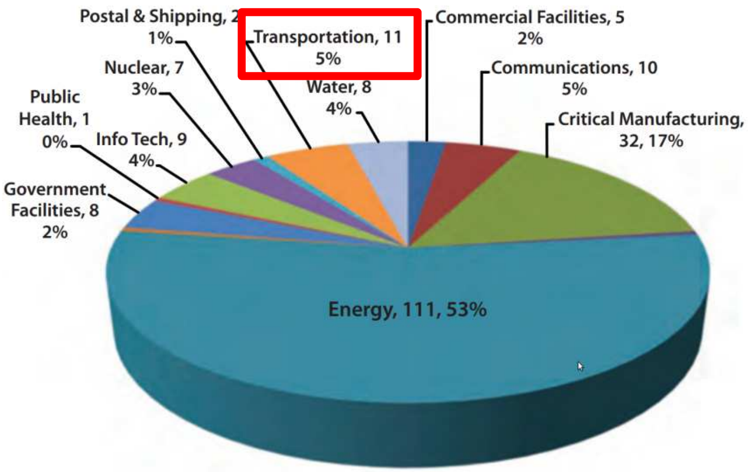
Impact of Signal Delay Attack on Voltage Control for Electrified Railways

Hoang Hai Nguyen[1] **Rui Tan**[1] David K. Y. Yau[1,2]

[1]Advanced Digital Sciences Center (Singapore),
University of Illinois at Urbana-Champaign

[2]Singapore University of Technology and Design

Motivation



3rd largest cluster of cyber-physical attacks
[U.S. CERT / ICS-CERT, 2013]

2014 Moscow derailment
[Image from USNews]

- Cyber-attacks on industrial control systems
  - Dragonfly, Stuxnet
  - 11 transportation intrusions in 2013
- Voltage control in traction power systems
  - Cybernated, safety-critical
  - Voltage drop before Moscow derailment

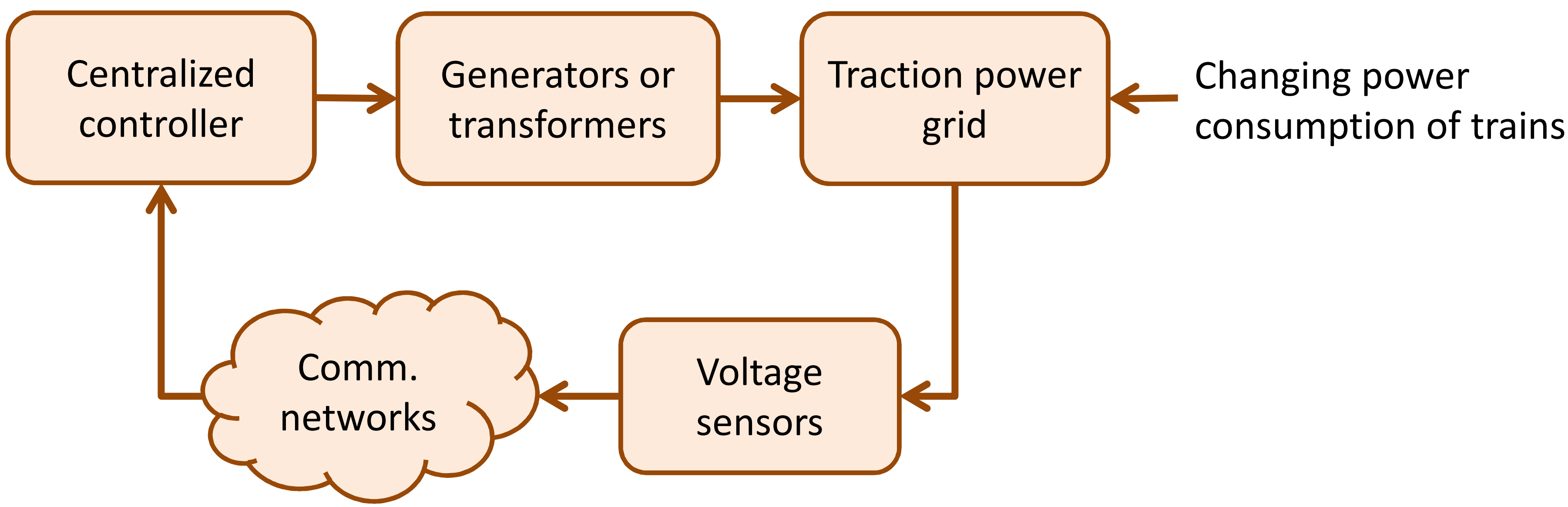
https://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013_3.pdf

Background

- AC traction power systems
  - Up to 50 kV
  - Substations connected to utility grid or **dedicated power grid**
- Large voltage fluctuations
  - Trains: moving loads
  - De-accelerating trains: moving generators
  - Train shift between sections causes step change

Background

- AC traction power systems
  - Up to 50 kV
  - Substations connected to utility grid or **dedicated power grid**
- Large voltage fluctuations
  - Trains: moving loads
  - De-accelerating trains: moving generators
  - Train shift between sections causes step change



Voltage Control

- State-space model for multi-bus power grid

$$\mathbf{x}[k] \approx \mathbf{x}[k-1] + \mathbf{Cu}[k] + \mathbf{B}(\mathbf{q}[k] - \mathbf{q}[k-1])$$

Voltage Control

- State-space model for multi-bus power grid

$$\mathbf{x}[k] \approx \mathbf{x}[k-1] + \mathbf{C}\mathbf{u}[k] + \mathbf{B}(\mathbf{q}[k] - \mathbf{q}[k-1])$$

substation voltages

generator/transformer voltages

substation reactive power draws

Voltage Control

- State-space model for multi-bus power grid

$$\mathbf{x}[k] \approx \mathbf{x}[k-1] + \mathbf{C}\mathbf{u}[k] + \mathbf{B}(\mathbf{q}[k] - \mathbf{q}[k-1])$$

substation voltages

generator/transformer voltages

substation reactive power draws

  – Maintain **x** at nominal $\mathbf{x}_0$ when **q** changes

Voltage Control

- State-space model for multi-bus power grid

$$\mathbf{x}[k] \approx \mathbf{x}[k-1] + \mathbf{C}\mathbf{u}[k] + \mathbf{B}(\mathbf{q}[k] - \mathbf{q}[k-1])$$

substation voltages

generator/transformer voltages

substation reactive power draws

  – Maintain **x** at nominal $\mathbf{x}_0$ when **q** changes

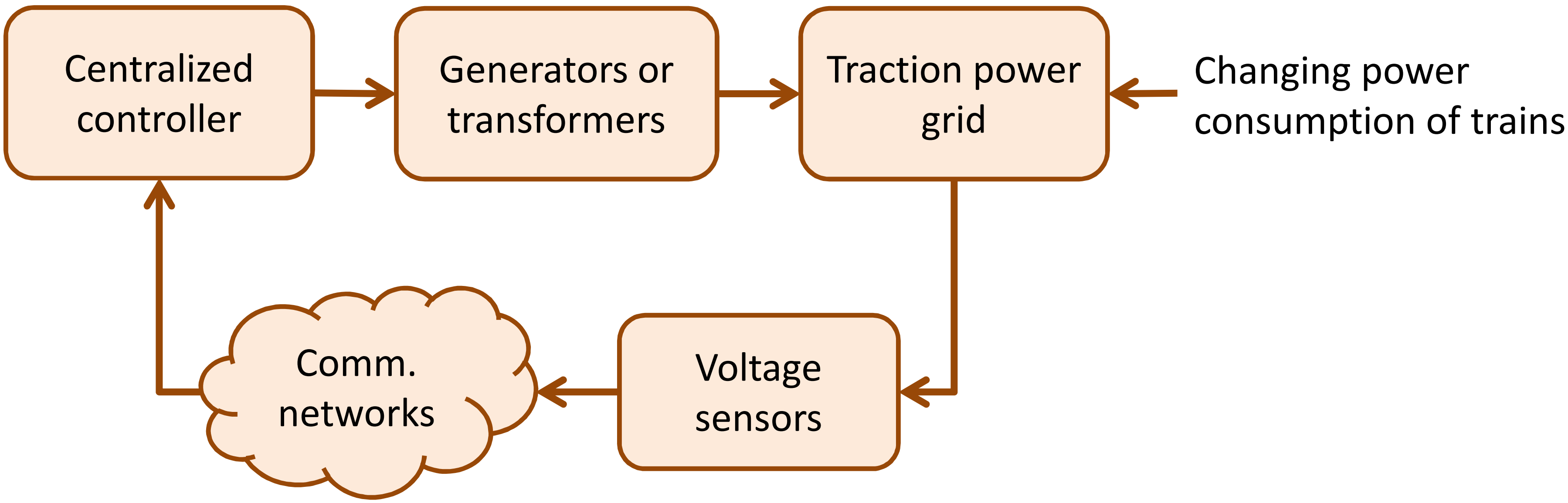
- Control algorithm

$$\mathbf{u}[k] = \alpha \mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[k])$$

  – BIBO stable if $0 < \alpha < 2$

  – Similar controls applied in practice

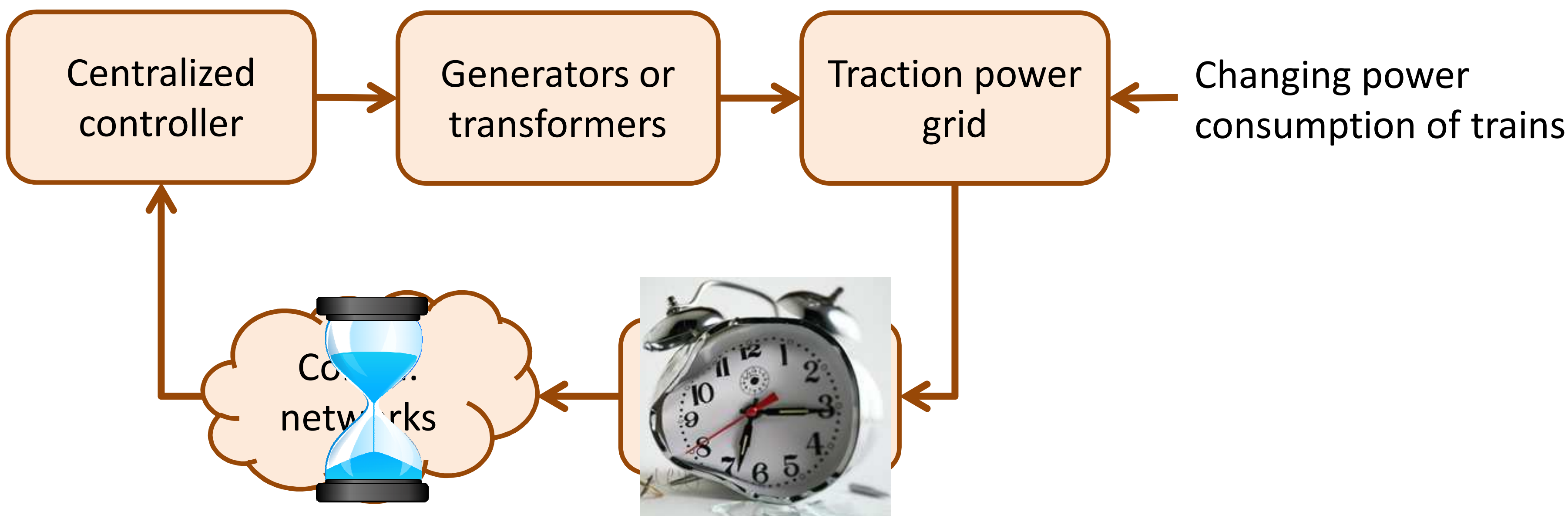
Signal Delay Attack



- Controller uses **old voltage measurements**

$$\mathbf{u}[k] = \alpha \mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[k - \tau])$$

Signal Delay Attack



- Controller uses **old voltage measurements**

$$\mathbf{u}[k] = \alpha \mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[k - \tau])$$

  - Network congestion, time desynchronization
  - Easier than data integrity attacks

Impact of Attack on Stability

- System state transform

$$\mathbf{y}[n] = \left[\mathbf{x}[n]-\mathbf{x}_0, \mathbf{x}[n-1]-\mathbf{x}_0, \cdots, \mathbf{x}[n-\tau]-\mathbf{x}_0\right]$$

  – New state transition model

$$\mathbf{y}[n+1] = \mathbf{G}\cdot\mathbf{y}[n] \qquad \mathbf{G} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & -\alpha\mathbf{I} \\ \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{0} \end{bmatrix}$$

- G's characteristic polynomial

$$\lambda^{\tau+1} - \lambda^{\tau} + \alpha = 0$$

  – Stable: All roots in unit circle of complex plane

Impact of Attack on Stability

- System state transform

$$\mathbf{y}[n] = \left[\mathbf{x}[n] - \mathbf{x}_0, \mathbf{x}[n-1] - \mathbf{x}_0, \cdots, \mathbf{x}[n-\tau] - \mathbf{x}_0\right]$$

  – New state transition model

$$\mathbf{y}[n+1] = \mathbf{G} \cdot \mathbf{y}[n] \qquad \mathbf{G} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & -\alpha\mathbf{I} \\ \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{0} \end{bmatrix}$$

- G's characteristic polynomial

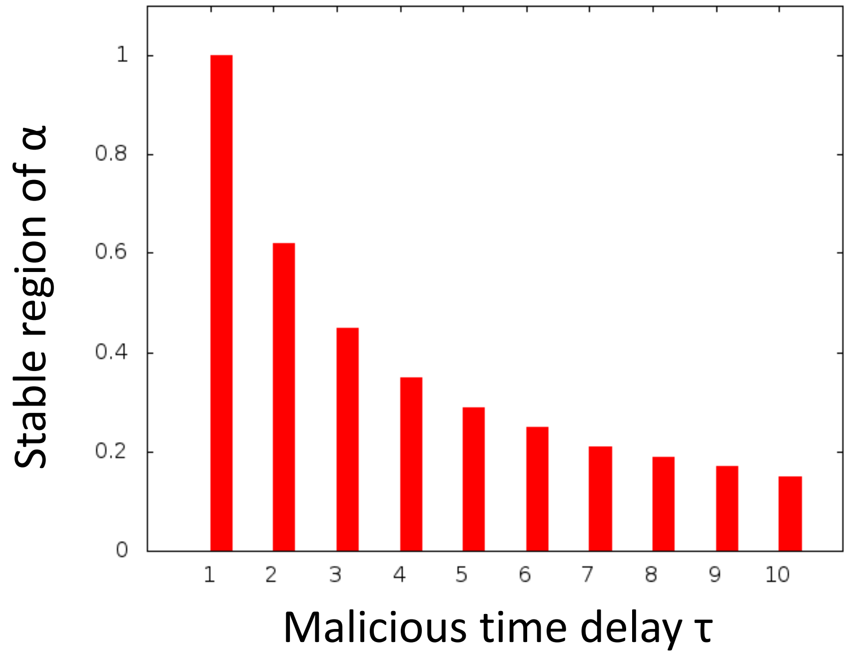
$$\lambda^{\tau+1} - \lambda^{\tau} + \alpha = 0$$

$\mathbf{u}[n] = \alpha \mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[n-\tau])$

  – Stable: All roots in unit circle of complex plane

Stable Region

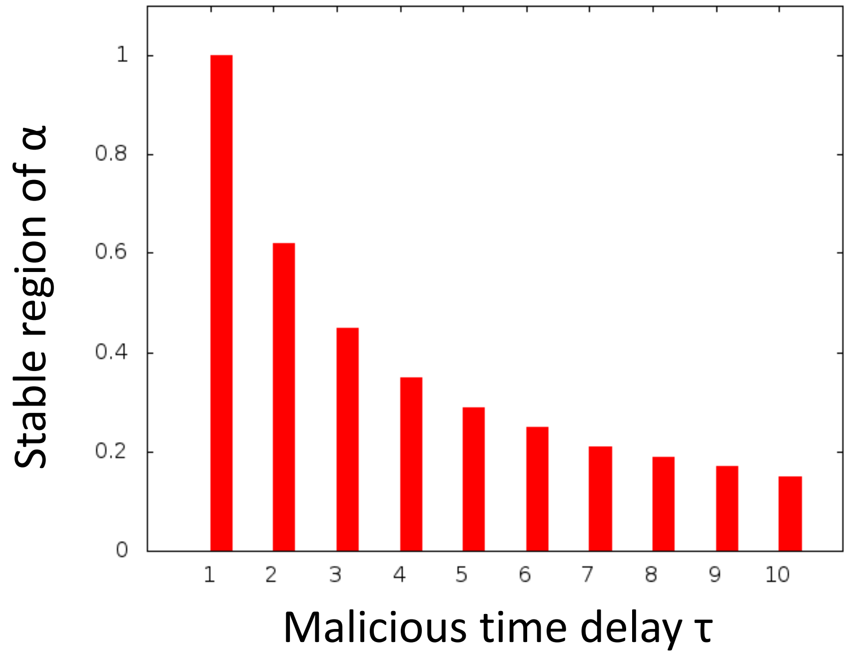
- $\lambda^{\tau+1} - \lambda^{\tau} + \alpha = 0$
  - No closed-form solutions
  - Jury test



Stable Region

- $\lambda^{\tau+1} - \lambda^{\tau} + \alpha = 0$
  - No closed-form solutions
  - Jury test

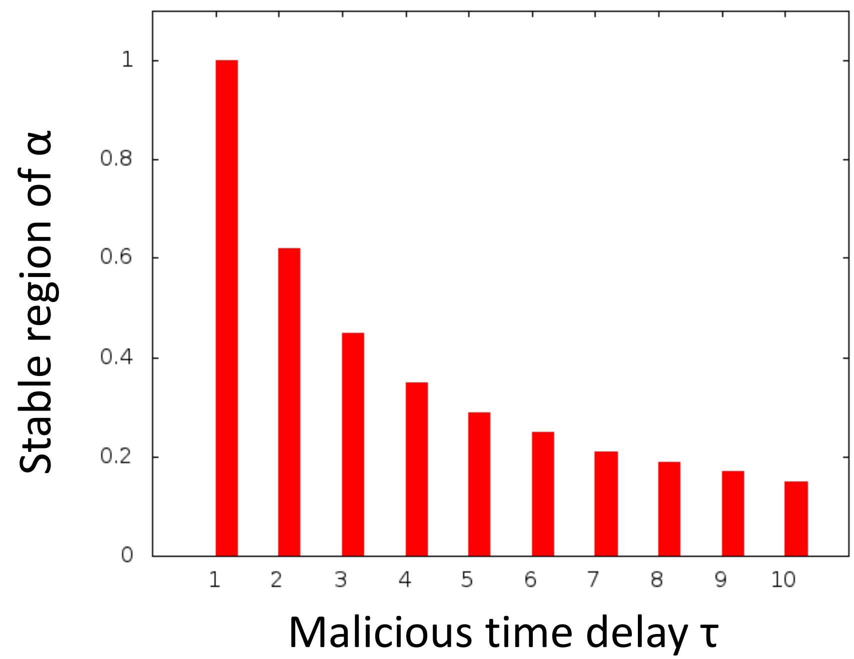
When no attack
- Faster convergence
- Smaller fluctuation



Stable Region

- $\lambda^{\tau+1} - \lambda^{\tau} + \alpha = 0$
  - No closed-form solutions
  - Jury test

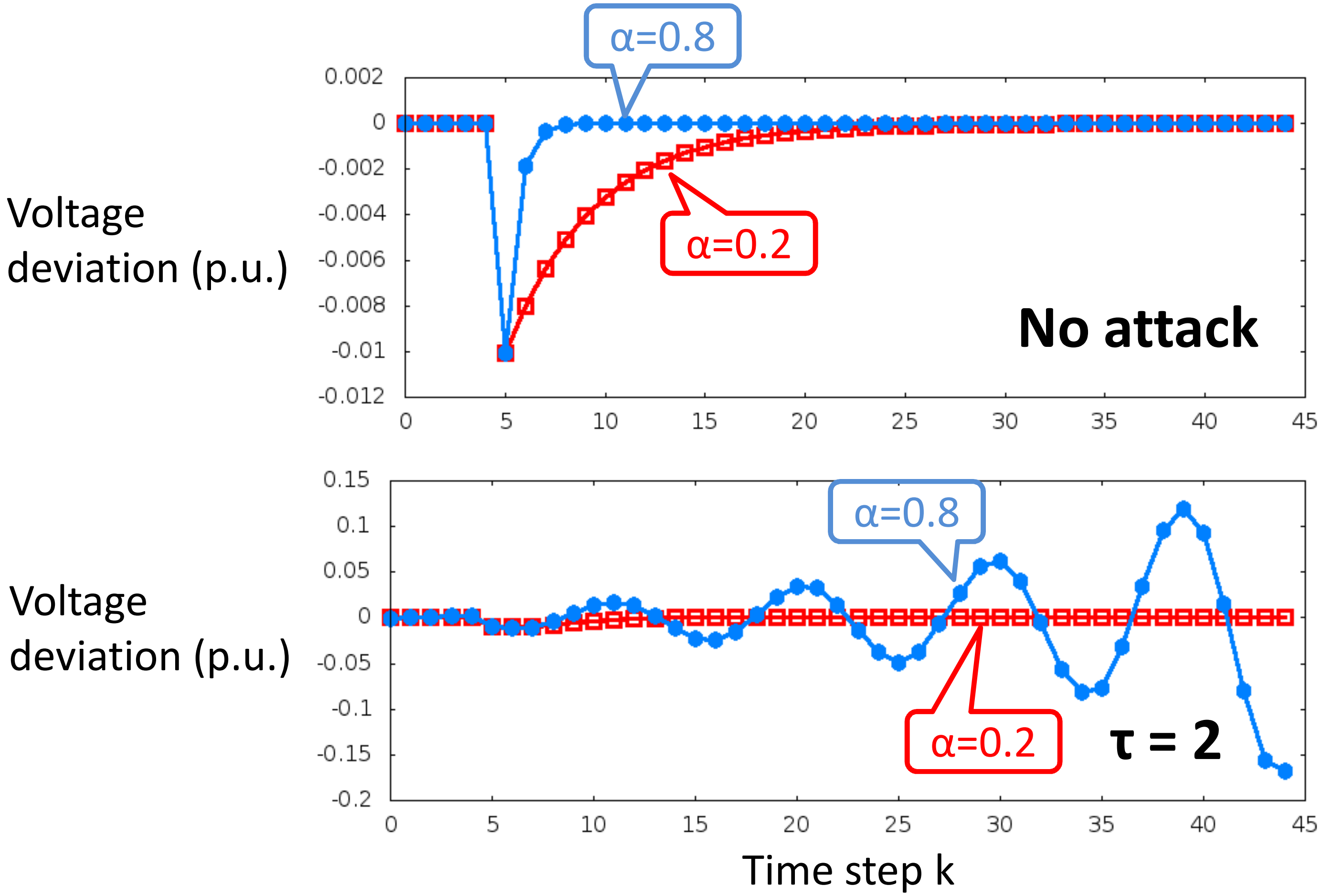
When no attack
- Faster convergence
- Smaller fluctuation



Trade-off btw control performance and tolerable malicious delay

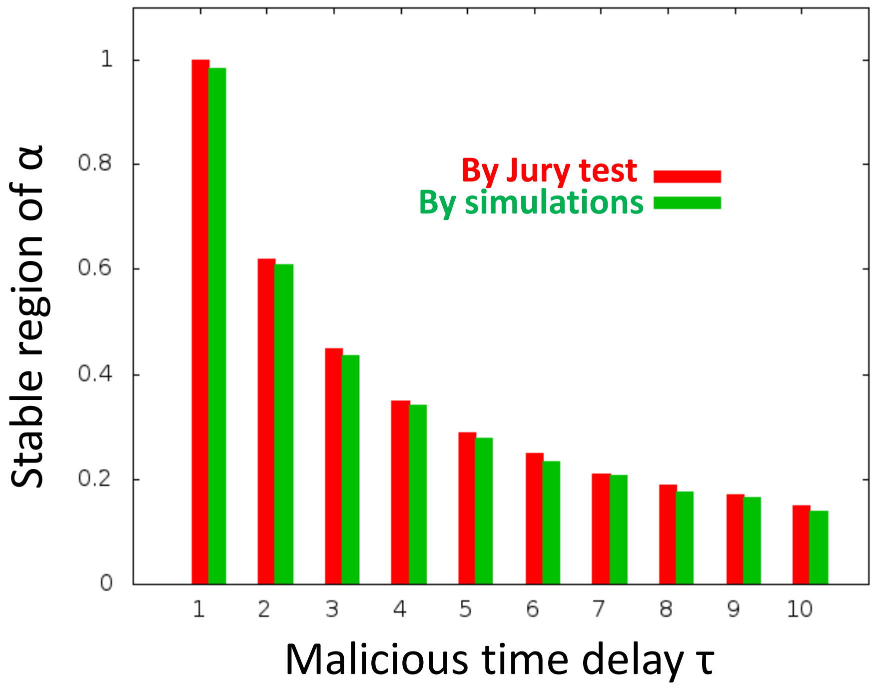
An Example

- PowerWorld simulations
  - 37-bus power system
  - 10 feeder buses under voltage control



Analysis Verification

- Approximations in system modeling
  - Affect accuracy of stability analysis



Summary and Future Work

- Stability condition of voltage control under signal delay attack
- Trade-off between
  - Voltage convergence speed when no attack
  - Tolerable time delay in terms of stability
- Future work
  - Other voltage control approaches
  - Attack mitigation