
KTH Electrical Engineering

# Security of Smart Distribution Grids

## – Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures

André Teixeira
György Dán
**Henrik Sandberg**

ACCESS Linnaeus Centre,
KTH Royal Institute of Technology,
Stockholm, Sweden

Robin Berthier
Rakesh B. Bobba
Alfonso Valdes

Information Trust Institute,
University of Illinois Urbana-Champaign,
Urbana, IL, USA

American Control Conference, Portland, OR, June 4-6, 2014

KTH Electrical Engineering

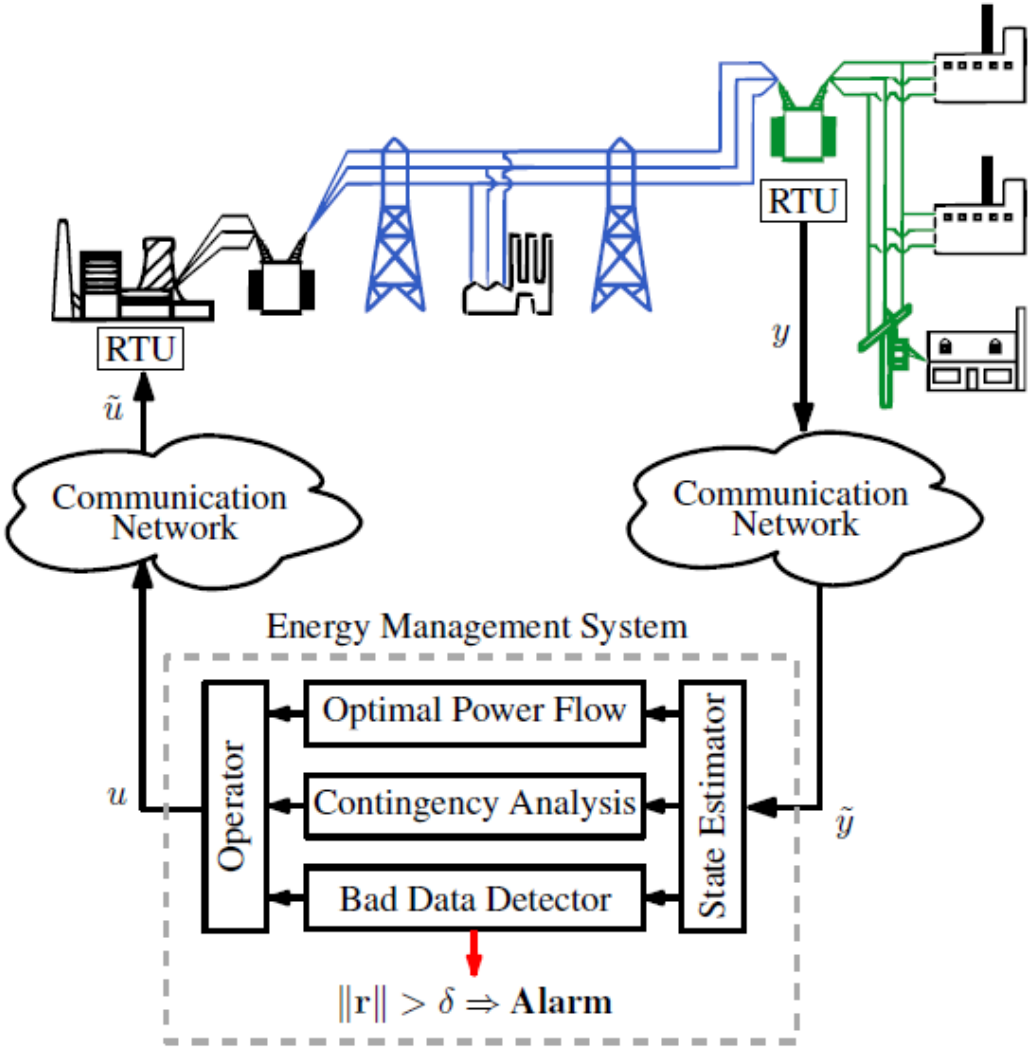
# Outline

- Smart distribution grids – Possibilities and threats
- Models and problem formulation
- Stealthy integrity attacks and games
- Example

KTH Electrical Engineering

# The Transmission Grid Today

**Power system control and monitoring over networks**

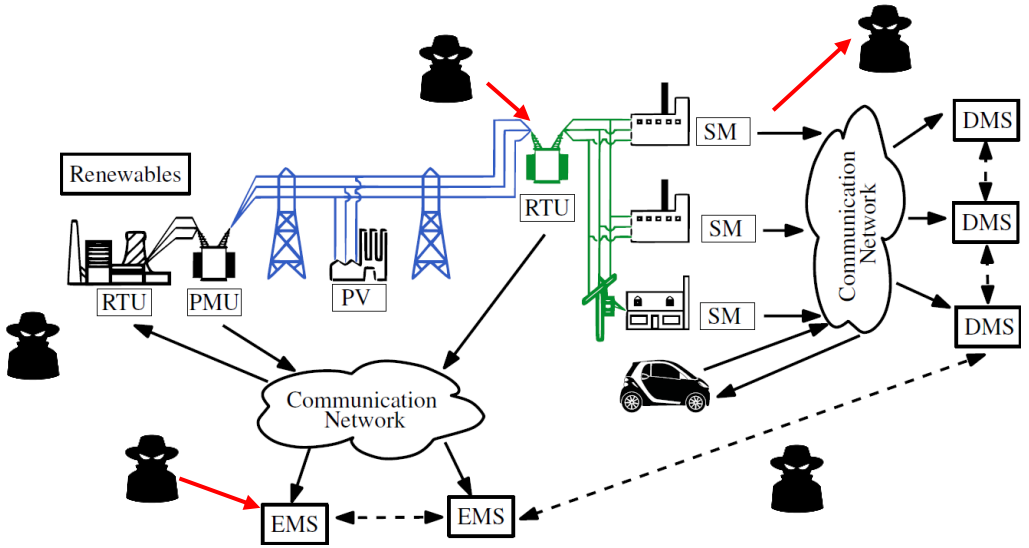


KTH Electrical Engineering

# The Smart Grid and Its Cyber Threats

## Smart Grid

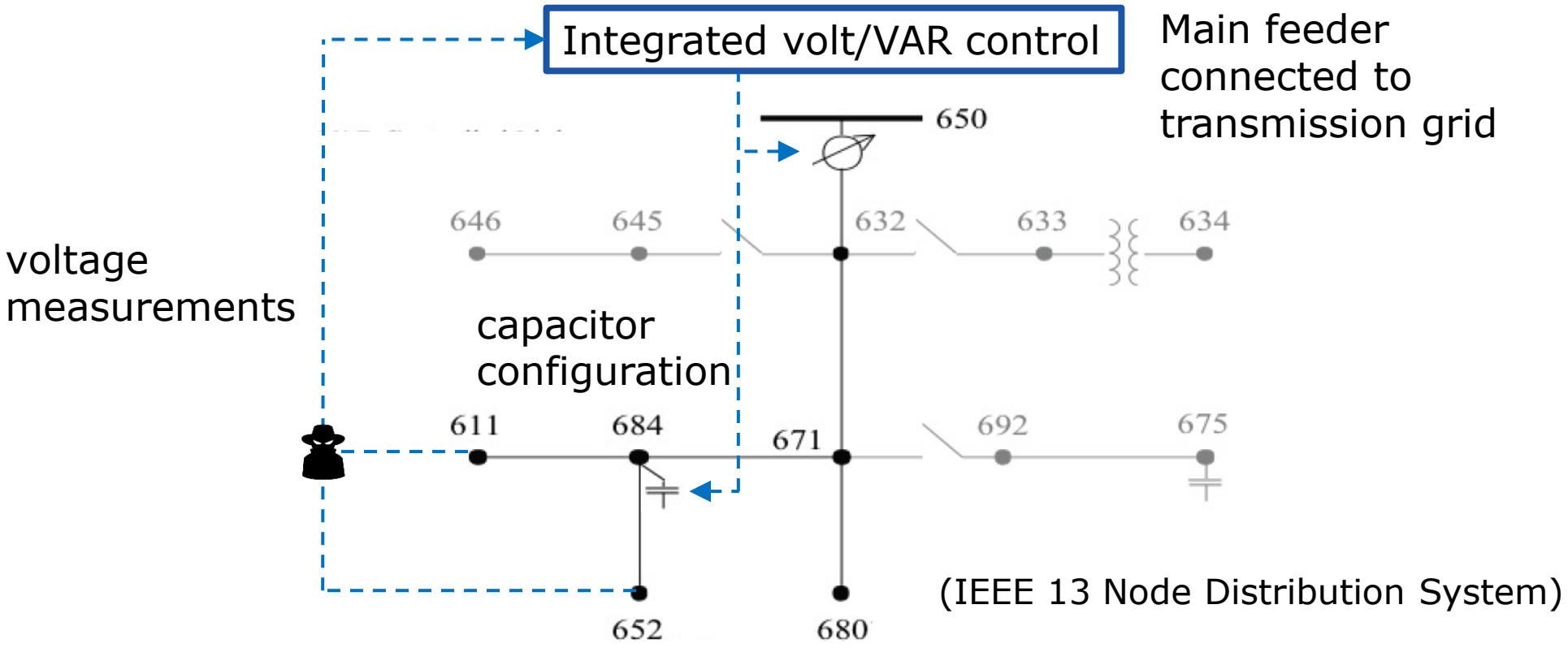
- More smart devices and control loops
- Large increase in communication and data
- Leads to increasing vulnerability to cyber-physical threats with many potential points of attacks



KTH Electrical Engineering

# Integrated Volt/VAR Control

- Maintain voltage at end of line within limits and minimize losses
- Energy saving around 3 % [Roytelman and Landenberger, 2009]
- **Our scenario:** Compromised measurements



KTH Electrical Engineering

# Problem Formulation and Contributions

- Is it possible to perform **undetectable data attacks** against integrated volt/VAR controllers?
  - **Yes.** If-and-only-if characterization of stealthy attacks provided
- How should volt/VAR controllers be designed to **minimize possible damage**?
  - Use game theory and **mixed strategies** to hedge against stealthy attacks
- Are the attacks **feasible in practice**?
  - **Yes.** Theoretical results (partially) confirmed by simulations in GridLAB-D

KTH Electrical Engineering

# Related Work

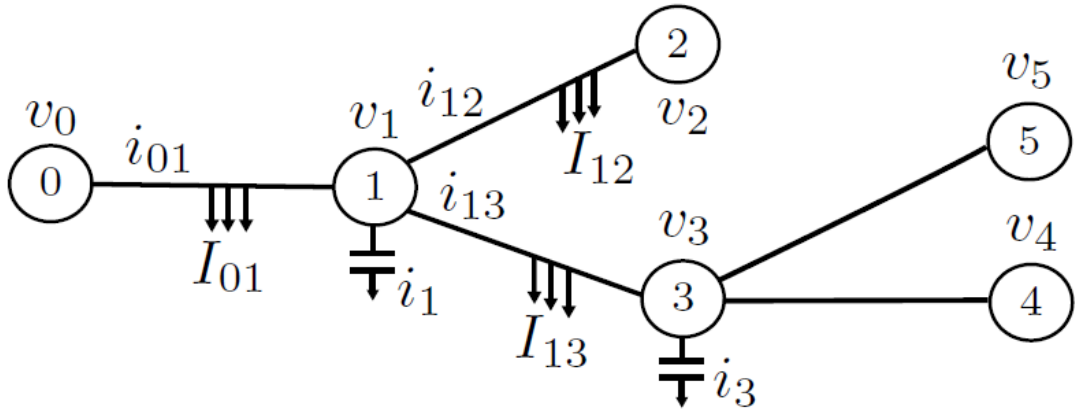
- Cyber-threats against SCADA/EMS
  - [Kropp, 2006], [Giani *et al*., 2009], [Amin, 2010]

- Stealthy integrity attacks in the transmission grid
  - [Liu, Ning, Reiter, 2009], [Sandberg, Teixeira, Johansson, 2010], [Bobba *et al.*, 2010], [Dán, Sandberg, 2010], [Xie, Mo, Sinopoli, 2010]

- Security games for voltage control
  - [Law, Alpcan, Palaniswami, 2012]

KTH Electrical Engineering

# Distribution Grid Model




- Kirchoff's current law:

$$i_{ij} = I_{ij} + i_j + \sum_{k \in \mathcal{N}_j \setminus \{i\}} i_{jk}$$

- Kirchoff's voltage law:

$$v_j = v_i - Z_{ij} \left( \frac{1}{2} I_{ij} + \sum_{k \in \mathcal{N}_j} i_{jk} + i_j \right)$$

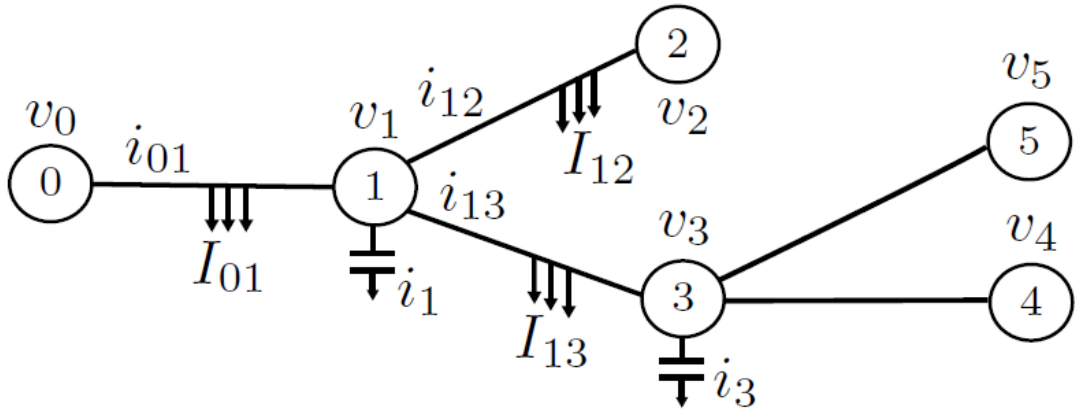
- System state:

$$\mathbf{y} = \begin{pmatrix} I_{01} & I_{12} & \dots \end{pmatrix}^\top \in \mathbb{C}^n \text{ and } v_0$$

- Control (capacitor configuration): $C_k = \{\sigma_1, \dots, \sigma_m\}$

KTH Electrical Engineering

# Distribution Grid Model




$$\begin{bmatrix} \mathbf{v}^k - v_0^k \mathbf{f}_1(C_k) \\ (S^k/v_0^k)^* - v_0^k \mathbf{f}_2(C_k) \end{bmatrix} = \begin{bmatrix} H_v(C_k) \\ H_S(C_k) \end{bmatrix} \mathbf{y}$$

KTH Electrical Engineering

# Consumer and Operator Models

- **Consumer model:**
  - The state $\mathbf{y}$ (current loads) and $v_0$ (main feeder voltage) is independent on capacitor configuration $C_k$
  - Consumers report voltage violations

- **Operator model:** Integrated volt/VAR controller optimizes the capacitor configuration

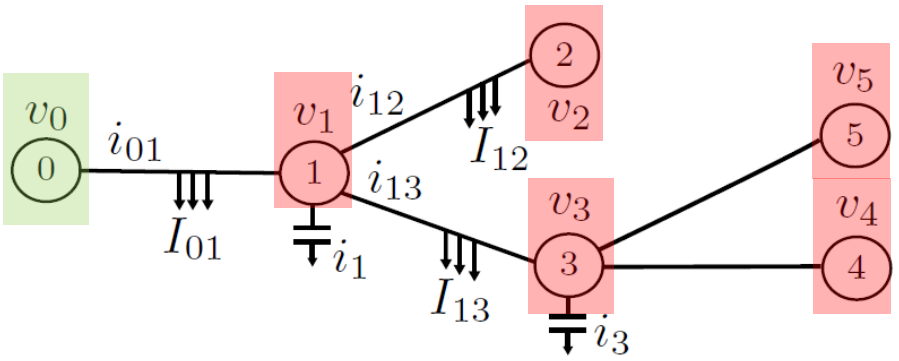
$$C^*(\mathbf{x}) = \arg \min_{C \in \mathcal{C}_{\mathcal{F}}(\mathbf{x})} V(\mathbf{x}, C)$$

  - minimize cost function (e.g., $V =$ total power injection)
  - subject to end-of-line voltage constraints
  - $\mathbf{x}$ is estimated, possibly corrupted, system state

KTH Electrical Engineering

# Adversary Model

- **Adversary's goal:** Increase operator's cost ($V$), while remaining undetected
- The adversary may alter voltage measurements $\mathbf{v}$, but not main feeder power injection and voltage




- The adversary performs a one-shot attack $\mathbf{v} \to \mathbf{v} + \mathbf{a}$
- **Questions:**
  - When can the volt/VAR controller detect the attacks $\mathbf{a}$?
  - How can it limit the effects of the attacks?

KTH Electrical Engineering

# Stealthy Measurements Attacks (1)

- The attack $\mathbf{a}$ is a $C_k$-**stealth attack** if there exists

$$\boldsymbol{\Delta}\mathbf{y}: \quad \mathbf{a} = H_v(C_k)\boldsymbol{\Delta}\mathbf{y} \text{ and } 0 = H_v(C_k)\boldsymbol{\Delta}\mathbf{y}$$

- "When the grid is in configuration $C_k$, there exists a physical state explaining the received measurements"

*Theorem 1:* Let the columns of the matrix $B_k \in \mathbb{C}^{n\times(n-1)}$ form an arbitrary basis of $\mathcal{N}(H_S(C_k))$. Then $\mathbf{a}$ is a $C_k$-stealth attack if and only if there exists an $\alpha \in \mathbb{C}^{n-1}$ such that

$$\mathbf{a} = H_v(C_k)B_k\alpha.$$

The corresponding non-refutable state bias is $\boldsymbol{\Delta}\mathbf{y} = B_k\alpha$.

KTH Electrical Engineering

# Stealthy Measurements Attacks (2)

- The attack $\mathbf{a}$ is a $\mathcal{C}$-**stealth attack** if there exists **one** $\mathbf{\Delta y}$ : $\mathbf{a} = H_v(C_k)\mathbf{\Delta y}$ and $0 = H_v(C_k)\mathbf{\Delta y}$ for **all** capacitor configurations $C_k$
- "No matter how the control switches, the received measurements are physically consistent"

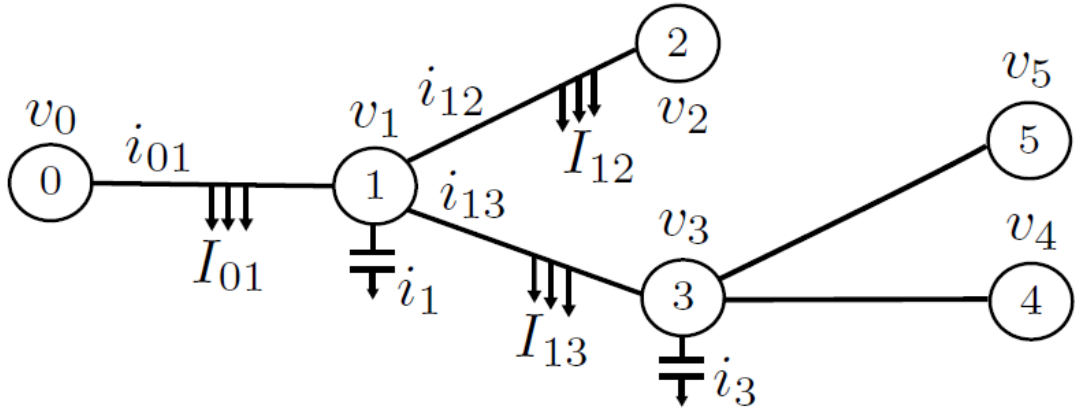
*Theorem 2:* Let the columns of the matrix $B_{\mathcal{C}} \in \mathbb{C}^{n\times m}$ form an arbitrary basis of the nullspace $\mathcal{N}\left(\begin{bmatrix}\Delta H_v(\mathcal{C}) \\ H_S(\mathcal{C})\end{bmatrix}\right)$, where

$$\Delta H_v(\mathcal{C}) = \begin{bmatrix} H_v(C_1) - H_v(C_2) \\ H_v(C_2) - H_v(C_3) \\ \vdots \end{bmatrix}, \quad H_S(\mathcal{C}) = \begin{bmatrix} H_S(C_1) \\ H_S(C_2) \\ \vdots \end{bmatrix}.$$

Then $\mathbf{a}$ is a $\mathcal{C}$-stealth attack if and only if there exists an $\alpha \in \mathbb{C}^m$ such that $\mathbf{a} = H_v(C_1)B_{\mathcal{C}}\alpha$. The corresponding non-refutable state bias is $\mathbf{\Delta y} = B_{\mathcal{C}}\alpha$.

KTH Electrical Engineering

# Example

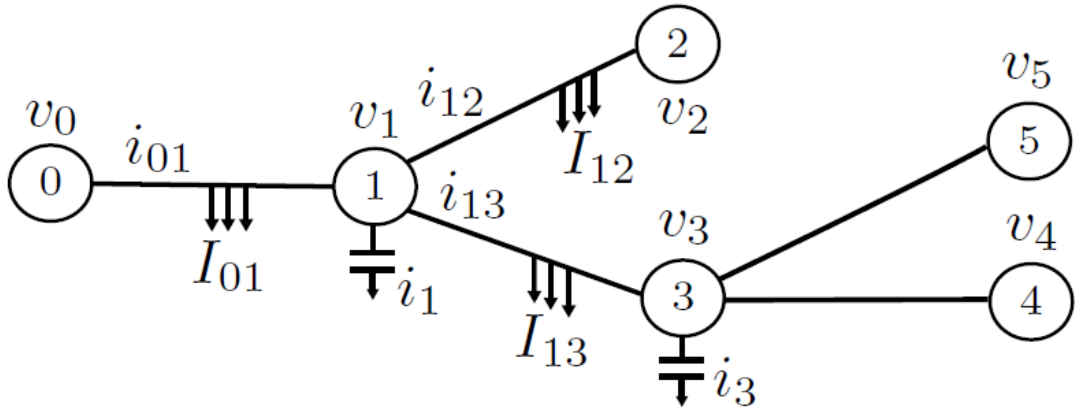



- Control configurations:

$$
\begin{aligned}
C_1: &\quad z_1 = -0.28j\,\text{pu} && z_3 = -1.66j\,\text{pu}\\
C_2: &\quad z_1 = \infty\,\text{pu} && z_3 = -1.66j\,\text{pu}\\
C_3: &\quad z_1 = -0.28j\,\text{pu} && z_3 = \infty\,\text{pu}\\
C_4: &\quad z_1 = \infty\,\text{pu} && z_3 = \infty\,\text{pu}
\end{aligned}
$$

KTH Electrical Engineering

# $C_1$-Stealth Attack Example



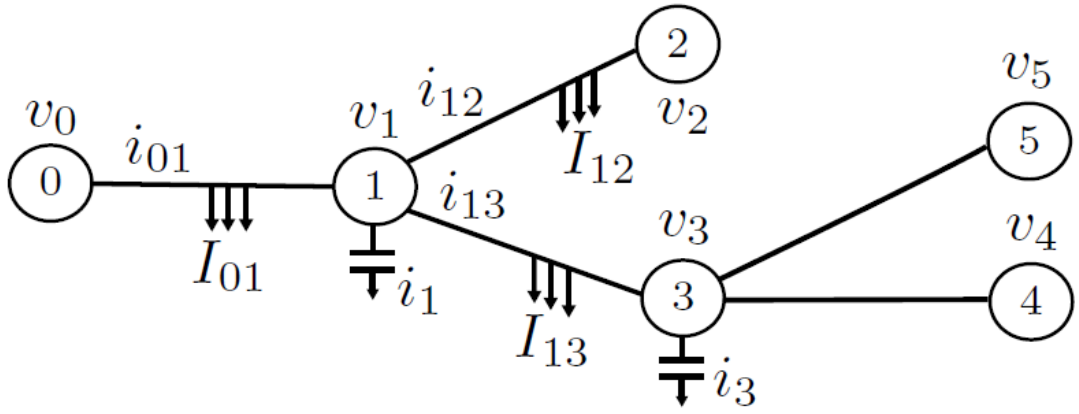

$$C_1: \quad z_1 = -0.28j \text{ pu} \qquad z_3 = -1.66j \text{ pu}$$

- Basis of all $C_1$-stealth attacks:

$$H_v(C_1)B_1 = \begin{pmatrix} 0.00 & 0.00 & 0.05 + 0.03j & 0.10 + 0.01j \\ 1.00 & 0.00 & 1.00 & -0.40 + 0.59j \\ 0.00 & 0.00 & -0.82 + 0.43j & 1.00 \\ 0.00 & 1.00 & -0.80 + 0.32j & 0.96 - 0.19j \\ 0.25 & -1.00 & -0.80 + 0.32j & 0.91 + 0.40j \end{pmatrix}$$

KTH Electrical Engineering

# $\mathcal{C}$-Stealth Attack Example




- Basis of all $\mathcal{C}$-stealth attacks:

$$H_v(C_1)B_{\mathcal{C}} = \begin{pmatrix} 0.00 & 0.00 \\ 1.00 & 0.00 \\ 0.00 & 0.00 \\ 0.00 & 1.00 \\ 0.25 & -1.00 \end{pmatrix}$$

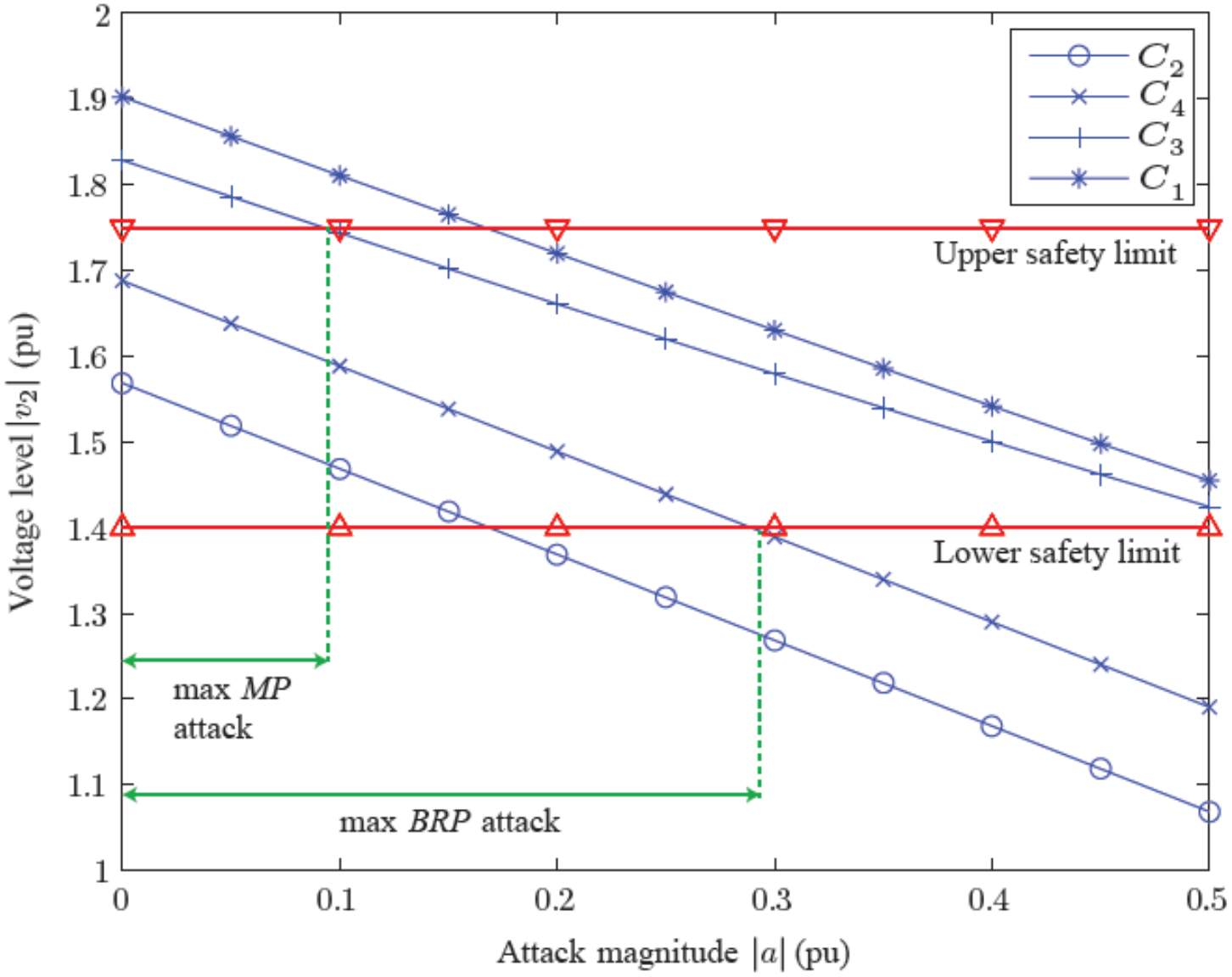
KTH Electrical Engineering

# The Operator vs the Adversary

- Stealthy measurement attacks exist
- Attacks may even be stealthy under arbitrary control actions
- Use **game theory** and **mixed strategies** to limit impact
  - Pure strategy: use $C^*(\mathbf{x}) = \arg \min_{C \in \mathcal{C}_{\mathcal{F}}(\mathbf{x})} V(\mathbf{x}, C)$
  - Mixed strategy: use $C^*(\mathbf{x})$ with high probability
- Example next

KTH Electrical Engineering

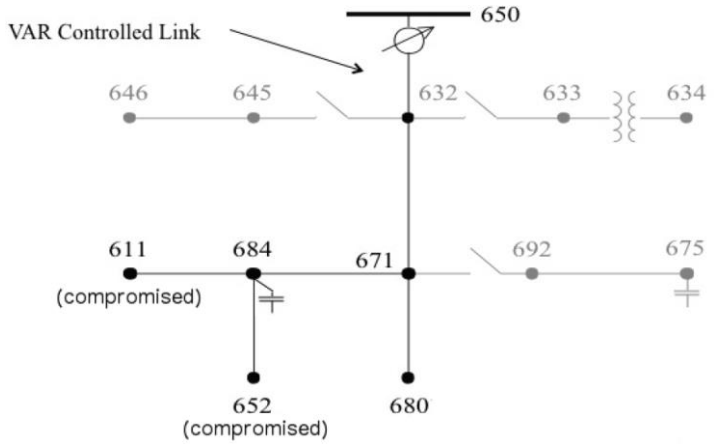
# Operator vs Adversary Game

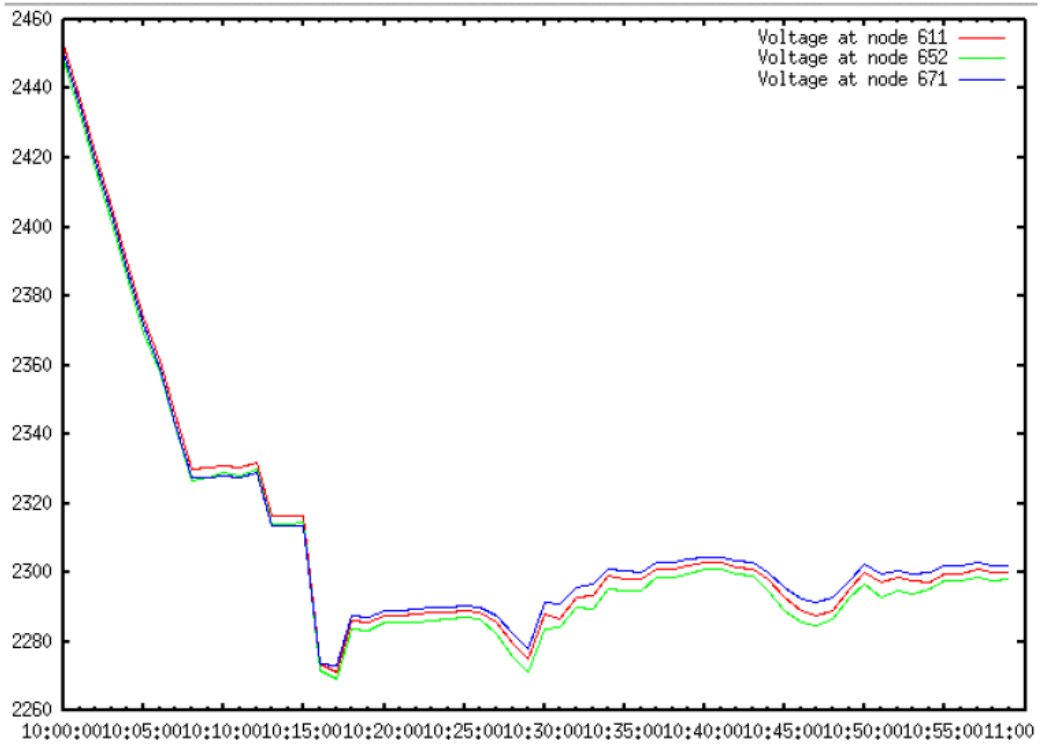



**MP=Mixed operator strategy** **BRP=Pure operator strategy**

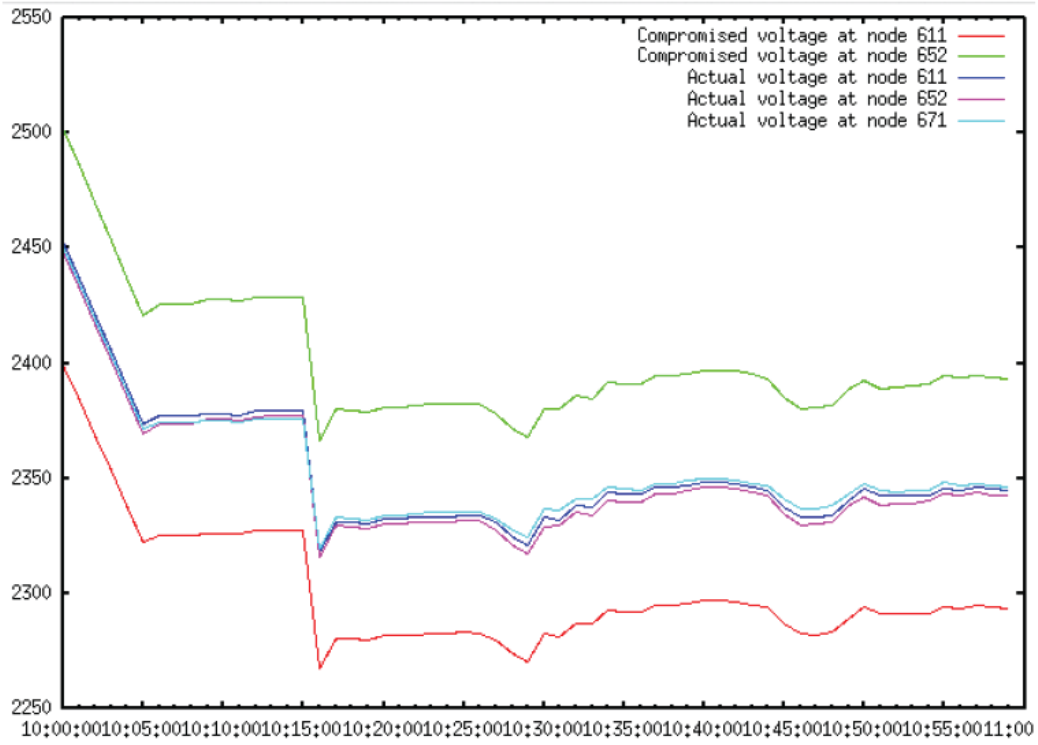
KTH Electrical Engineering

# GridLAB-D Simulation




**No measurement attack**




**Measurement attack**

KTH Electrical Engineering

# Summary

- Cyber attacks against the smart grid a great concern
- If-and-only-if characterization of stealth attacks against volt/VAR control
- Use game theory and mixed strategies to limit impact
- Future work: More realistic consumer models

**Thank you!**

Contact: **hsan@kth.se**