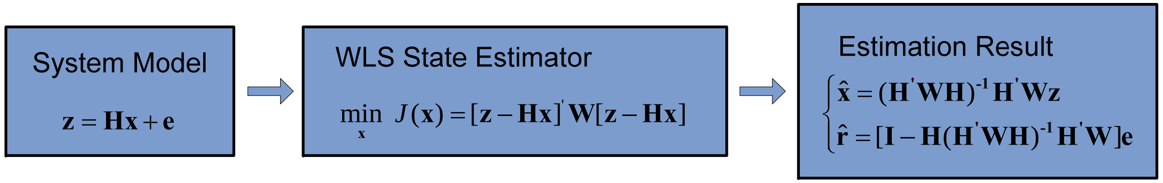
Cyber Security in Electric Power Systems

- With the development of Smart Grid, tighter integration of communication and information technologies makes Electric Power Systems more vulnerable to cyber-attacks by adversaries around the globe
  - It is reported that the United States electrical grid has been penetrated by cyber spies
- Cyber Attacks on EMS/SCADA Systems
  - Attacks on SCADA systems will directly affect state estimation and all EMS applications



False Data Injection Attack

- Definition
  - A type of cyber attacks against SE through SCADA
  - Cooperatively modifies selected measurements
  - Attack vector **a** is a linear combination of the column vectors of the Jacobian matrix **H**
- State estimation (Weighted lease square (WLS) estimator)



System Model

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

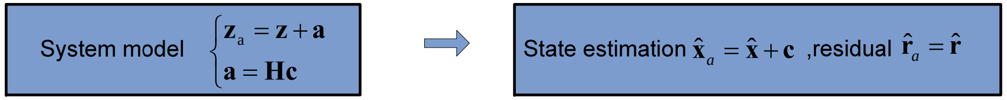
WLS State Estimator

$\min_{\mathbf{x}} \; J(\mathbf{x}) = [\mathbf{z} - \mathbf{H}\mathbf{x}]' \mathbf{W} [\mathbf{z} - \mathbf{H}\mathbf{x}]$

Estimation Result

$$\begin{cases} \hat{\mathbf{x}} = (\mathbf{H}'\mathbf{W}\mathbf{H})^{-1}\mathbf{H}'\mathbf{W}\mathbf{z} \\ \hat{\mathbf{r}} = [\mathbf{I} - \mathbf{H}(\mathbf{H}'\mathbf{W}\mathbf{H})^{-1}\mathbf{H}'\mathbf{W}]\mathbf{e} \end{cases}$$

- State estimation under false data injection attacks



System model $\begin{cases} \mathbf{z}_a = \mathbf{z} + \mathbf{a} \\ \mathbf{a} = \mathbf{H}\mathbf{c} \end{cases}$

State estimation $\hat{\mathbf{x}}_a = \hat{\mathbf{x}} + \mathbf{c}$,residual $\hat{\mathbf{r}}_a = \hat{\mathbf{r}}$

  - An error c is injected while the estimated measurement residual has not changed
- Characteristics
  - Can be easily constructed if attacker gains access to **H** matrix
  - May only need to modify a few measurements since **H** matrix is sparse
  - Manipulate state estimation result in an arbitrary and predicted way
  - Can bypass any of the existing bad data detection algorithm

Load Redistribution (LR) Attack

- More realistic false data injection attack with limited access to specific measurements
  - $\text{Unattackable Measurements} \begin{cases} \text{generator output measurements} \\ \text{power injection mesurements for zero-injection bus} \end{cases}$
  - $\text{attackable Measurements} \begin{cases} \text{load measurements} \\ \text{branch power flow measurements} \end{cases}$
- LR attack model
  - The sum of attack injection on all load measurements is zero

$$\sum_d \Delta D_d = 0$$

  - Attack on load measurements can not deviate too much from their true value

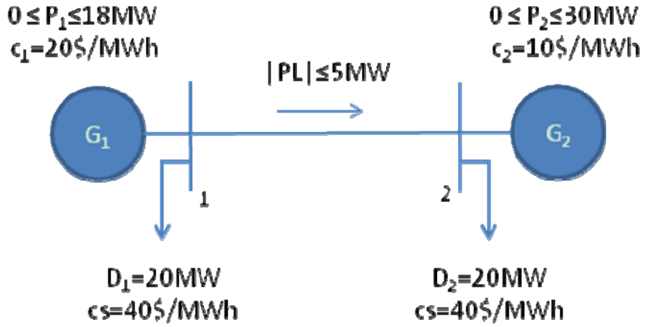
$$-\tau D_d \le \Delta D_d \le \tau D_d \qquad \forall\ d$$

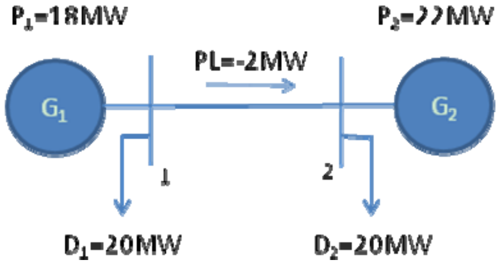
  - Power flow measurements has to be cooperatively modified. **SF** and **KD** are also system topology information, can be derived from **H**

$$\mathbf{\Delta PL} = -\mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D}$$

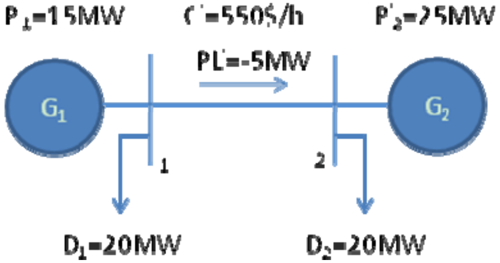
Physical Impact of LR Attacks

- 2-bus system





original system state



original SCED solutions

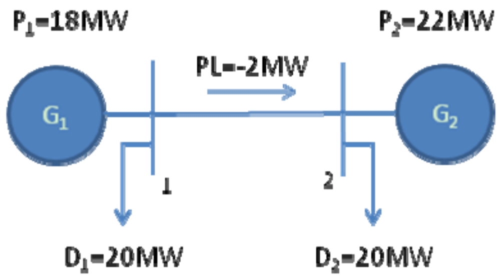
- LR attacks

$$\Delta PL = -[0 \quad -1]\cdot\begin{bmatrix}\Delta D_1\\ \Delta D_2\end{bmatrix}$$

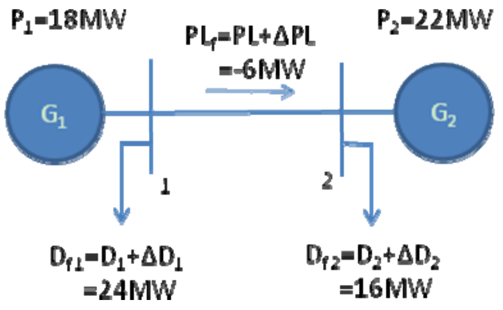
(bus 1 is the reference bus)

Physical Impact of LR Attacks (Cont'd)

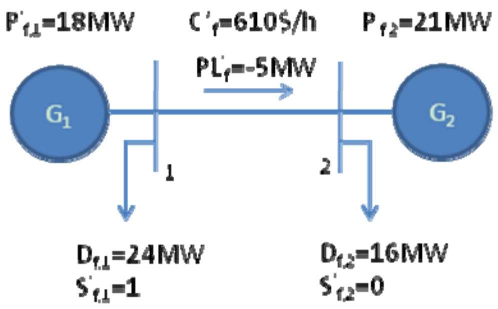
- Immediate attacking effect



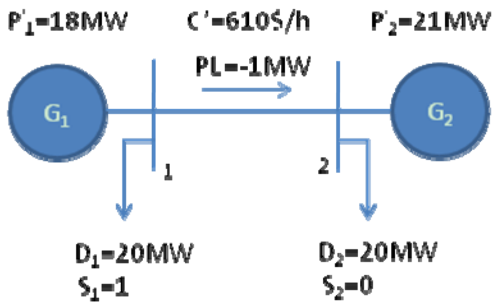
original system state



false system state under attack



false SCED solution

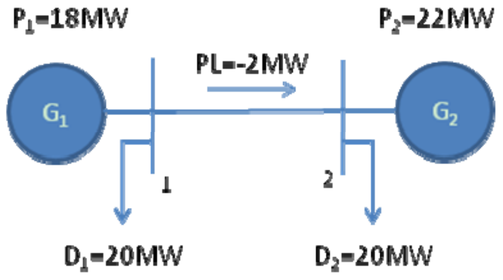


actual operating state after SCED

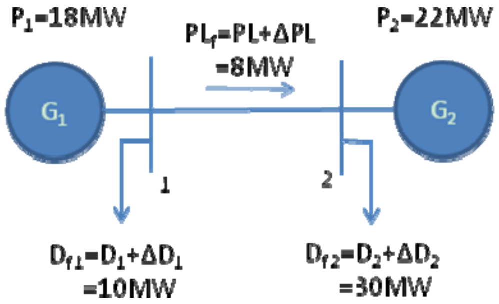
  - Non-optimal dispatch, load shedding

Physical Impact of LR Attacks (Cont'd)

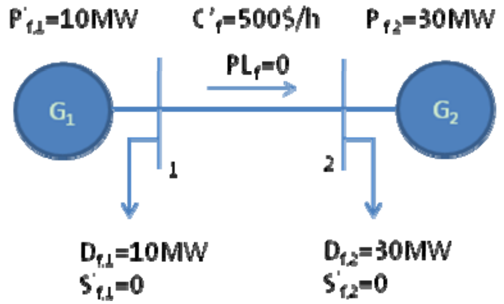
- Delayed attacking effect



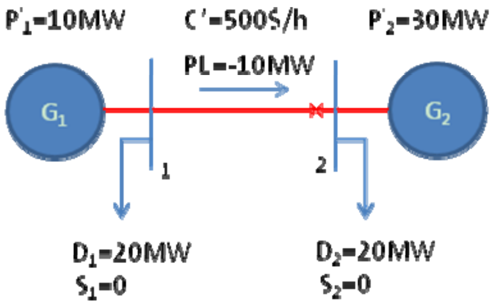
original system state



false system state under attack



false SCED solution

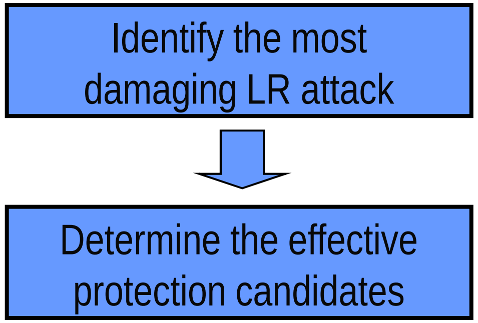


actual operating state after SCED

  - Insecure operating state

Proposed Protection Strategies

- Protection strategies in literatures
  - Perfect protection
  - Imerfect protection
- Proposed protection strategy
  - Deploy protection to mitigate the damage to power system operation.



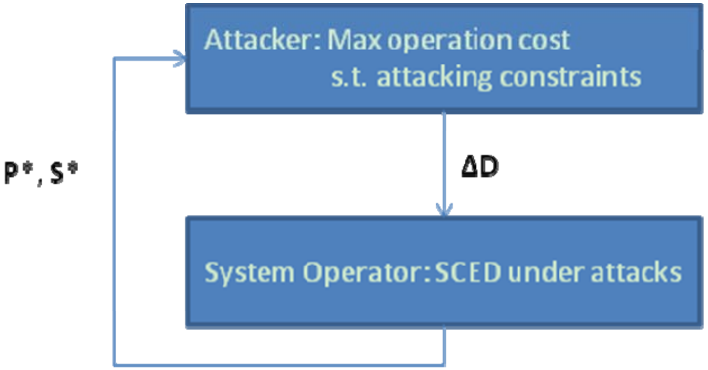
Identify the most damaging LR attack

Determine the effective protection candidates

  - By considering the most damaging effect, our proposed plans will be appropriately conservative and the protection resource can be used efficiently.

Modeling of Immediate LR Attacks

- Bi-level attacker-defender model, identify the most damaging immediate LR attack



Attacker: Max operation cost s.t. attacking constraints
ΔD
System Operator: SCED under attacks
P*, S*

$$\underset{\mathbf{\Delta D}}{Max}\ \sum_g c_g P_g^* + \sum_d cs_d S_d^*$$

$$\left.\begin{array}{ll}\text{s.t.}\ \sum_d \Delta D_d = 0 & \\ -\tau D_d \le \Delta D_d \le \tau D_d & \forall\ d \\ \mathbf{\Delta PL} = -\mathbf{SF}\cdot\mathbf{KD}\cdot\mathbf{\Delta D} & \end{array}\right\}\ \text{legitimate LR attack}$$

$$\left.\begin{array}{ll}\Delta D_d = 0 \Leftrightarrow \delta_{D,d} = 0 & \forall\ d \\ \Delta PL_l = 0 \Leftrightarrow \delta_{PL,l} = 0 & \forall\ l \\ \sum_d \delta_{D,d} + 2\sum_l \delta_{PL,l} \le R & \forall\ l \end{array}\right\}\ \text{attack resouce limitation}$$

$$\left\{\mathbf{P}^*,\ \mathbf{S}^*\right\} = \arg\left\{\underset{\mathbf{P,S}}{Min}\ \sum_g c_g P_g + \sum_d cs_d S_d\right\}$$

$$\begin{array}{ll}\text{s.t.}\ \sum_g P_g = \sum_d (D_d - S_d) & \forall\ d \\ \mathbf{PL} = \mathbf{SF}\cdot\mathbf{KP}\cdot\mathbf{P} - \mathbf{SF}\cdot\mathbf{KD}\cdot(\mathbf{D}+\mathbf{\Delta D}\text{-}\mathbf{S}) & \\ -PL_l^{\max} \le PL_l \le PL_l^{\max} & \forall\ l \\ P_g^{\min} \le P_g \le P_g^{\max} & \forall\ g \\ 0 \le S_d \le D_d + \Delta D_d & \forall\ d \end{array}$$

- Assumptions
  - DC power flow model
  - Only base case considered
  - System fully measured
- Solving Methodology
  - KKT-based method
  - Restart Benders Decomposition

Effective Protection Candidates Criterion

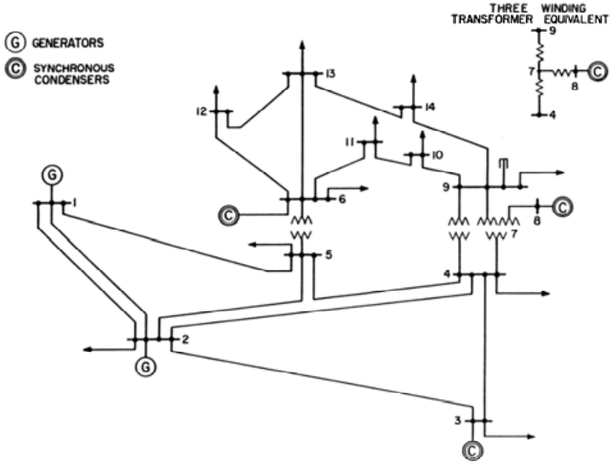
- Assume the stochastic error in the original measurements conform to normal distribution.

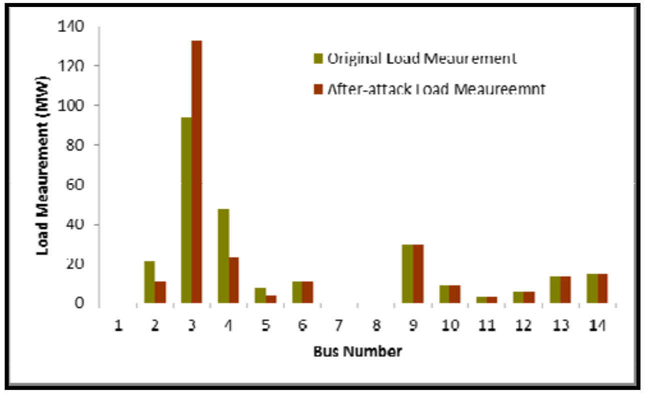
- For a specific attack ***a***, suppose measurement *p* is protected. Study the weighted sum of squared measurement residuals of the incomplete attack, J_{ap} , if $J_{a,p}^{lower} \geq \chi_{K,1-\alpha}^{2}$ with large probability, then measurement *p* is an effective protection candidate. Its effectiveness is insensitive to the measurement error in the original measurements.

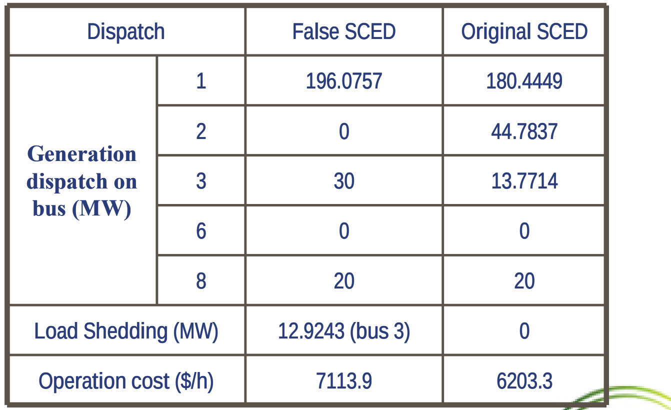
- If an effective candidate p is protected, the incomplete attack can be detected and bad data can be identified by Combinatorial Optimization Identification (COI) method.

Case Study

- IEEE 14 bus system
  - Fully measured
  - Modified system parameters (Transmission capacity: line 1 160MW, line 2-20 60MW)
- The most damaging immediate LR attack
- Damaging effect
  - Higher operation cost
  - Load shedding



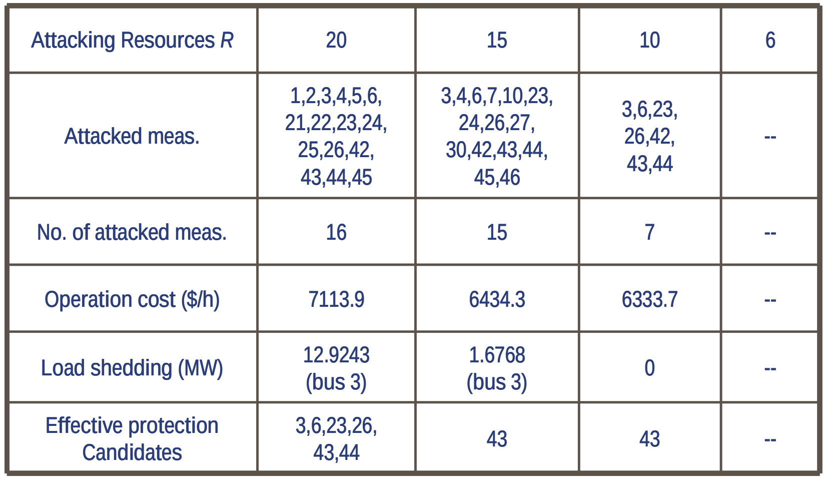




Dispatch		False SCED	Original SCED
Generation dispatch on bus (MW)	1	196.0757	180.4449
	2	0	44.7837
	3	30	13.7714
	6	0	0
	8	20	20
Load Shedding (MW)		12.9243 (bus 3)	0
Operation cost ($/h)		7113.9	6203.3

Case Study (Cont’d)

- The most damaging immediate LR attack under different attacking resources

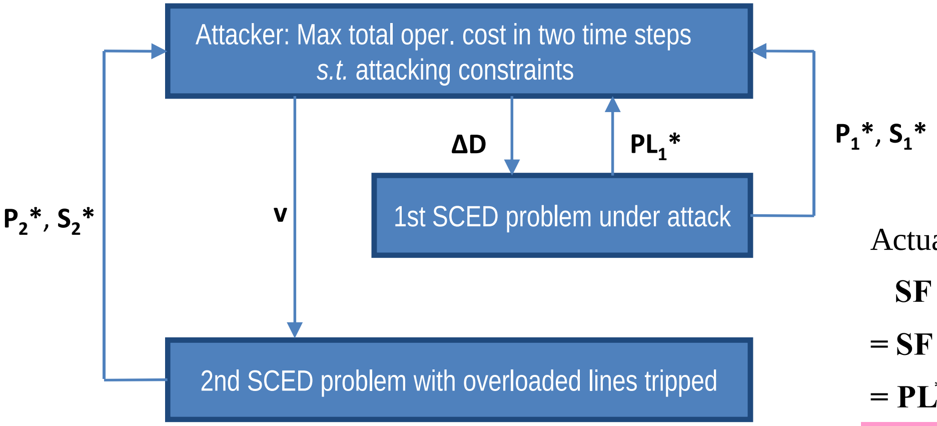


Attacking Resources *R*	20	15	10	6
Attacked meas.	1,2,3,4,5,6, 21,22,23,24, 25,26,42, 43,44,45	3,4,6,7,10,23, 24,26,27, 30,42,43,44, 45,46	3,6,23, 26,42, 43,44	--
No. of attacked meas.	16	15	7	--
Operation cost ($/h)	7113.9	6434.3	6333.7	--
Load shedding (MW)	12.9243 (bus 3)	1.6768 (bus 3)	0	--
Effective protection Candidates	3,6,23,26, 43,44	43	43	--

- Measurement 43 is always an effective protection candidate for a wide range of attacking resources
- After protecting measurement 43, the most damaging immediate LR attack under attacking resource R=20 leads to operation cost 6352.5$/h.

Modeling of Delayed LR Attacks

- Tri-level model, identify the most damaging delayed LR attack



Attacker: Max total oper. cost in two time steps *s.t.* attacking constraints

1st SCED problem under attack

2nd SCED problem with overloaded lines tripped

$$\underset{\Delta \mathbf{D}}{Max} \sum_g c_g (P_{1,g}^* + P_{2,g}^*) + \sum_d cs_d (S_{1,d}^* + S_{2,d}^*)$$

s.t. legitimate LR attack constraints

attack resource limitation

$$\text{-}PL_l^{\max} \le PL_{1,l}^* - \Delta PL_l \le PL_l^{\max} \Leftrightarrow v_l = 1$$

$$\left\{\mathbf{P}_1^*, \mathbf{S}_1^*, \mathbf{PL}_1^*\right\} = \arg\left\{ \underset{\mathbf{P}_1,\mathbf{S}_1}{Min} \sum_g c_g P_{1,g} + \sum_d cs_d S_{1,d} \right\}$$

s.t. 1st SCED constraints under attack

Actual power flow after false 1st SCED:

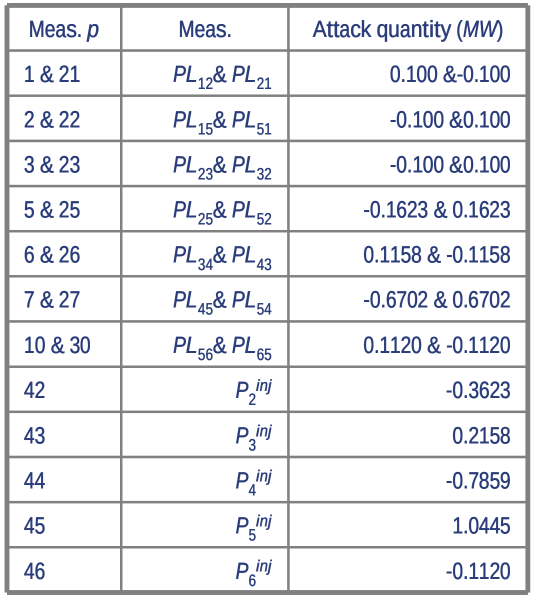
$$\begin{aligned} &\mathbf{SF} \cdot \mathbf{KP} \cdot \mathbf{P}_1^* \text{-} \mathbf{SF} \cdot \mathbf{KD} \cdot (\mathbf{D} \text{-} \mathbf{S}_1^*) \\ &= \mathbf{SF} \cdot \mathbf{KP} \cdot \mathbf{P}_1^* \text{-} \mathbf{SF} \cdot \mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D} \text{-} \mathbf{S}_1^*) + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} \\ &= \mathbf{PL}_1^* + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} = \mathbf{PL}_1^* \text{-} \Delta\mathbf{PL} \end{aligned}$$

$$\left\{\mathbf{P}_2^*, \mathbf{S}_2^*\right\} = \arg\left\{ \underset{\mathbf{P}_2,\mathbf{S}_2}{Min} \sum_g c_g P_{2,g} + \sum_d cs_d S_{2,d} \right\}$$

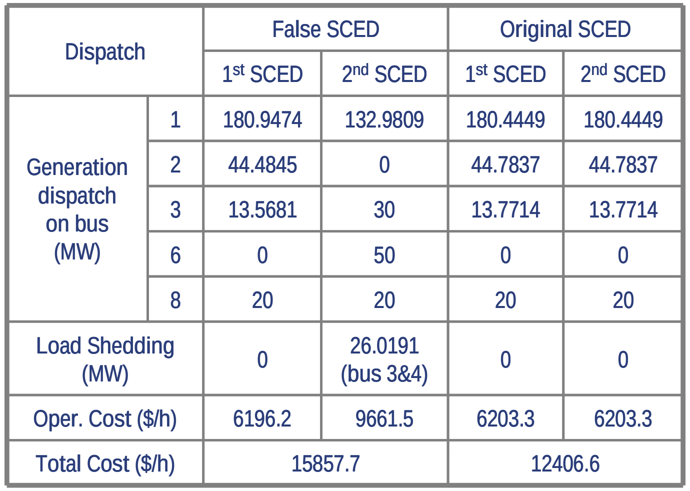
$$\begin{aligned} \text{s.t.}\quad & B_{MVA}{}^{-1} \cdot PL_{2,l} = x_l{}^{-1} \cdot v_l \cdot (\theta_l^{FR} \text{-} \theta_l^{TO}) && \forall\ l \\ & -\mathbf{KL} \cdot \mathbf{PL}_2 + \mathbf{KP} \cdot \mathbf{P}_2 + \mathbf{KD} \cdot \mathbf{S}_2 = \mathbf{KD} \cdot \mathbf{D} && \\ & -PL_l^{\max} \le PL_{2,l} \le PL_l^{\max} && \forall\ l \\ & P_g^{\min} \le P_{2,g} \le P_g^{\max} && \forall\ g \\ & 0 \le S_{2,d} \le D_d && \forall\ d \\ & -\theta_b^{\max} \le \theta_b \le \theta_b^{\max} && \forall\ b \end{aligned}$$

Case Study

- IEEE 14 bus system with modified system parameters
- The most damaging delayed LR attack
  - Attack quantities are very small
  - Line 1-5 and line 2-3 operate at their full capacities in the original SCED, an attack with small injection quantities may cause their overloading. After their trip, the 2nd SCED leads to a much higher operation cost with load shedding



Meas. *p*	Meas.	Attack quantity (*MW*)
1 & 21	PL_{12}& PL_{21}	0.100 &-0.100
2 & 22	PL_{15}& PL_{51}	-0.100 &0.100
3 & 23	PL_{23}& PL_{32}	-0.100 &0.100
5 & 25	PL_{25}& PL_{52}	-0.1623 & 0.1623
6 & 26	PL_{34}& PL_{43}	0.1158 & -0.1158
7 & 27	PL_{45}& PL_{54}	-0.6702 & 0.6702
10 & 30	PL_{56}& PL_{65}	0.1120 & -0.1120
42	P_2^{inj}	-0.3623
43	P_3^{inj}	0.2158
44	P_4^{inj}	-0.7859
45	P_5^{inj}	1.0445
46	P_6^{inj}	-0.1120



Dispatch		False SCED		Original SCED	
		1st SCED	2nd SCED	1st SCED	2nd SCED
Generation dispatch on bus (MW)	1	180.9474	132.9809	180.4449	180.4449
	2	44.4845	0	44.7837	44.7837
	3	13.5681	30	13.7714	13.7714
	6	0	50	0	0
	8	20	20	20	20
Load Shedding (MW)		0	26.0191 (bus 3&4)	0	0
Oper. Cost ($/h)		6196.2	9661.5	6203.3	6203.3
Total Cost ($/h)		15857.7		12406.6	

Summary

- Immediate LR attacks
  - The most damaging immediate LR attack redistribute load in order that some lines are heavily loaded and load shedding is necessary to bring their power flow back into secure range.
  - The most damaging immediate LR attacks under a wide range of attack resources have the same load redistribution trend.
- Delayed LR attacks
  - Delayed LR attacks is equivalent to physical interdiction of transmission lines.
  - For some systems, there are lines operating at or close to their capacity limit. Such systems are fairly vulnerable to delayed LR attacks, small attack injections can have delayed attacking effect.
- Since the introduction of deregulation, increased levels of consumption, lack of investment on transmission system upgrade are driving the operation of power systems to their static and dynamic limits. Power systems are increasing vulnerable to LR attacks.

Thanks