Resilient Distribution Networks
Secure control under DER/PV disruptions

Saurabh Amin
(joint work with Devendra Shelar)

Department of Civil and Environmental Engineering

MIT Solar Day
September 10, 2015
Reliability failures in distribution networks

Local disruptions to cascading failures (blackouts)
“Smart” distribution networks

Sensor-actuator webs: New functionalities

- Distributed Energy Resources (DERs): PVs, EVs, DGs
- State awareness
- Network control
- Demand response

Cyber-physical interactions: New threats

- Off-the-shelf IT devices
  \[ \Rightarrow \] software bugs and hardware flaws
- Open networks
  \[ \Rightarrow \] remote accessibility
- Multi-party management
  \[ \Rightarrow \] incentives for misbehavior
- Large number of field devices
  \[ \Rightarrow \] increased attack surface
Cyber-attacks & the Stuxnet Worm

Maroochy Shire sewage plant (2000)

Tehama Colusa canal system (2007)

Los Angeles traffic control (2008)

Cal-ISO power system computers (2007)
Main questions

When malicious entities (or random failures) compromise DERs/PVs:

- How to perform security threat assessment of distribution networks under DER/PV disruptions?
- How to design decentralized defender (network operator) strategies?
Hackers: Disruption of supply and protection devices

Hacking substation communications

- Target PVs, EVs, DERs
- Hack substation communications
- Introduce incorrect set-points
- Disable supply & safety devices
- Cause voltage & freq. violations
- Induce cascading failures
Attacker-defender interaction

Game-theoretic model

- Attacker compromises a subset of DERs/PVs;
- Defender response by implementing network control.

Problem statement:

- Determine worse-case attack plan (compromise DERs/PVs) to induce:
  - loss of voltage regulation
  - loss due to load shedding
  - loss of frequency regulation [esp., for large PV installations]
- Best defender response (reactive control):
  - Non-compromised DERs provide active and reactive power (VAR)
  - Load control: demand at consumption nodes may be partly satisfied
Effect of attack on loss of voltage regulation

Optimal defender response under DER/PV disruptions

- Voltage regulation can be improved by selective load control
- If load control is costly, defender permits loss of voltage regulation
Effect of attack on cost of load control

Optimal defender response under DER/PV disruptions
- For small intensity attack, load control limits losses
- For high intensity attack, load control not effective
Theorem

Optimal attack plan show downstream preference.

\[ j \prec_i k \]
\[ e =_i k \]
\[ b \prec k \]
A homogeneous DN with optimally secure PVs has following properties:

- If any PV node is secure, secure all its child nodes
- At most one intermediate level with both vulnerable and secure nodes
- In this intermediate level, secure nodes uniformly at random

Theorem
Resilient defender response

Desirable properties of defender response:

1. **Security**: Centralized control strategy undesirable if CC-SS communication is vulnerable

2. **Compensation to owners**: Upstream DERs/PVs likely to be owned by distribution utilities $\Rightarrow$ $\uparrow$ costs when set-points change for larger DERs (esp. $\downarrow$ real power production)

3. **Flexibility**: Topology of DNs might be variable across time: configuration of worst affected nodes may change.

We propose a decentralized control strategy and find new set-points for non-compromised nodes using

- **Information**: local measurements (voltage & freq.) and location of the node with lowest voltage;

- **Diversification**: each node contributes either to voltage or to frequency regulation.
Decentralized DER/PV control

Theorem: Node diversification

- Detect attack
- Find worst affected nodes
- Launch distributed energy resources
- Control voltage & freq. violations
- Prevent cascading failures

Amin, Shelar (MIT)
Resilient Distribution Networks
September 10th, 2015
13 / 13