Threat From Being Social: Vulnerability Analysis of Social Network Coupled Smart Grid

CS 585
Tiffany Seale

Agenda:

- Why social network coupled smart grids?
- What is the Misinformation Attack Problem in Social-smart Grid (MAPSS)?
- Models behind power grids, information diffusion in the social network, and the integrated social/power network
- Attack/protection strategies for these networks
- Look at data gathered from experiment

Why SN-coupled smart grids?

- **Smart grid**: power grid based on information technology and real-time data processing which allows for the implementation of strategies to control and optimize an electric network.
- Want to look at the impact of social networks on the the smart grid when they are linked together.
- How can they be linked together?
    - The efficiency of a smart grid is dependant on the customers having access to demand response programs and being actively engaged in energy management.
- Social network for smart grid (SSG) could make the smart grid smarter by including the customers and their real time peer-to-peer data sharing.

Why SN-coupled smart grids?

TABLE 1. **Impact of social network.**

Literature	Impact of SSG
[7]	Smooth load curve for households, hence no extra costly power plant capacity will be required.
[8]	6% reduction in peak load, aggressive incentives reached a 14% reduction in peak load.
[10]	Consumers reduced their annual energy usage by an average of 2.8% when given comparison information with other peoples energy consumption.
[11]	Energy savings of 7-9% by mutual sharing through social network.

- There is a large opportunity for saving money and using less power just by using smart grids. Small programs have fared well in the past but consistently failed when scaled up.
- Table 1 (below) shows the known advantages to integrating customer interaction and continuous real time engagement.
- Current social network integrations:
    - GreenPacket: sharing experiences and contest participation
    - OPower: Facebook based community approach to sharing energy saving tips
    - Ensemble: customer interaction through incentives and competitions
    - "People want to do what others like them are doing"
- Within these utility based social networks, users can share or forward messages: general information, **load-shifting tips, evenergy-reduction tip**

What is the Misinformation Attack Problem in Social-smart Grid (MAPSS)?

- Finding the most critical nodes in the coupled social network, such that when those nodes believe in the misinformation on a smart grid, they may spread the misinformation to a large portion of nodes in the social network and in turn results in severe failure in the smart grid.
- The identification of these critical nodes can guide the application of precautions to failures
- BUT, this is complicated because instead of only considering the information diffusion and power network dynamics, one must also consider their interdependencies.

Models behind power grids, information diffusion in the social network, and the integrated social/power network

TABLE 2. Summary of notations for Section III.

Variable	Meaning
G_S	$G_S = (V_S, E_S, w)$, the social network
G_P	$G_P = (V_P, E_P)$, Power grid network with nodes and transmission lines.
P	Set of power generation nodes.
D	Set of demand nodes.
p_i	Power generation output of node i.
d_i	Load demand of node i.
f_{ij}	Power flow in transmission line (i, j).
u_{ij}	Capacity of transmission line (i, j).

Models behind information diffusion in the social network

$$G_S = (V_S, E_S, p)$$

-
- Information propagation: In order to model the information propagation in a social network, this paper focuses on the Independent Cascading model: initially no nodes adopt the misinformation.
  - Given a seed set S, the misinformation diffusion proceeds in rounds:
  - 0: all nodes in S are influenced by misinformation. No others are influences.
  - Next rounds: All of the nodes from the previous round try to influence those around them.
- I(S) is the expected number of influenced nodes with S as the seed set taken over the probability of information propagation

Models behind power grids

- Linearized DC power flow model:

$$G_P = (V_P, E_P),$$

$$\sum_{(i,j)\in\delta_i^+} f_{ij} - \sum_{(j,i)\in\delta_i^-} f_{ji} = \begin{cases} p_i & i \in P \\ -d_i & i \in D \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

1. Cascading Failure Model
2. Line Failure

Models behind power grids: Cascading Failure Model

Algorithm 1 Cascade Failure Model

Input: Connected Power grid Network $G(V, E)$

Output: S_1: Lines which failed, S_2: Nodes which failed

```
while Network is not stable do
    Adjust the total supply to the total demand within
    each island.
    Use equations (1)-(4) to calculate power flows in G.
    For all lines, compute the moving average
    f̃_ij^t = α f_ij + (1 − α) f̃_ij^{t−1}.
    Remove all lines that have moving average flows
    greater than the capacity (f̃_ij^t > u_ij) and add to S_1.
    Add the failed nodes to S_2.
    If no more line fails, then network is stable, break
    the loop.
```

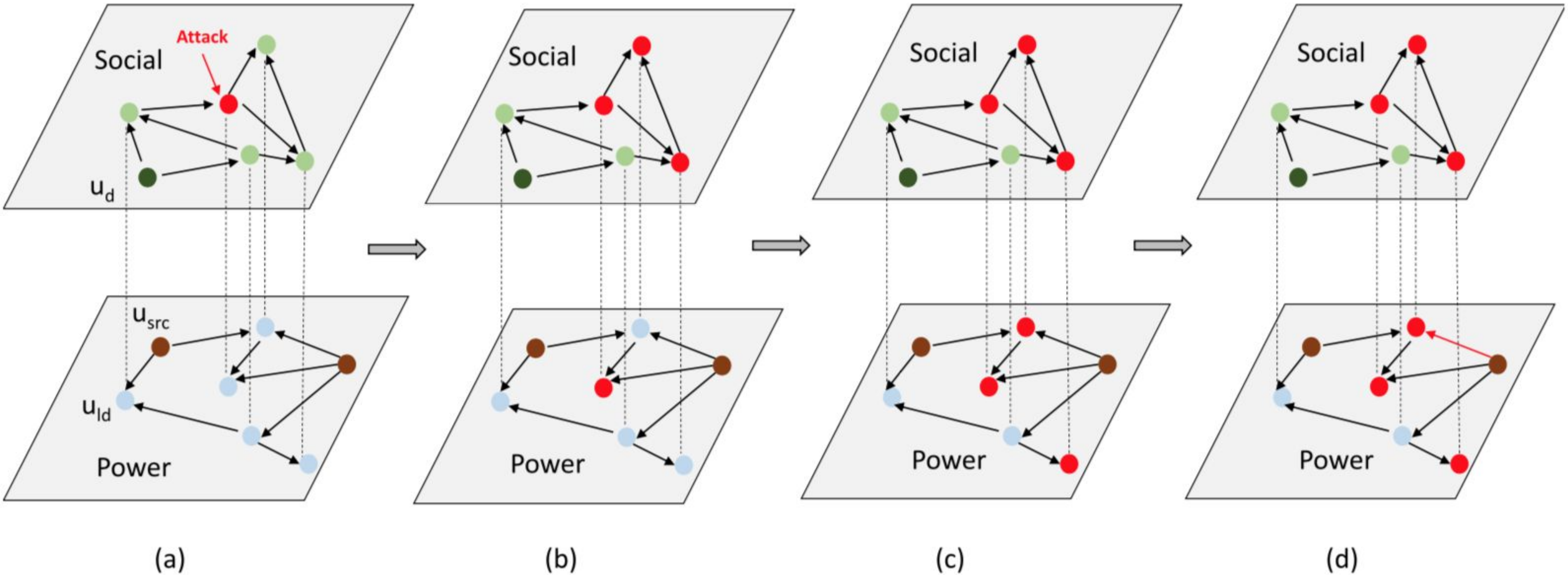
$$\theta_i - \theta_j - \pi_{ij} f_{ij} = 0, \quad \forall (i,j) \in E_P \tag{2}$$

$$p_i^{min} \leq p_i \leq p_i^{max}, \quad \forall i \in P \tag{3}$$

$$0 \leq d_j \leq d_j^{nom}, \quad \forall j \in D \tag{4}$$

Models behind the integrated social/power network

Definition 1 (MAPSS): Given the social network $G_S = (V_S, E_S, p)$*, power network* $G_P = (V_P, E_P)$ *and edge set* E_{PS}*, identify k nodes in* G_S*, whose activation would lead to maximum number of failed/disconnected nodes in* G_P *based on misinformation attack.*



Social
Attack
u_d
u_{src}
u_{ld}
Power
(a)
(b)
(c)
(d)

AI: Attacks Strategies

-Greedy Social Attack (GSA)

- Social Power Attack (SPA)

1. SPA-Concurrent
2. SPA-Sequential

Attack Strategies: Greedy Social Attack

Algorithm 2 Greedy Social Attack (GSA)

Input: $G_S(V_S, E_S)$, $V_S^p \subseteq V_S$,k
Output: S, $F(G_P)$

1 Initialize $S = \emptyset$
2 Calculate S, $|S| \leq k$ based on the algorithm BCT [26] with uniform cost and V_S^p as the target set. Set benefit for all $v \in V_S^p$ as 1 and benefit for all other nodes as 0.
3 **Return** S

Attack Strategies: Social Power Attack - Cascading Impact calculator

Algorithm 3 Cascading Impact Calculator (CIC)

Input: $G_S(V_S, E_S)$, $G_P(V_P, E_P)$, S

Output: CI

for $i \in V_P$ **do**

    Calculate $ci_i.pload$ ▷ Nodes to attack in G_P to fail i

    Calculate $ci_i.nodes$ by Alg 1 ▷ Damage when $ci_i.pload$ nodes are attacked.

    $A_S = ci_i.pload \rightarrow V_S$ ▷ Project power to social

    while $|A_S| < |I_{A_S}(S')|$ **do**

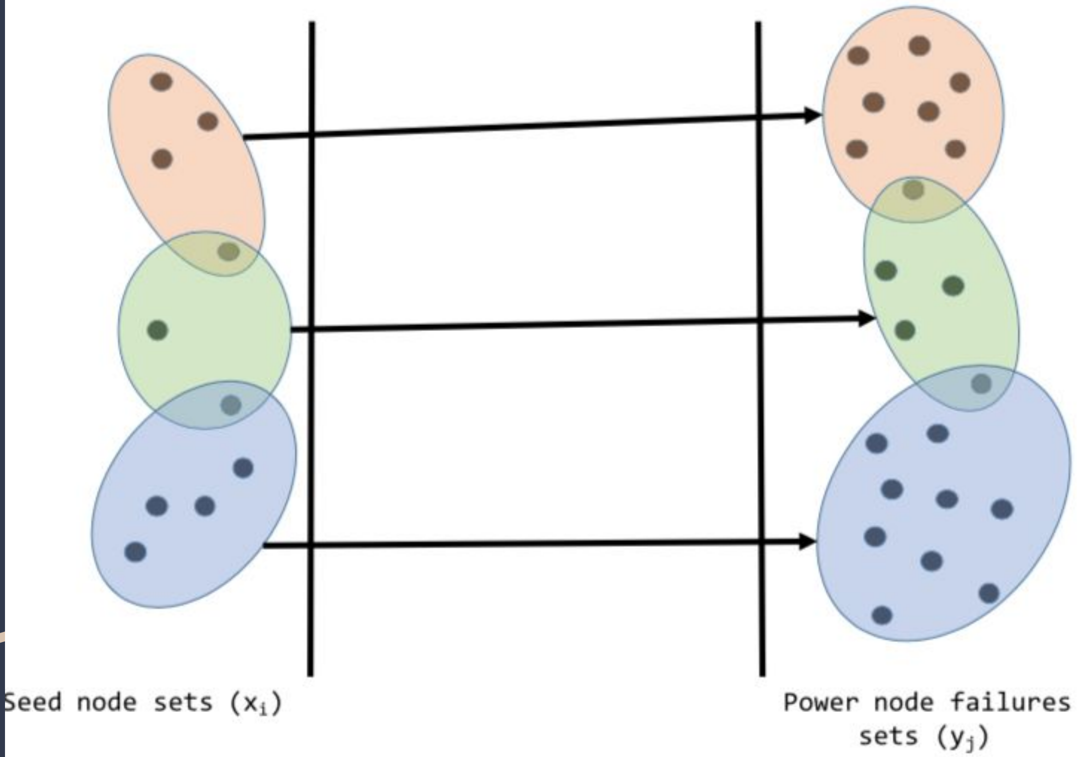
        select $u_S = argmax_{v_S \in V_S \setminus S'}(I_{A_S}(S' \cup v_S) - I_{A_S}(S'))$

        $S' = S' \cup \{u_S\}$

    $ci_i.seeds = S' - S$

Return CI

Attack Strategies: Social Power Attack - SPA-Current



Attack Strategies: Social Power Attack - SPA-Sequential

Algorithm 4 Social Power Attack Sequential (SPA-S)

Input: $G_S(V_S, E_S)$, $G_P(V_P, E_P)$, k

Output: S

$k' = 0, S = \emptyset$

while $k' < k$ **do**

  $CI = CIC(G'_P, G_S, S)$

  Sort CI based on $ci.nodes$

  foreach $ci_i \in CI$ **do**

    if $\#ci_i.seed < k - k'$ **then**

      $S = S \cup ci_i.seed$

      $k' = |S|$

      $G'_P = G'_P - ci_i.nodes$ ▷ Remove failed nodes

      break

Return S

Protection Strategies: Controlled Load Shedding

- Load curtailment (large industrial customers have agreement with utility companies, so that they can be instructed to reduce demand in order to balance the system)
- load shedding in case load curtailment does not stabilize the system

Testing

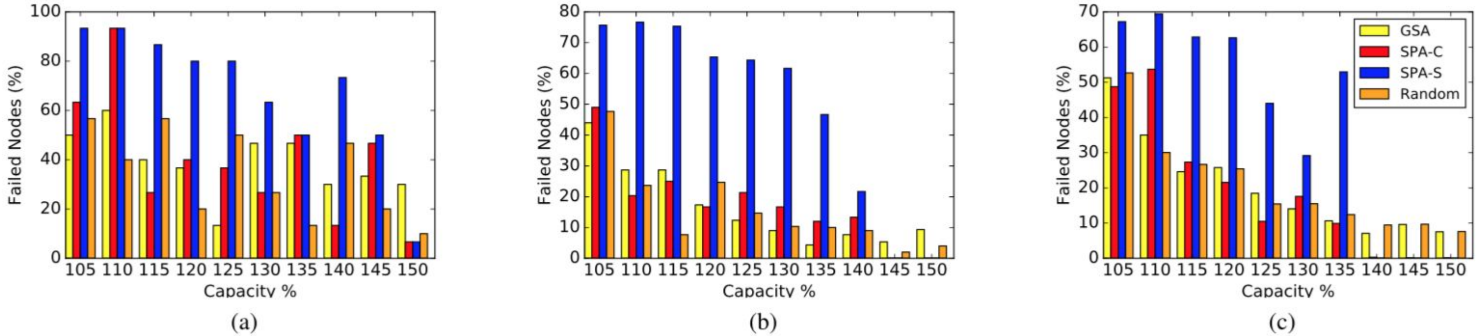
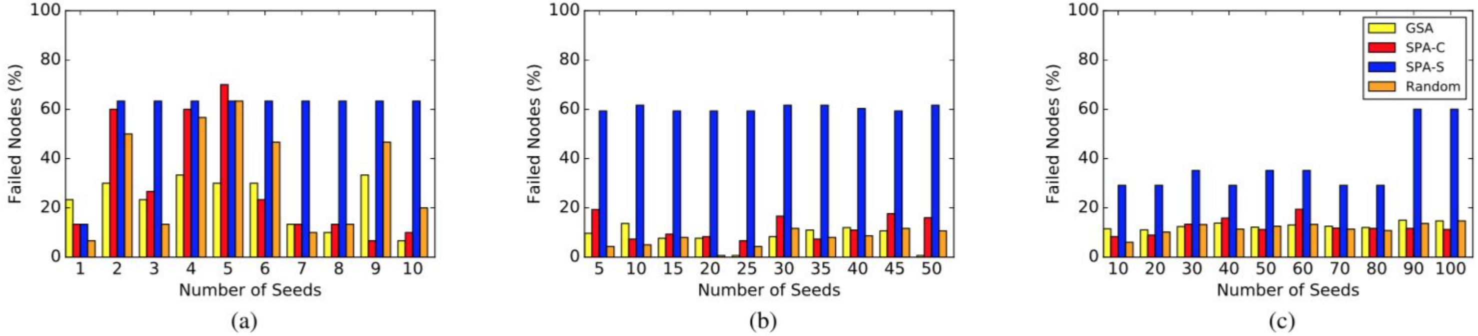


FIGURE 4. **Varying Line Capacity. (a) IEEE 30 Bus. (b) IEEE 300 Bus. (c) Pegase 1354 Bus.**



Testing