Defending Against Strategic Adversaries in Dynamic Pricing Markets for Smart Grids

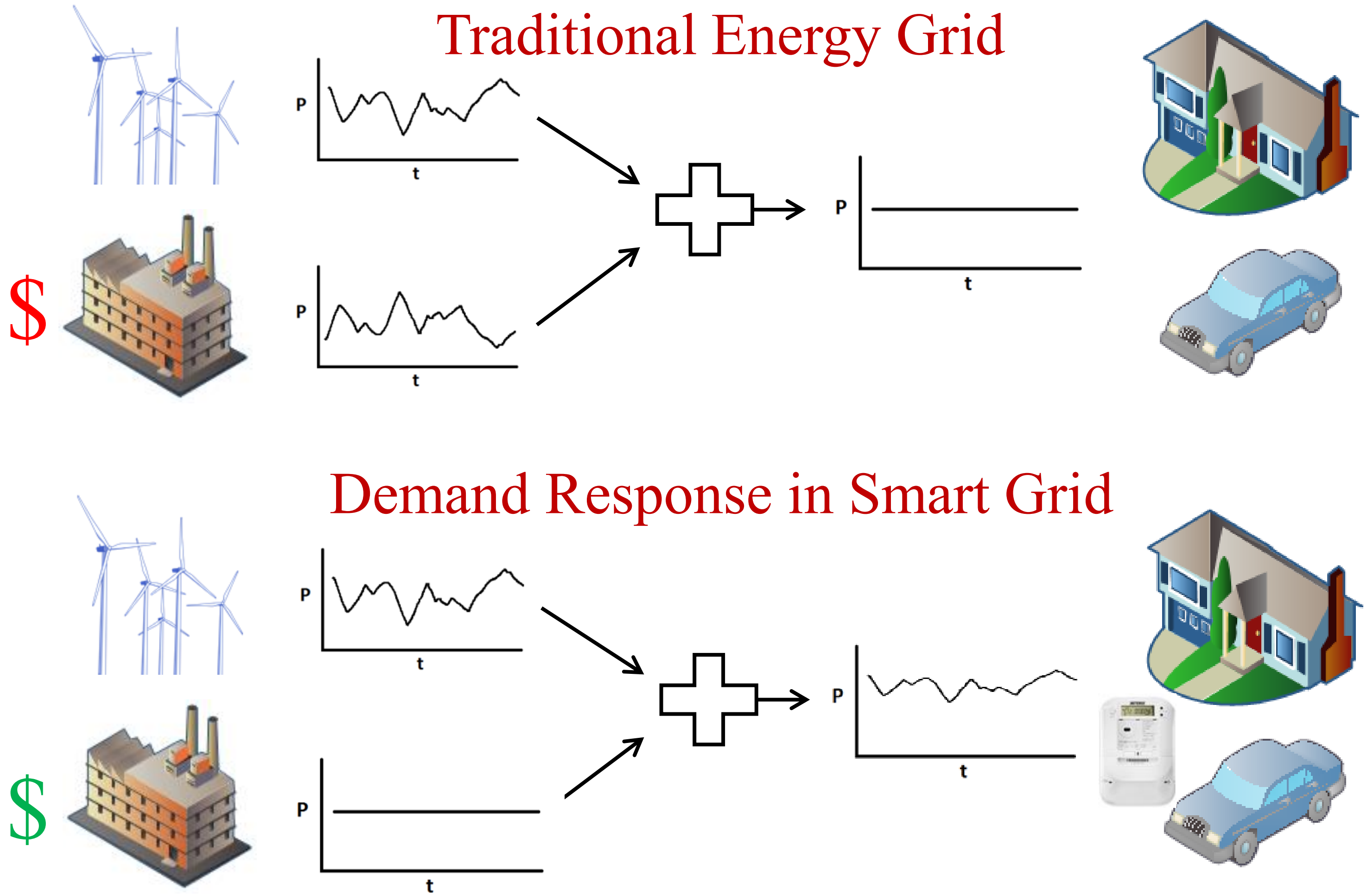
Paul Wood, ***Saurabh Bagchi***
Purdue University
[pwood,sbagchi]@purdue.edu

Alefiya Hussain
USC/ISI
hussain@isi.edu

Outline

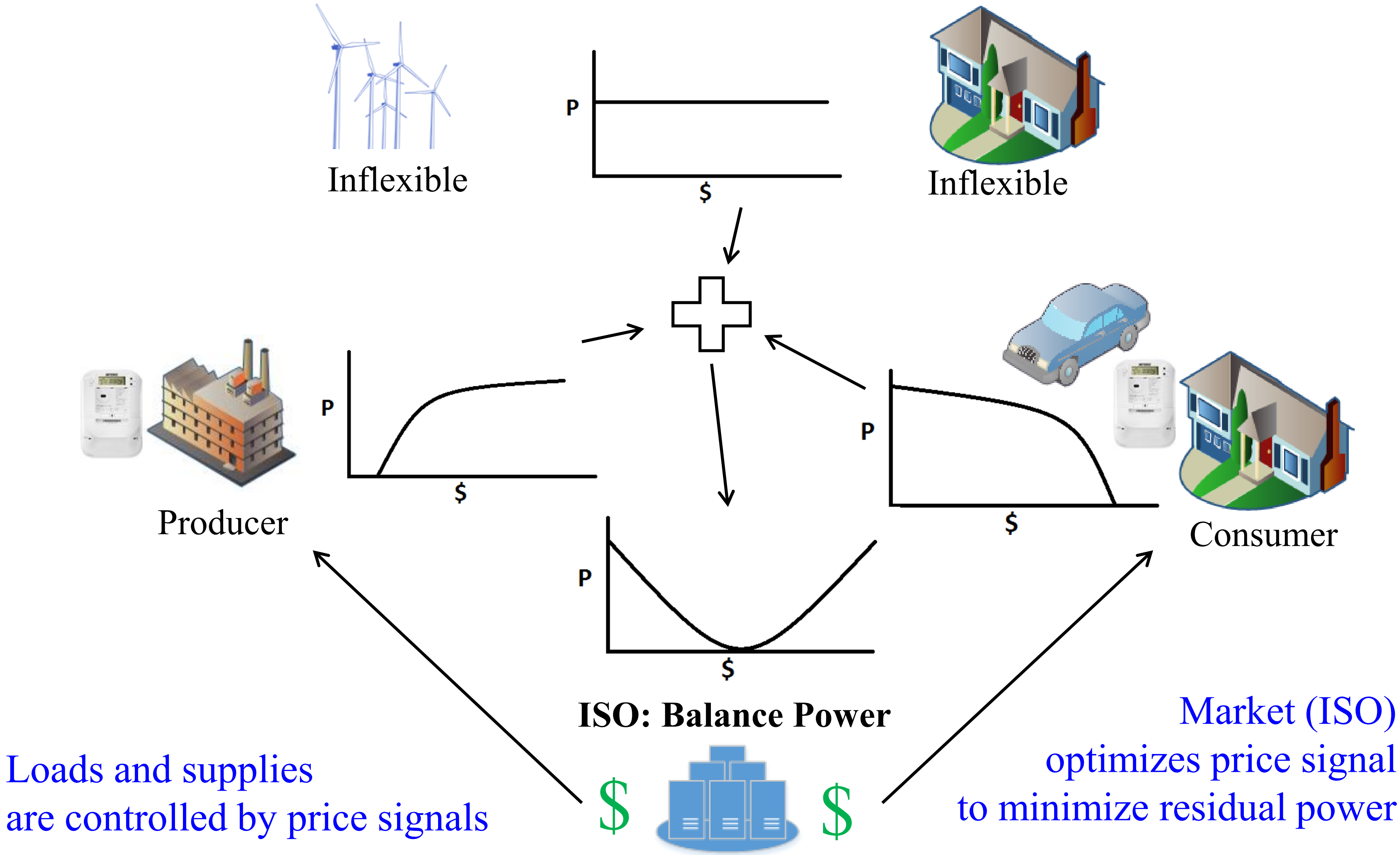
- Smart Grid, Demand Response, and Related Work
- Attack and Defense Strategies
- Experimental Results
- Conclusions

Demand Response in Electricity Networks



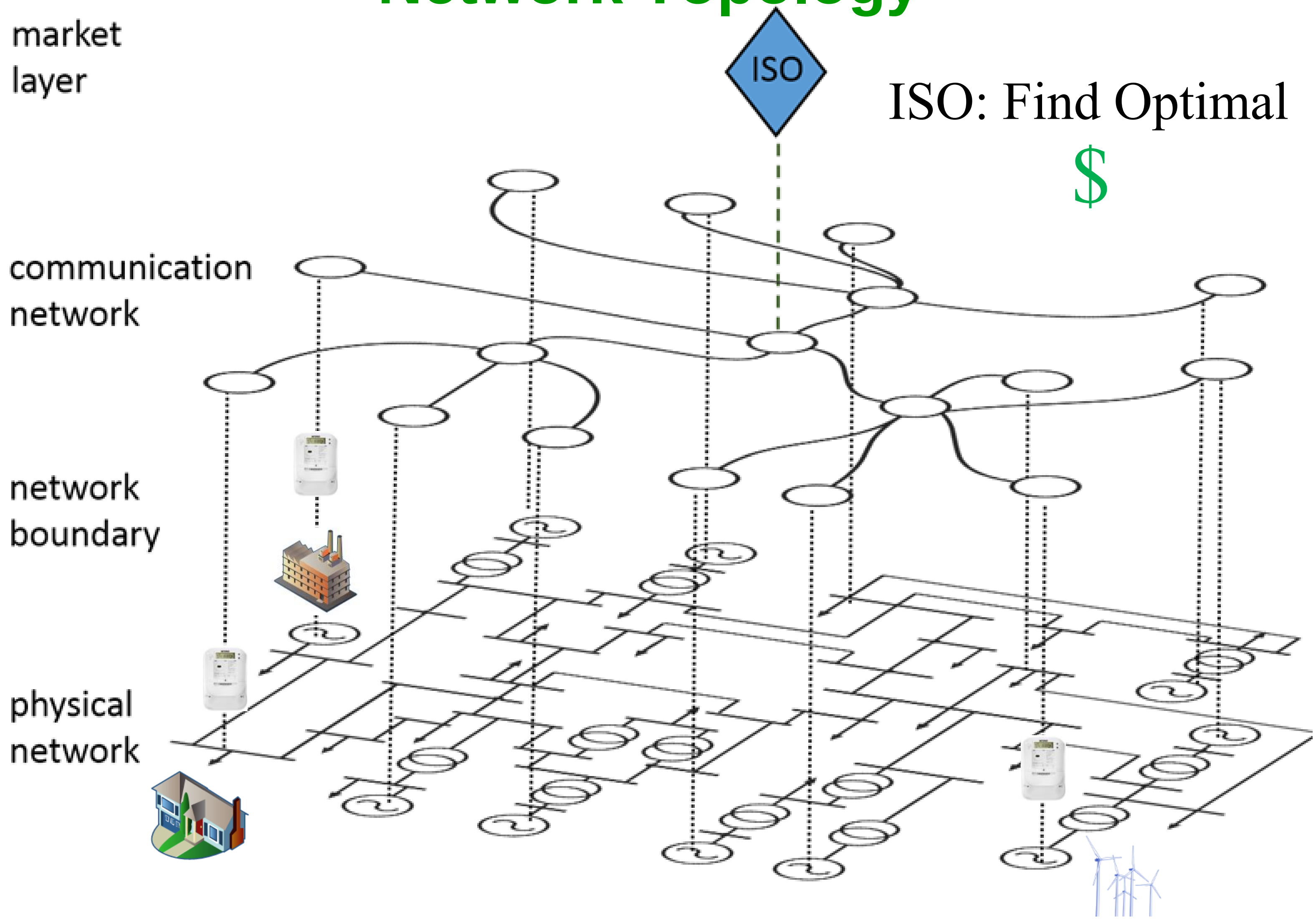
Demand response improves efficiency of the power market by modulating load in response to fluctuating demands and supplies

Dynamic Markets



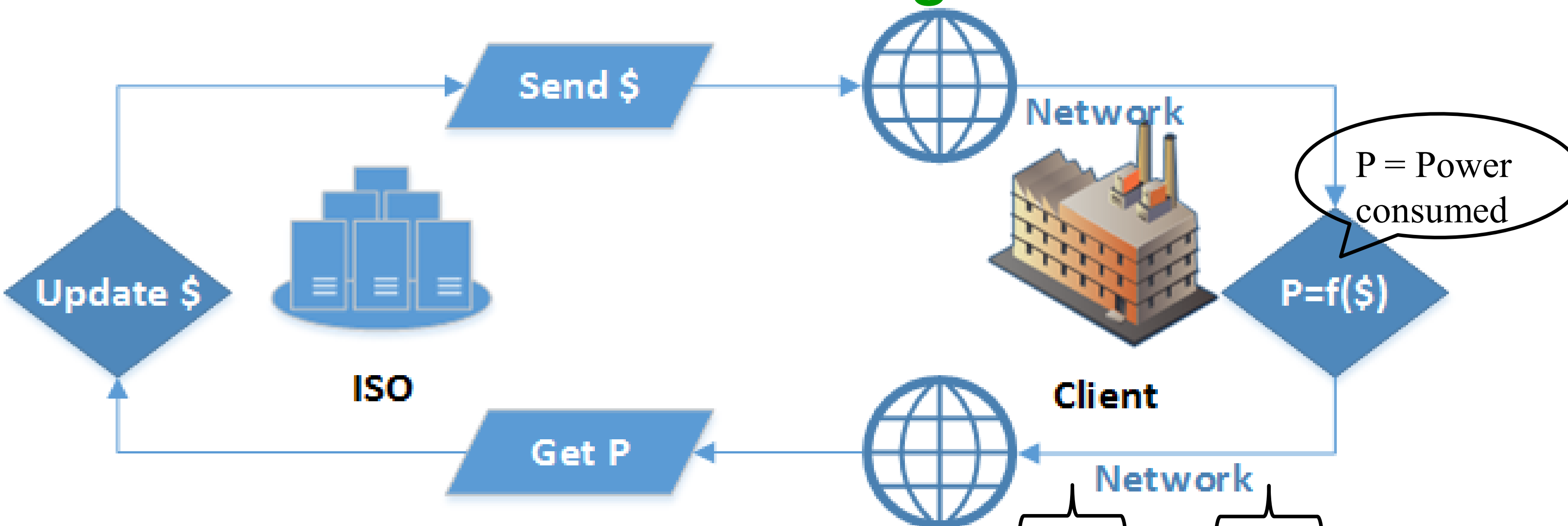
PURDUE
UNIVERSITY

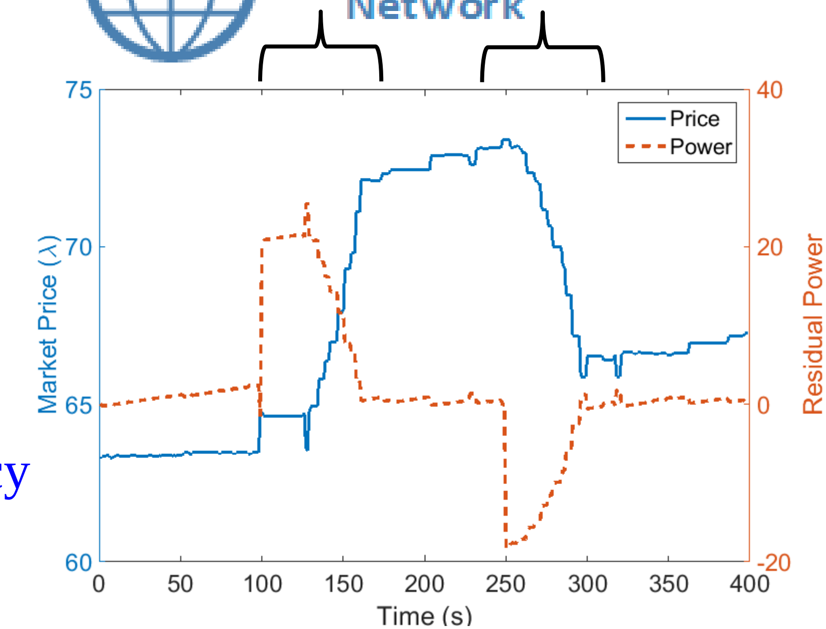
Network Topology



The ISO must communicate price signals across a network to the grid-connected loads

Iterative Market Negotiation

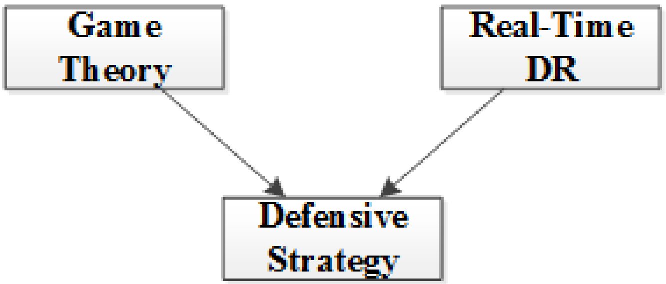




- Real-time communication of price signal by ISO to consumers used for controlling the market
  - Lower latency means better efficiency

Related Work

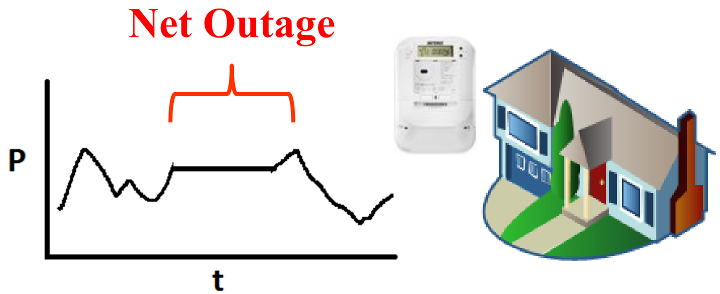
- In [1], latency impacts in real-time communication in DR is evaluated but without any economic incentives
- In [2], economic incentives are introduced but without real-time communications
- Our work combines real-time DR with game theory to formulate defensive strategies



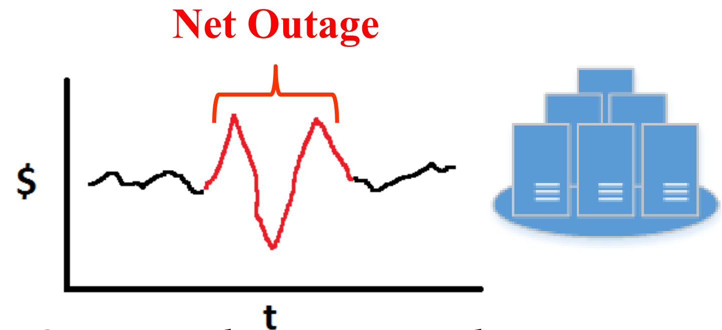
[1] Tan, Rui, et al. "Impact of integrity attacks on real-time pricing in smart grids." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS)*. ACM, 2013.

[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.

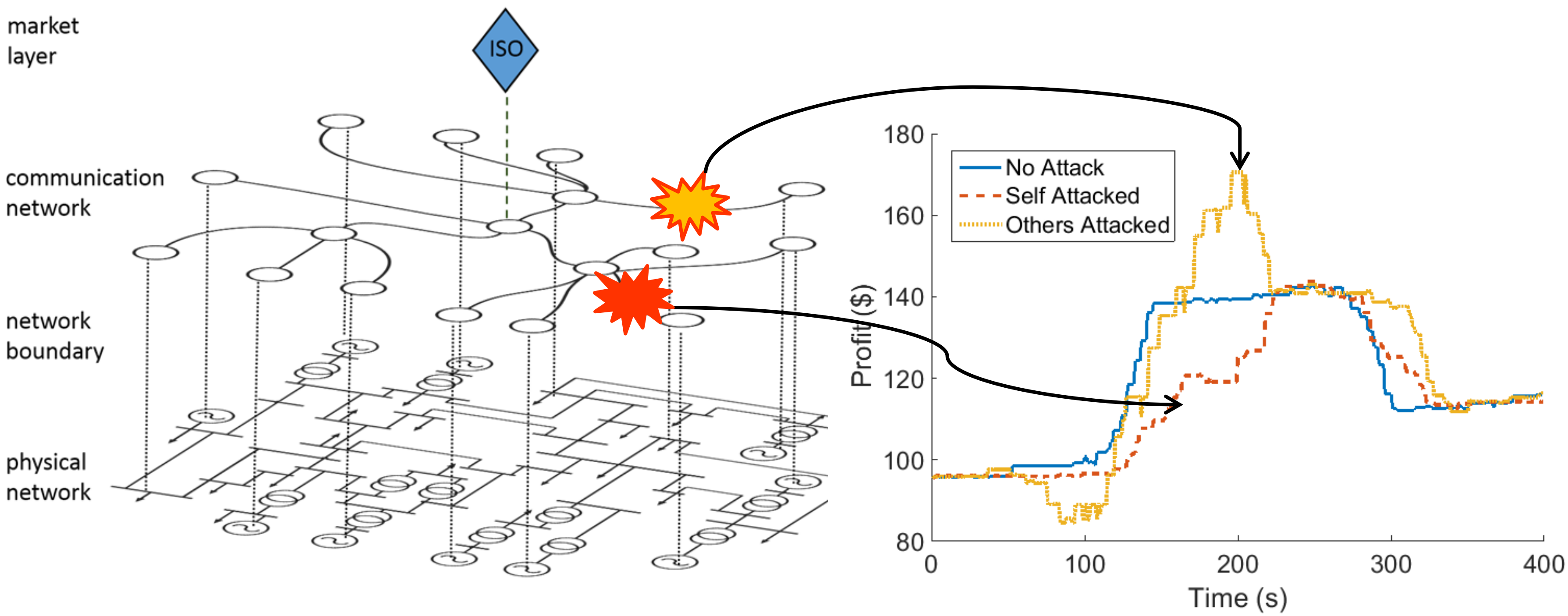
Faults and Attacks



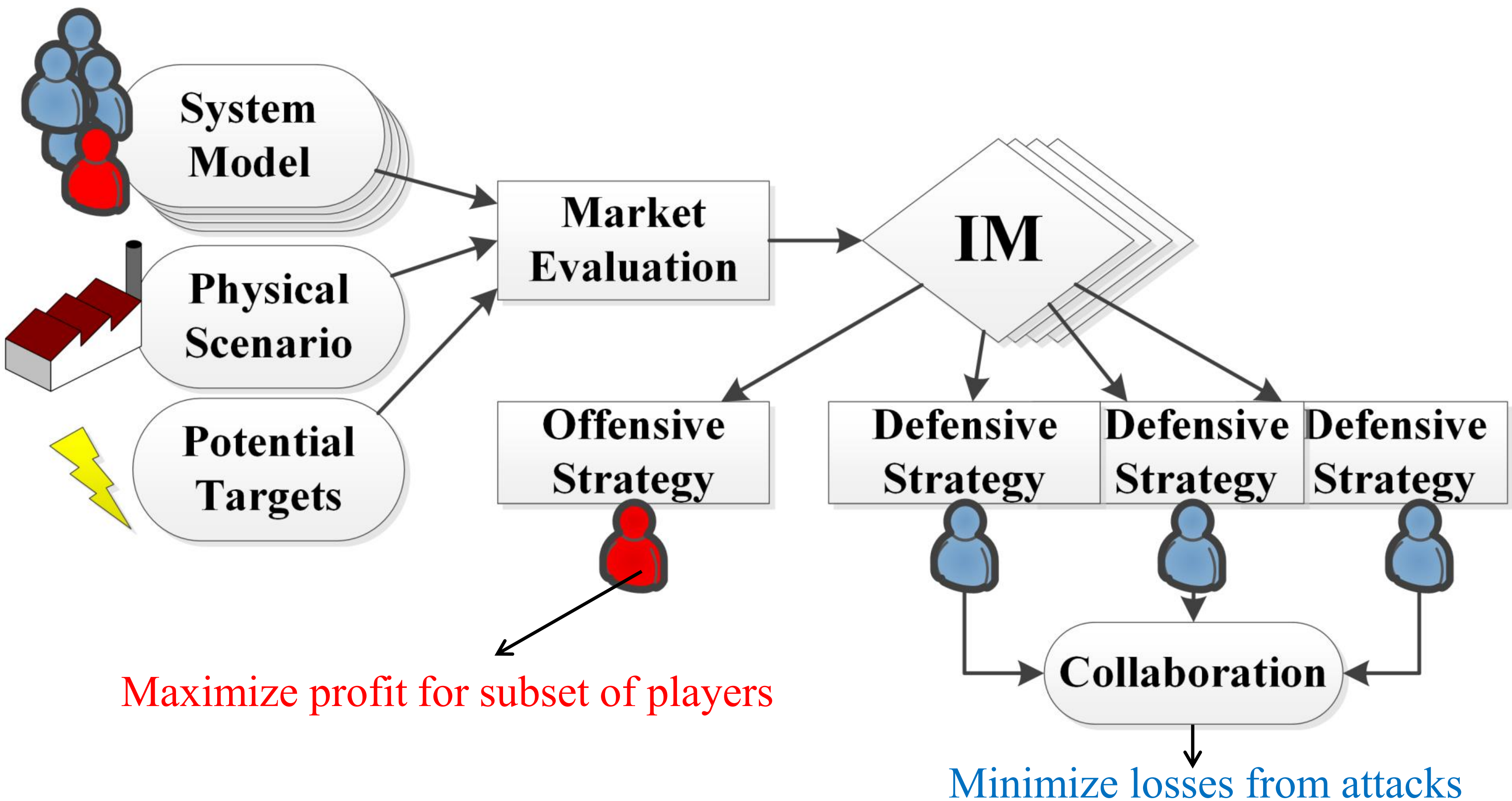
Outage reduces demand response



Outage changes market price



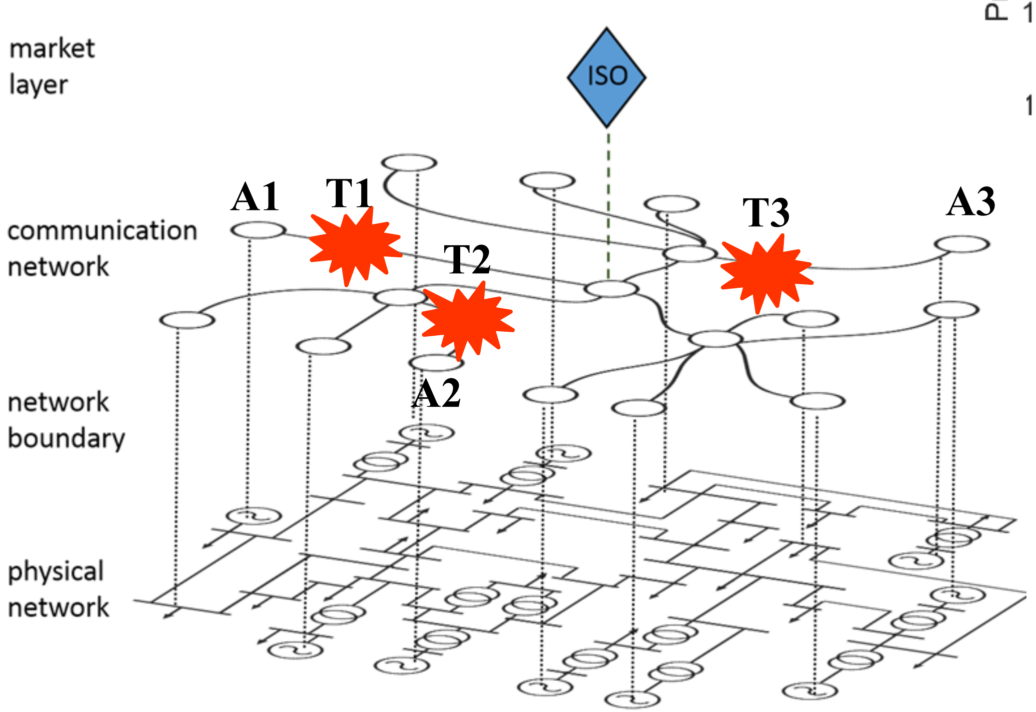
Attack and Defense

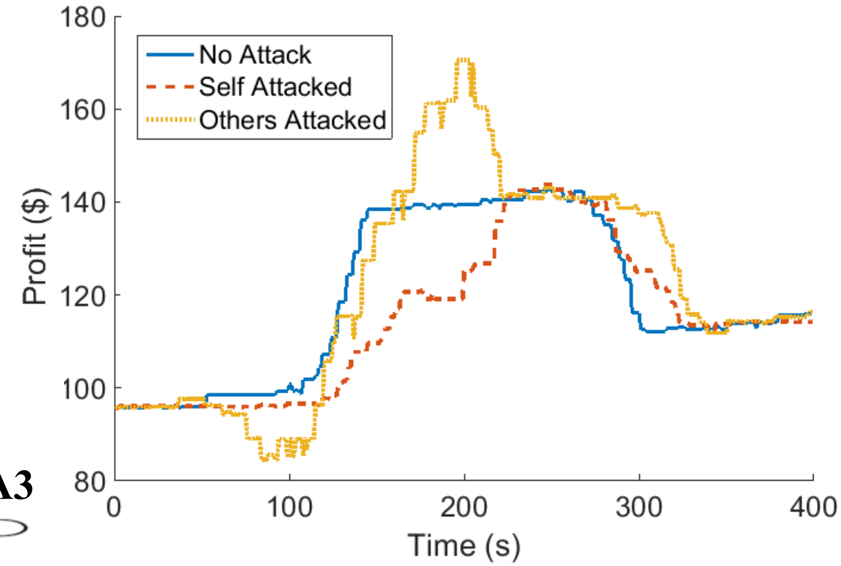


Target Impact Matrix

The impact of attacking different targets is captured in a matrix (IM)

No-attack compared with attack profits

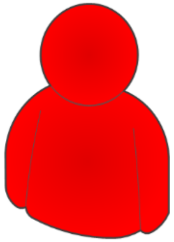


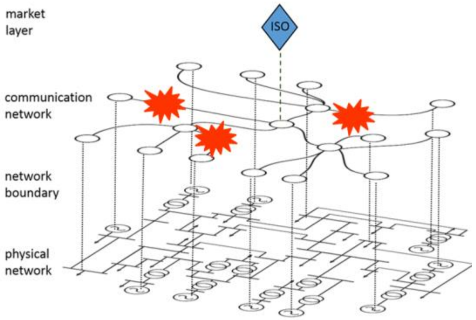


	T1	T2	T3
A1	-2	-2	3
A2	4	-4	-2
A3	-4	2	-4

Impact Matrix (IM)

Attacker Strategy





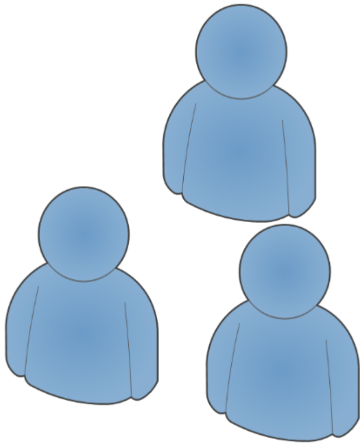
	T1	T2	T3
A1	-2	-2	3
A2	4	-4	-2
A3	-4	2	-4

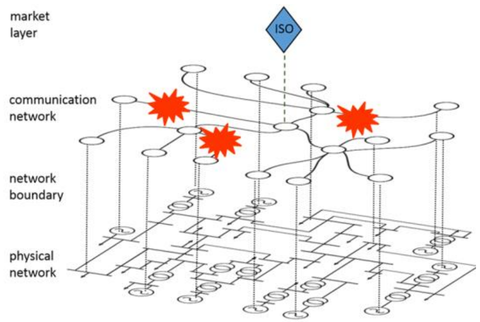
$$\text{argmax}_{A,I} \sum_{a \in A, i \in I} \text{IM}[a, i]$$

A set of market players
I set of target network links

$\text{IM}[a, i]$ impact or change in profit realized by market player a when network link i is attacked

Defender Strategy





T1 most likely attacked

	T1	T2	T3
A1	-2	-2	3
A2	4	-4	-2
A3	-4	2	-4

A1,A3 share benefit from defending T1, so can share costs

$$\max \sum_{\forall a \in A} \sum_{i \in I} A_i \overbrace{\mathrm{IM}[a,i]}^{\text{Comes from defender's estimate}}(1 - D_i) - D_i C_i$$

D_i boolean indicating if network link i is defended

C_i cost to defend asset i

A_i boolean indicating if network link i is attacked

Sampling and Solving

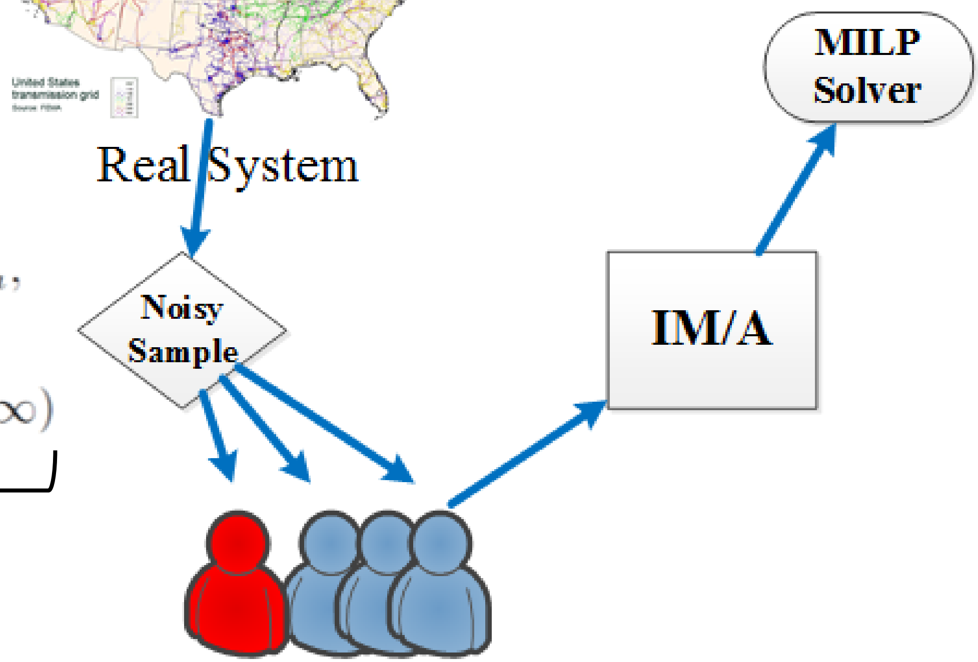
The real system is sampled
to provide mixed strategies
for the attackers and defenders

Knowledge level

$$\underbrace{\begin{gathered} x' = \mathcal{N}(x, \sigma_a^2)\ \forall x \in GA,\ x \notin O_a, \\ x' = x\ \ \forall x \in GA, x \in O_a \\ x' \in (-\infty, 0] \text{ if } x' < 0,\ \text{else } x' \in [0, \infty) \end{gathered}}_{\textit{Constraint maintenance}}$$

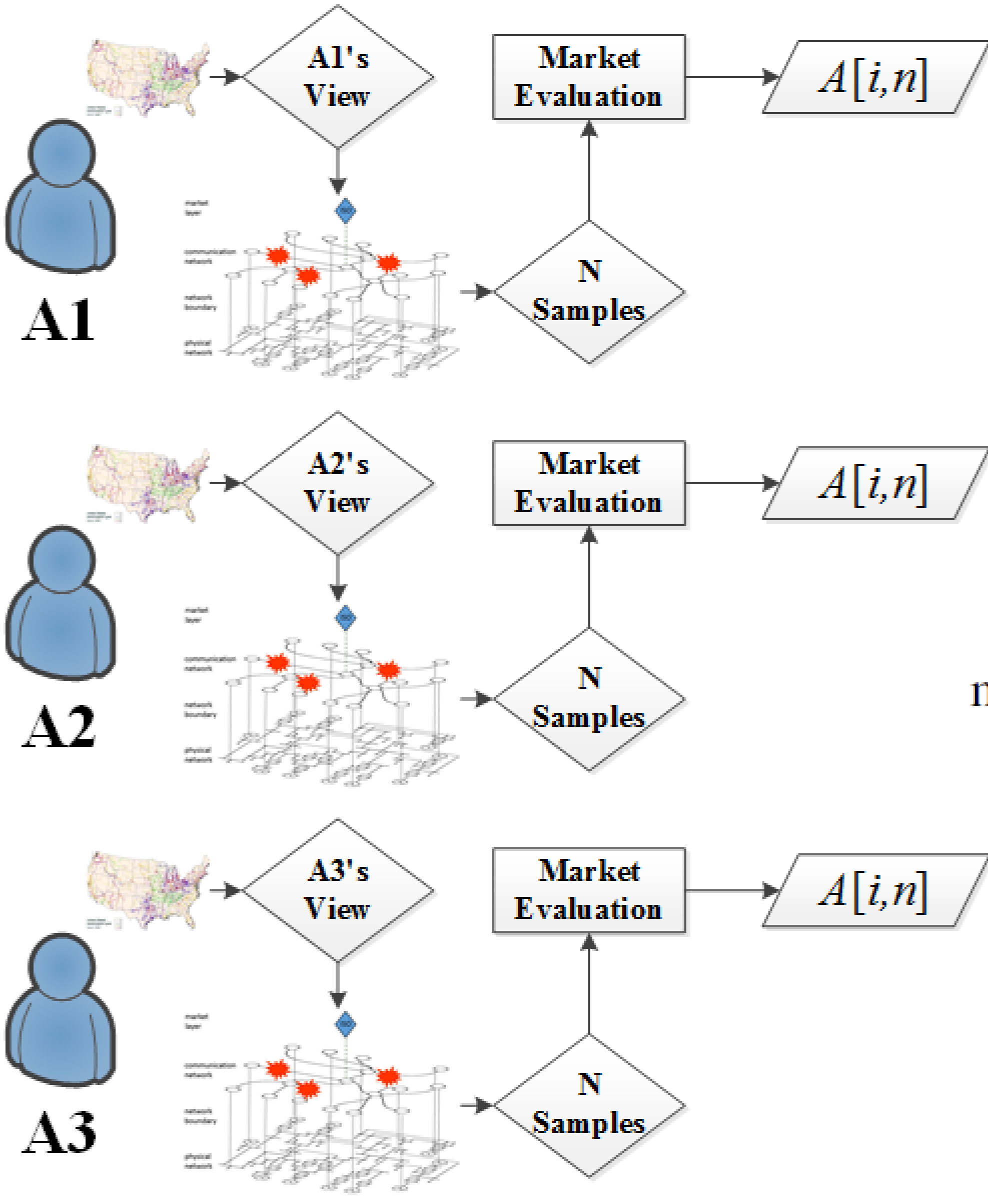
$$\text{argmax}_{A,I} \sum_{a \in A, i \in I} \text{IM}[a, i]$$

$$\max \sum_{\forall a \in A} \sum_{i \in I} P_i^a \text{IM}[a, i](1 - D_i) - D_i C_i$$



PURDUE
UNIVERSITY

Mixed Defender Strategies



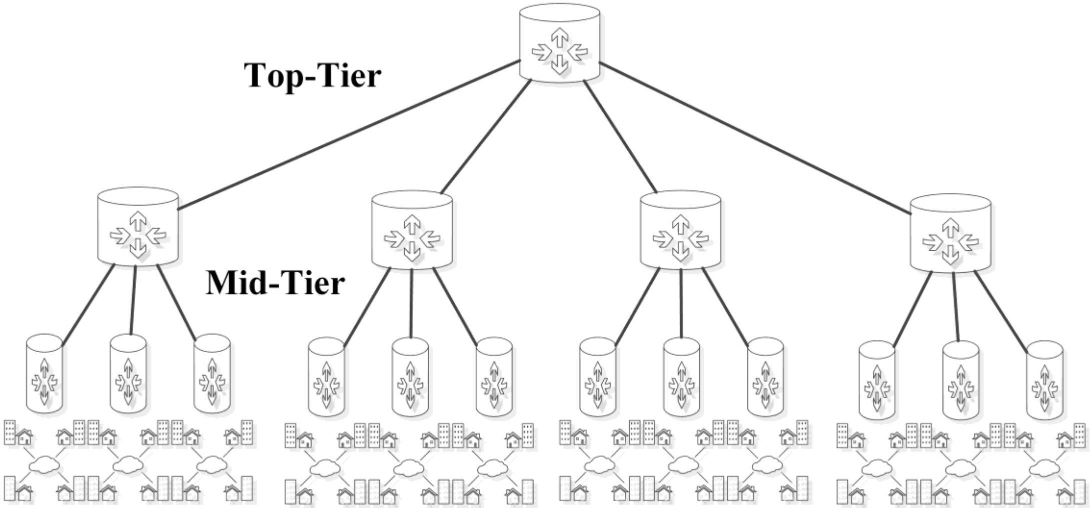
$$P_i^a = \frac{\overbrace{\sum_{n \in N}}^{\textit{N samples of underlying game}} A[i,n]}{N}$$

$$\max \sum_{\forall a \in A} \sum_{i \in I} P_i^a \mathrm{IM}[a,i](1 - D_i) - D_i C_i$$

Each A1-A3 has a different market view, thus different view on probability of attack

PURDUE UNIVERSITY

Experimentation Topology



20 Generators 100 Consumers

Iterative Nelder-Meade (NM) used to solve market

Cost parameters for attacking or defending each target = 1

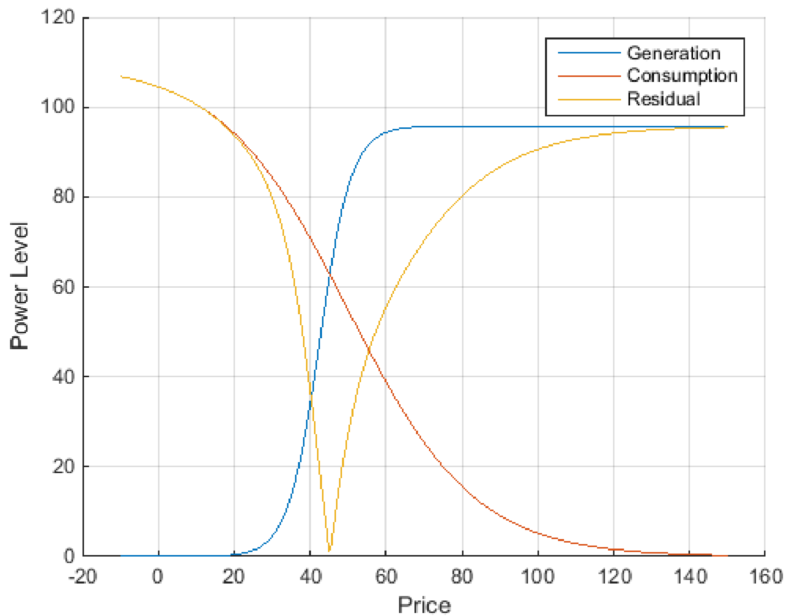
Power-Price Model

Price Scaling (Min/Max Price)

$$\lambda_s = 6 * \frac{\lambda - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}} - 3$$

Price to Power Mapping (Min/Max Power)

$$P(\lambda) = \underbrace{\frac{P_{\max} - P_{\min}}{1 + e^{\lambda_s}}}_{\textit{Sigmoid function}} + P_{\min}$$

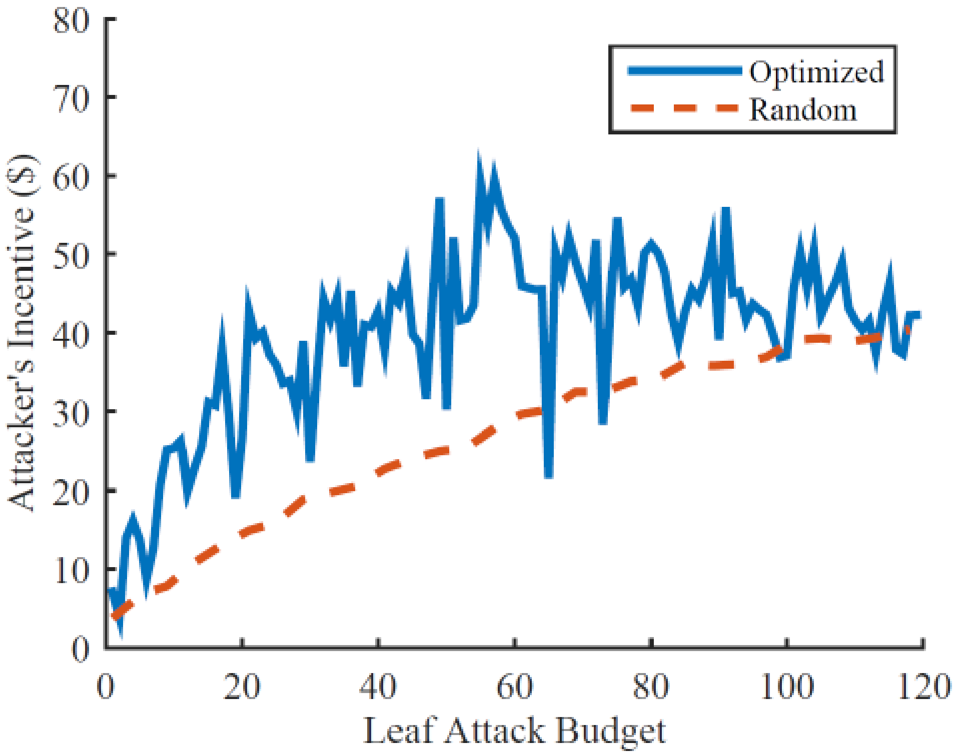


Full parameter definitions in paper

PURDUE UNIVERSITY

Attack Profits – Leaf Attacks

- Attack strategy run for fixed computation limit
  - Impractical to completely search large MILP
    - Best found solution used
- Attack saturated at high budgets
  - Target value is imbalanced

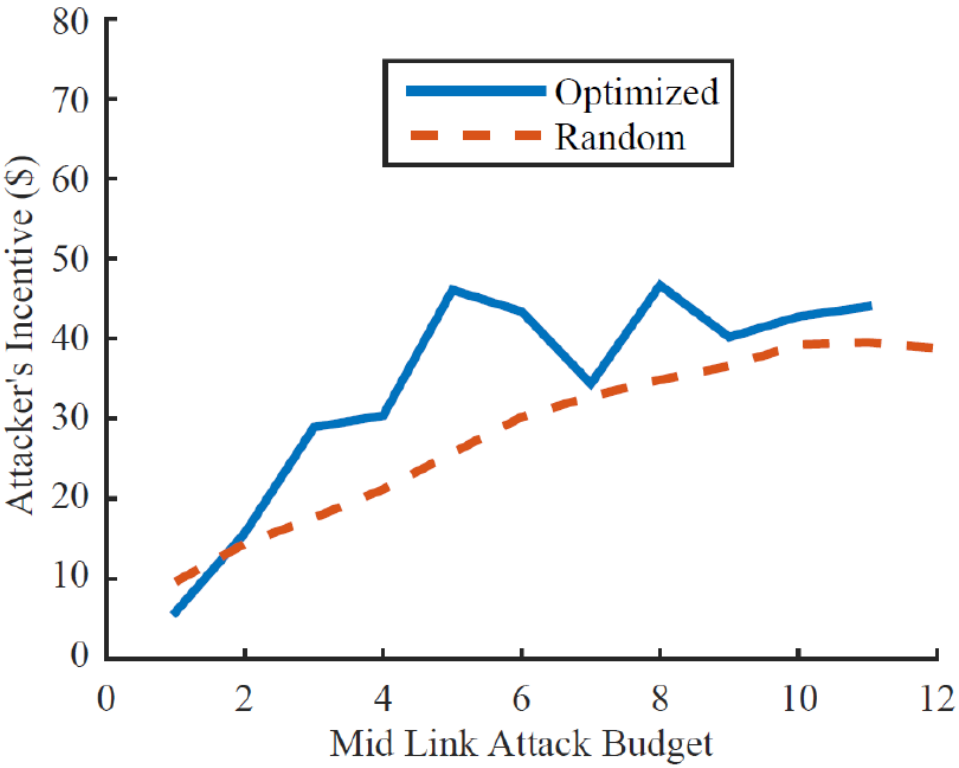


$$\operatorname{argmax}_{A,I} \sum_{a \in A, i \in I} \mathrm{IM}[a, i]$$

PURDUE UNIVERSITY

Attack Profits – Mid-Tier Attacks

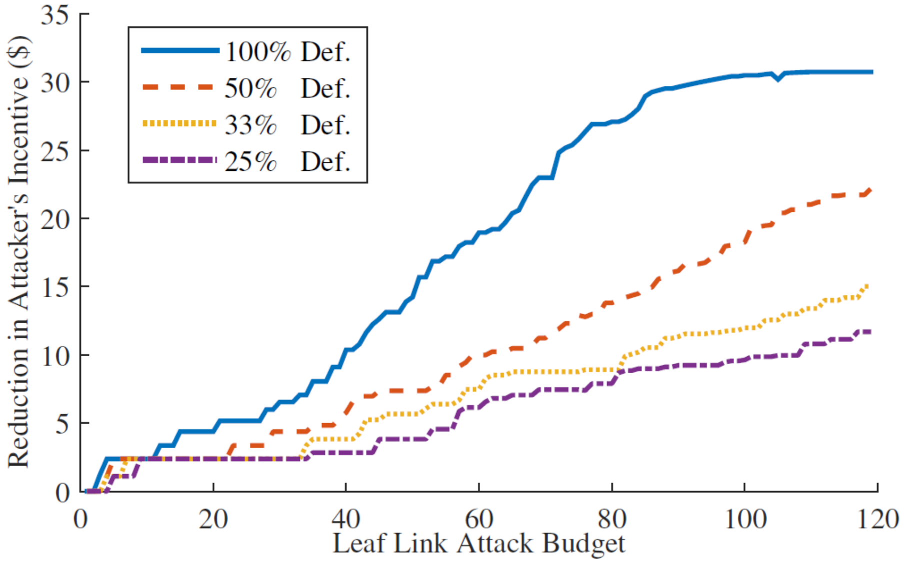
- In this experiment, multiple mid-tier links are attacked
  - IM calculated from mid-tier link attacks only
- Only a few links at this layer need to be attacked to extract profit



$$\text{argmax}_{A,I} \sum_{a \in A, i \in I} \text{IM}[a, i]$$

Defensive Strategy

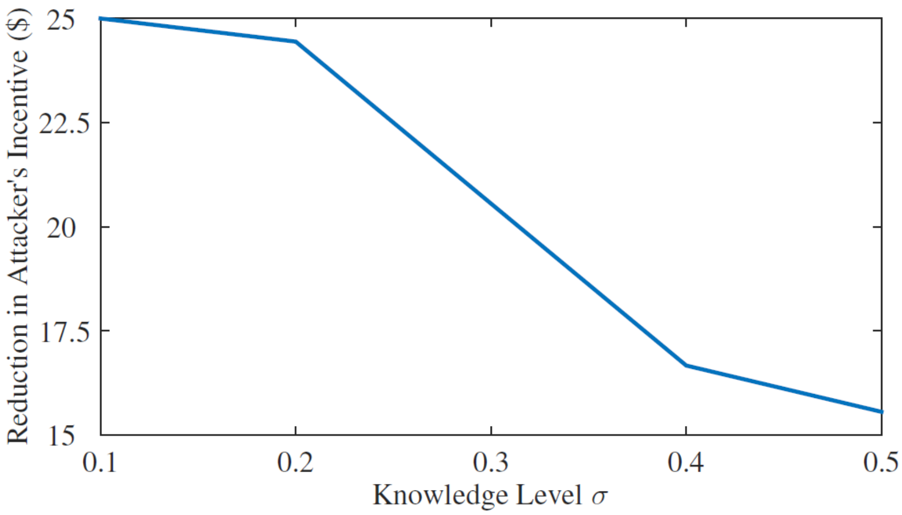
- The defensive strategy is tested with increasing defensive budgets
  - With 100% defense the attacker has no success
  - The attacker is unaware of defensive maneuvers
  - Defenders have imperfect system knowledge



$$\max \sum_{\forall a \in A} \sum_{i \in I} A_i \mathrm{IM}[a,i](1-D_i) - D_i C_i$$

Reduced System Knowledge

- The defenders' knowledge is reduced (higher σ) and a defensive strategy for 75 targets is optimized
  - The strategy's effectiveness decreases with less system knowledge
  - Defenders should share system information when possible to maximize effectiveness



$$x' = \mathcal{N}(x, \sigma_a^2)\ \forall x \in GA,\ x \notin O_a,$$
$$x' = x \quad \forall x \in GA, x \in O_a$$
$$x' \in (-\infty, 0] \text{ if } x' < 0,\ \text{else } x' \in [0, \infty)$$

Conclusions and Future Work

Conclusion

- Future smart grid (DR) may be vulnerable to attacks
- Attack/defense strategies
  - Attacker can improve profits by planning attacks based on estimated impact matrix
  - Defender can reduce impact by optimally selecting targets
  - Knowledge sharing and cost sharing among defenders can improve system resilience

Future Work

- On-line strategies
  - Attack/defense in response to real-time, unpredictable transients
  - Strategy improvement over time (machine learning)
- Topology optimization
  - Defense via architecture
  - Select topology to minimize impact of attacks