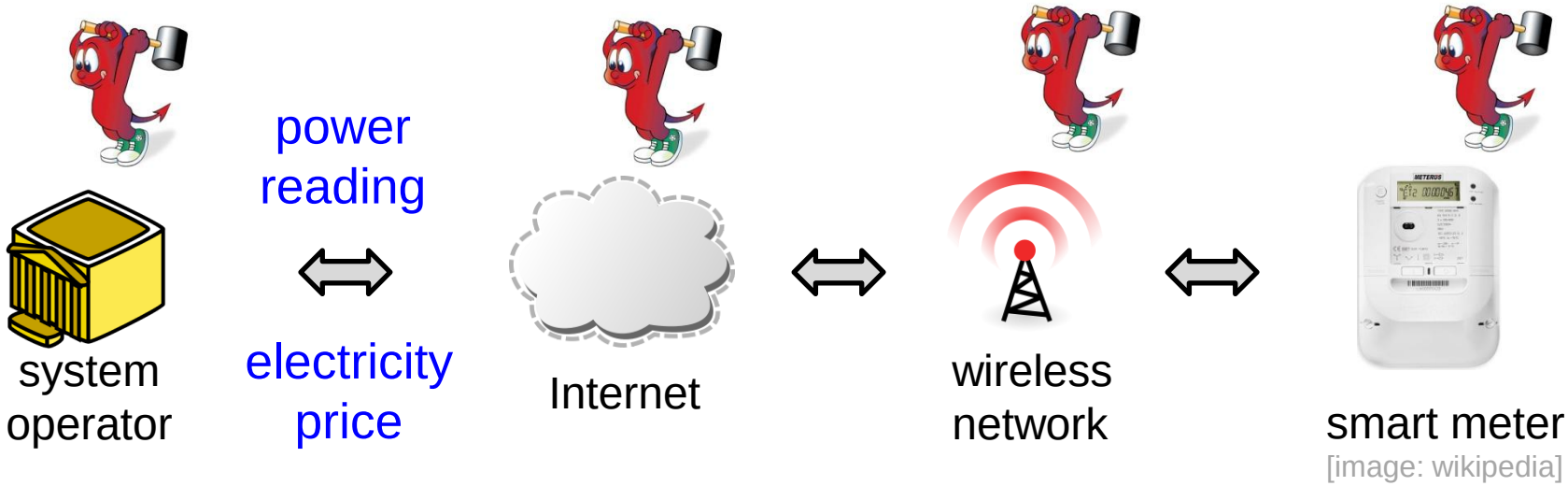
Impact of Integrity Attacks on Real-Time Pricing in Smart Grids

Rui Tan[1] Varun Badrinath Krishna[1]
David K. Y. Yau[1,2] Zbigniew Kalbarczyk[3]

[1]Advanced Digital Sciences Center, Illinois at Singapore
[2]Singapore University of Technology and Design
[3]University of Illinois at Urbana-Champaign

Cyber Attacks on Smart Grids



- Communication and device vulnerabilities incur threats
  - A worm controls **15,000** emulated meters in **24** hours [Blackhat Demo 2009]
  - **40%** of attacks on critical infrastructures target power grids [US DHS 2012]

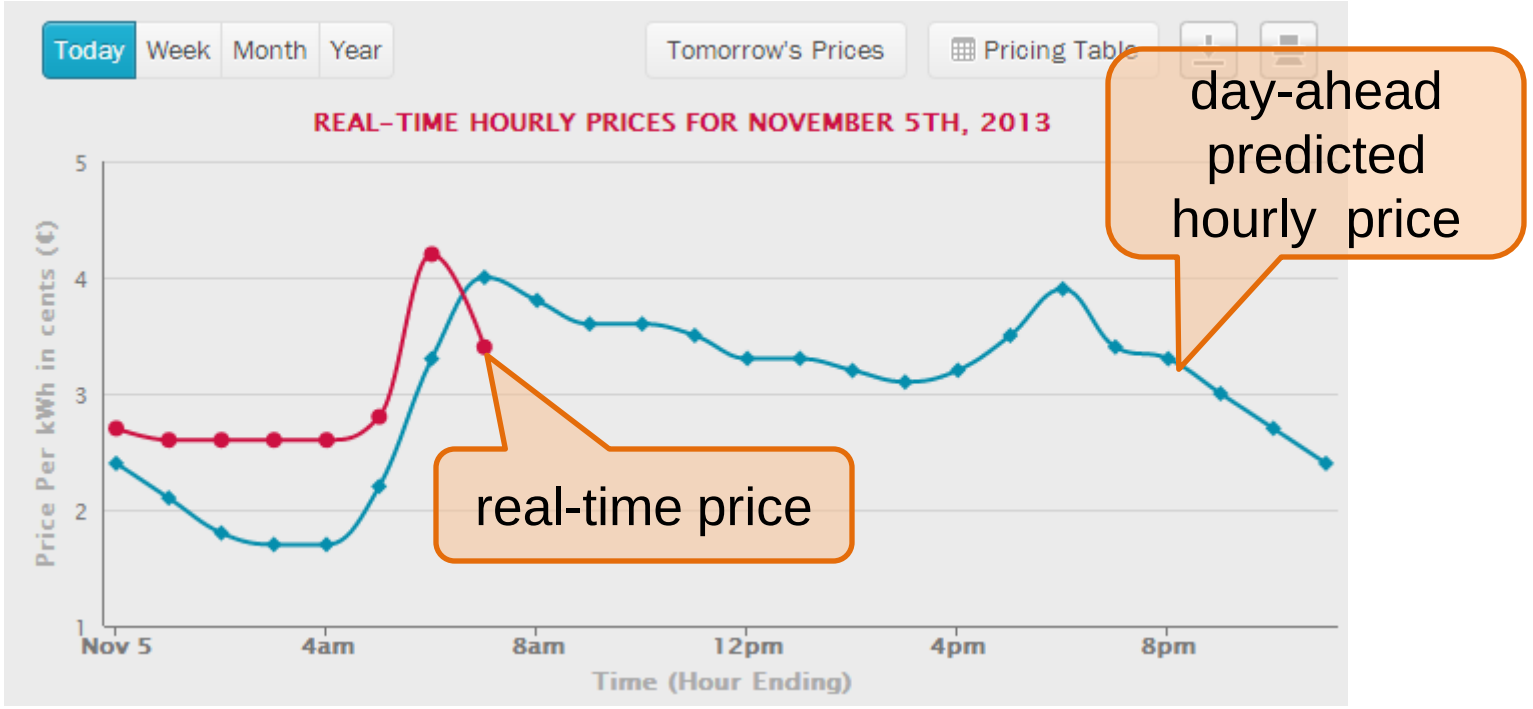
Existing Studies

- False data injection
  - Bypass bad data detection [CCS'09]
  - Disorder grid operations
    - Generation dispatch [TSG'11]
    - Energy routing [ICCPS'12]
    - Wholesale pricing [TSG'11, ICSS'12]

Measurement data in power systems (bus power meters)
vs.
Data to/from smart meters at end users

Real-Time Pricing

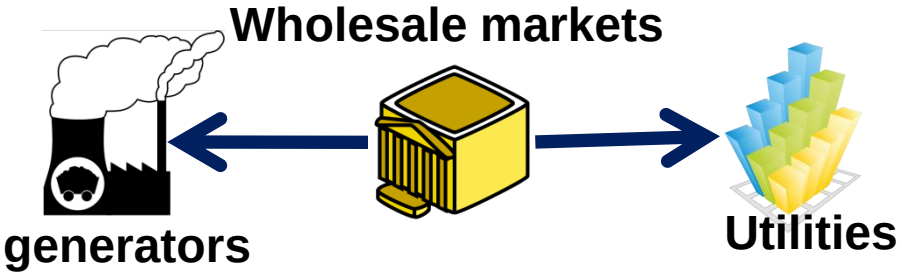
- (Sub-)hourly changing electricity prices
- Reflect market condition and improve efficiency
- Physical impact



Commonwealth Edision Company (ComEd), Illinois
rrtp.comed.com/live-prices

Real-Time Pricing

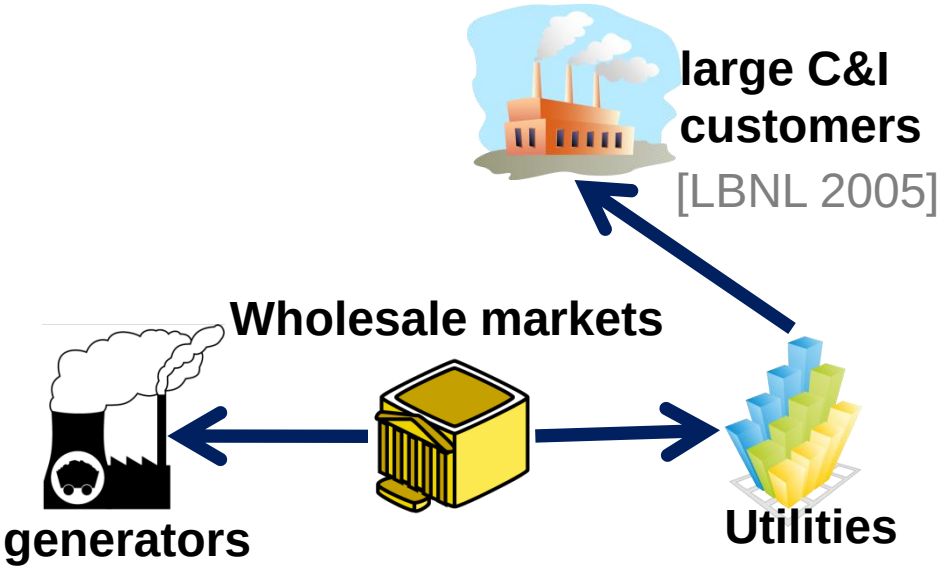
- (Sub-)hourly changing electricity prices
- Reflect market condition and improve efficiency
- Physical impact



price signal

Real-Time Pricing

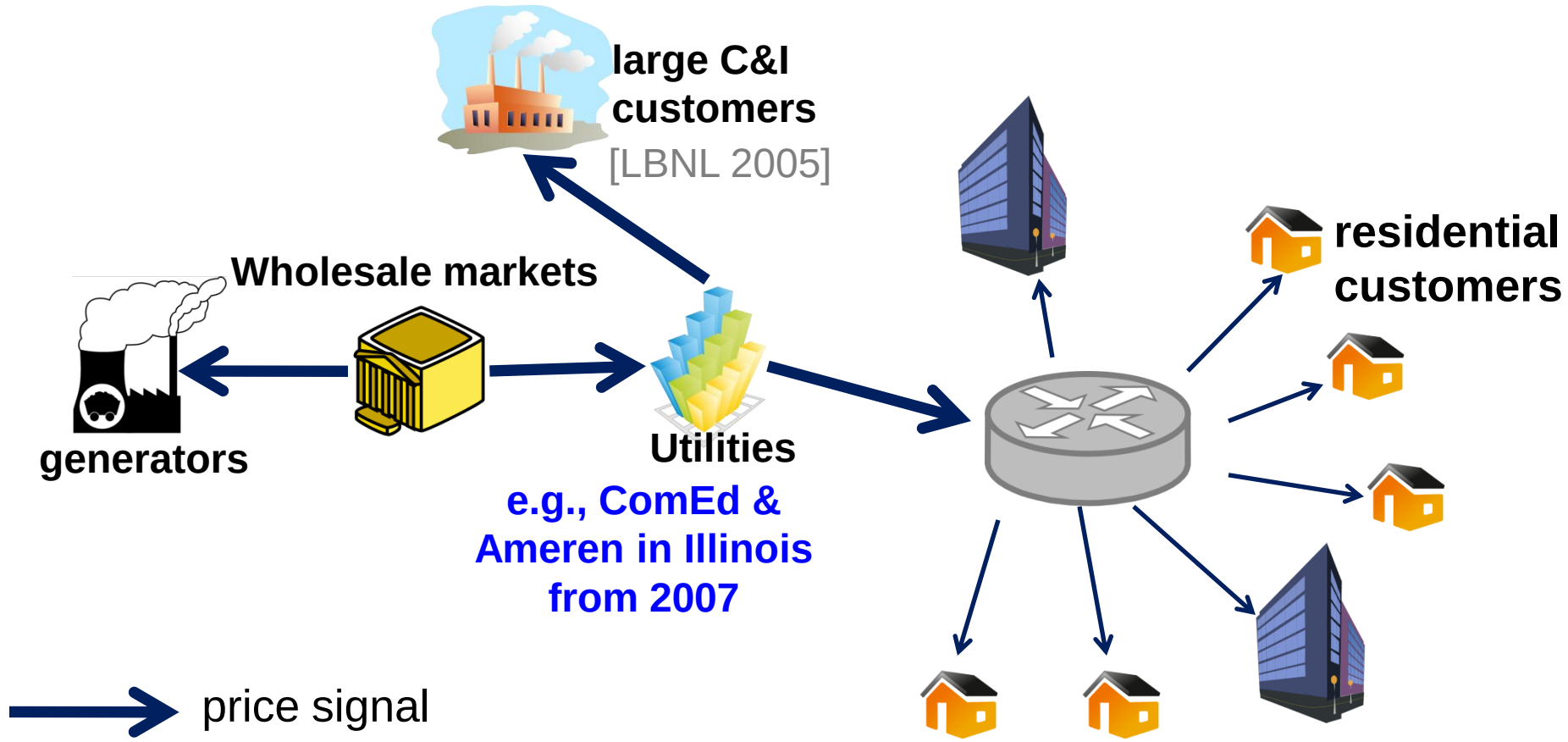
- (Sub-)hourly changing electricity prices
- Reflect market condition and improve efficiency
- Physical impact



price signal

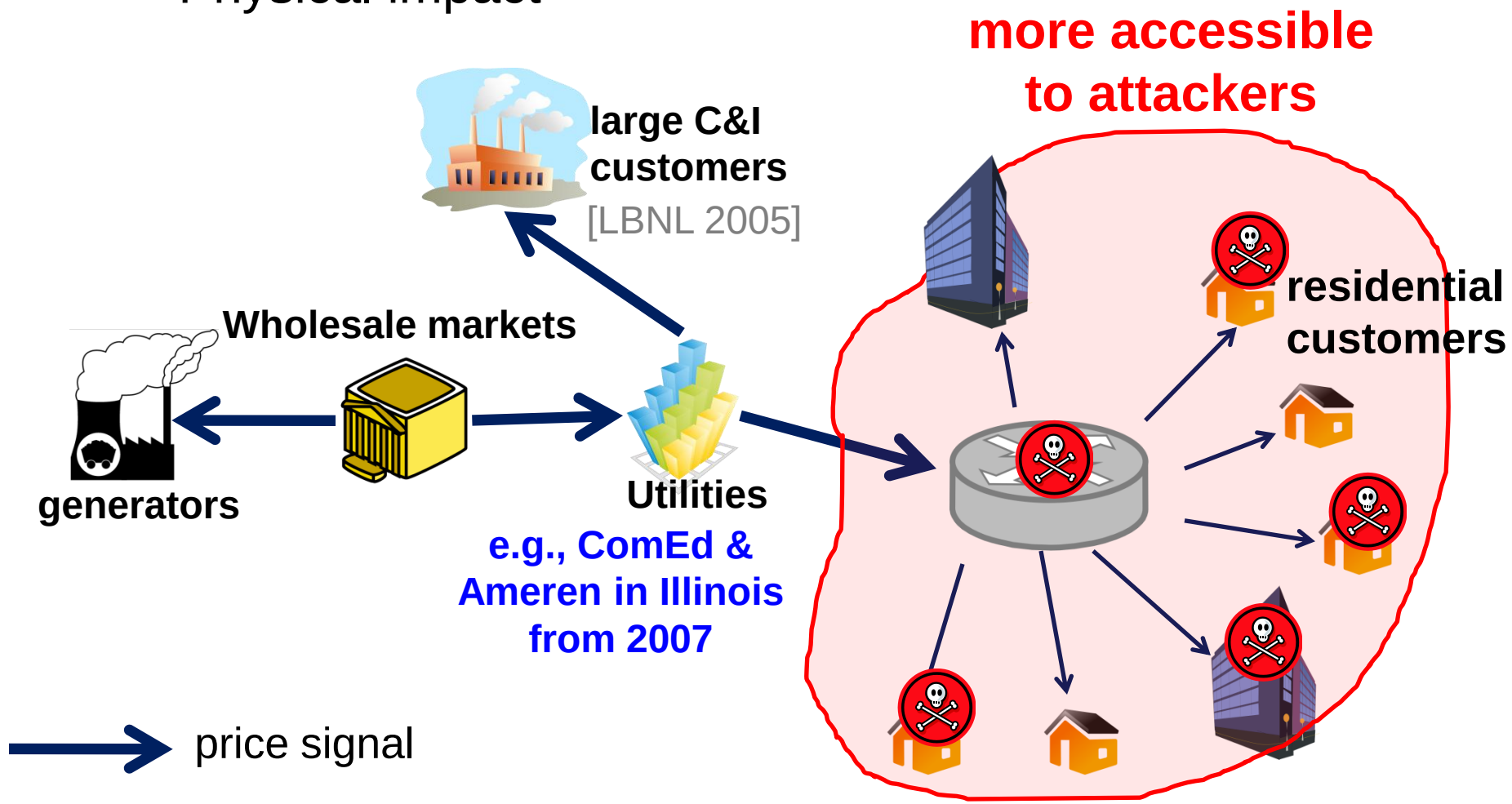
Real-Time Pricing

- (Sub-)hourly changing electricity prices
- Reflect market condition and improve efficiency
- Physical impact



Real-Time Pricing

- (Sub-)hourly changing electricity prices
- Reflect market condition and improve efficiency
- Physical impact



Problem

- Impact of malicious modifications to price signals
  - Can they destabilize the pricing system?

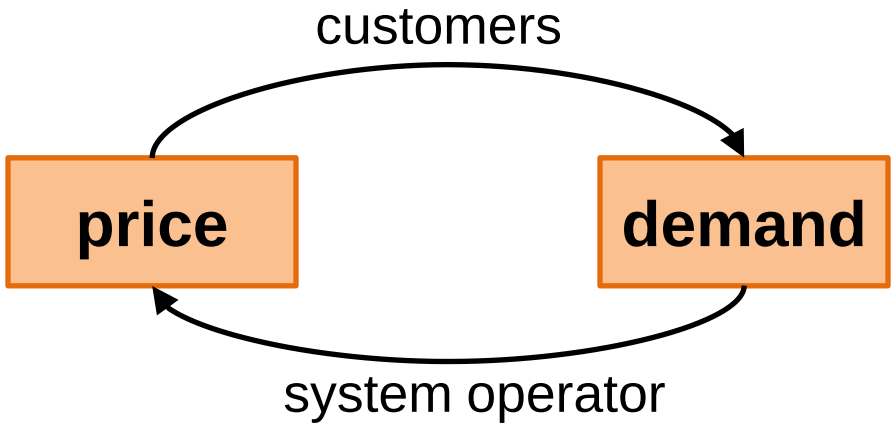
[Image: www.bluephoenixinc.com]

Problem

- Impact of malicious modifications to price signals
  - Can they destabilize the pricing system?

- Closed loop
  - Mutually dependent price and demand
  - Difficult performance analysis
  - Harder with attacks

[Image: www.bluephoenixinc.com]



Outline

- Background & Motivation
- Formulation of Real-Time Pricing
- Impact of Attacks
- Simulations

Pricing Model

price for next period

price for next period

Suppliers

Profit-neutral system operator

Consumers

- System operator
  - Match supply and demand by periodic pricing
  - Same price for suppliers and consumers

ComEd:
Households pay real-time wholesale price from system operator

Supply and Demand Models

- Scheduled supply

$$s(\lambda) = \sum_i s_i(\lambda)$$

  - λ: price

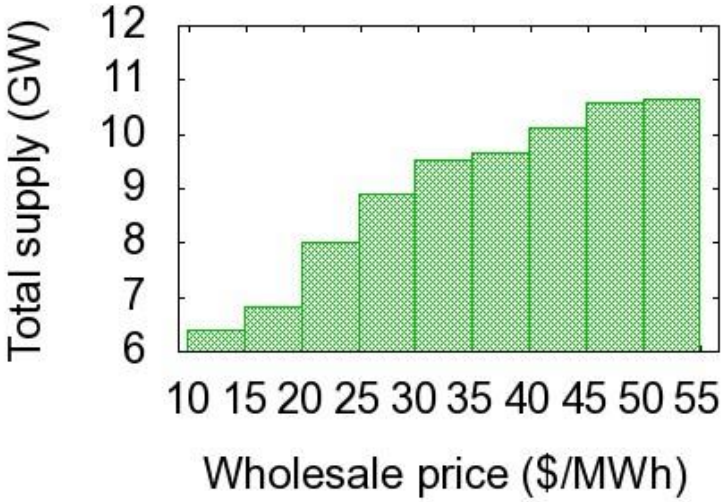
Supply and Demand Models

- Scheduled supply

$$s(\lambda) = \sum_i s_i(\lambda)$$

A supplier (increasing)

  - λ: price



Australian Energy Market Operator

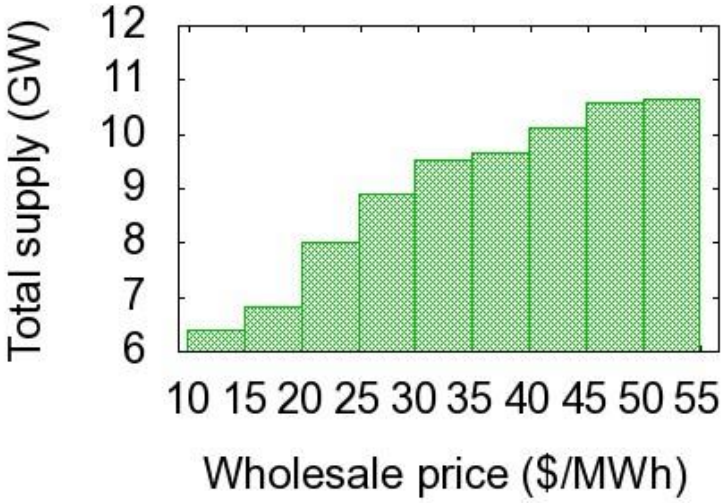
Supply and Demand Models

- Scheduled supply

$$s(\lambda) = \sum_i s_i(\lambda)$$

A supplier (increasing)

  - λ: price



Australian Energy Market Operator

- Demand

$$d(\lambda) = \sum_i e_i(\lambda) + \text{baseline}_i$$

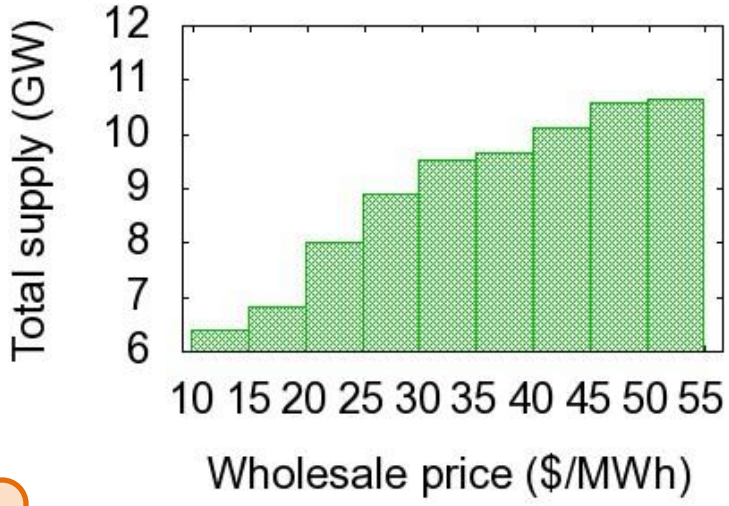
Supply and Demand Models

- Scheduled supply

$$s(\lambda) = \sum_i s_i(\lambda)$$

A supplier (increasing)

  - λ: price



Australian Energy Market Operator

- Demand

elastic demand (decreasing)

$$d(\lambda) = \sum_i e_i(\lambda) + \text{baseline}_i$$

time-varying

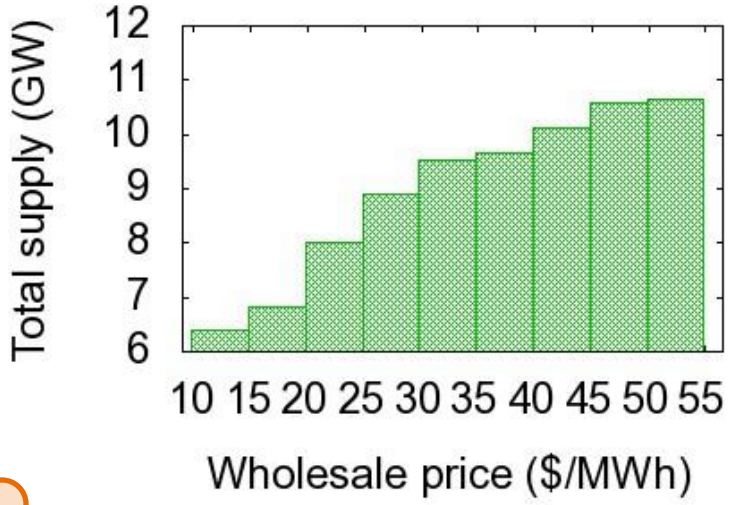
Supply and Demand Models

- Scheduled supply

$$s(\lambda) = \sum_i s_i(\lambda)$$

A supplier (increasing)

  - λ: price



Australian Energy Market Operator

- Demand

elastic demand (decreasing)

$$d(\lambda) = \sum e_i(\lambda) + \text{baseline}_i$$

time-varying

  - Human-induced demand response
  - Smart appliances
    (e.g., ComEd's price-based air conditioning cycling)

Principles of Current Schemes

- Find ex-ante price λ_k for k^{th} pricing period

$$s(\lambda_k) = d(\lambda_k)$$

Principles of Current Schemes

- Find ex-ante price λ_k for k^{th} pricing period

$$s(\lambda_k) = d(\lambda_k)$$

known unknown

Principles of Current Schemes

- Find ex-ante price λ_k for k^{th} pricing period

$$s(\lambda_k) = d(\lambda_k) \Rightarrow s(\lambda_k) = \tilde{d}(\lambda_k)$$

known unknown predicted

Principles of Current Schemes

- Find ex-ante price λ_k for k^{th} pricing period

$$s(\lambda_k) = d(\lambda_k) \Rightarrow s(\lambda_k) = \tilde{d}(\lambda_k)$$

known unknown predicted

- Autoregressive prediction
  - Unstable closed loop [Roozbehani 2012]

$$s(\lambda_k) = d(\lambda_{k-1})$$

Principles of Current Schemes

- Find ex-ante price λ_k for k^{th} pricing period

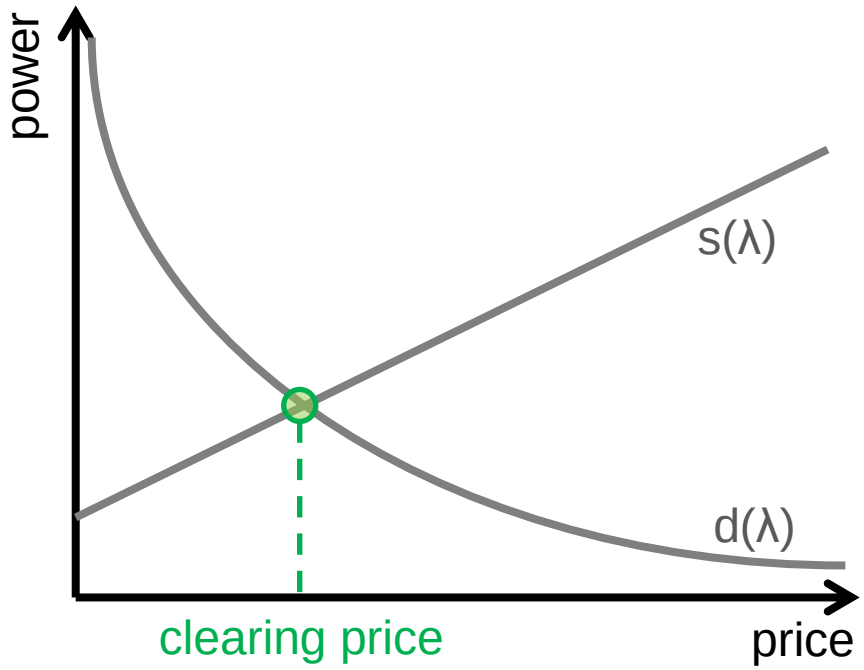
$$s(\lambda_k) = d(\lambda_k) \Rightarrow s(\lambda_k) = \tilde{d}(\lambda_k)$$

known — unknown — predicted

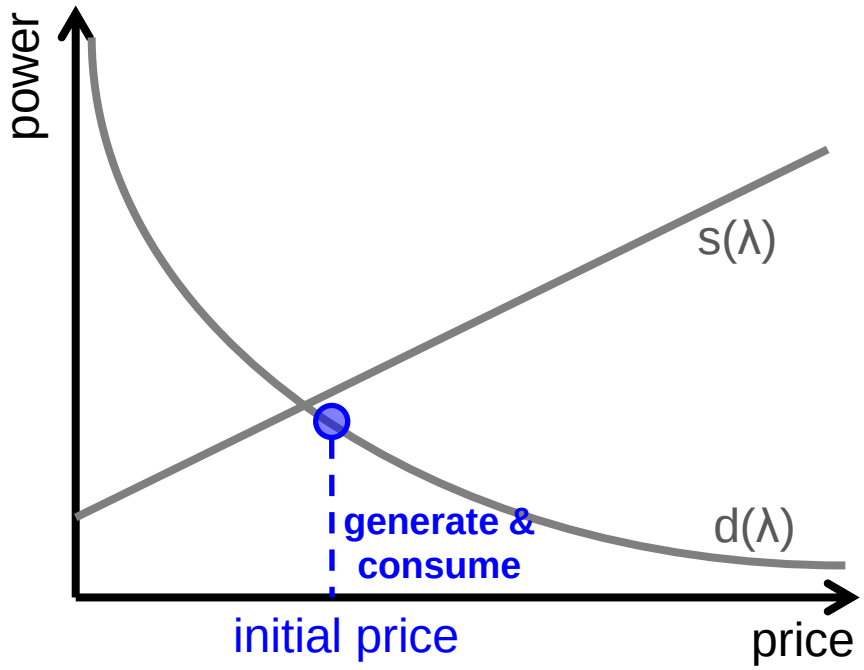
- Autoregressive prediction
  - Unstable closed loop [Roozbehani 2012]

$$s(\lambda_k) = d(\lambda_{k-1}) \Rightarrow \lambda_k = s^{-1}(d(\lambda_{k-1}))$$

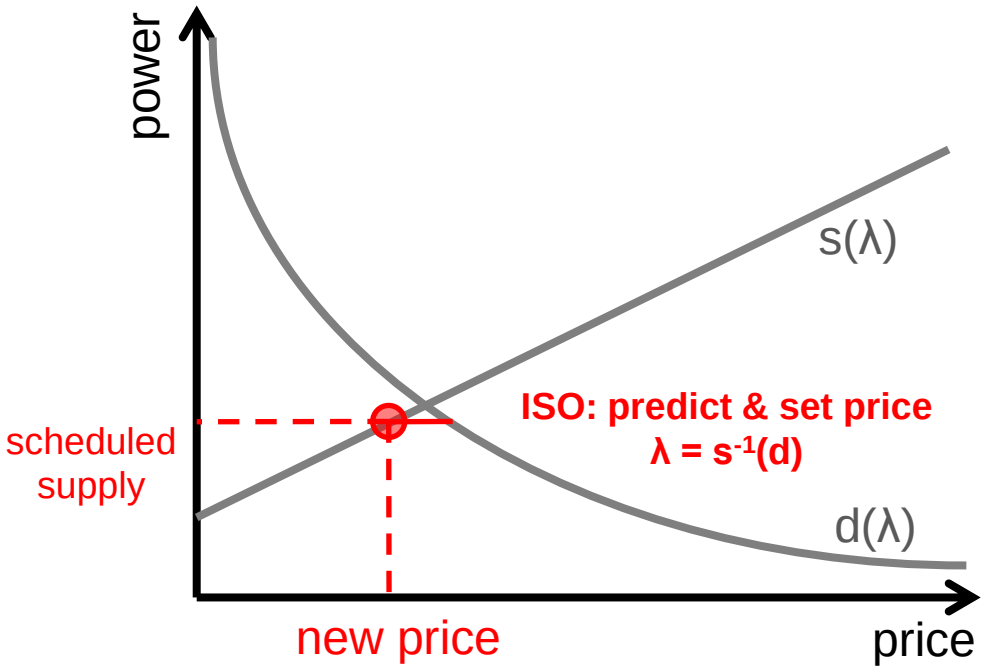
Unstable Real-Time Pricing



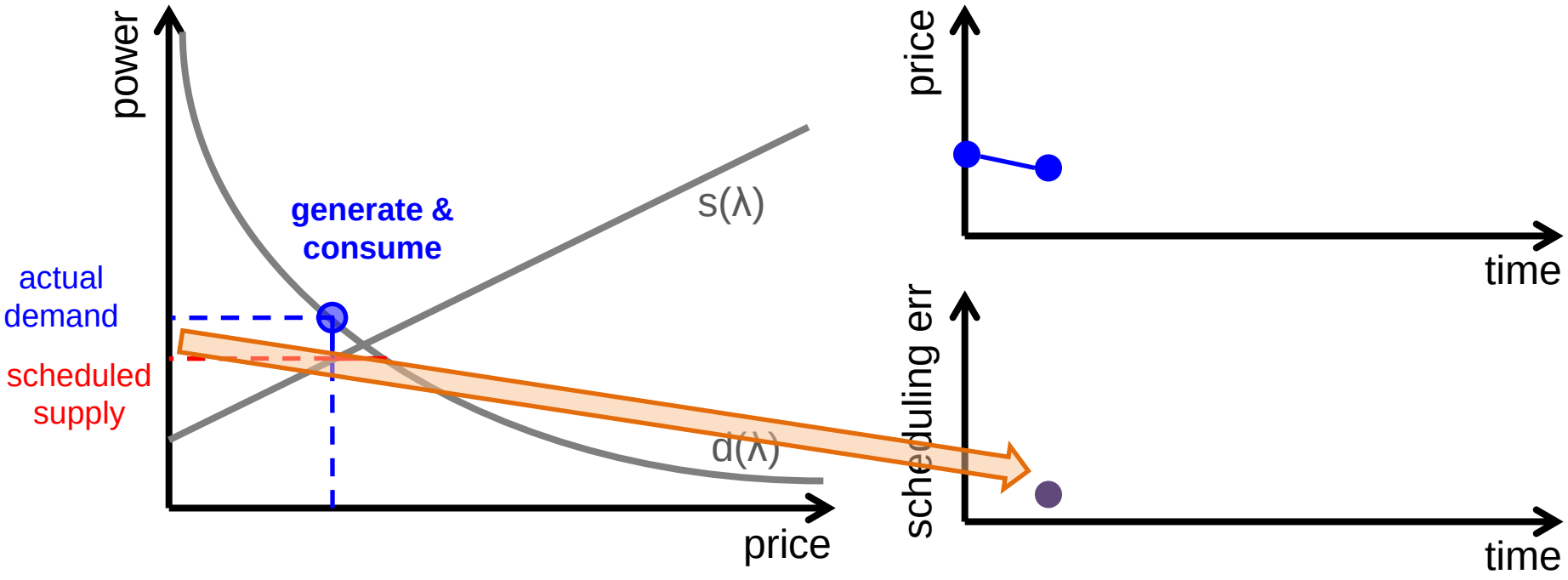
Unstable Real-Time Pricing



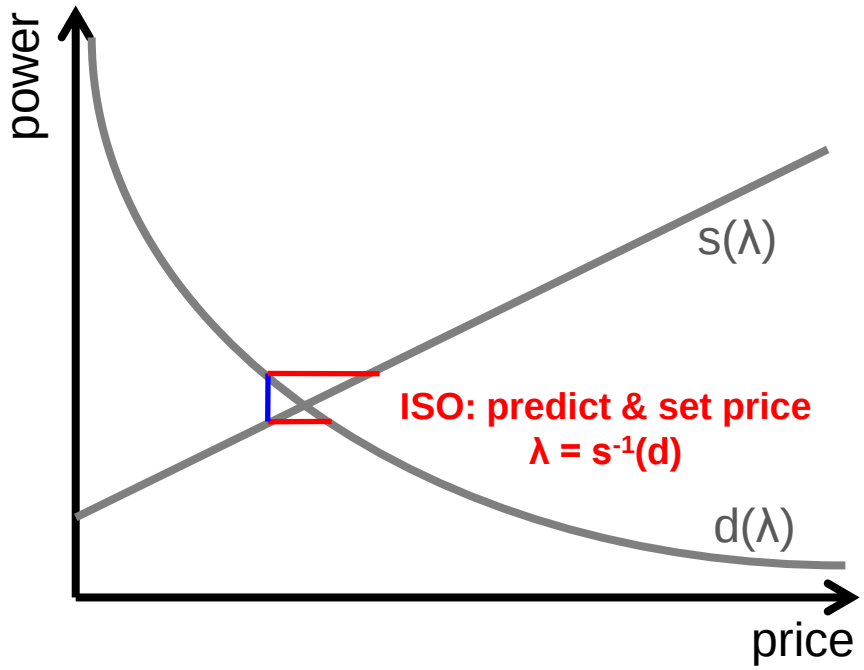
Unstable Real-Time Pricing

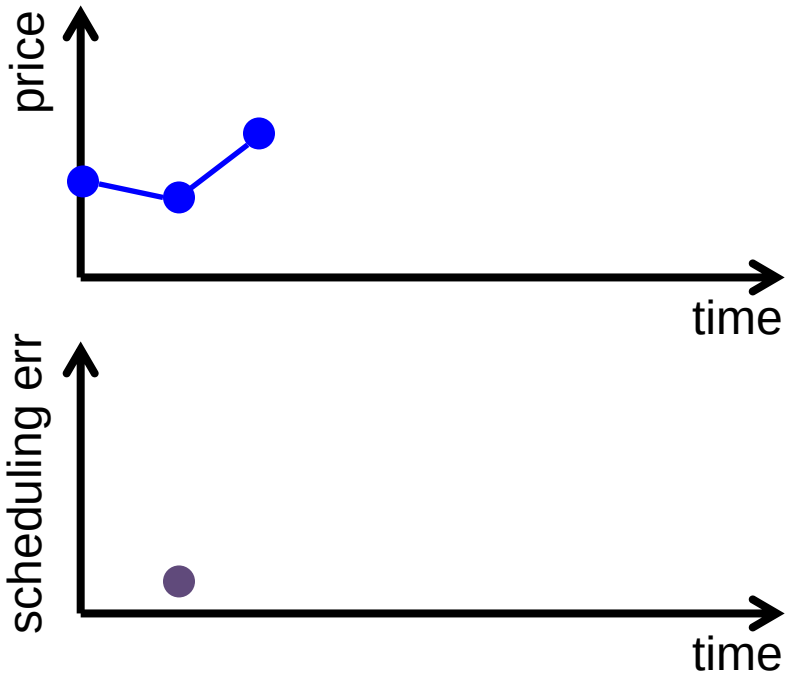


Unstable Real-Time Pricing

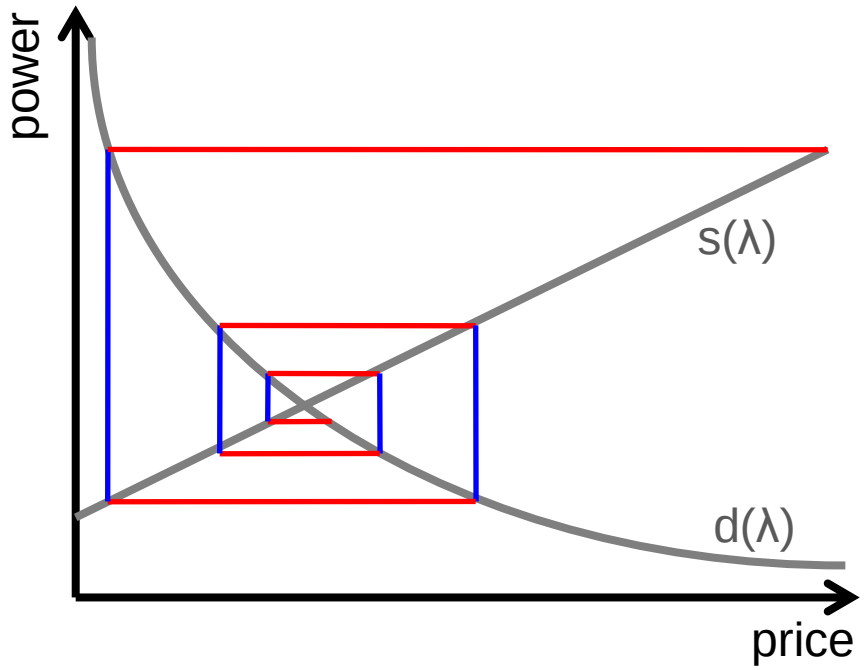


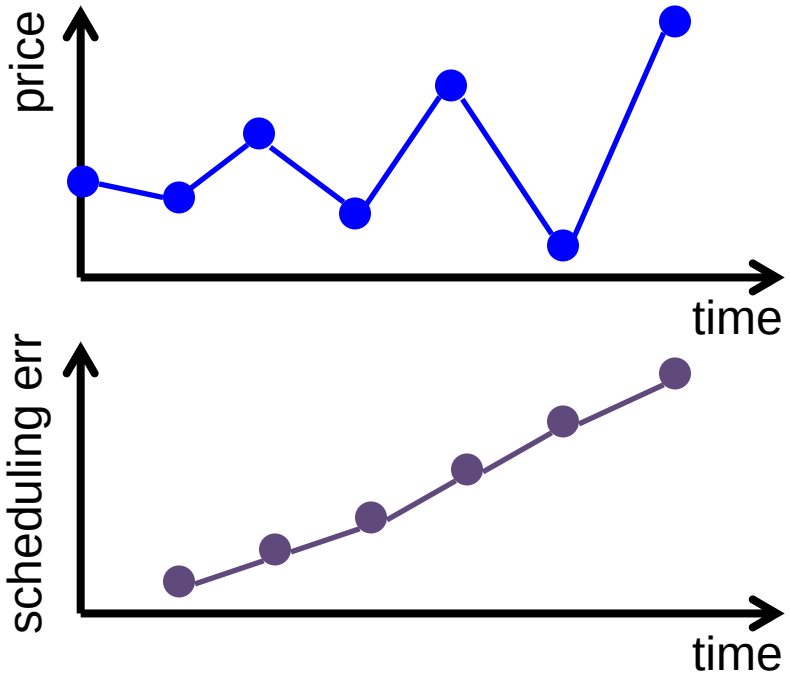
Unstable Real-Time Pricing



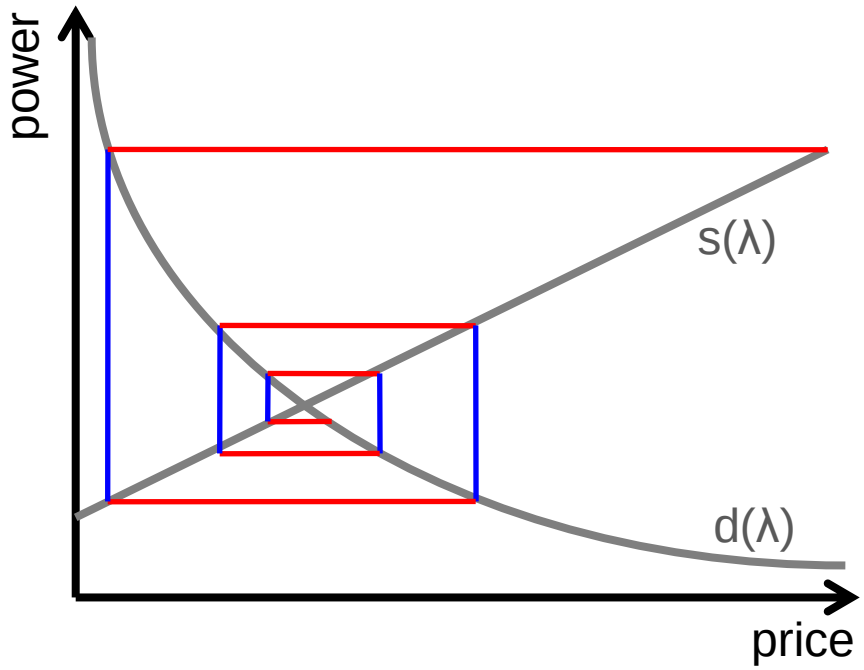


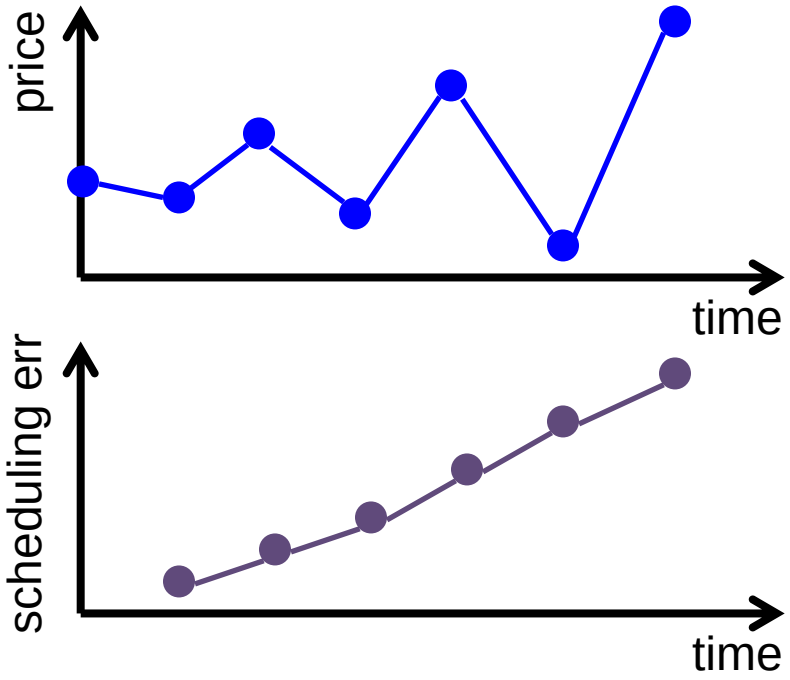
Unstable Real-Time Pricing





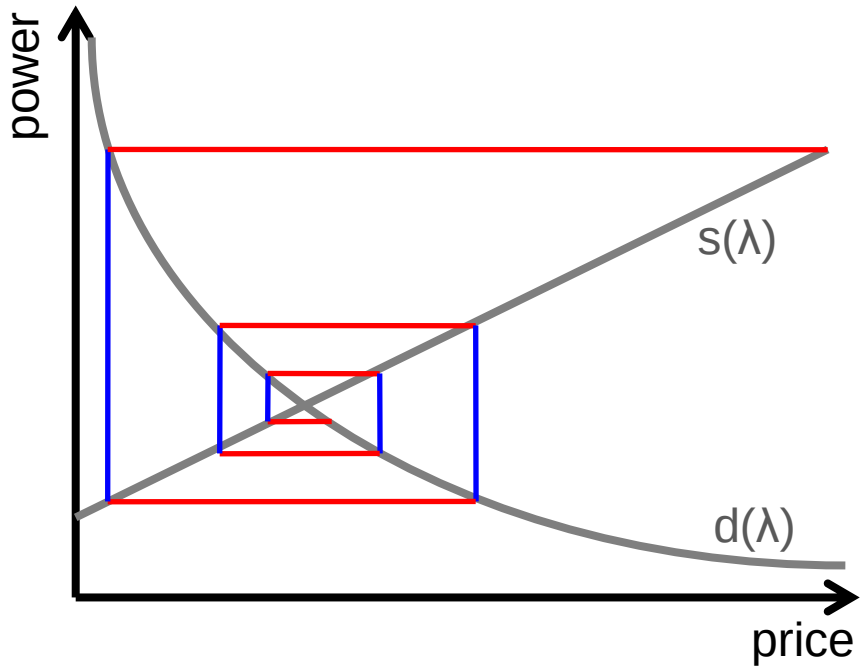
Unstable Real-Time Pricing

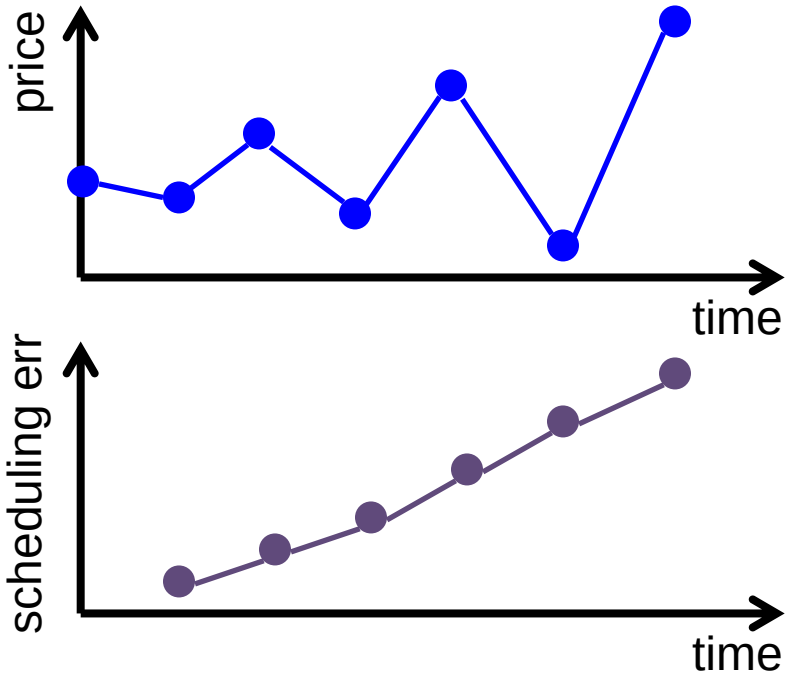




- Oscillating or diverging price
  - Overloaded power networks
  - Increased operational cost

Unstable Real-Time Pricing



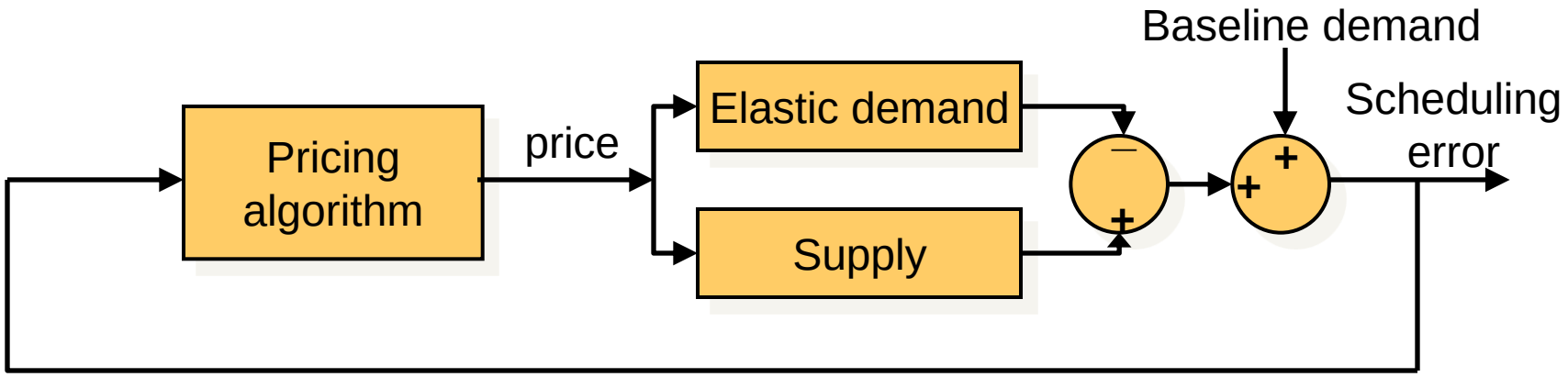


- Oscillating or diverging price
  - Overloaded power networks
  - Increased operational cost
- Stable solution is desirable

Control-Theoretic Solution

– Set price based on observed scheduling error

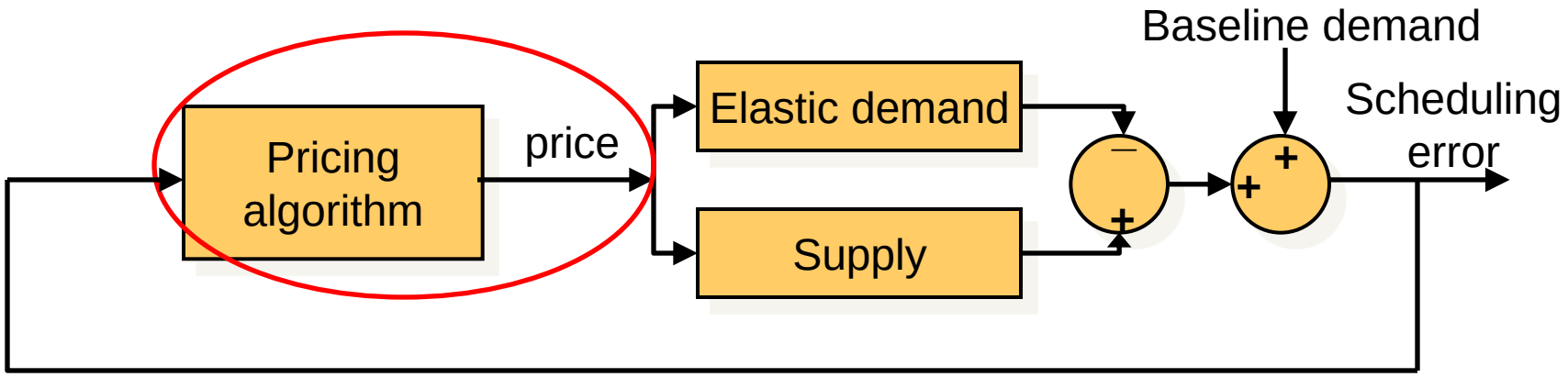
scheduling error = scheduled supply – actual demand



Control-Theoretic Solution

– Set price based on observed scheduling error

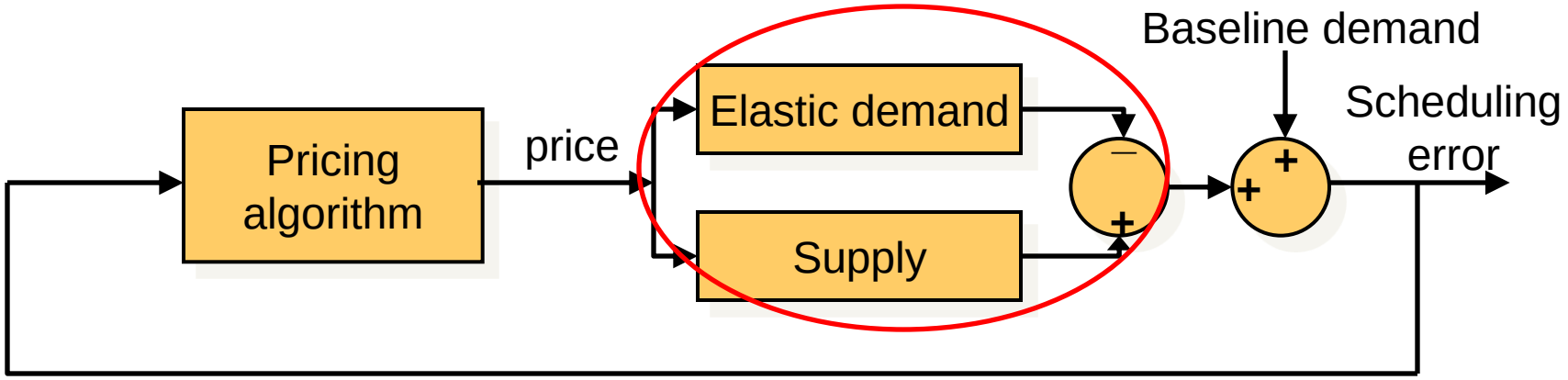
scheduling error = scheduled supply – actual demand



Control-Theoretic Solution

– Set price based on observed scheduling error

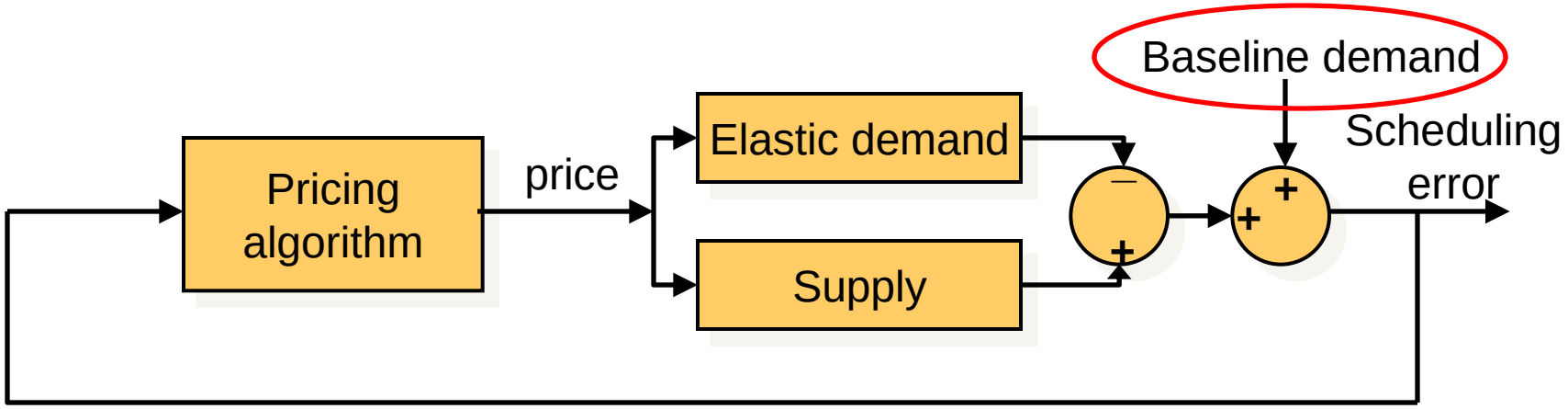
scheduling error = scheduled supply – actual demand



Control-Theoretic Solution

– Set price based on observed scheduling error

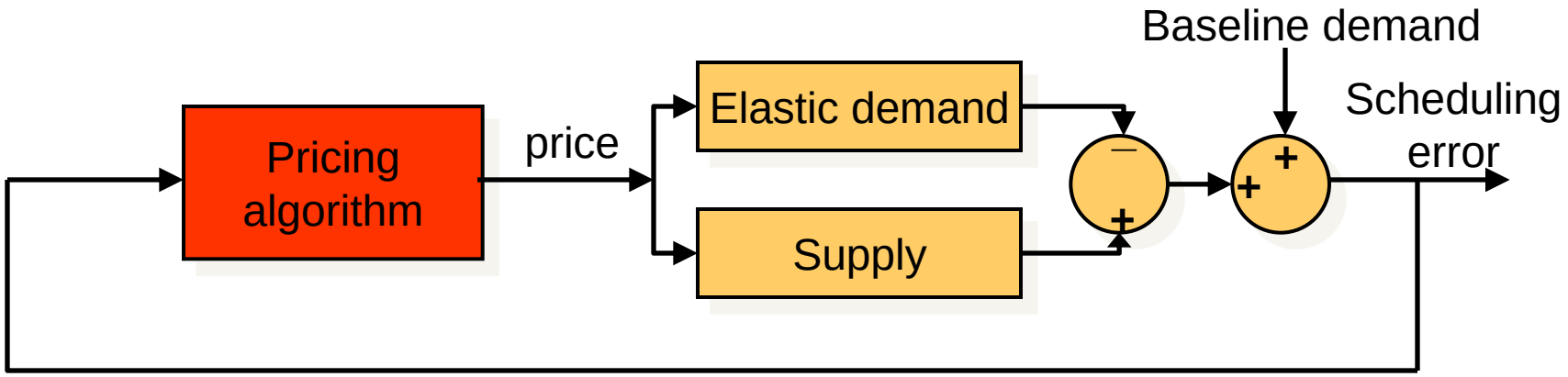
scheduling error = scheduled supply – actual demand



Control-Theoretic Solution

– Set price based on observed scheduling error

scheduling error = scheduled supply – actual demand

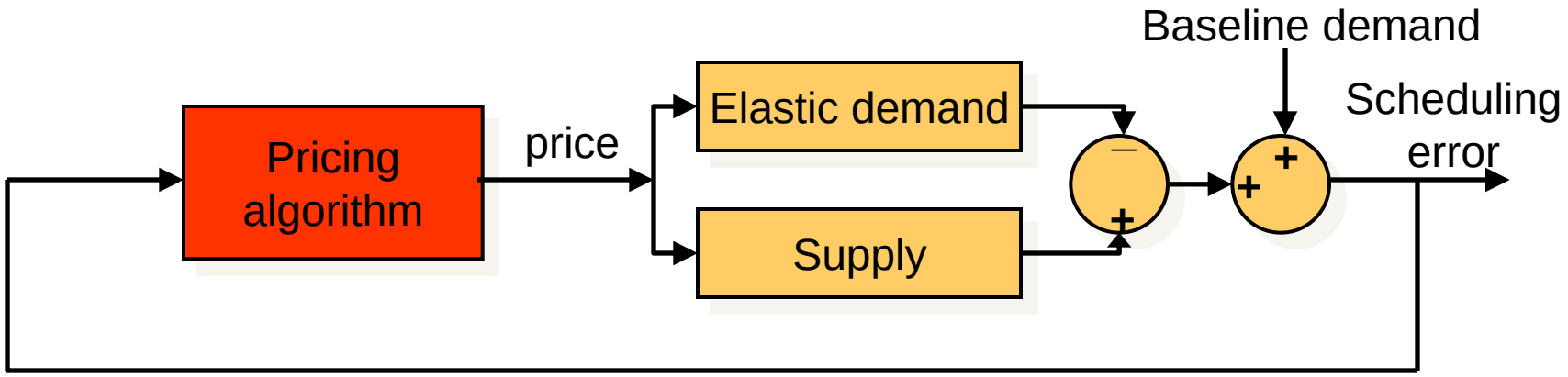


$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

Control-Theoretic Solution

– Set price based on observed scheduling error

scheduling error = scheduled supply – actual demand



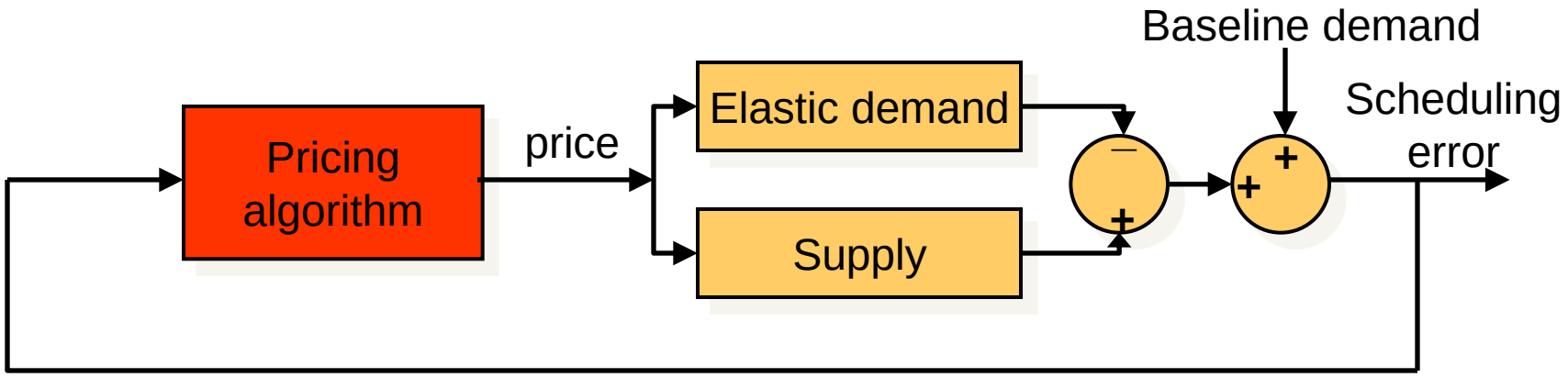
$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

scheduling error

Control-Theoretic Solution

– Set price based on observed scheduling error

scheduling error = scheduled supply – actual demand



gain ∈ (0,1)

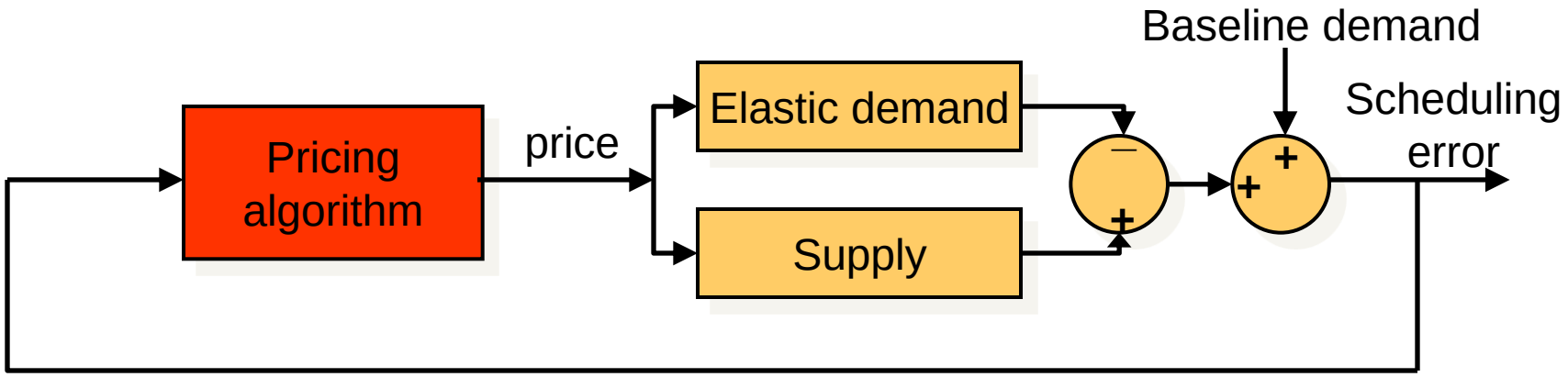
$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

scheduling error

Control-Theoretic Solution

– Set price based on observed scheduling error

scheduling error = scheduled supply – actual demand



gain ∈ (0,1)

$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

scheduling error

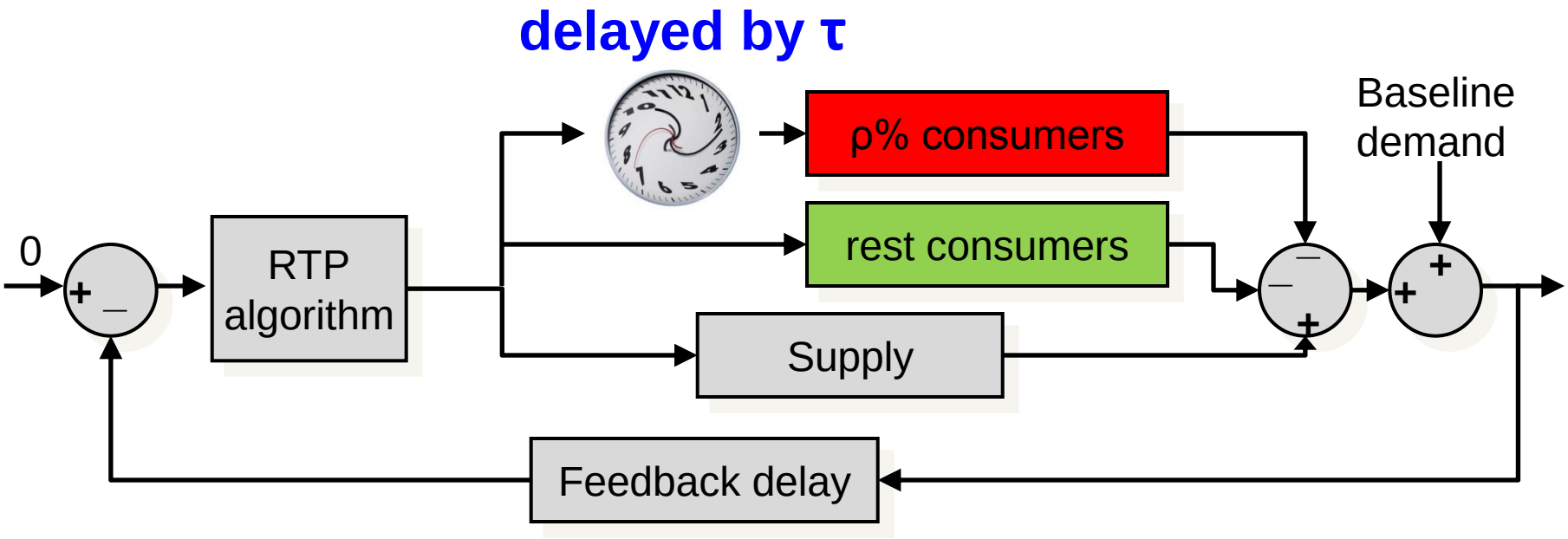
func of last price

Outline

- Background & Motivation
- Formulation of Real-Time Pricing
- Impact of Attacks
- Simulations

Attack Models

- Delay attack



ρ: capability of attacker

τ: intensity of attack

- Scaling attack (skip)

Attack Realization

- Follow certain rules (delay & scale)
  - Lower capability & resource requirements
  - Direct modifications to data packets
  - Launch indirectly

Attack Realization

- Follow certain rules (delay & scale)
  - Lower capability & resource requirements
  - Direct modifications to data packets
  - Launch indirectly

true time

Pricing Period	Price ($/MWh)
[1pm, 2pm]	10
[2pm, 3pm]	11

Attack Realization

- Follow certain rules (delay & scale)
  - Lower capability & resource requirements
  - Direct modifications to data packets
  - Launch indirectly

true time

Pricing Period	Price ($/MWh)
[1pm, 2pm]	10
[2pm, 3pm]	11

meter clock

Attack Realization

- Follow certain rules (delay & scale)
  - Lower capability & resource requirements
  - Direct modifications to data packets
  - Launch indirectly

true time

Pricing Period	Price ($/MWh)
[1pm, 2pm]	10
[2pm, 3pm]	11

meter clock

Attack Realization

- Follow certain rules (delay & scale)
  - Lower capability & resource requirements
  - Direct modifications to data packets
  - Launch indirectly

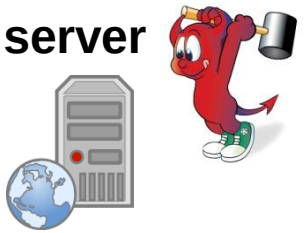
Large-scale spoofing [CCS'12]

true time

Pricing Period	Price ($/MWh)
[1pm, 2pm]	10
[2pm, 3pm]	11

meter clock

time server



NTPd vulnerabilities
CVE-2009-3563
CVE-2009-1252
CVE-2009-0159
…

Region of Stability

- Region of η for stability under attack

$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

  – Time-varying baseline demand tracking quality

Region of Stability

- Region of η for stability under attack

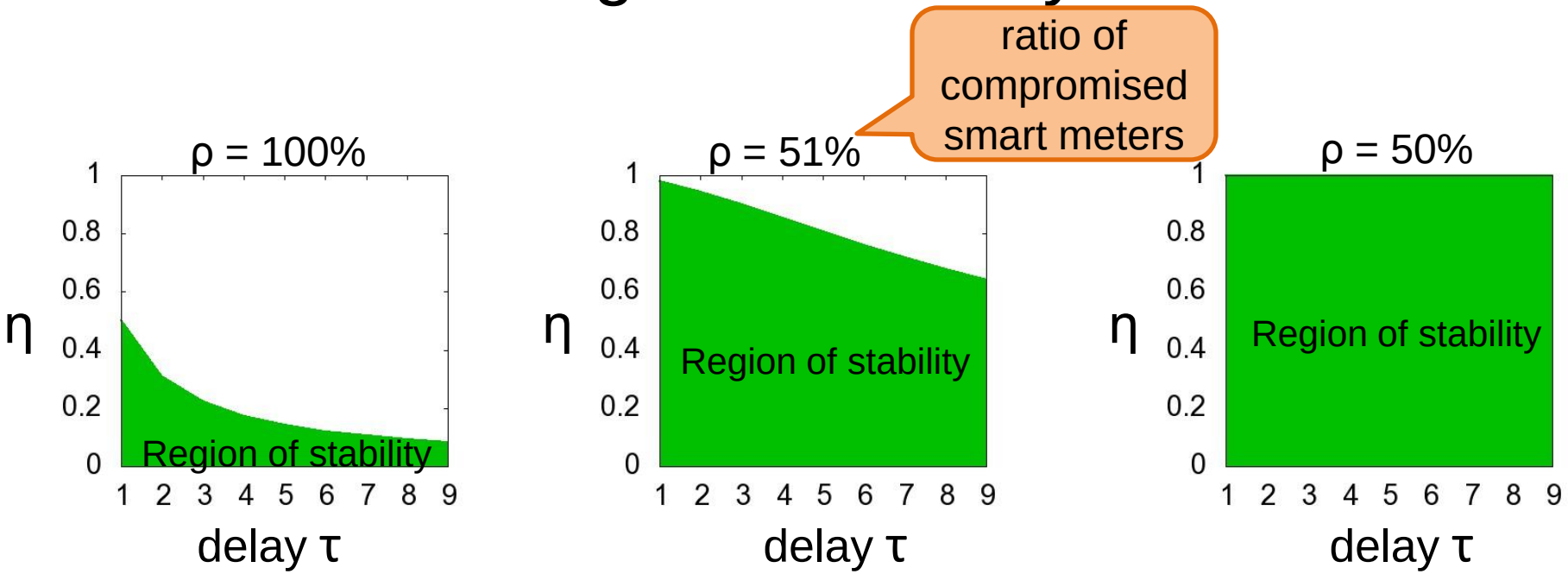
$$\lambda_k = \lambda_{k-1} + \frac{2 \cdot \eta}{f(\lambda_{k-1})} \cdot (s_{k-1} - d_{k-1})$$

  – Time-varying baseline demand tracking quality

- Smaller region of stability
  – Less flexibility in tuning tracking performance subject to stability under attacks

Analytical Results

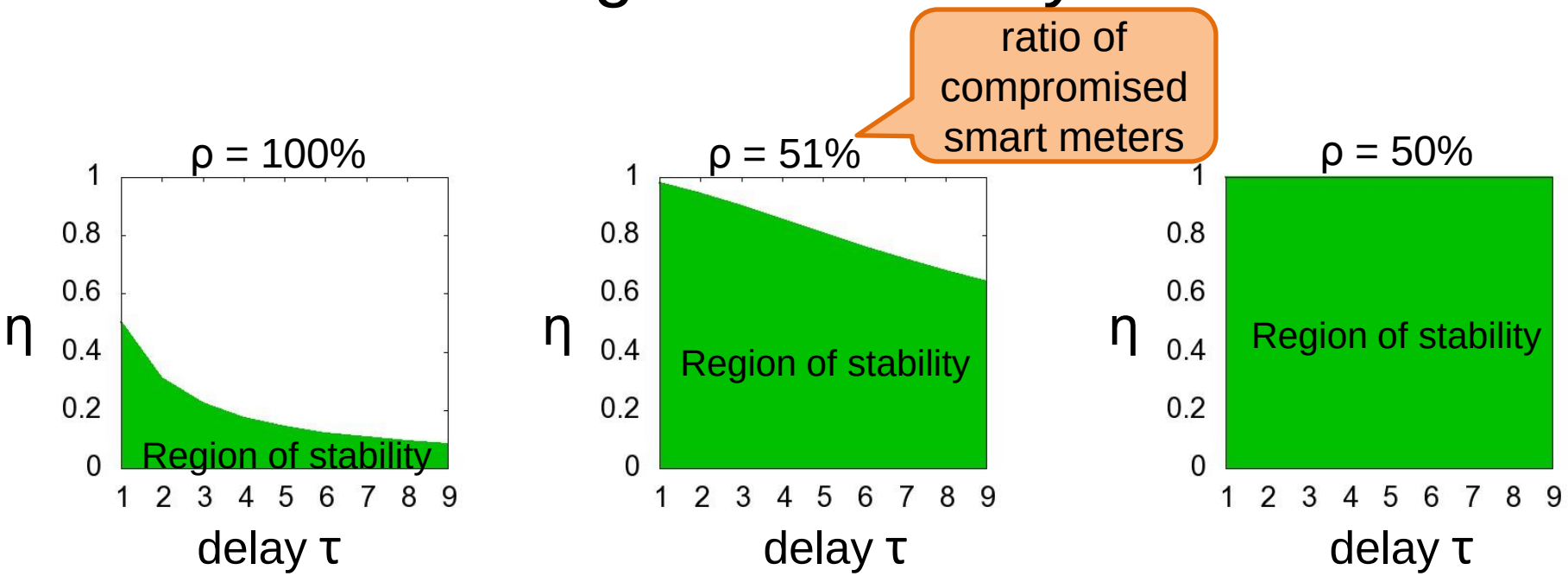
- Closed-form region of stability



shrinks with delay (τ) and ratio of compromised smart meters (ρ)

Analytical Results

- Closed-form region of stability

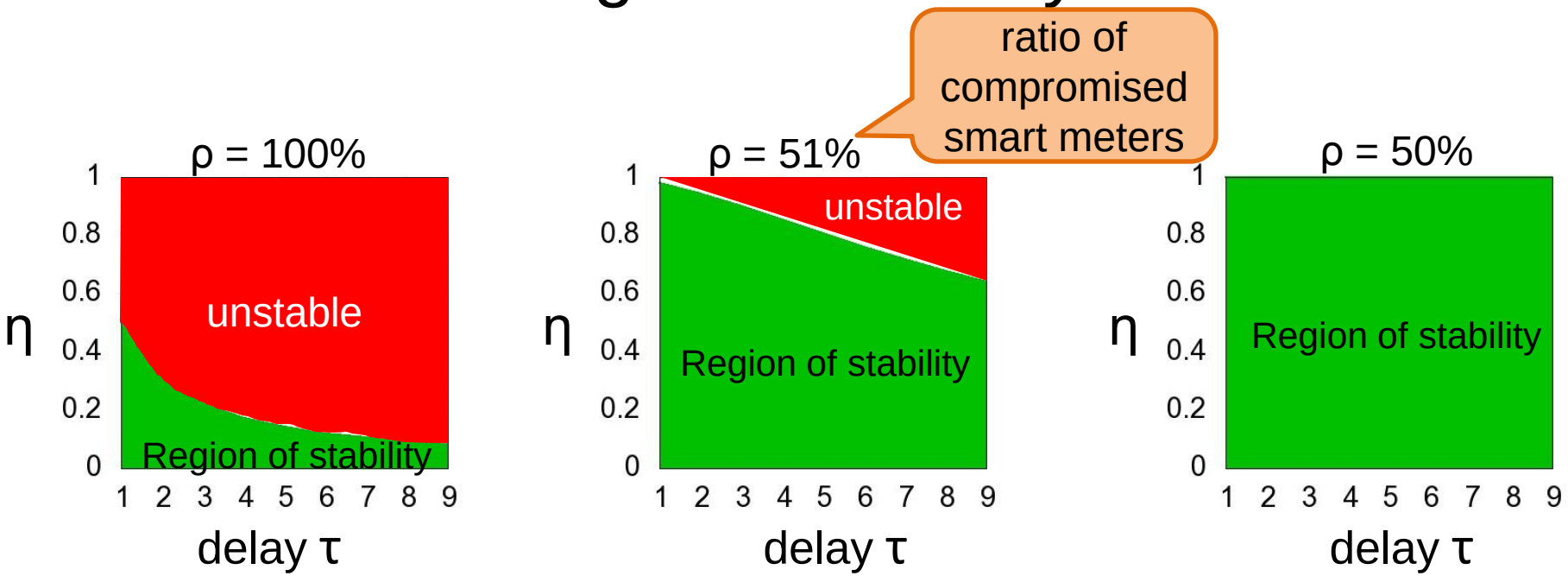


shrinks with delay (τ) and ratio of compromised smart meters (ρ)

If less than half of consumers are under delay attack, system is stable.

Analytical Results

- Closed-form region of stability



shrinks with delay (τ) and ratio of compromised smart meters (ρ)

If less than half of consumers are under delay attack, system is stable.

- Break this condition, system can be unstable

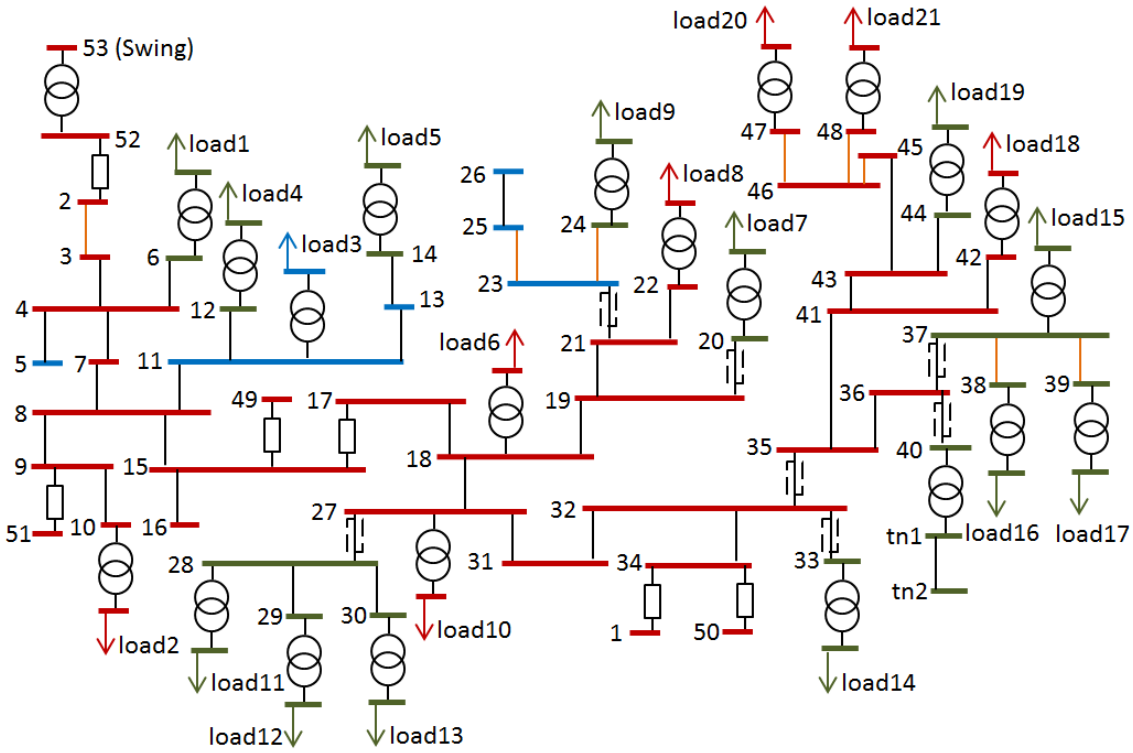
- Attacker/operator focus on critical infrastructures

Outline

- Background & Motivation
- Formulation of Real-Time Pricing
- Impact of Attacks
- Simulations

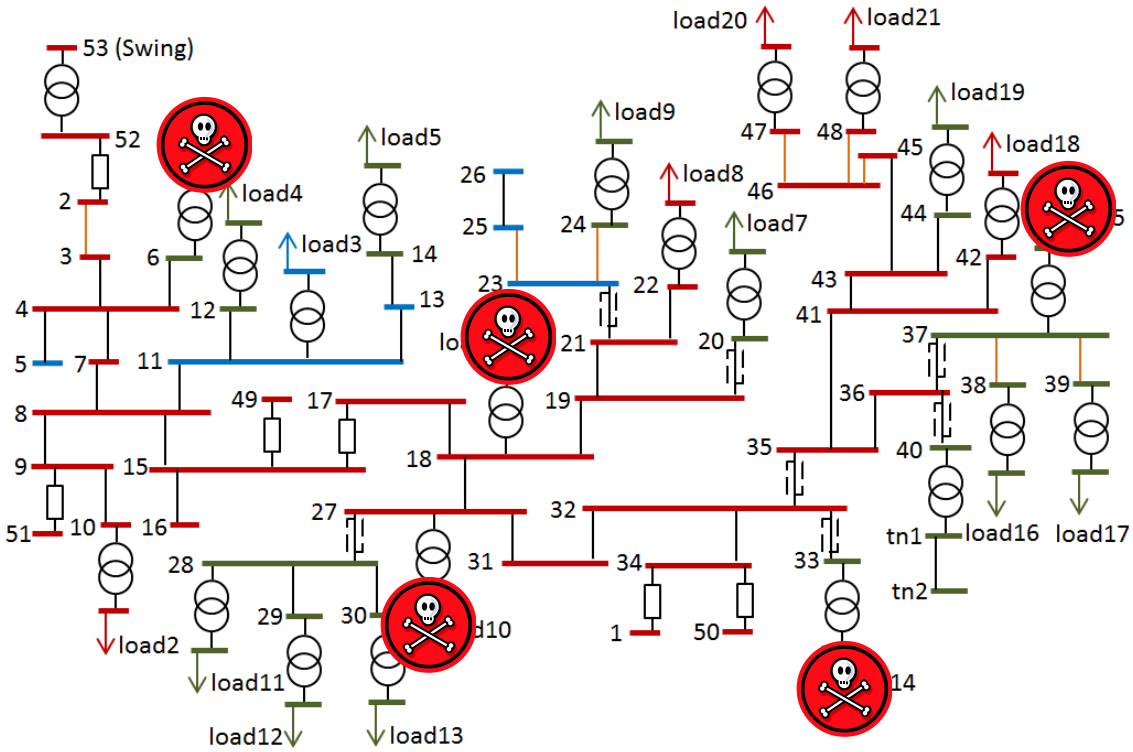
Simulation Methodology

- GridLAB-D
  - Physical aspects, emergency events
  - 1405 consumers
  - Scaled real load data as baseline demand

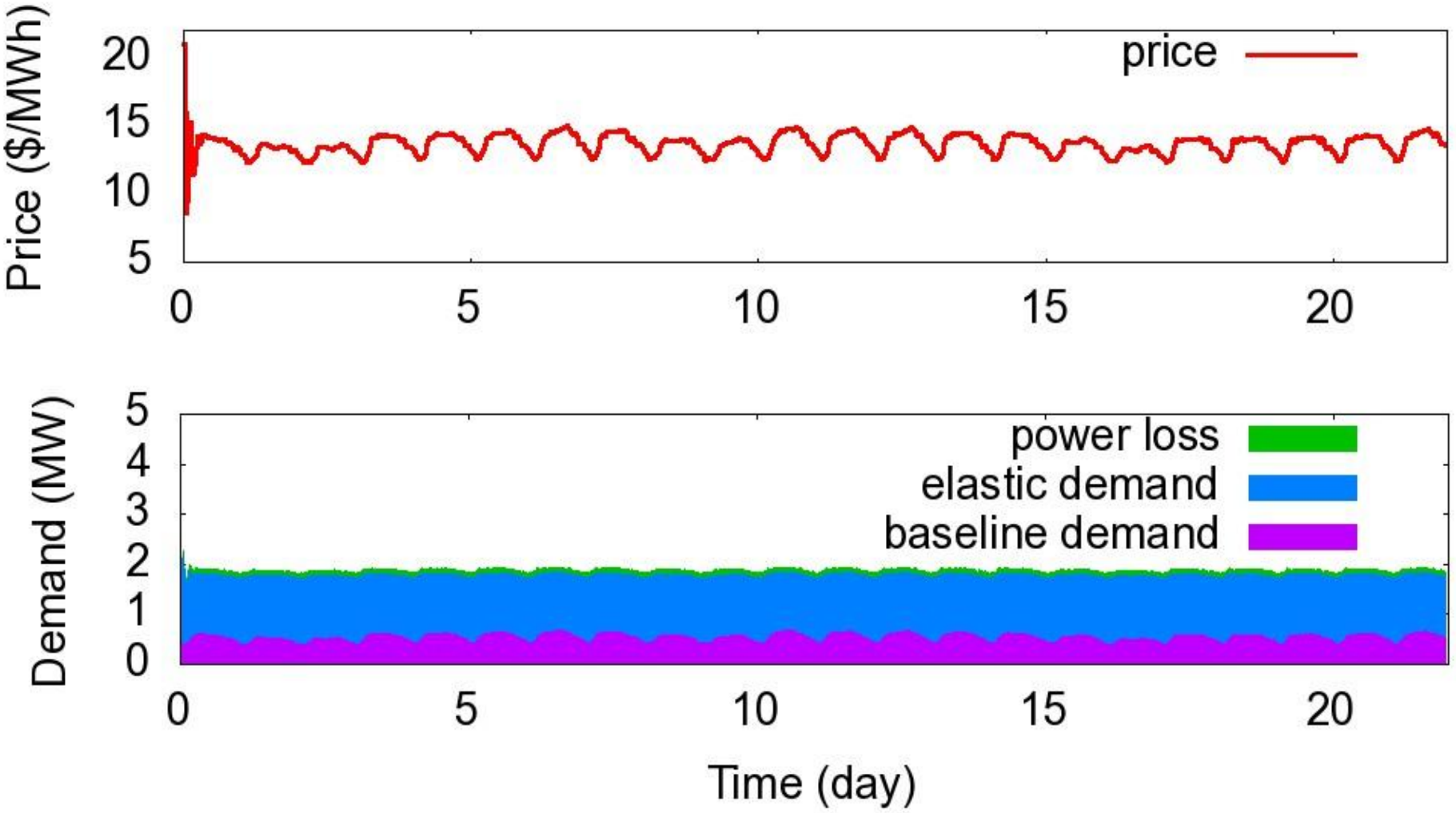


Simulation Methodology

- GridLAB-D
  - Physical aspects, emergency events
  - 1405 consumers
  - Scaled real load data as baseline demand

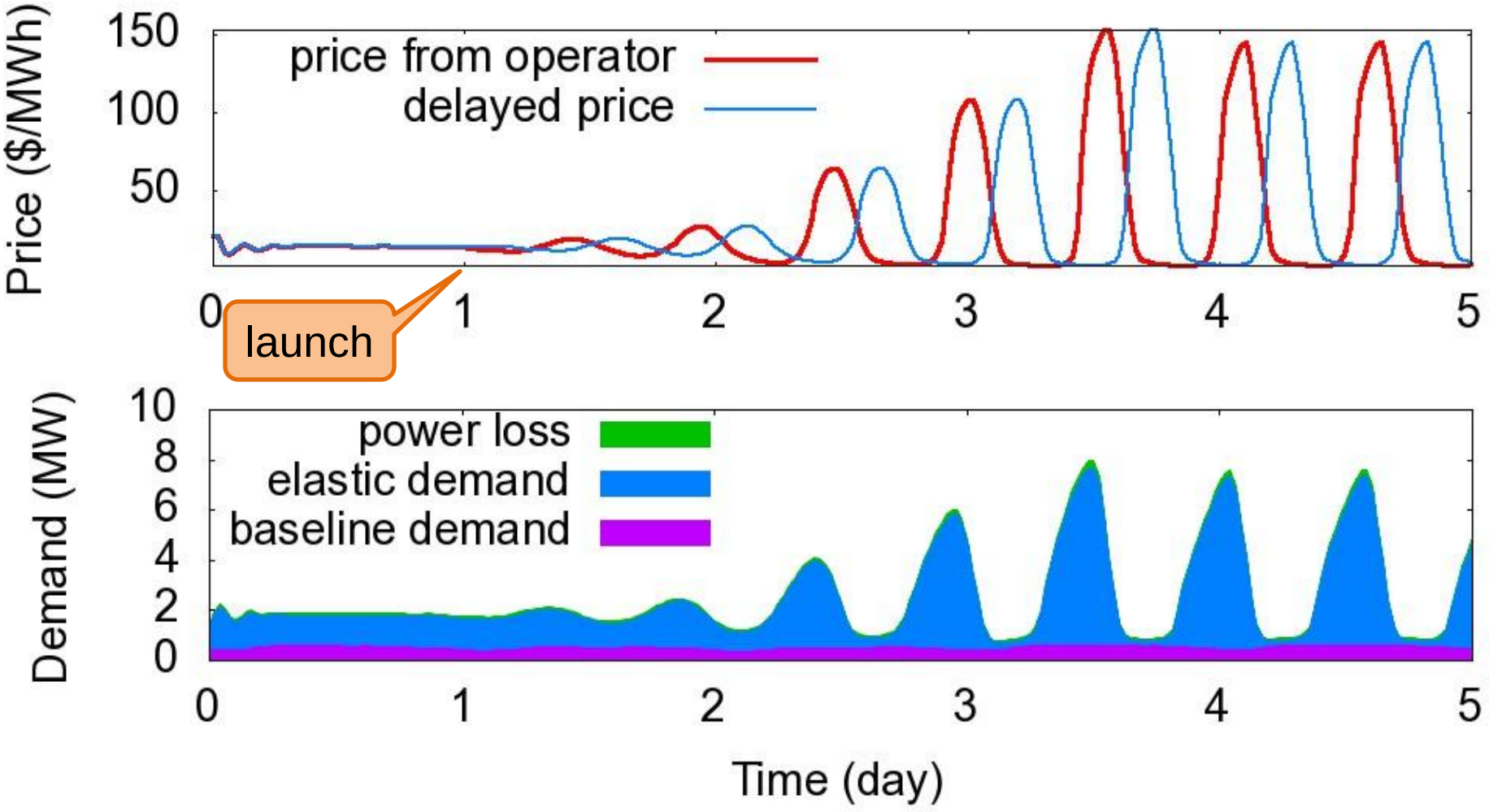


No Attacks



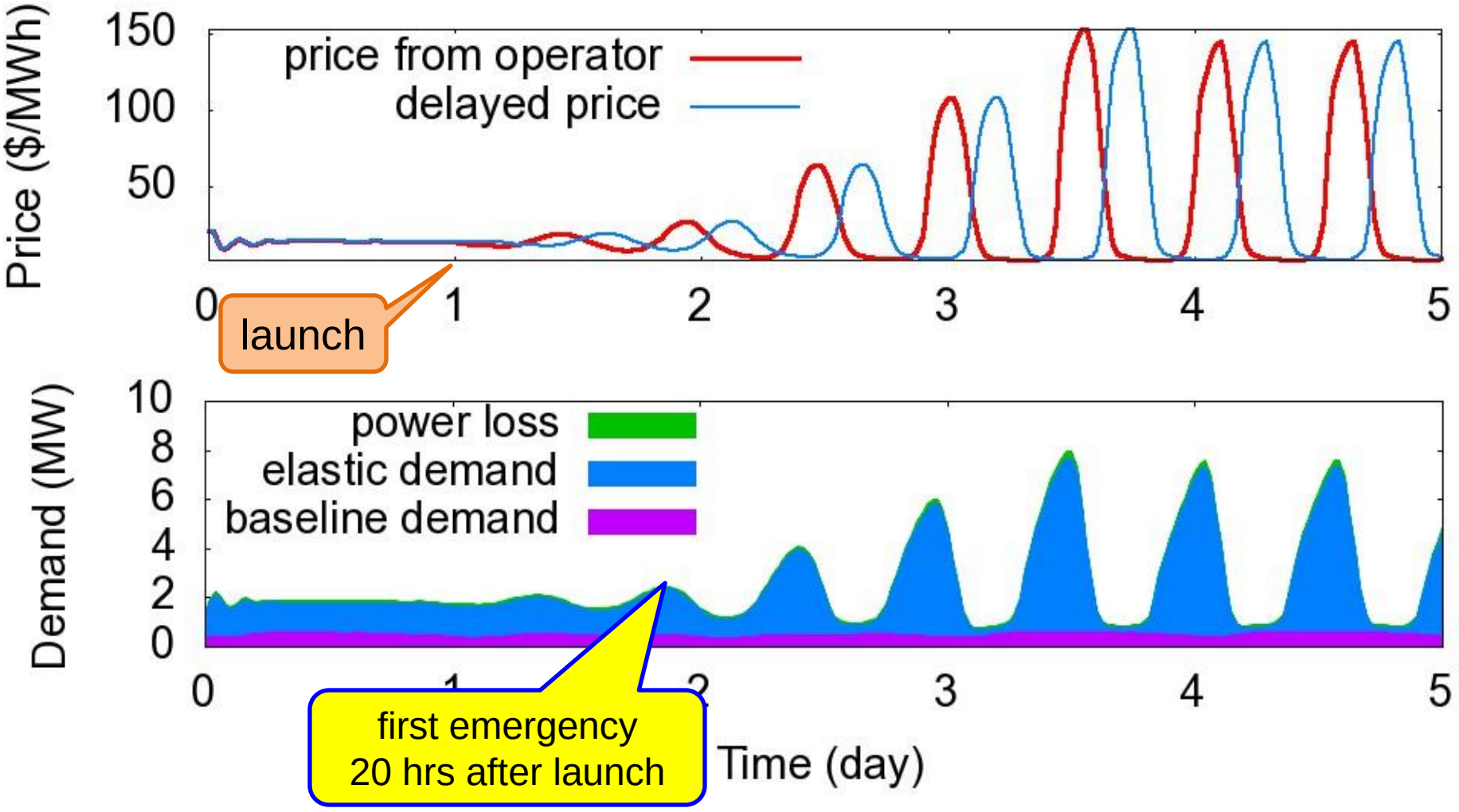
- Result price tracks the clearing price

Delay Attack



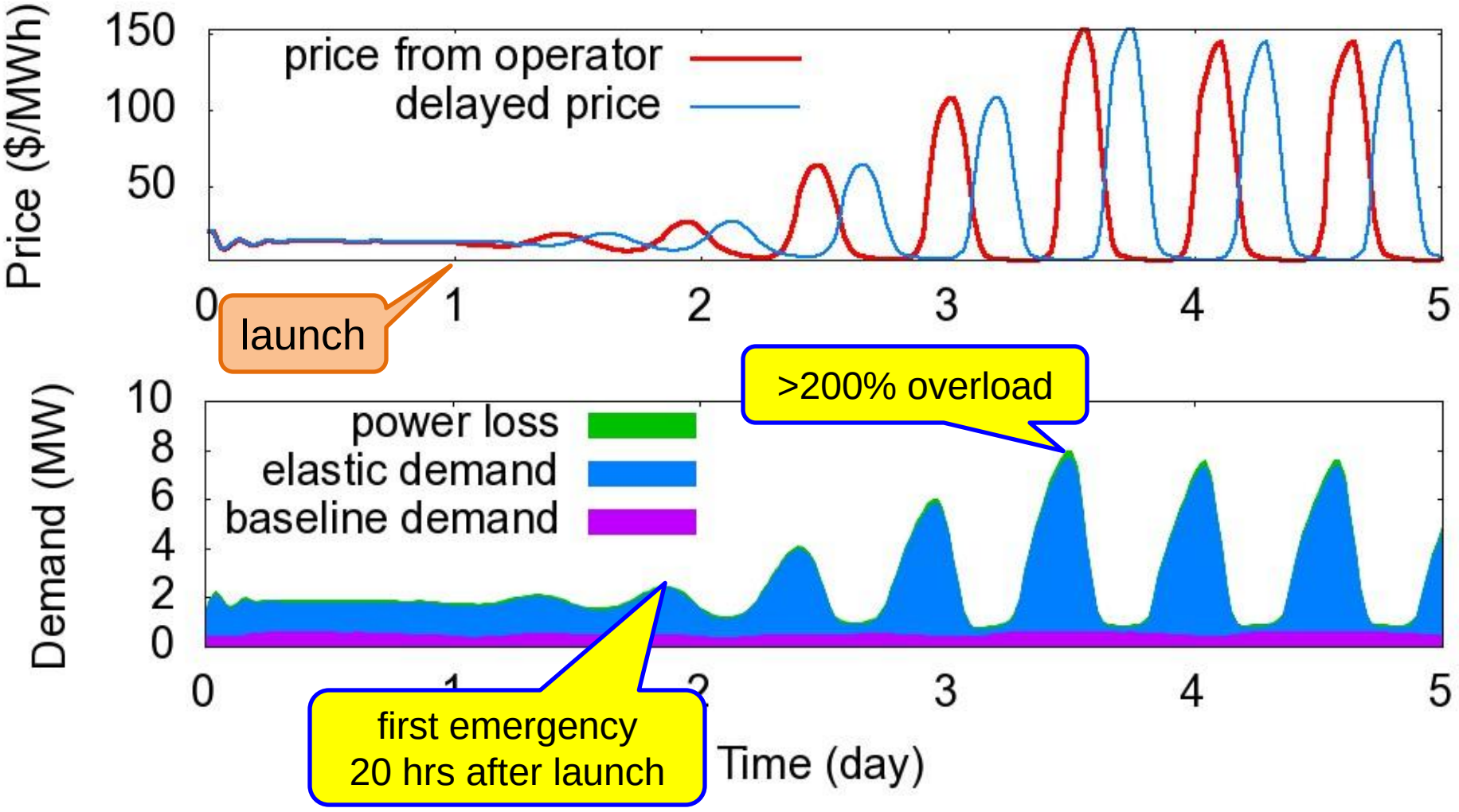
all smart meters compromised, delay = 4.5 hours

Delay Attack



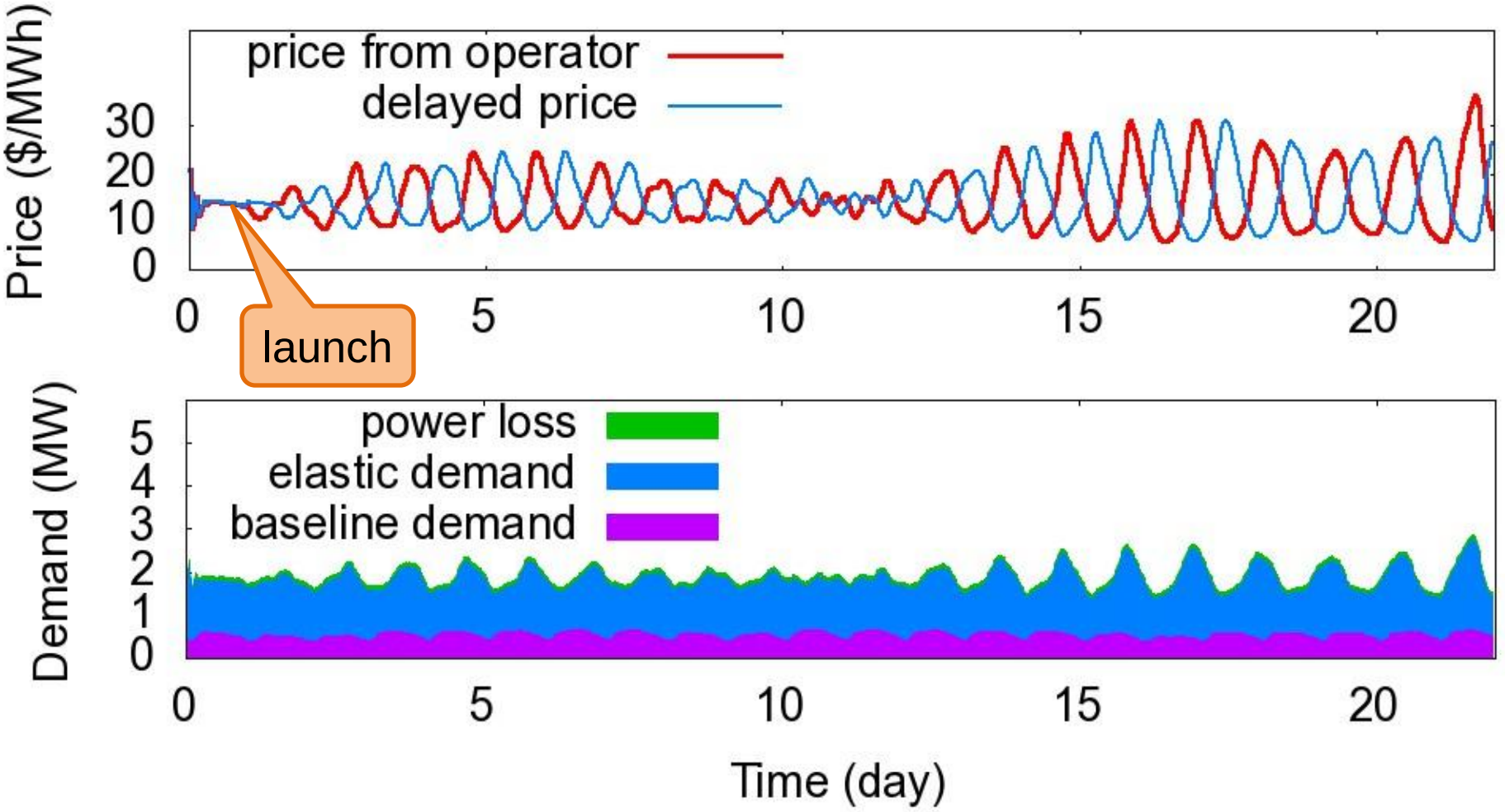
all smart meters compromised, delay = 4.5 hours

Delay Attack



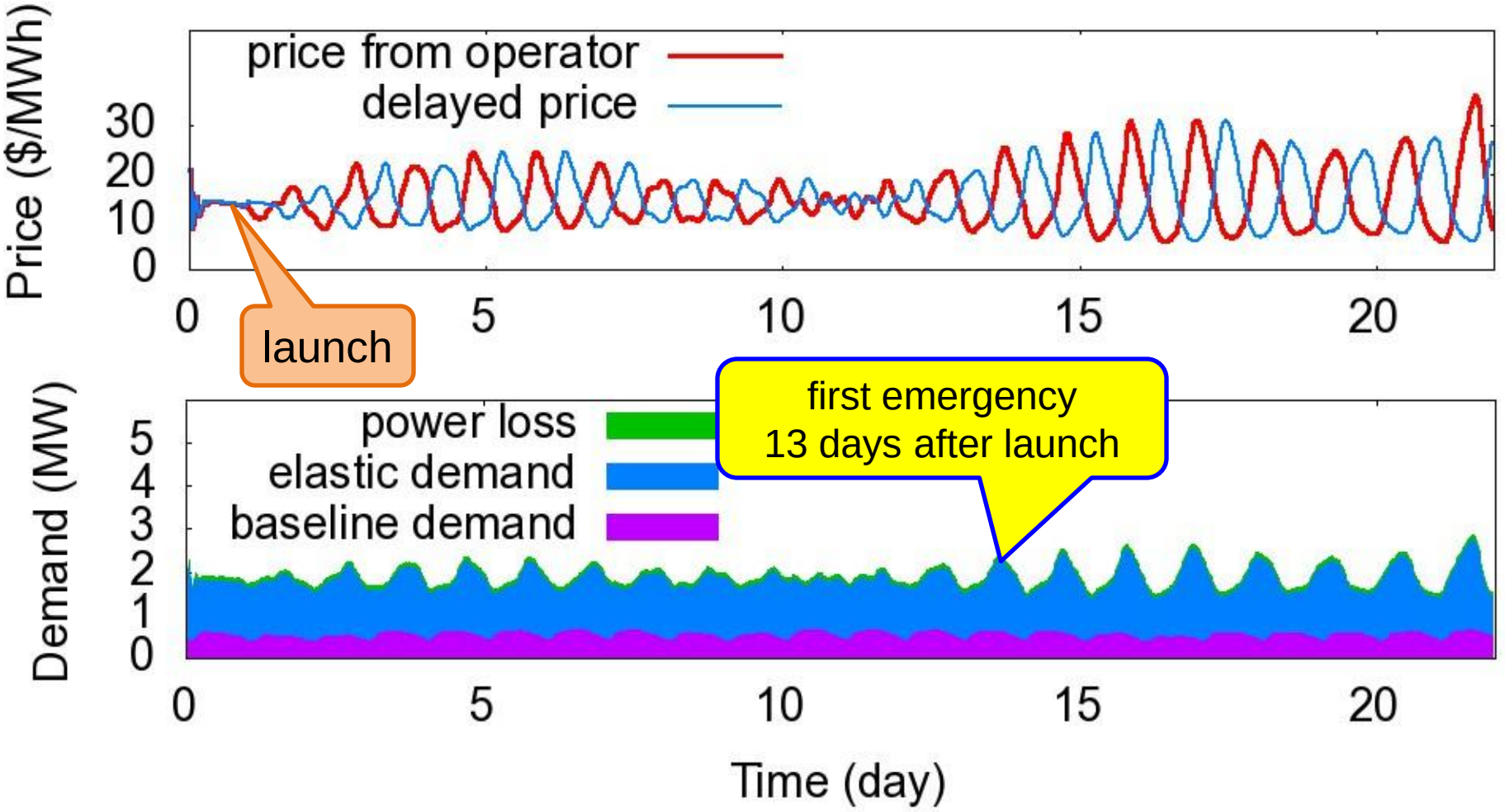
all smart meters compromised, delay = 4.5 hours

Weaker Delay Attack



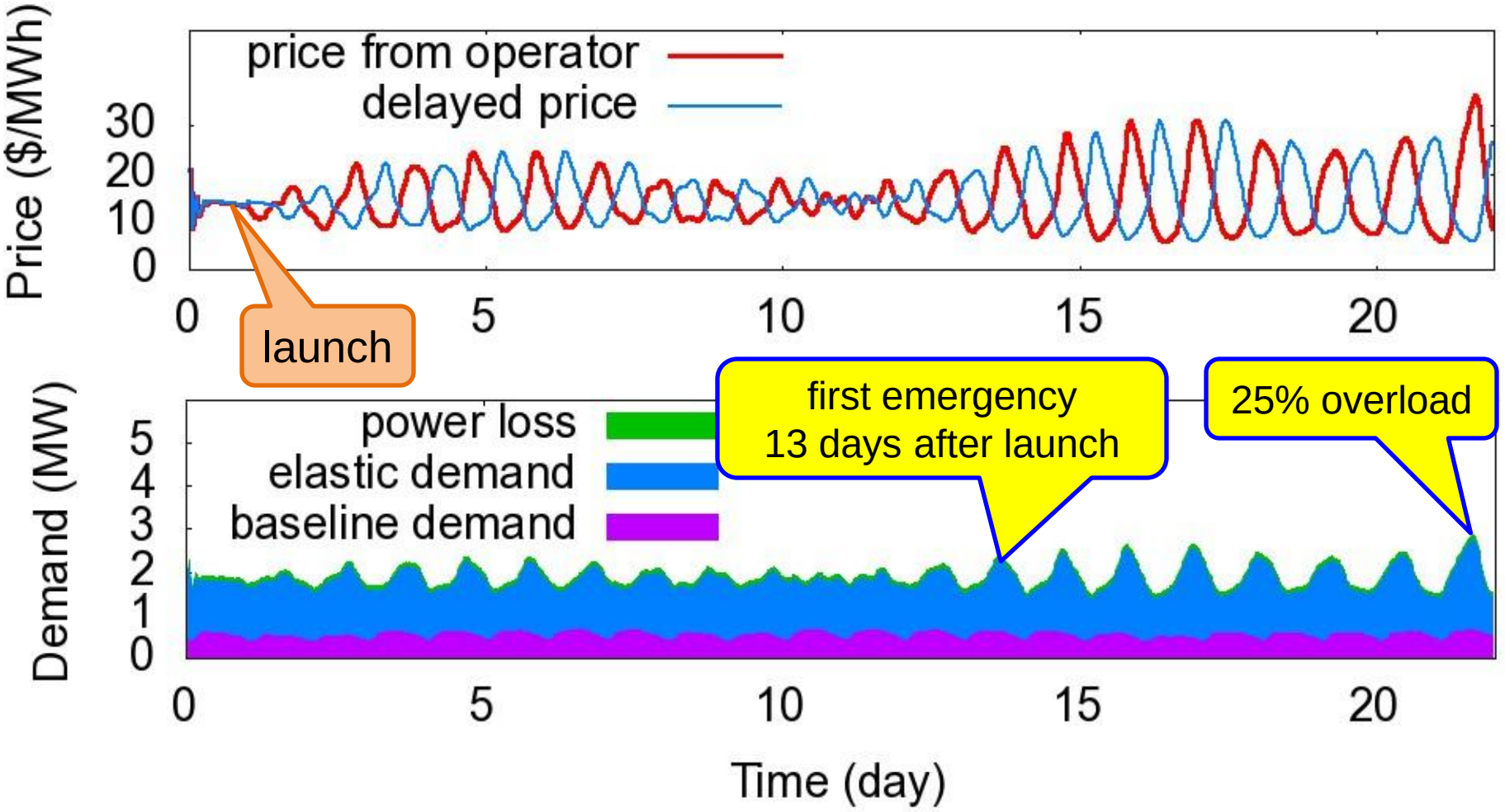
65% smart meters compromised

Weaker Delay Attack



65% smart meters compromised

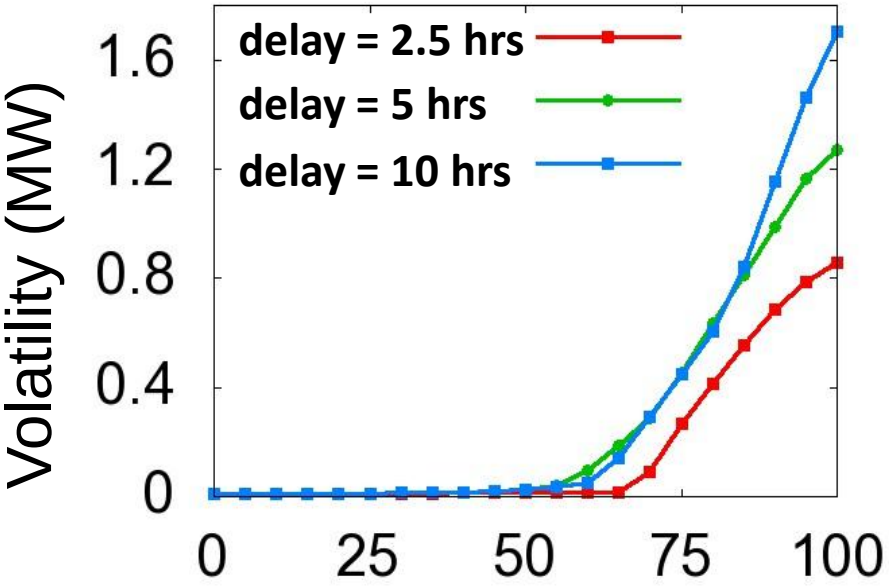
Weaker Delay Attack



65% smart meters compromised

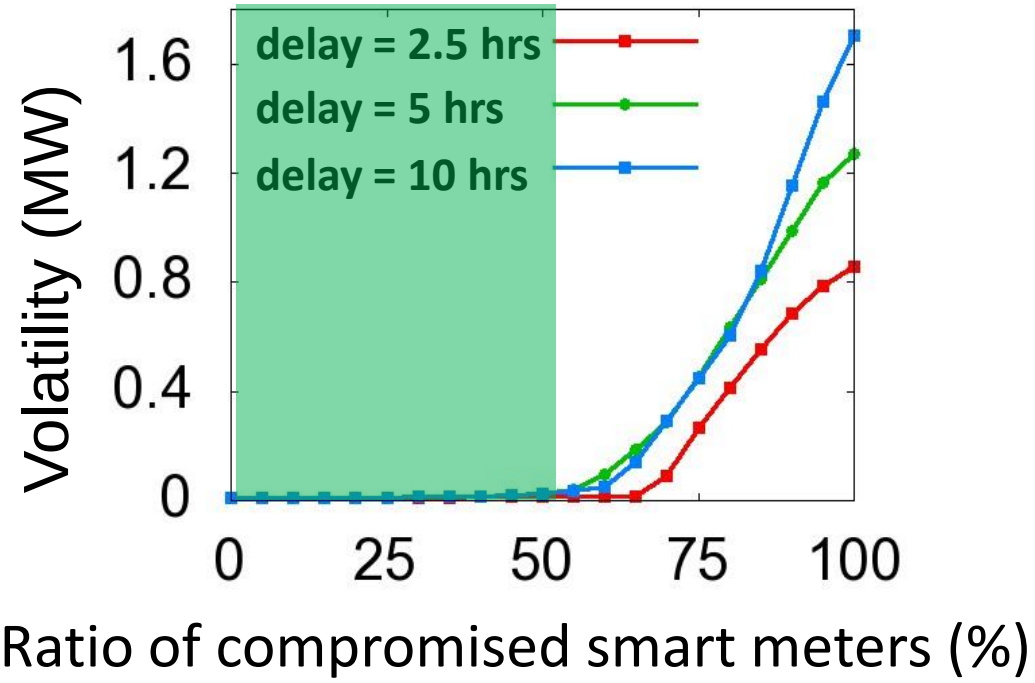
Volatility

- Volatility = std(scheduling errors)
  - 0: stable & converging
  - Else: increased operation cost



Volatility

- Volatility = std(scheduling errors)
  - 0: stable & converging
  - Else: increased operation cost



Conclusion and Future Work

- Impact of integrity attacks on real-time pricing
  - Region of stability
  - Delay more than half of smart meters
- Future work
  - Other realistic factors
    (e.g., a portion of consumers use fixed price)
  - Countermeasures
    (e.g., intrusion detection)