ROYAL INSTITUTE OF TECHNOLOGY

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Tools and Metrics for Vulnerability Assessment

Henrik Sandberg,
Kaveh Paridari, André Teixeira

KTH Department of Automatic Control

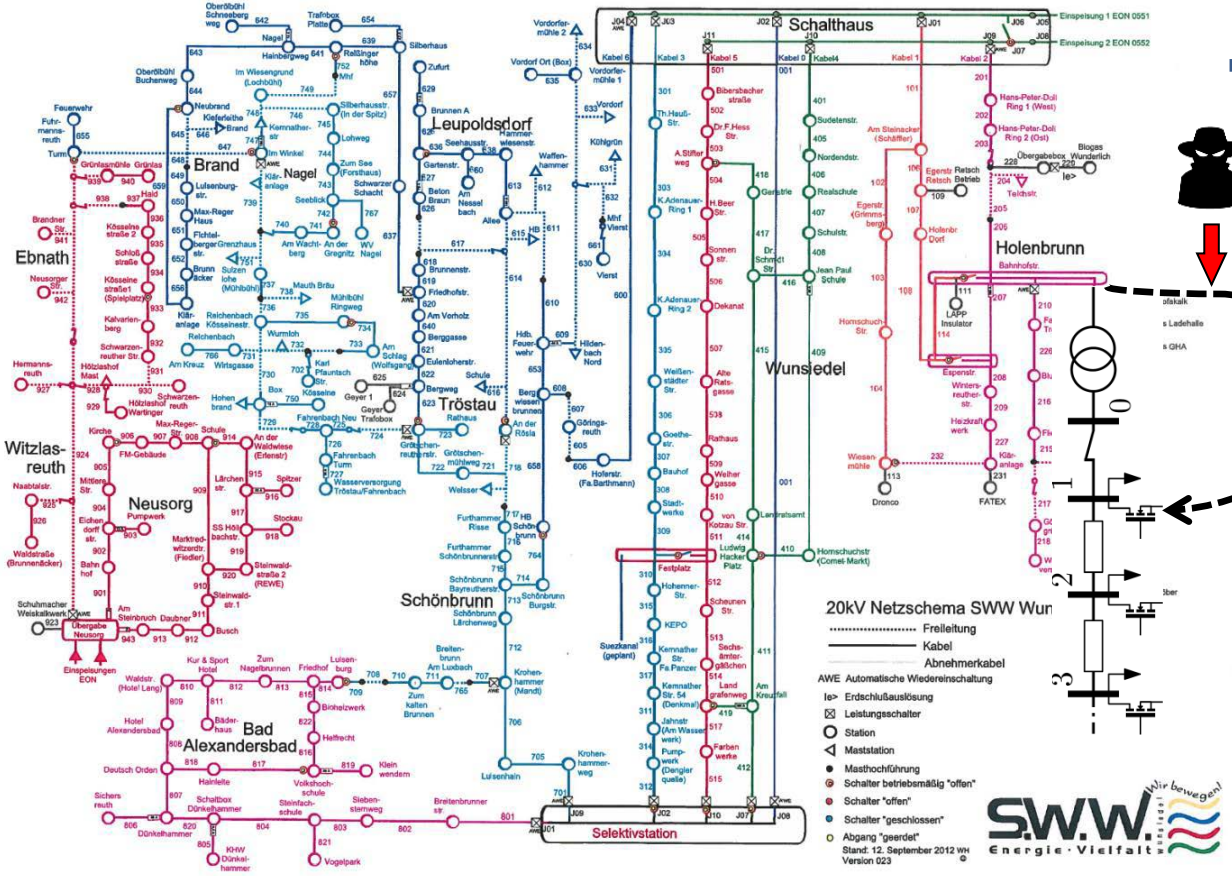
SPARKS Stakeholder Workshop, Cork, Ireland, March 25th, 2015

EU FP7 Programme Contract No. 608224

A Scenario Inspired by EPRI/NESCOR Threat Scenario ET.16

SMART GRID PROTECTION AGAINST CYBER ATTACKS

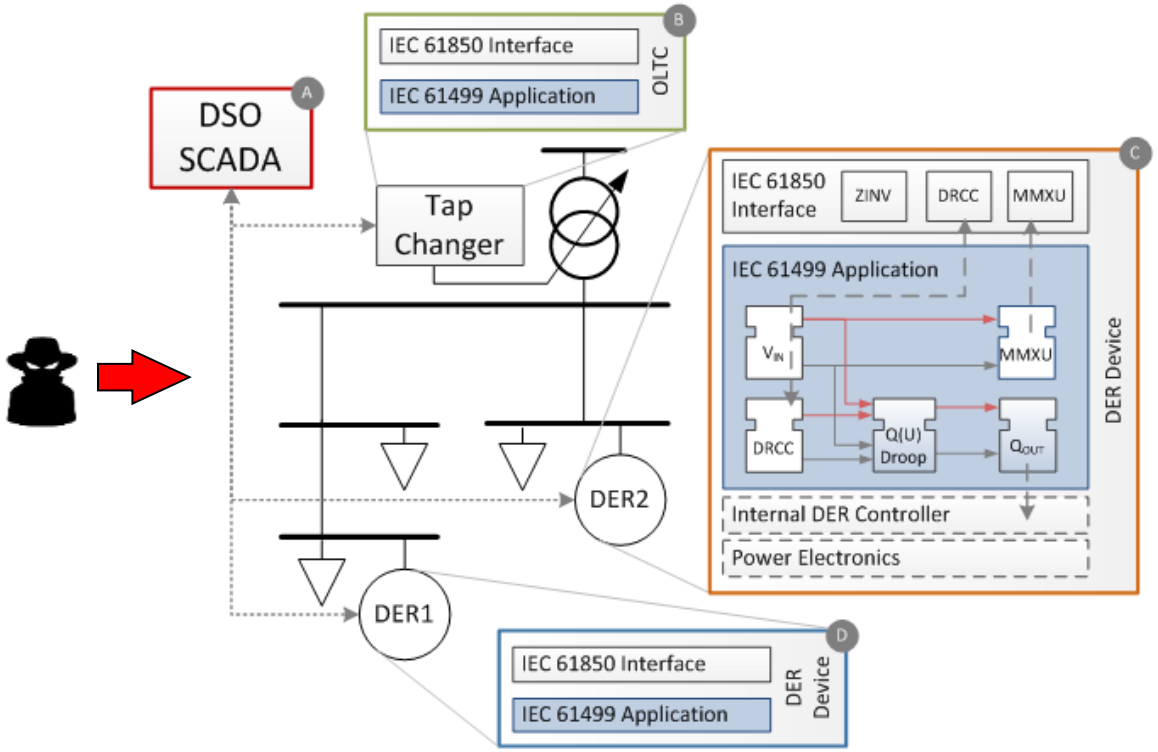
A set of EVs/PVs/DERs is Exploited to Threaten Transformer or Substation



- **Vulnerability:** no protection of data integrity. Configuration commands may be corrupted
- **Consequences:**
  - Damage to transformer
  - Cascading failure
  - Economic losses
- **Questions:**
  - What EVs/PVs/DERs are most vulnerable?
  - Will cascading failure occur?
  - How fast must the attack be detected?
  - …

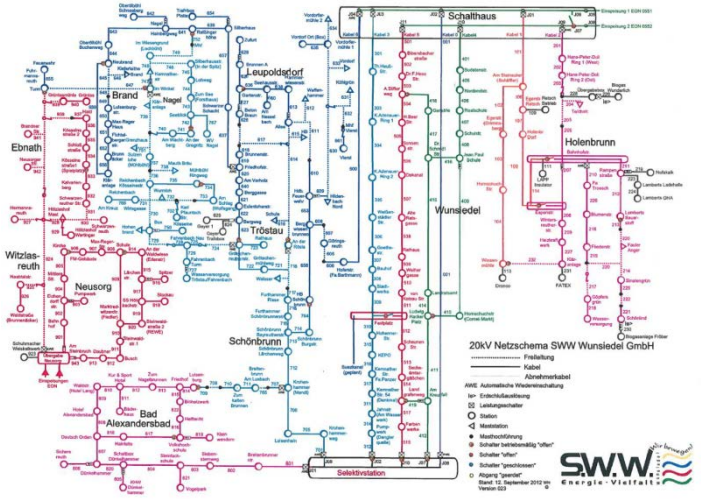
EU FP7 Programme Contract No. 608224

IEC 61850 Standard: Distributed Control Approach for DER



[Andrén *et al.*, IEEE Trans. Energy Conv., 2014]

Goals and Challenges: Tools and Metrics



- Impossible to simulate

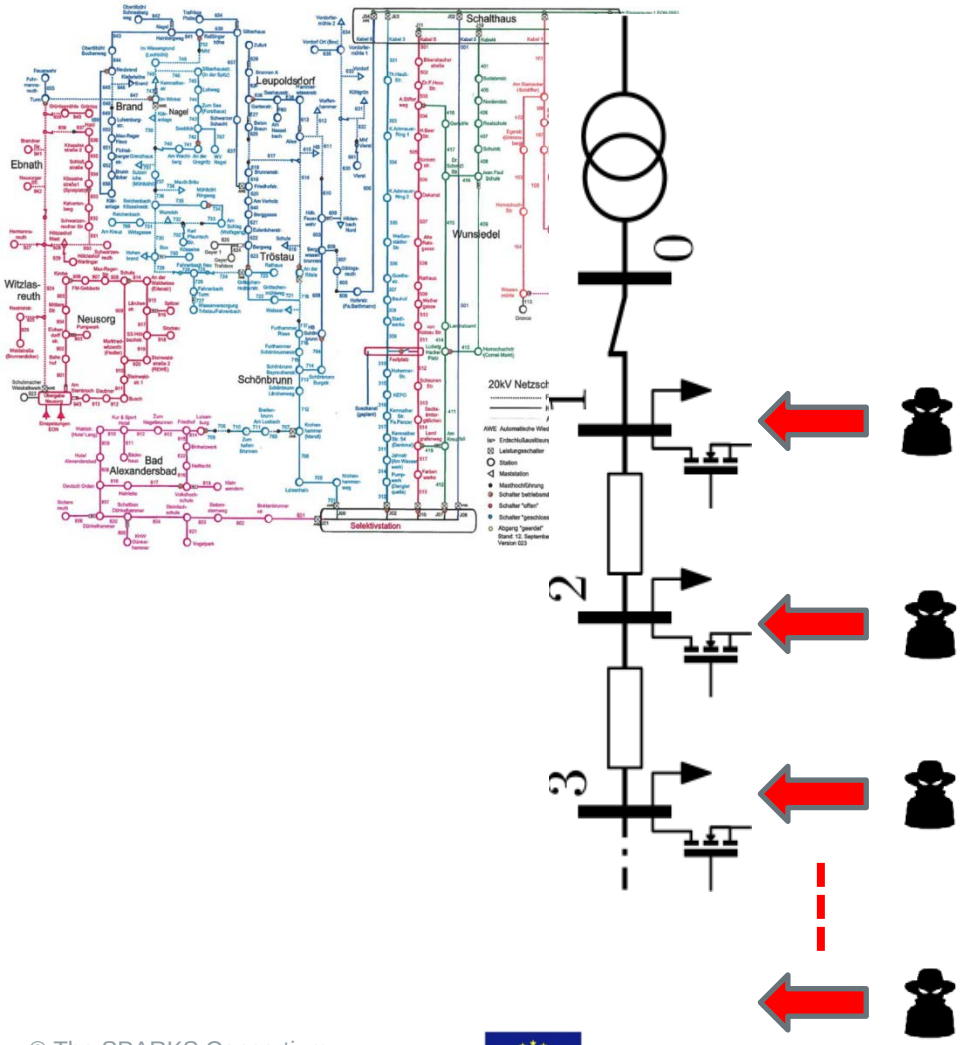
every possible threat scenario

- Develop quantitative tools to localize most critical signals and equipment
  - Verification using detailed simulation
  - Allocation of protective resources
  - Design of resilient controllers

- Need simplified models to obtain tractable computational problems

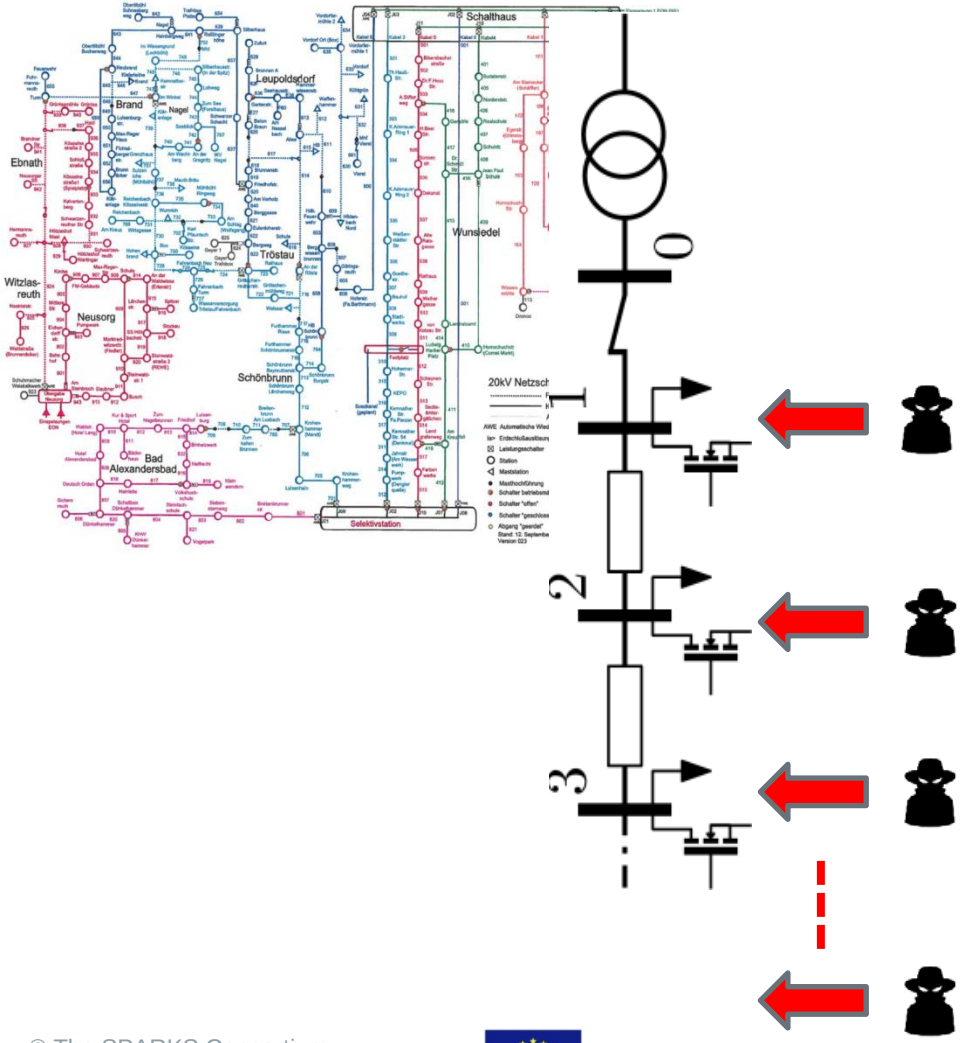
EU FP7 Programme Contract No. 608224

Example of Current Work



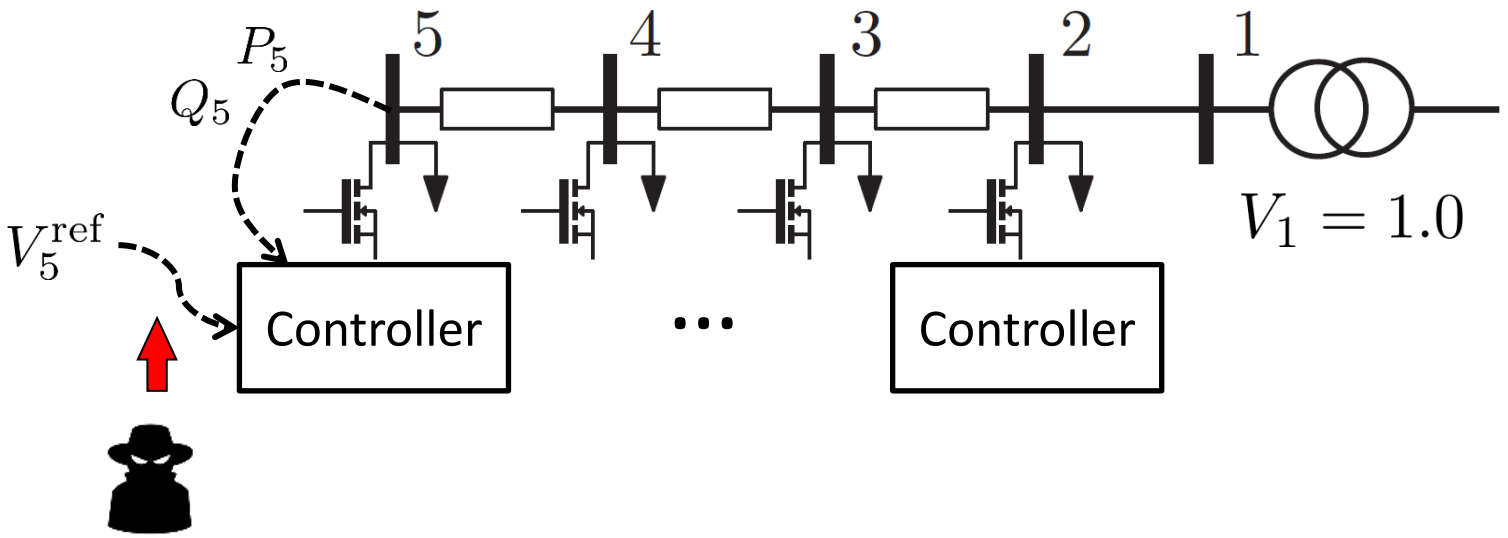
- PV controllers on a line attacked
- Possible damage
  - Fuses blown or components damaged
  - Forced islanding or load shedding
  - Degraded performance due to oscillation, or power quality
  - Forced switch in transformers and volt/VAR control, but no damage/instability
  - Economic losses

Example of Current Work



- Scenarios
  - Coordinated (botnet) attack
  - Local attack
- Metric
  - Electrical impact vs. #attacked PV control signals

A 5-Node System: Setpoint for Node 5 Attacked

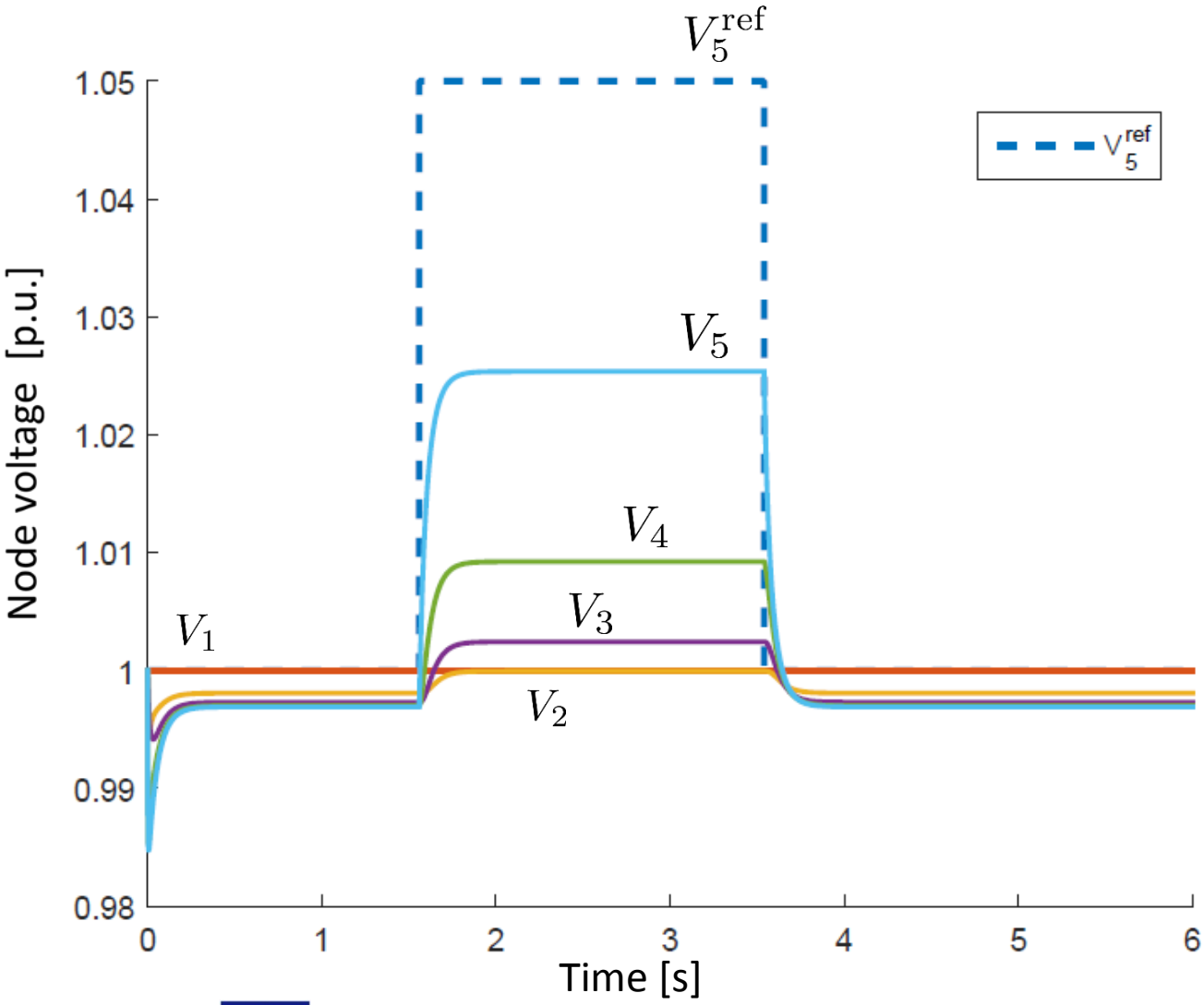


- PV inverter node dynamics (C_i control gains):

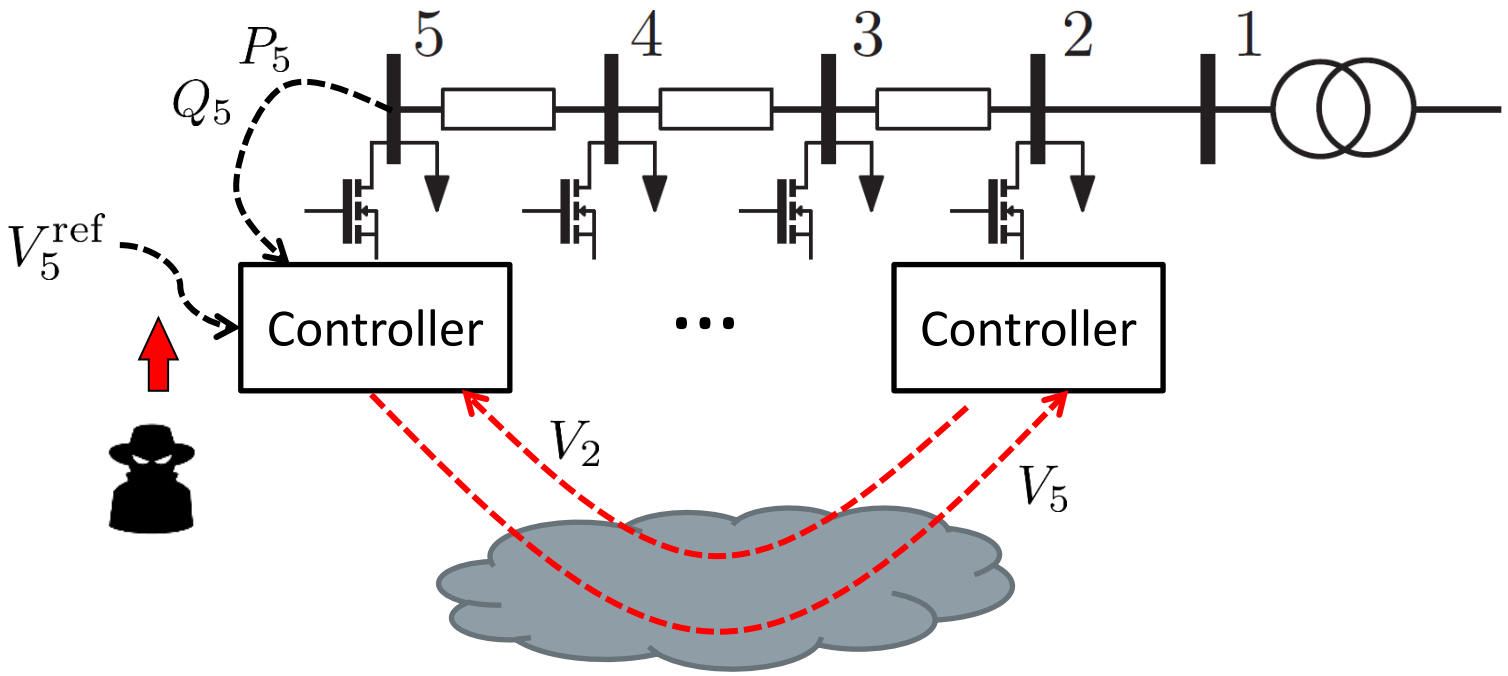
$$\tau_i \dot{V}_i(t) = -C_i V_i(t)\left[V_i(t) - V_i^{\text{ref}}(t)\right] - \tilde{Q}_i(t), \quad i = 2,3,4,5$$

$$\tilde{Q}_i(t) = \frac{1}{1+\rho^2}\left[Q_i(t) - \rho P_i(t)\right]$$

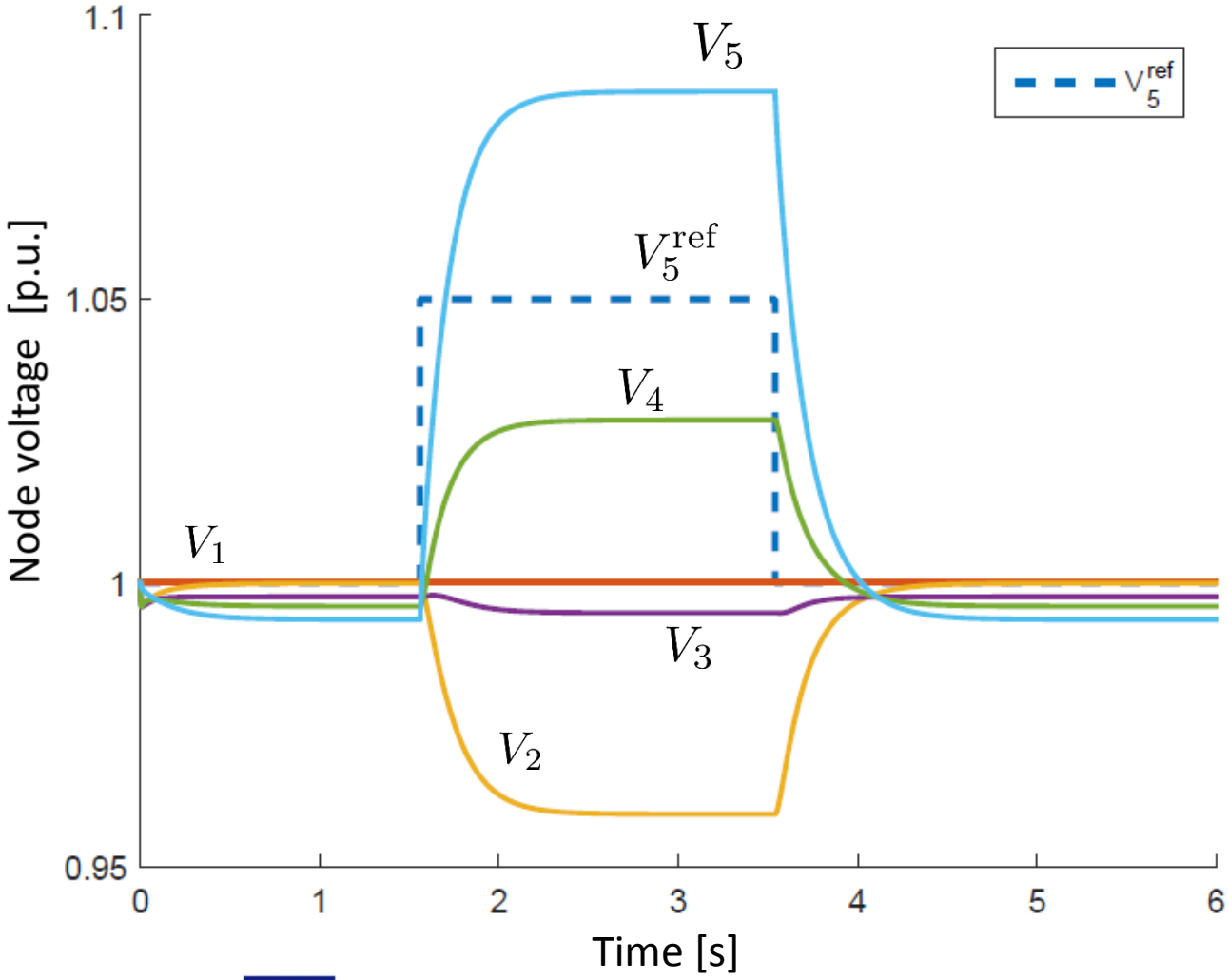
Simulation Result



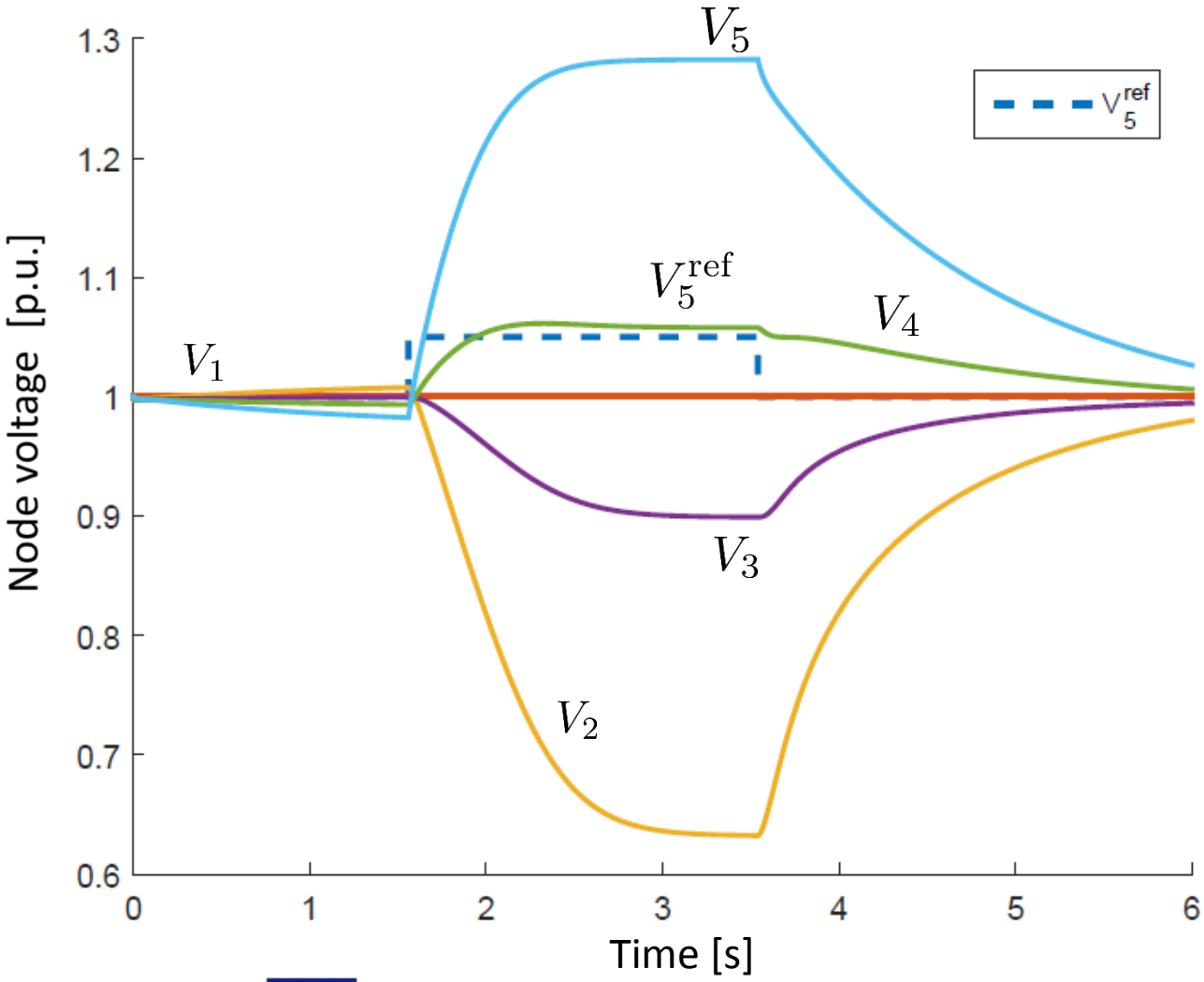
A 5-Node System: Attacker Swaps Measurements for Node 2 and 5



Simulation Result



Simulation Result (50% Higher Control Gains C_i)



Insights from Simulations

- Effects of attack against the reference decay with electrical distance

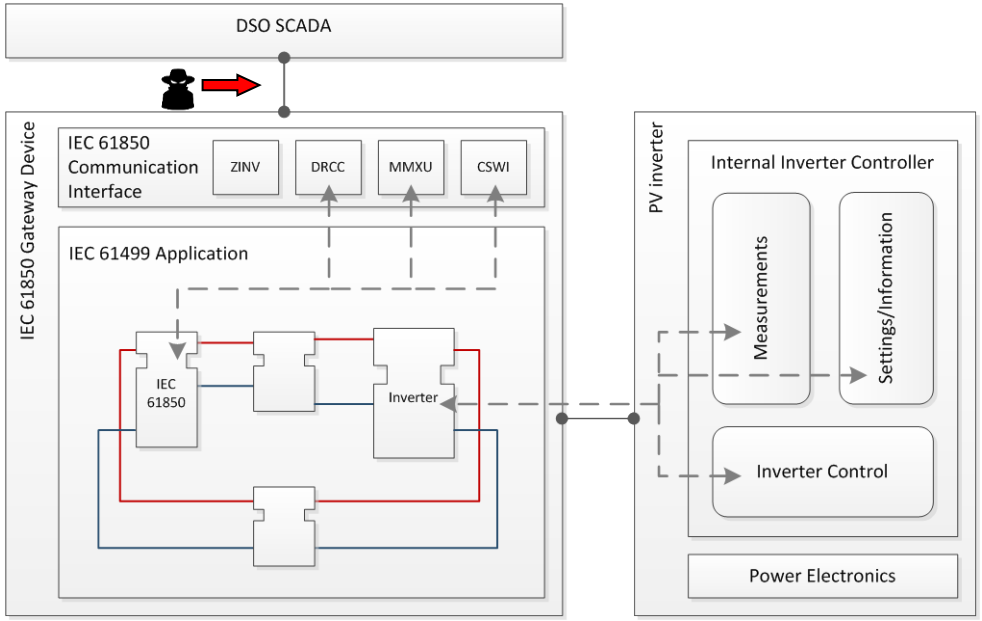
- But attacker may also swap measurements on the communication bus
  - Complete change of dynamical behavior: non-decaying perturbations, over- and undershoot, oscillations, …
  - How to detect swaps?
  - Which swaps are dangerous?
  - How far can the misbehavior spread?
  - …

EU FP7 Programme Contract No. 608224

Summary and Discussion

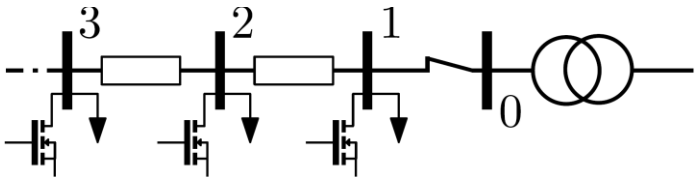
- Combinatorial explosion of the number of possible attacks in a Smart Grid…
- Need for quantitative tools and metrics for vulnerability assessment and resilient control design
- Example: Local and coordinated attacks against PV nodes in a Smart Grid
- A simple simulation example

Communication Protocol: IEC 61850



- **Search for weaknesses in**
  - IEC 61850-90-7 — Object Models for Photovoltaic, Storage and other DER inverters
  - IEC 61850-7-420 — Communications systems for Distributed Energy Resources (DER) - Logical nodes

Simple Model of PV Inverters and Controllers



- States
  - Voltage level: V_i
  - Phase angle: θ_i
- Transmission Line $Y_{ij} = G_{ij} + \mathrm{j}B_{ij}$
  - Homogeneous line ratio: $\rho = \dfrac{G_{ij}}{B_{ij}}$
- Power injections:

$$P_i = \sum_{j \in \mathcal{V}} V_i V_j \left(G_{ij} \cos(\theta_i - \theta_j) + B_{ij} \sin(\theta_i - \theta_j) \right),$$

$$Q_i = \sum_{j \in \mathcal{V}} V_i V_j \left(G_{ij} \sin(\theta_i - \theta_j) - B_{ij} \cos(\theta_i - \theta_j) \right)$$

- Voltage droop controller:

$$\tau_i \dot{V}_i = -C_i V_i \left(V_i - V_i^{\mathrm{ref}} \right) - \tilde{Q}_i$$

$$\tilde{Q}_i = \frac{1}{1+\rho^2} (Q_i - \rho P_i)$$