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

		
Paul Wood PURDUE UNIVERSITY	Saurabh Bagchi PURDUE UNIVERSITY	Alefiya Hussain USC INFORMATION SCIENCES INSTITUTE

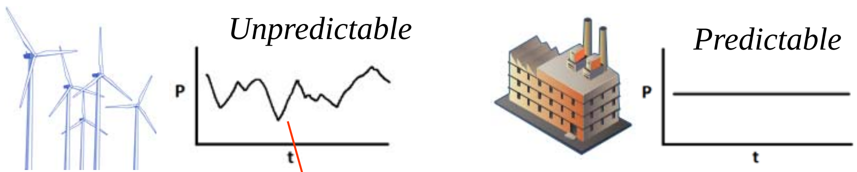
PURDUE UNIVERSITY

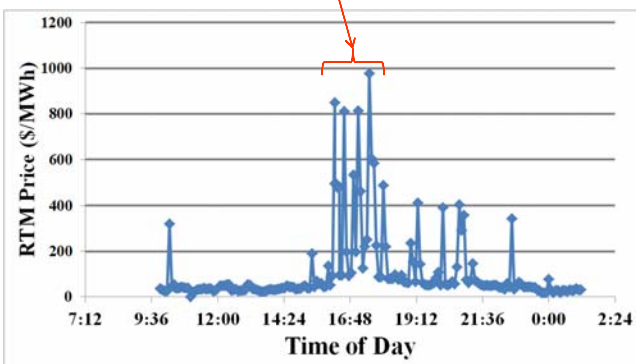
Outline

- 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

PURDUE UNIVERSITY

Grid Challenges: Uncertainty of Renewables

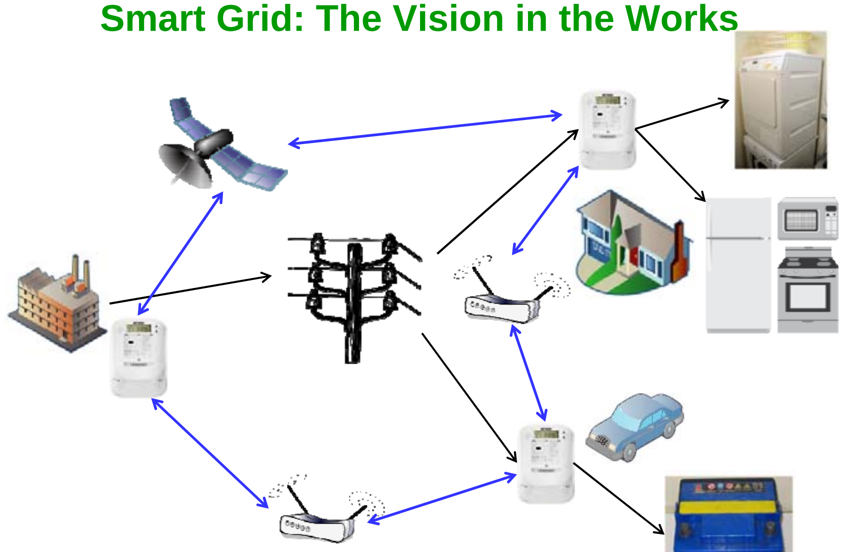




Source: nyiso.com

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

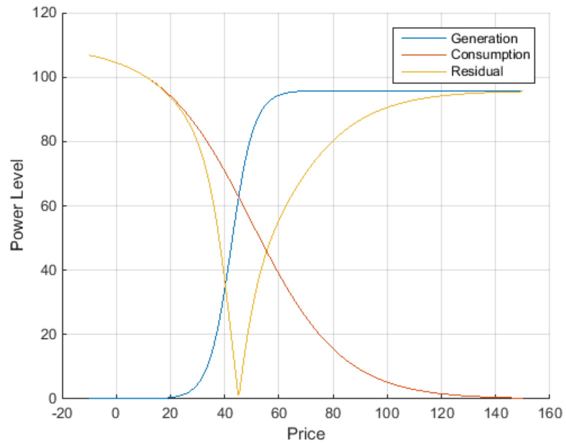
Smart Grid: The Vision in the Works



Efficiency through coordination

ECON 101: Balance Demand and Supply

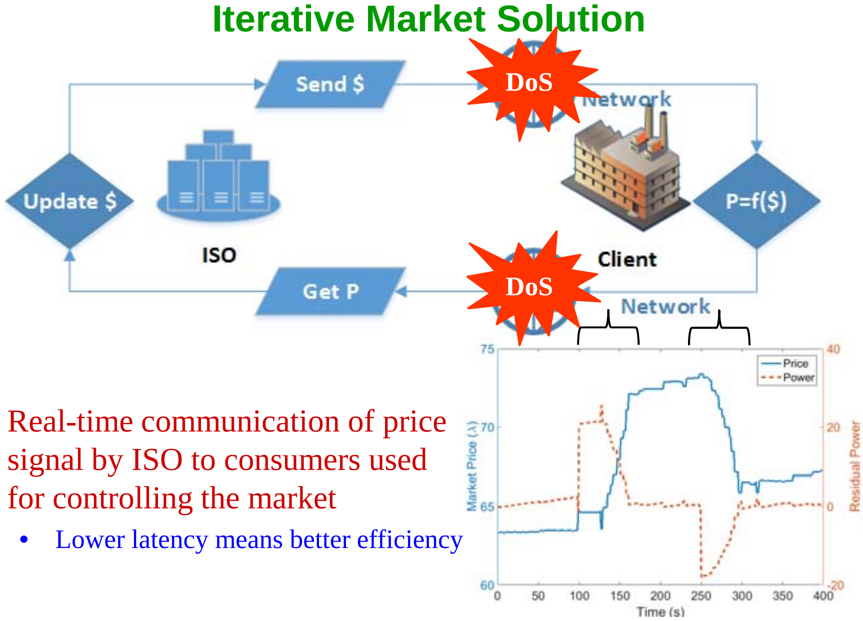
- Consumers use less with high price ($)
- Producers supply more with high $
- Residual Power = Supply-Demand
- + RP ⇒ Power is wasted
- – RP ⇒ Blackouts, voltage drops



Goal: Minimize RP

PURDUE UNIVERSITY

Iterative Market Solution



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

PURDUE UNIVERSITY

Related Work

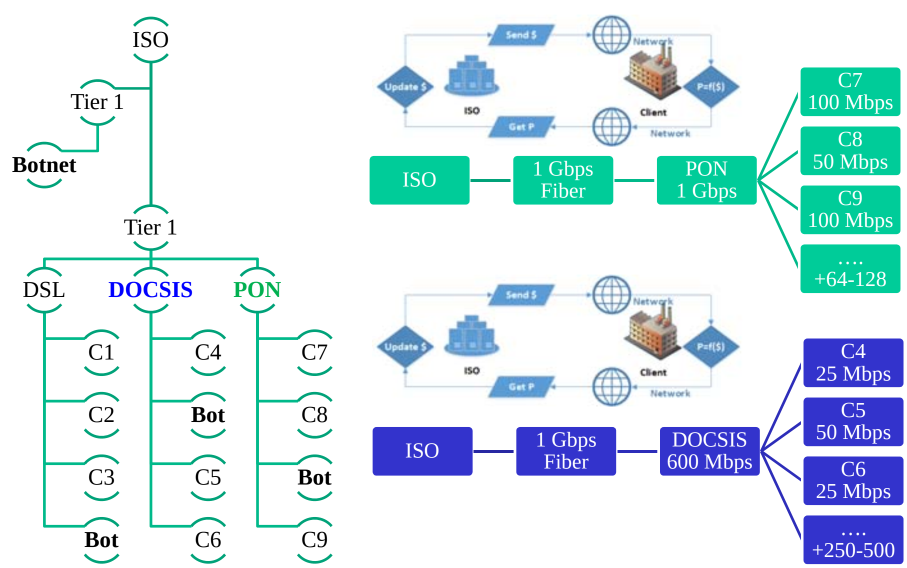
- In [1], latency impacts in real-time communication in DR is evaluated but without any economic incentives
- In [2], economic incentives are introduced but without real-time communications
- In [3], we combined real-time DR with game theory for theoretical strategies
- This work introduces practical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

[1] Tan, Rui, et al. "Impact of integrity attacks on real-time pricing in smart grids." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS)*. ACM, 2013.

[2] Barreto, Carlos, et al. "CPS: market analysis of attacks against demand response in the smart grid." *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. ACM, 2014.

[3] Wood, Paul, et al. "Defending against strategic adversaries in dynamic pricing markets for smart grids." *2016 8th International Conference on Communication Systems and Networks (COMSNETS)*. IEEE, 2016.

Consumer Communication Topology



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

PURDUE UNIVERSITY

Attack Operating Principle

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

$$D_1 = 2$$

$$D_2 = 3$$

$$\lambda_{t=1} = 5$$

$$\lambda_{t=1} \cdot D_1 + \lambda_{t=1} \cdot D_2 + P(t) = 9$$

$$5 \cdot 2 + 5 \cdot 3 - 16 = 9 \text{ RP}$$

$$\lambda_{t=2} = 4$$

$$4 \cdot 2 + 4 \cdot 3 - 16 = 4$$

$$\lambda_{t=3} = 3.2$$

$$3.2 \cdot 2 + 3.2 \cdot 3 - 16 = 0$$

PURDUE UNIVERSITY

Attack Operating Principle

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

$D_1 = 2$

$D_2 = 3$

$\lambda_{t=1} = 5$

$\lambda_{t=1} \cdot D_1 + \lambda_{t=1} \cdot D_2 + P(t) = 9$

$5 \cdot 2 + 5 \cdot 3 - 16 = 9$

$\lambda_{t=2} = 4$

$5 \cdot 2 + 4 \cdot 3 - 16 = 6$

$\lambda_{t=3} = 3$

$5 \cdot 2 + 3 \cdot 3 - 16 = 3$

$\lambda_{t=4} = 2$

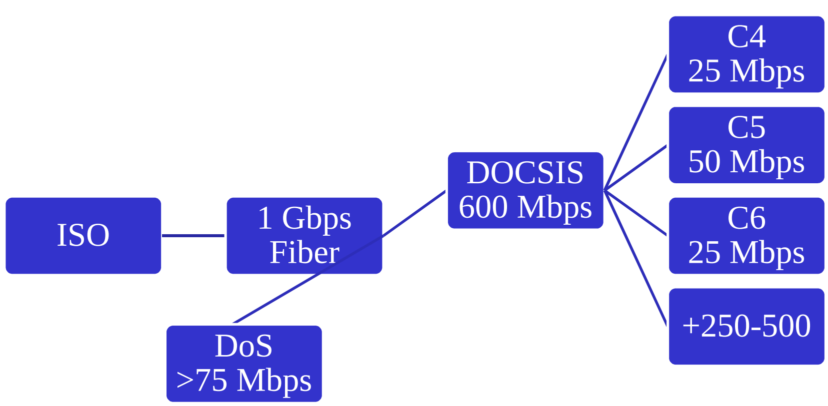
$5 \cdot 2 + 2 \cdot 3 - 16 = 0$

$\lambda = 3.2$

$\lambda^* = 2$

Market price reduced by $1.2 by attacking client #1

DoS Attack Method



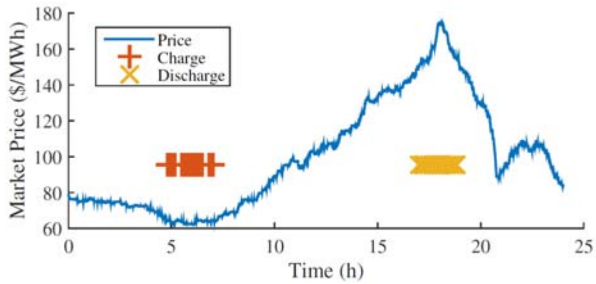
Arbitrage Profit Model

Sample system:

- Power from 2014 NYISO load data
- 100 Consumers
- 2 Generators

Attacker's Battery:

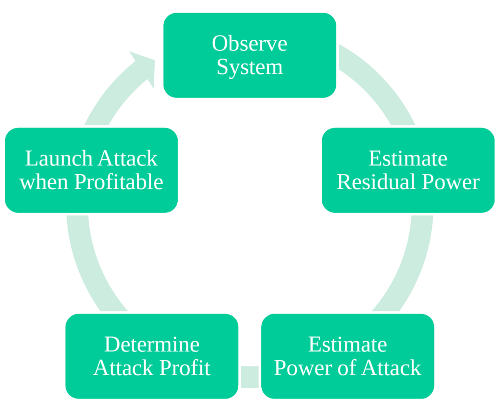
- 1200 kWh
- 2 hour dis/charge



Smart Meter + Battery = $71

PURDUE UNIVERSITY

Optimizing Attacker Strategy



Power of Attack

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

Buying Threshold

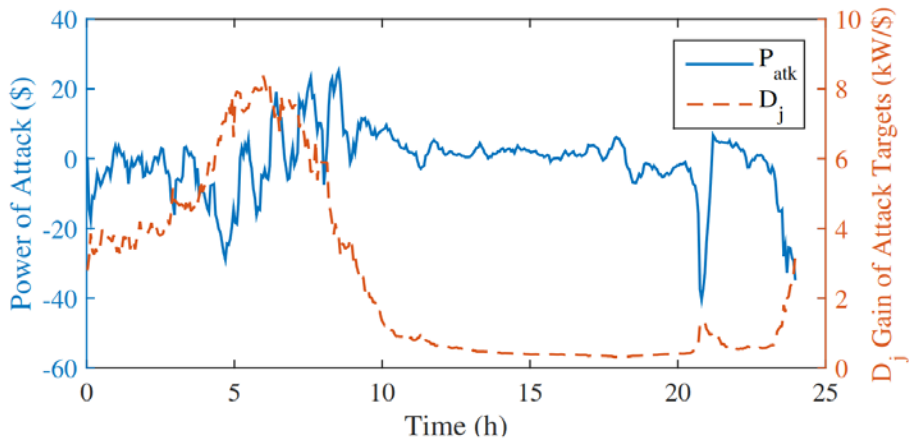
- Market price under which power is purchased

Selling Threshold

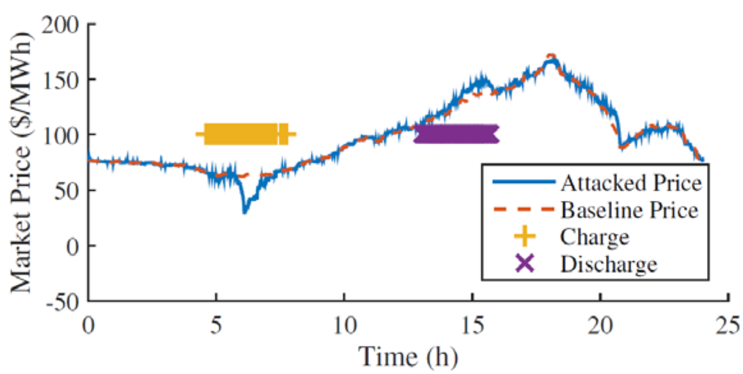
- Market price over which power is sold

PURDUE UNIVERSITY

Projected Power of Attack over Time

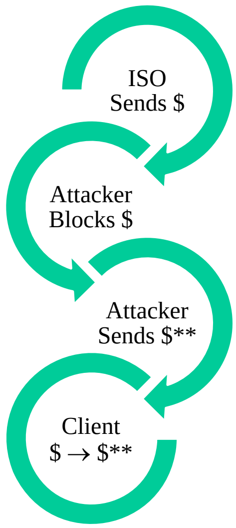


DDoS Attack Profits



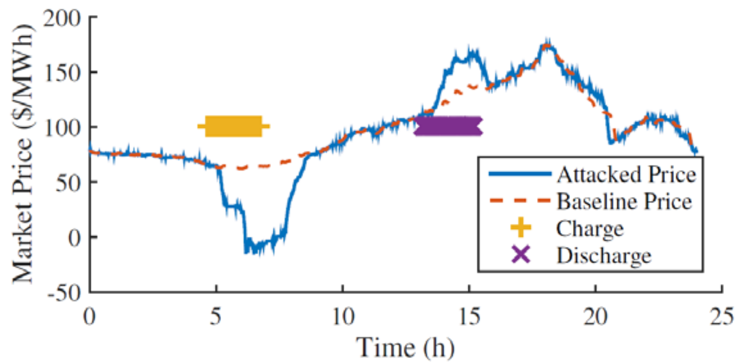
Smart Meter + Battery + DDoS (20/100) = $120 +69%

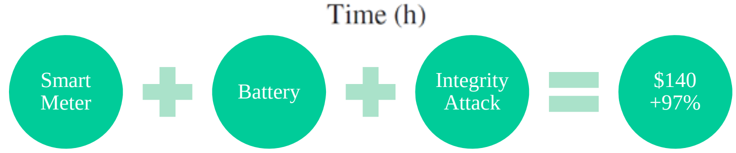
Stronger Adversary



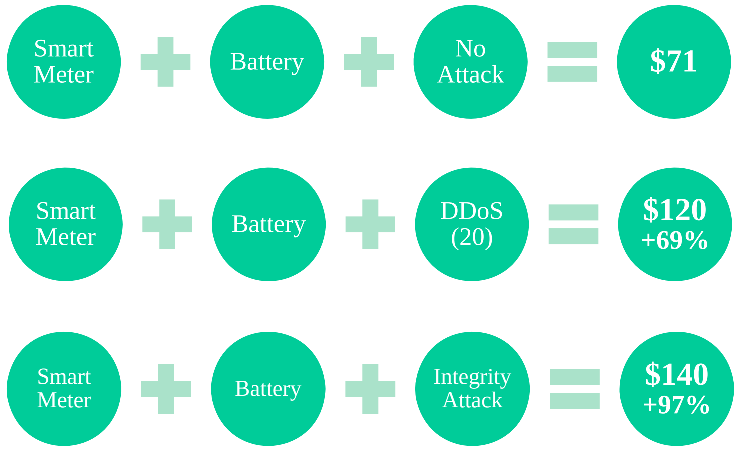
- Integrity attack
- More difficult than DoS
  - Compromised software
  - Race conditions
    - (e.g. DNS spoofing)
  - Compromised comms
    - (e.g. Man-in-the-Middle)

Integrity Attack Profits

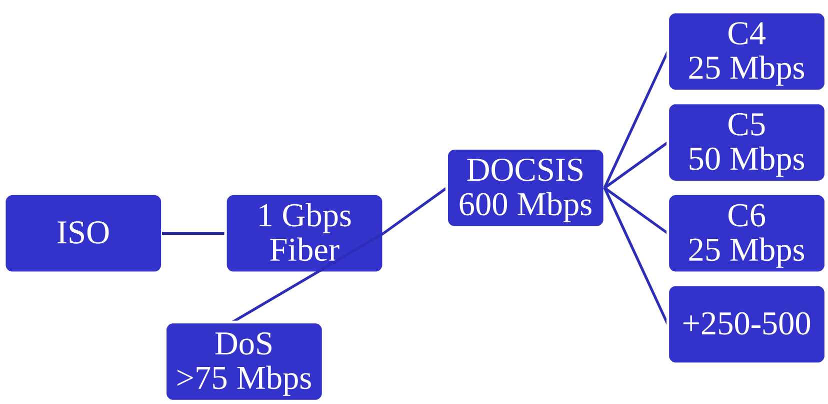




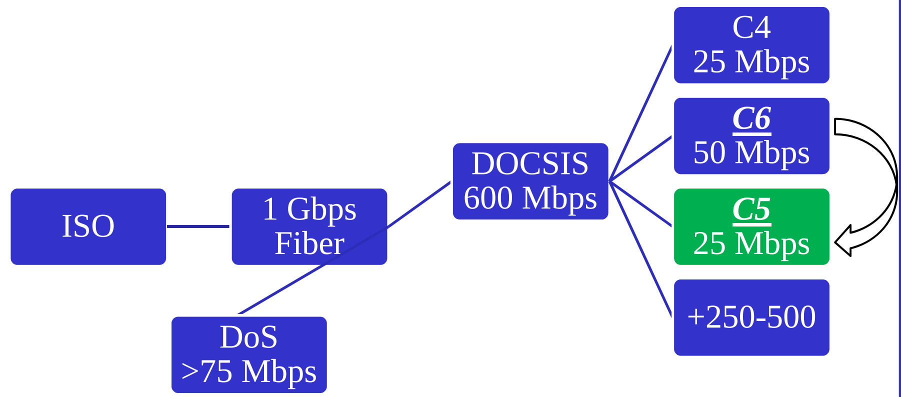
Daily Attack Profitability



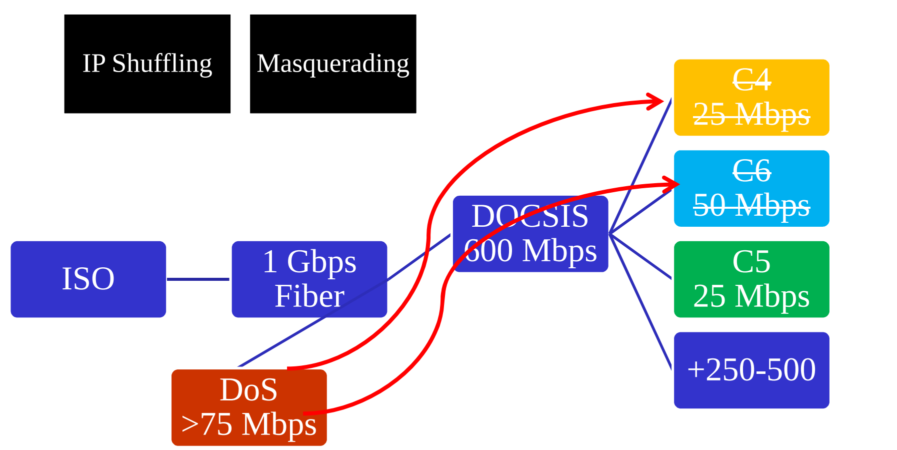
Defensive Strategy



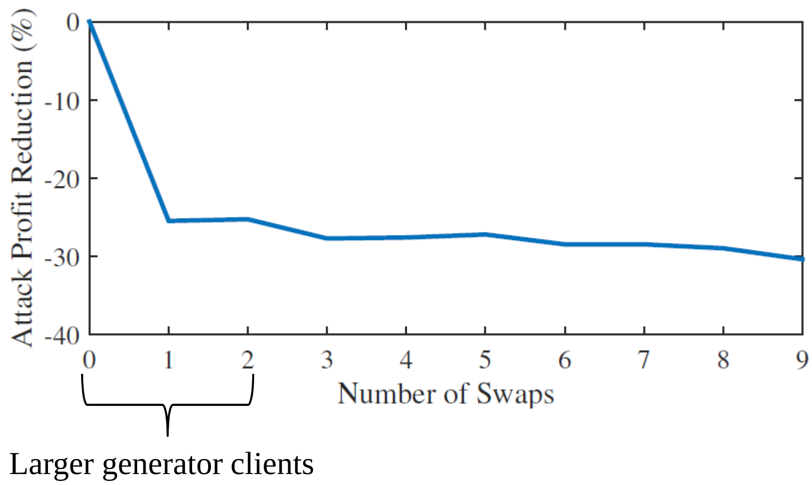
Defensive Strategy



Defensive Strategy: Moving Targets



Defensive Strategy: Moving Targets



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

PURDUE
UNIVERSITY