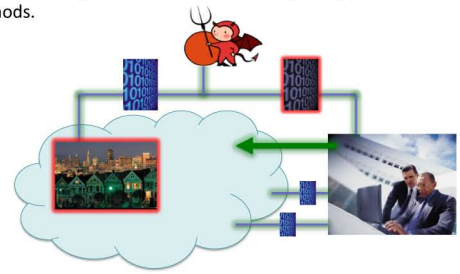
TCIPG

Power Flow Cyber Attacks and Perturbation-Based Defense

Katherine R. Davis, Kate L. Morrow, Rakesh Bobba, Erich Heine

Goals

- Reliable detection of bad-data injection attacks that are potentially undetectable by conventional methods, by using perturbation-based methods.



- Accurate modeling of effects on the power system of perturbations implemented to detect attacks.
- Improved understanding of full taxonomy of attacks that now are potentially undetectable by conventional methods.

Fundamental Questions/Challenges

- Is there an iterative algorithm, based on application of perturbations to an electrical system and observation of the results, for identifying "bad-data" attacks without trusting any of the received measurements as valid?
- Does a cyber-physical system have inherent properties that can be used to undermine a cyber-only attack on it?
- What advantages against an attacker who wishes to remain undetected can a defender gain from physical assets and full system knowledge?

Research Results

- We have presented and demonstrated an algorithm that produces attack vectors that simultaneously target arbitrary, specific measurements *and* result in altered measurements that satisfy the full AC power flow model equations—rendering the attack undetectable by conventional methods.

TRUE DATA VALUES

Bus Num.	V(pu)	Theta(deg)	Pinj(pu)	Qinj(pu)
1	1.04	0	0.717	0.270
2	1.025	9.279	1.63	0.066
3	1.025	4.664	0.85	-0.109
4	1.026	-2.217	0.0	0.0
5	0.996	-3.989	-1.25	-0.5
6	1.013	-3.688	-0.9	-0.3
7	1.026	3.718	0.0	0.0
8	1.016	0.726	-1.0	-0.35
9	1.032	1.966	0.0	0.0

ATTACK POWER FLOW VALUES

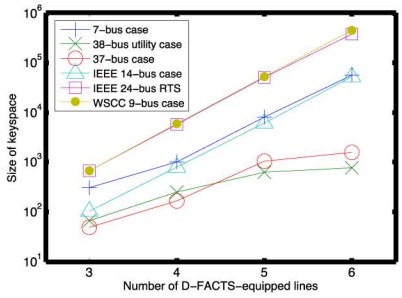
Bus Num.	V(pu)	Theta(deg)	Pinj(pu)	Qinj(pu)
1	1.04	0	0.716	0.270
2	1.025	9.280	1.63	0.066
3	1.025	4.664	0.850	-0.109
4	1.026	-2.217	-0.001	-0.640
5	0.996	-3.989	-1.25	-0.500
6	1.070	-4.173	-0.9	0.7
7	1.026	3.720	0.000	0
8	1.016	0.727	-1	-0.350
9	1.032	1.966	0.010	-0.345

(Values given by attack algorithm example on the WSCC 9-bus test system)

- The attack algorithm is essentially the reverse of the typical iterative power flow solution:
  - Rather than set one bus as the slack and solve for V & Θ (PQ buses) or Q & Θ (PV buses) at all other points, we chose all buses over which the attacker does not have control as effectively slack buses—fixing their V & Θ and solving for P & Q.
  - What that effectively does is allow the adversary to find a physically viable attack vector that will change only specifically targeted measurements—such as sending of bad data showing the voltage at a particular bus to be too high (demonstrated in [1])—plus some measurements at adjacent "boundary" buses.
  - Those boundary bus modifications are needed to maintain the physically required power balance, and are analogous to the requirement that the defender be able to protect a set of "basic measurements" in order to detect attacks under the DC model.

Research Results (continued)

- Initial feasibility analysis of the perturbation-based approach indicates potential utility. Computational experiments were run using six test systems (ranging from 7 to 38 buses), with D-FACTS devices on select lines used as the perturbation mechanism.
  - Possible spaces of perturbations (or "keys") were large enough that a randomly chosen key was effectively unguessable by the adversary.
  - The sizes of those possible spaces (or "keyspaces") were still sufficiently large even with the constraint that the effected changes had to be larger than some noise level.



Broader Impact

- Rather than use the perturbation-based method to detect attacks reactively based on suspicion when something is amiss, one could also use this method to check for attacks preventatively on some continual, routine basis.
- While the work focuses on the impact of D-FACTS devices, it could be extended to work for other physical perturbations, including those continuously ongoing in the power grid during normal operations.

Publications

1 K. R. Davis, K. L. Morrow, R. Bobba, E. Heine. "Power Flow Cyber Attacks and Perturbation-Based Defense." To be presented at *SmartGridComm 2012*.

2 K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, T. J. Overbye. "Topology Perturbation for Detecting Malicious Data Injection." In *Proceedings of the 45th Hawaii International Conference on Systems Sciences (HICSS '12)*, Maui, Hawaii, January 2012.

Interaction with Other Projects

- Presented demo at 2011 TCIPG Industry Workshop (Urbana, IL) using DETER experiment and RTDS simulation to demonstrate detection of a compromised set of power flow measurements.

Future Efforts

- Continue work on characterization of possible attack space: how the adversary would implement a given attack, and what that attack would look like to the defender. Can attacks be uniquely identified?
- More work to be done on modeling the operational effects of the proposed perturbation-based defense.
- Design an algorithm that uses perturbation key sequences to quickly detect and accurately determine the specific data injection attack being performed.