CERIAS

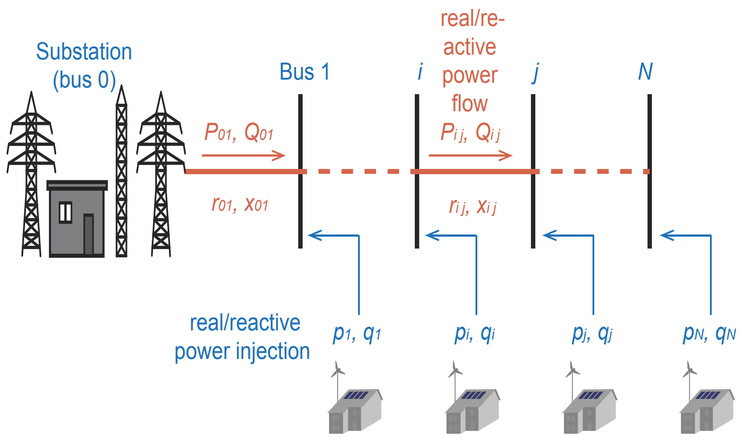
The Center for Education and Research in Information Assurance and Security

Adversarial Attacks to Distributed Voltage Control in Power Distribution Networks with DERs

Peizhong Ju and Xiaojun Lin, School of Electrical and Computer Engineering, Purdue University

Abstract: It has been recently proposed that the reactive power injection of distributed energy resources (DERs) can be used to regulate the voltage across the power distribution network, and simple distributed control laws have been developed in the literature for performing such distributed Volt/VAR control. However, enabling the reactive-power injection capability of DERs also opens the door for potential adversarial attacks. We study the potential damage (in terms of the voltage disruption) of such adversarial attacks and how to mitigate the damage by controlling the allowable range of reactive power injection at each bus. We demonstrate that an intelligent attacker can actually exploit the response of the legitimate buses to amplify the damage by two times. Such a higher level of damage can be attained even when the adversary has no information about the network topology. We then formulate an optimization problem to limit the potential damage of such adversarial attacks.

Volt/VAR Control



$$P_{ij} - \sum_{k \in \mathcal{S}_j} P_{jk} = -p_j,$$

$$Q_{ij} - \sum_{k \in \mathcal{S}_j} Q_{jk} = -q_j,$$

$$V_i - V_j = r_{ij} P_{ij} + x_{ij} Q_{ij}.$$

$$\mathbf{q}^g(t+1) = \left[\mathbf{q}^g(t) - \mathbf{D}(\mathbf{V}(t) - 1)\right]^+$$

Why need control?

- *Voltage rises because of DER real-power injection*

How to control

- *Traditional / centralized voltage control*
  - *Use CB (capacitor bank) and/or OLTC (on-load tap-changing transformer)*
  - *CB and OLTC incur wear-and-tear cost and cannot be operated too frequently as renewable changes*
- *Distributed voltage control*
  - *Use VAR injection of DER*
  - *Each node measures the voltage mismatch and adjusts the VAR injection amount*

Potential attacks

- *The adversary can compromise a subset of DERs and use their reactive power to disrupt the voltage profile across the distribution network*

Adversary model

network topology → $\mathbf{X}_{bb}$; step size → $\mathbf{D}_b$

$$\check{\mathbf{q}}_b^g(t+1) = (\mathbf{I} - \mathbf{D}_b \mathbf{X}_{bb}) \check{\mathbf{q}}_b^g(t) - \mathbf{D}_b \mathbf{X}_{ba} \check{\mathbf{q}}_a^g(t)$$

$$\check{\mathbf{V}}_b(t) = \mathbf{X}_{ba} \check{\mathbf{q}}_a^g(t) + \mathbf{X}_{bb} \check{\mathbf{q}}_b^g(t)$$

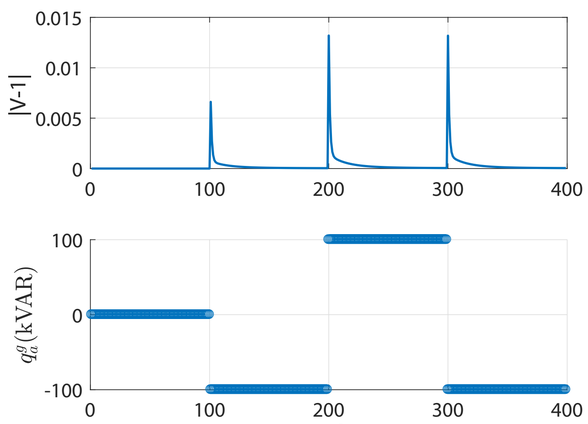
reactive power injection of attacker buses → $\check{\mathbf{q}}_a^g(t)$

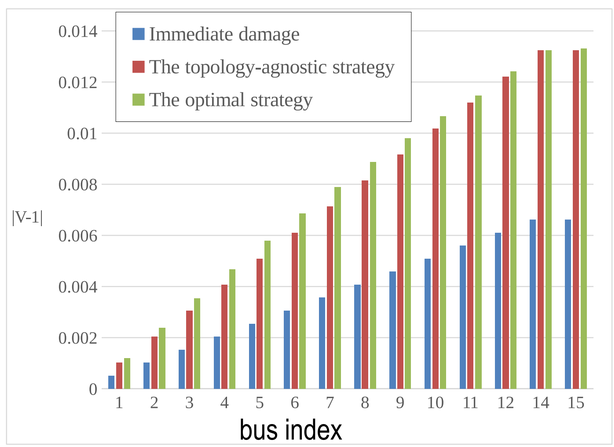
reactive power injection of benign buses → $\check{\mathbf{q}}_b^g(t)$

Attack strategy

The topology-agnostic strategy

- *Leverage the response of the legitimate nodes to cause twice the immediate damage*
- *Does not need any network topology information.*
- *The adversary holds one extreme value for a sufficient long time, waiting for the legitimate buses to approach their equilibrium, and flip the sign in the next time slot.*
- *Close to the performance of the optimal attack strategy*





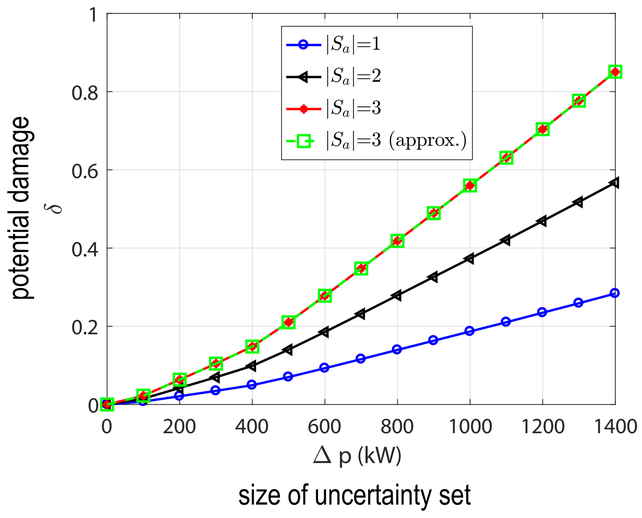
Limit the damage

Objective

- *Minimize the potential damage caused by attackers by setting the range of reactive-power injection*

Constraint

- *Be able to regulate the voltage under varying legitimate inputs in an uncertainty set*
- *We formulate it as a robust optimization problem*



PURDUE UNIVERSITY Discovery Park

CERIAS