Analyzing Cascading Failures in Smart Grids under Random and Targeted Attacks

Sushmita Ruj[1] and Arindam Pal[2]

[1]Indian Statistical Institute, Kolkata, India
Email: sush@isical.ac.in
[2]TCS Innovation Labs, Kolkata, India
Email: arindamp@gmail.com

May 14, 2014
AINA 2014
University of Victoria

Today's Agenda

- Smart grids and interdependent networks
- Random and targeted attacks
- Cascading failures in interdependent networks
- Fault-tolerance of networks and giant components
- Our contributions
- Analysis of targeted attack on the communication network
- Experimental results
- Conclusion and future work

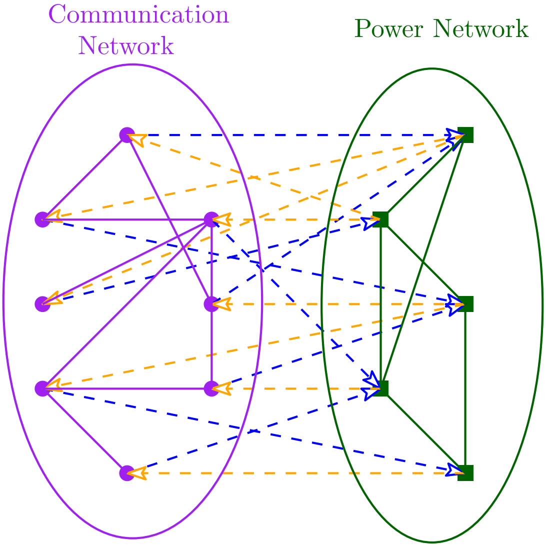
Our Contribution

- We model smart grids as complex interdependent networks.
- We study targeted attacks in smart grids for the first time.
- A node is compromised with probability proportional to its degree.
- We study attacks on different types of interdependent networks having binomial and power law degree distributions.
- We show that current power grid networks (having power law distribution) are more vulnerable to targeted attacks compared to random attacks.

Smart grids and interdependent networks

- Smart grids are next generation electricity grids in which the power network and the communication network work in symphony.
- An interdependent network is a combination of two networks, where in addition to the intralinks within the networks, there are interlinks across the networks.
- The two networks depend on each other for seamless operation.

The smart grid as an interdependent complex network



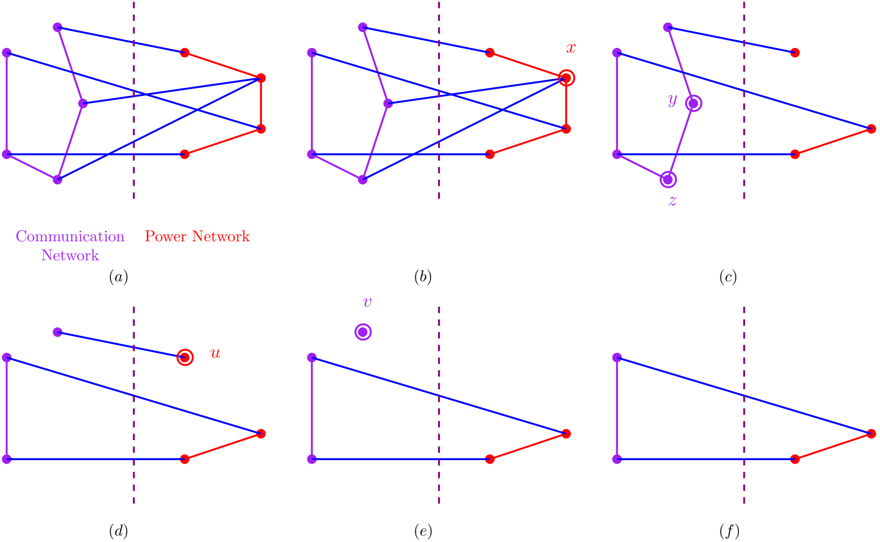
Network model

- Consider two interdependent scale-free networks.
- One is a communication network $N_A = (V_A, \alpha_A)$, and the other is a power network $N_B = (V_B, \alpha_B)$.
- N_A has the power law degree distribution $P_A(k) \propto k^{-\alpha_A}$, which means that the fraction of nodes with degree k is $P_A(k)$.
- Similarly, N_B has the power law distribution $P_B(k) \propto k^{-\alpha_B}$.
- We assume that there are more communication nodes than power stations, which implies that $n_A > n_B$.

Network model . . .

- The interlinks or support links are directed edges from one network to the other.
- We assume that a communication link supports one power station and is powered by one power node.
- This implies that both the in-degree and out-degree of a communication node is one.
- A power node is controlled by multiple communication node and supplies power to multiple communication nodes.
- This implies that both the in-degree and the out-degree of a power node is at least one.

Cascading Failure in Smart Grids



(a) (b) (c) (d) (e) (f)

Attack model

- We consider two types of attacks.
- In targeted attacks, the attacker selects a node with probability proportional to the degree of the node and makes it faulty.
- This implies that a high degree node is more prone to attack than a low degree node.
- Targeted attacks are more likely to arise in real-world situations, as we have seen during the recent Stuxnet attack.
- Intuitively, attacking the high degree nodes result in more nodes and links being disrupted, thus disrupting the network.
- In random attacks, the attacker selects a node uniformly at random from the set of all nodes.
- Here all nodes are equally likely to be attacked.

Giant Component

- A giant component in a graph on n vertices is a maximal connected component with at least cn vertices, for some constant c.
- If $c = 0.5$, this means that the giant component should have at least half of the vertices in the graph.
- A vertex can be deleted from the graph in two ways.
  - If the vertex is attacked.
  - If the vertex is not attacked, but all its support links on the other network has been attacked.
- Due to this kind of cascading failure of nodes, many more nodes will be compromised.
- This is different from the normal scenario, where only the attacked nodes are compromised.
- In this paper we analyze the sizes of giant components under random and targeted attacks.

Finding the sizes of Giant components in Smart Grids

- Let ϕ_k be the probability that a node i of degree k in communication node is not removed.

$$\begin{aligned}\phi_k &= 1 - \frac{deg(i)}{\sum_{v \in V_A} deg(v)} \\ &= 1 - \frac{Ak^{-\alpha_A}}{2m_A},\end{aligned}$$

- Fraction of nodes in the initial giant component as μ_{A_1}. (calculated in paper)
- Fraction of nodes in N_B disconnected due to attack on N_A is given by,

$$r_{B_2} = \sum_{\tilde{k}_B=0}^{\infty} \tilde{P}_B(\tilde{k}_B)(1-\mu_{A_1})^{\tilde{k}_B} \tag{1}$$

- Fraction of nodes in the giant component of Network N_B is μ_{B_2}.

Finding the sizes of Giant components in Smart Grids

- Continuing similarly, The fraction of nodes in N_A which fail due to failure of node in N_B is given by,

$$r_{A_3} = \sum_{\tilde{k}_A=0}^{\infty} \tilde{P}_A(\tilde{k}_A)(1 - \mu_{B_2}). \tag{2}$$

- Fraction of nodes in the giant component of Network N_A is μ_{A_3}.
- At steady state,

$$\mu_{A_{2n-1}} = \mu_{A_{2n+1}} = \mu_{A_{2n+3}} = \dots \tag{3}$$

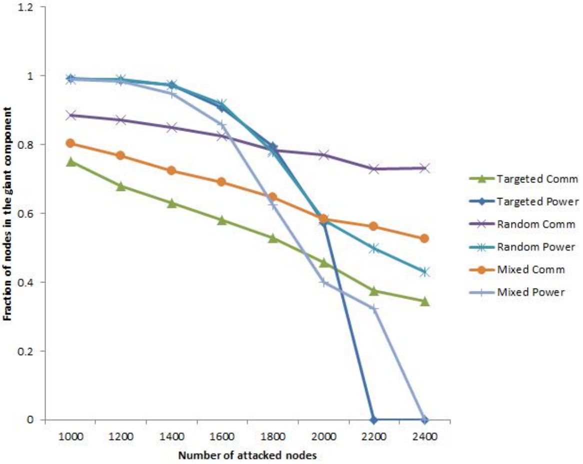
$$\mu_{B_{2n-2}} = \mu_{B_{2n}} = \mu_{B_{2n+2}} = \dots \tag{4}$$

Experimental methodology

- We use the software library *igraph* to simulate smart grids.
- The communication and power networks are generated using an Erdos-Renyi model and a Barabasi-Albert model.
- For each communication node, an interlink is assigned by choosing a power node at random.
- We consider three types of attack on the communication network – targeted, random and a combination of the first two.
- We study the effect of compromise by running the experiment 50 times for each input.
- Every time the same graphs are considered.

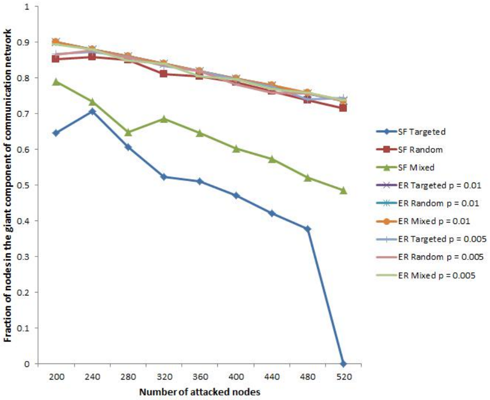
Fraction of nodes in giant component for different attacks

- The power and the communication network has 1,000 and 10,000 nodes respectively. The communication/power network is generated using the Barabasi-Albert model.



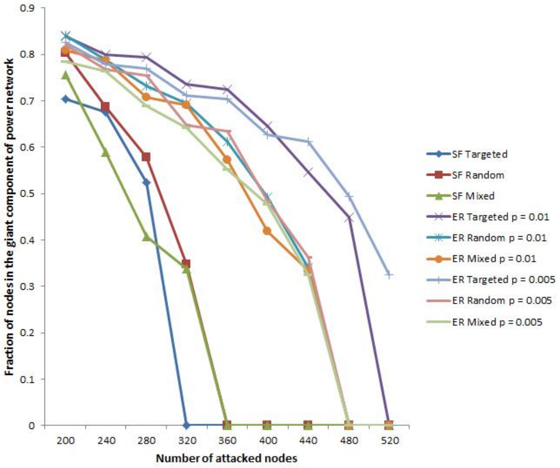
Fraction of nodes in giant component of communication network

- The power and the communication network has 1,000 and 2,000 nodes respectively. The communication/power network is generated using Erdos-Renyi and Barabasi-Albert model.



Fraction of nodes in giant component of power network

- The power and the communication network has 1,000 and 2,000 nodes respectively. The communication/power network is generated using Erdos-Renyi and Barabasi-Albert model.



Conclusion and future work

- In this work, we model the power and communication networks as two interdependent networks, and analyze cascading failure in smart grids for targeted attacks.
- We have carried out experiments to show that a targeted attack gives an advantage to the adversary over random attacks.
- A challenging open problem is to obtain a closed-form solution for the size of the giant component from the mathematical analysis that we have presented.
- Another important question is to present a good model of smart grids, which will be resilient to both random and targeted attacks.
- The structure of both the power and communication networks and the assignment of interlinks need to be studied.

Thank You!