Profiting from Attacks on Real-Time Price Communications in Smart Grids

Slide 1/26

Outline

- Smart Grid (SG) and real-time pricing (RTP)
- Profit through arbitrage
- Attack model overview
  - Practical instantiation of attack
  - Experimental results and profit analysis
- Defensive techniques
  - Moving target defense
  - Experimental results and sensitivity analysis
- Conclusions
Grid Challenges: Uncertainty of Renewables

U.S. Power by Source:
- Coal = 33%
- Natural gas = 33%
- Nuclear = 20%
- Hydropower = 6%
- Other renewables = 7%
- Wind 4.7%
Source: eia.gov

Source: nyiso.com

Smart Grid: The Vision in the Works

Efficiency through coordination
ECON 101: Balance Demand and Supply

- Consumers use less with high price ($)
- Producers supply more with high $
- Residual Power = Supply-Demand
- $RP \Rightarrow$ Power is wasted
- $-RP \Rightarrow$ Blackouts, voltage drops

Goal: Minimize RP

Iterative Market Solution

- Real-time communication of price signal by ISO to consumers used for controlling the market
  - Lower latency means better efficiency
Related Work

- In [1], latency impacts in real-time communication in DR is evaluated but without any economic incentives.
- In [2], economic incentives are introduced but without real-time communications.
- In [3], we combined real-time DR with game theory for theoretical strategies.
- This work introduces practical strategies for adversaries participating in a real-time pricing market and practical defense measures.


Attacker’s Model

Detect
- Scan local IP ranges
- Sniff RTP messages or detect by freq. analysis (PON/DOCSIS)

Attack
- Choose optimal targets (C1,C2,...)
- Pass IP’s to DDoS system
- Change market prices

Profit
- Buy at artificially lower prices
- Sell at artificially higher prices

Slide 9/26

Attack Operating Principle

\[ f(\lambda_{t=T}) = \lambda_{t=T} \cdot D_i \]

\[ \lambda_{t=1} = 5 \]
\[ \lambda_{t=1} \cdot D_1 + \lambda_{t=1} \cdot D_2 + P(t) = 9 \]
\[ 5 \cdot 2 + 5 \cdot 3 - 16 = 9 \text{ RP} \]

\[ D_1 = 2 \]
\[ D_2 = 3 \]

\[ \lambda_{t=2} = 4 \]
\[ 4 \cdot 2 + 4 \cdot 3 - 16 = 4 \]

\[ \lambda_{t=3} = 3.2 \]
\[ 3.2 \cdot 2 + 3.2 \cdot 3 - 16 = 0 \]
**Slide 11/26**

**Attack Operating Principle**

\[ f(\lambda_t) = \lambda_t \cdot D_i \]

\[ \lambda_t = 5 \]

\[ D_1 = 2 \]

\[ D_2 = 3 \]

\[ \lambda_t \cdot D_1 + \lambda_t \cdot D_2 + P(t) = 9 \]

\[ 5 \cdot 2 + 5 \cdot 3 - 16 = 9 \]

\[ \lambda_t = 4 \]

\[ 5 \cdot 2 + 4 \cdot 3 - 16 = 6 \]

\[ \lambda_t = 3 \]

\[ 5 \cdot 2 + 3 \cdot 3 - 16 = 3 \]

\[ \lambda_t = 2 \]

\[ 5 \cdot 2 + 2 \cdot 3 - 16 = 0 \]

Market price reduced by $1.2 by attacking client #1

---

**Slide 12/26**

**DoS Attack Method**

- ISO
- 1 Gbps Fiber
- DOCSIS 600 Mbps
- C4 25 Mbps
- C5 50 Mbps
- C6 25 Mbps
- +250-500

DoS >75 Mbps
Arbitrage Profit Model

Sample system:
- Power from 2014 NYISO load data
- 100 Consumers
- 2 Generators
Attacker’s Battery:
- 1200 kWh
- 2 hour dis/charge

Optimizing Attacker Strategy

- Observe System
- Estimate Residual Power
- Launch Attack when Profitable
- Determine Attack Profit
- Estimate Power of Attack

Power of Attack
- Estimate change in market price for attacking client C at current time

Buying Threshold
- Market price under which power is purchased

Selling Threshold
- Market price over which power is sold
Projected Power of Attack over Time

DDoS Attack Profits

- Smart Meter
- Battery
- DDoS (20/100)

$120 +69\%
Stronger Adversary

- Integrity attack
- More difficult than DoS
  - Compromised software
  - Race conditions
    - (e.g. DNS spoofing)
  - Compromised comms
    - (e.g. Man-in-the-Middle)

Integrity Attack Profits

- Smart Meter
- Battery
- Integrity Attack
- $140
  + 97%
**Daily Attack Profitability**

- Smart Meter + Battery + No Attack = $71
- Smart Meter + Battery + DDoS (20) = $120 +69%
- Smart Meter + Battery + Integrity Attack = $140 +97%

**Defensive Strategy**

- ISO
- 1 Gbps Fiber
- DOCSIS 600 Mbps
- DoS >75 Mbps
- C4 25 Mbps
- C5 50 Mbps
- C6 25 Mbps
- +250-500
Defensive Strategy

ISO -> 1 Gbps Fiber -> DOCSIS 600 Mbps

C4: 25 Mbps
C6: 50 Mbps
C5: 25 Mbps
+250-500

DoS >75 Mbps

Defensive Strategy: Moving Targets

ISO -> 1 Gbps Fiber -> DOCSIS 600 Mbps

C4: 25 Mbps
C6: 50 Mbps
C5: 25 Mbps
+250-500

IP Shuffling, Masquerading

DoS >75 Mbps
Conclusions & Takeaways

- RTP systems are susceptible to manipulation
  - Network interruptions (DDoS)
  - Compromised implementations (Integrity)
- Such manipulations may be profitable
  - Adversarial strategies yield substantial gains in profit
  - Other consumers suffer degraded efficiency
- Moving targets can reduce susceptibility to attacks
  - Introducing deception against the adversary
  - Concealing operational states is also effective
- Future work:
  - Defense through stochastic loading functions $f($)$
  - Attacks with different market models
Most Powerful Attack Model