THE UNIVERSITY OF RHODE ISLAND

Smart Grid Security: An Integrative Approach for Power System Attack Analysis based on Grid Topology and Power Flow Analysis

Jun Yan, Haibo He, Yan Sun, Department of Electrical, Computer and Biomedical Engineering

Problem Statement

- **Power grids are vulnerable to cyber-attacks**
  - Smart grid brings cyber security challenges for power systems;

  Failure cascading is complicated
  - Attack on a small set of components may trigger a fallout of failure;
- **Traditional Topological Model**
  - Power transmission is ***NOT*** shortest paths problem
- **Call for a comprehensive model**
  - Integration of topology and real physical characteristics of the power grids

New System Model

- Topology of Complex Network
  - Topological analysis is robust and well-developed;
- Power Flow Model
  - Represent the physical characteristics of a power system (i.e. DC model and AC model) based on power flow analysis;
- Cascading Model
  - Failure of initial victim nodes/links will cause fatal overloading in the system and leads to cascading effect.

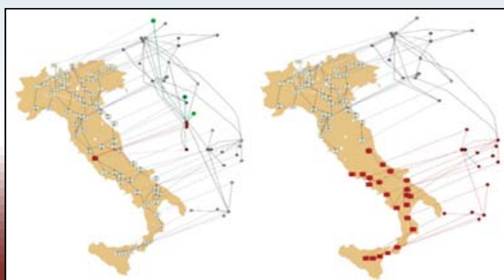

Fig. 2 Cascading failures of the power grid and internet communication network, September 28, 2003, Italy.
(Picture source: S. V. Buldyrev, et al, "Catastrophic cascade of failures in interdependent networks," Nature, 464: 1025 -- 1028, 2010.)

An Extended Power flow Analysis

- Power Transfer Distribution Factor
  - Sensitivity of power transmission;
- Load of Power
  - The total power flow into a node/through a branch;
- Failure Cascading
  - Disconnected components will cause overloading and leads to a disastrous failure propagation;
  - How system tolerance affects the percentage of failure and loss of power.

Assessment of Attack Strategies

- Impact of bus failure: more disastrous, more costly;
- Impact of branch failure: less effective, still works;
- Aims at:
  - Locate the most vulnerable components;
  - Present the most effective attack strategy.

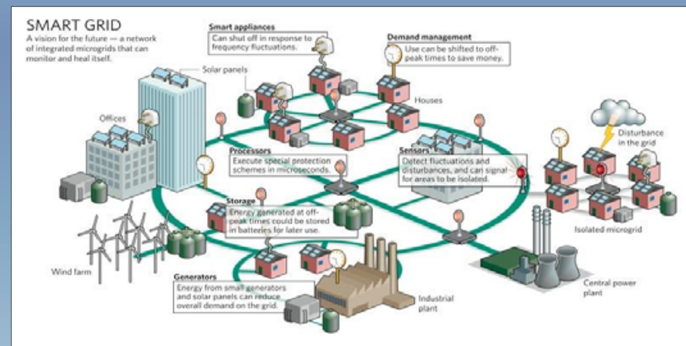

Fig. 1 A vision of smart grid
Figure source: http://energyinformative.org/smart-grid-overview-benefits-problems/

Modeling and Simulation: IEEE 118-bus system

Table 1 Most effective *1* node attack

Tolerance	ID	Pct. of Failure	Tolerance	ID	Power Loss
1.0	30	78.0%	1.0	30	99.8%
1.2	70	40.7%	1.2	65	93.7%
1.4	38	20.3%	1.4	65	89.5%
1.6	65	13.6%	1.6	65	85.1%
1.8	38	14.4%	1.8	38	73.1%

Table 2 Most effective *1* branch attack

Tolerance	ID	Pct. of Failure	Tolerance	ID	Power Loss
1.0	147	74.6%	1.0	112	99.6%
1.2	120	31.4%	1.2	120	92.3%
1.4	110	9.3%	1.4	140	53.9%
1.6	100	12.7%	1.6	100	30.0%
1.8	110	8.5%	1.8	156	24.3%

Table 3. *2 nodes / branches* attacked

Tolerance	Pct. of Node Failure	Power Loss	Pct. of Link Failure	Power Loss
1.0	77.1%	99.8%	77.1%	99.8%
1.2	47.5%	96.4%	33.9%	95.3%
1.4	34.7%	94.2%	10.2%	58.0%
1.6	29.7%	93.9%	14.4%	30.5%
1.8	24.6%	91.0%	9.3%	25.5%

Table 4. *3 nodes / branches* attacked

Tolerance	Pct. Of Node Failure	Power Loss	Pct. of Link Failure	Power Loss
1.0	77.1%	99.8%	77.1%	99.7%
1.2	47.5%	96.4%	26.3%	90.3%
1.4	34.7%	94.2%	17.8%	78.3%
1.6	29.7%	93.9%	15.3%	33.3%
1.8	24.6%	91.0%	9.3%	25.9%

Conclusions

- The extended model approximates the power grids well and the impacts are easy to be analyzed;
- A set of potential attack victims that maximize the impact could be identified;
- Defensive approaches could thus be developed.

Impact

- A comprehensive model to present cascading failure in power systems;
- Identify vulnerability of power grid components under various attack types and intensity;
- Decision support for system enhancement and defensive strategies against malicious attacks in smart grid.

THINK BIG WE DO

Research sponsored by the National Science Foundation