Optimizing Defensive Investments in Energy-Based Cyber-Physical Systems

Paul Wood (Purdue University),
Saurabh Bagchi (Purdue), and Alefiya Hussain (USC/ISI)

DPDNS 15, May 29, 2015

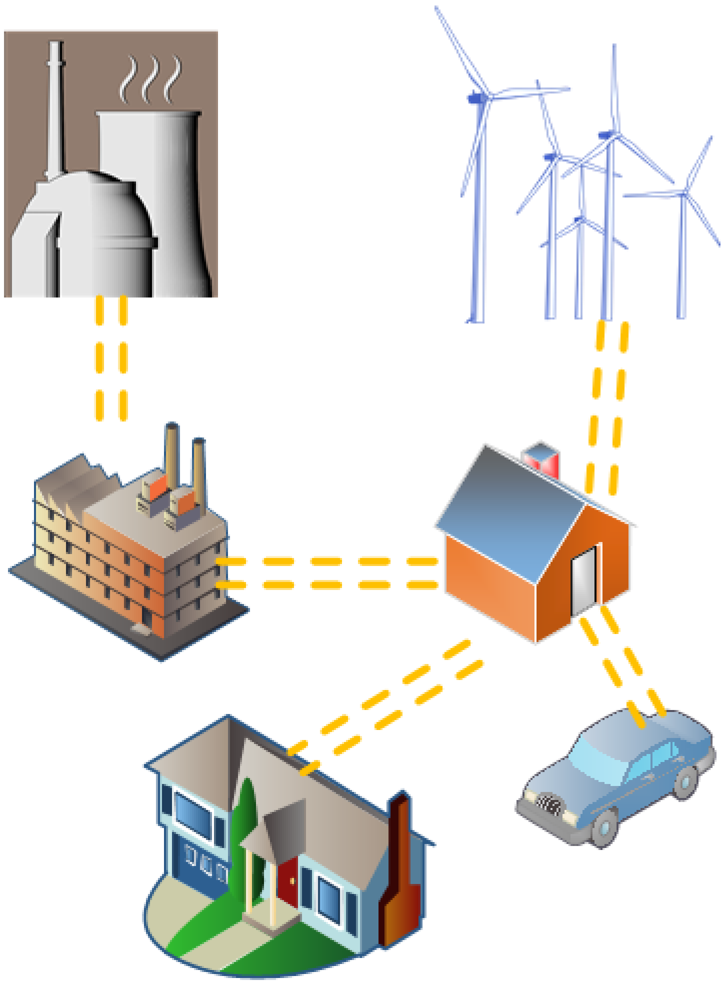
Energy-Based Cyber-Physical Systems

- Energy-based
  - Difficult resource to store
  - Efficiency gains from real-time control
- Cyber-Physical System
  - Part cyber
    - Computation, communication
  - Part physical
    - Electric power, controls

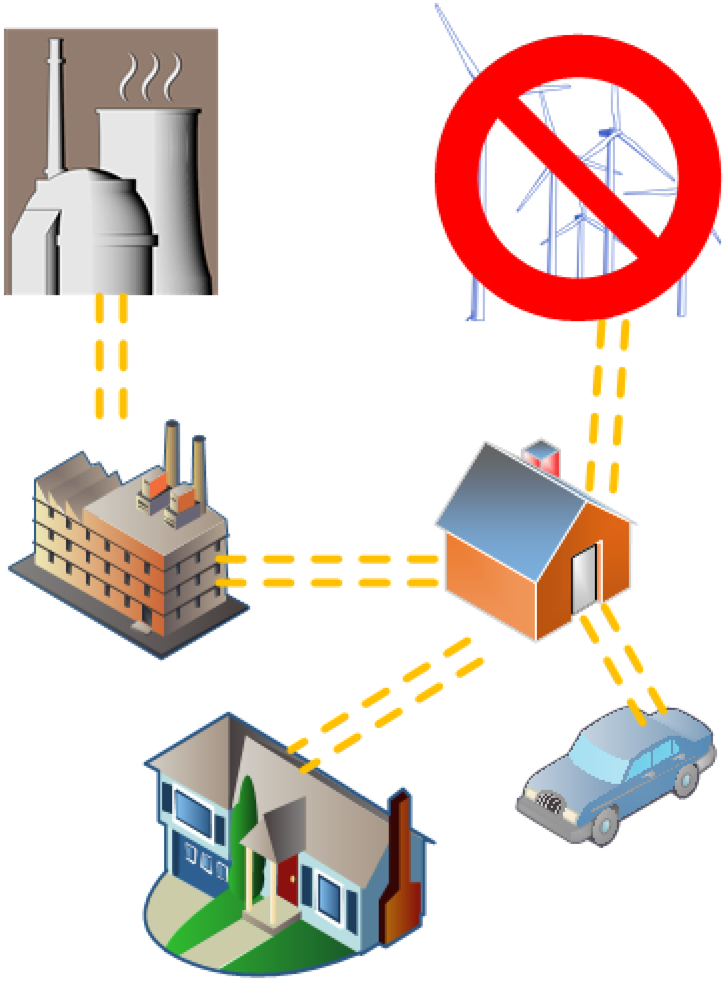
Energy System Trends

- Increasing Renewables
  - – Unpredictability
- Extended feedback loops
  - – Smart meter controls
- Deregulated and dynamic markets
  - – Near real-time prices
- ICS-CERT trends
  - – Control system hacks plausible

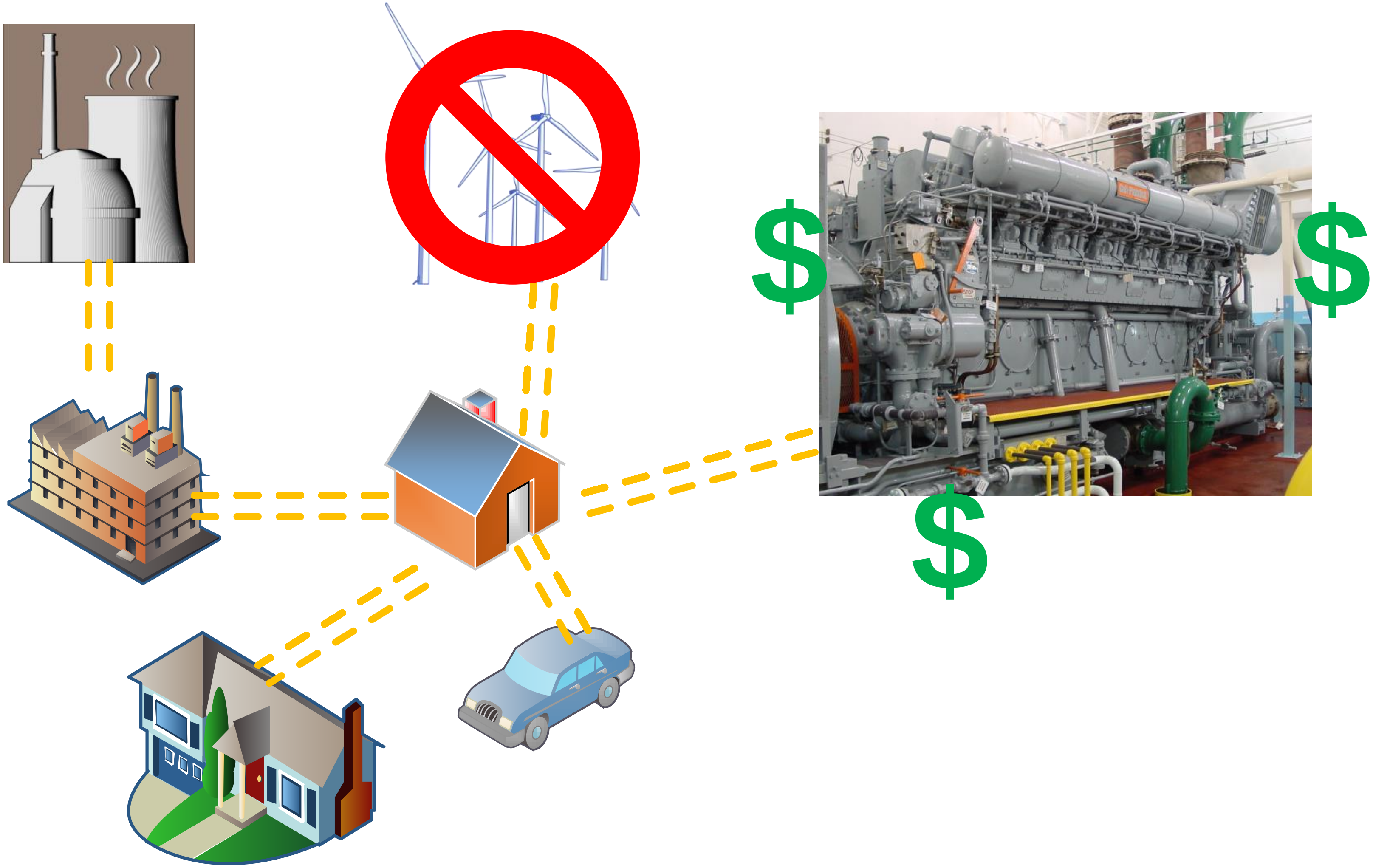
Renewables and Smart Grids



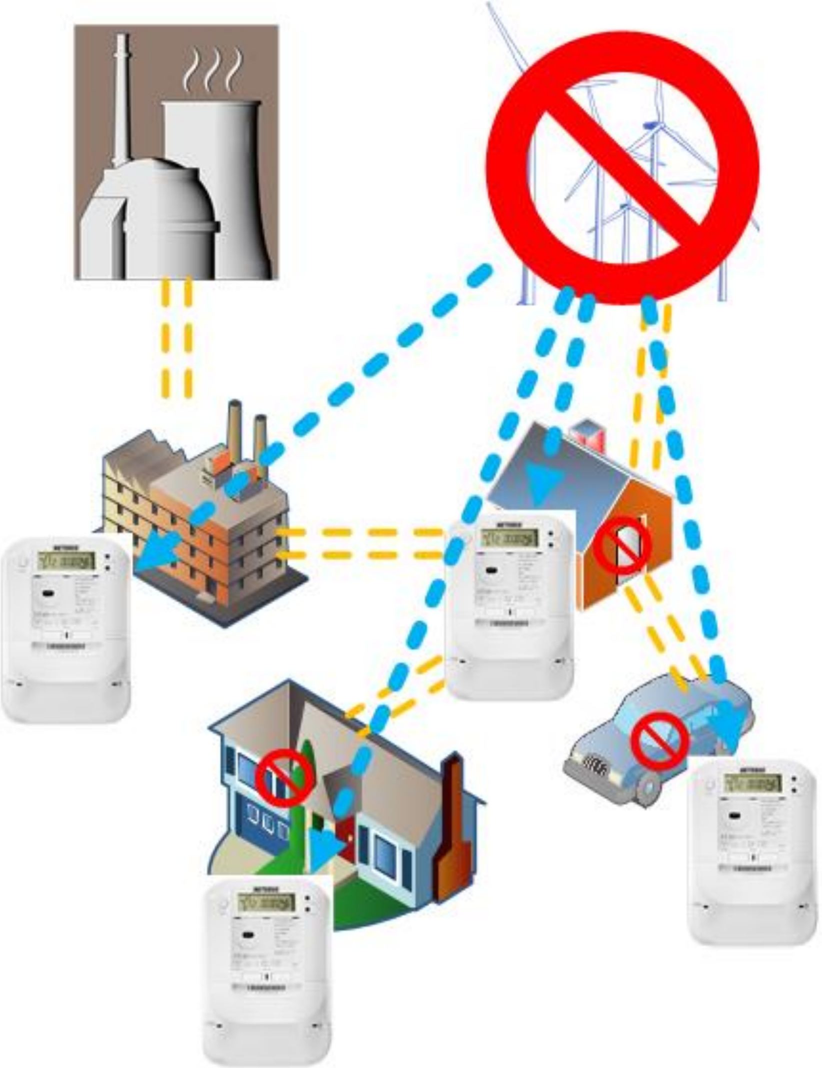
Renewables and Smart Grids



Renewables and Smart Grids

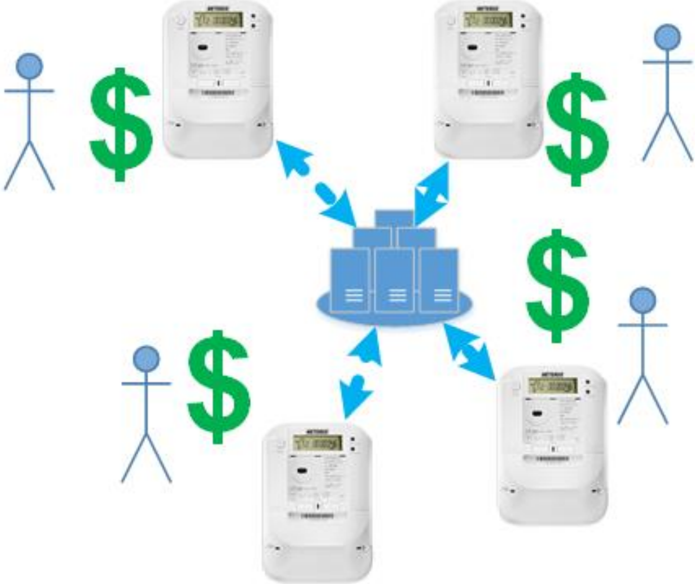


Renewables and Smart Grids



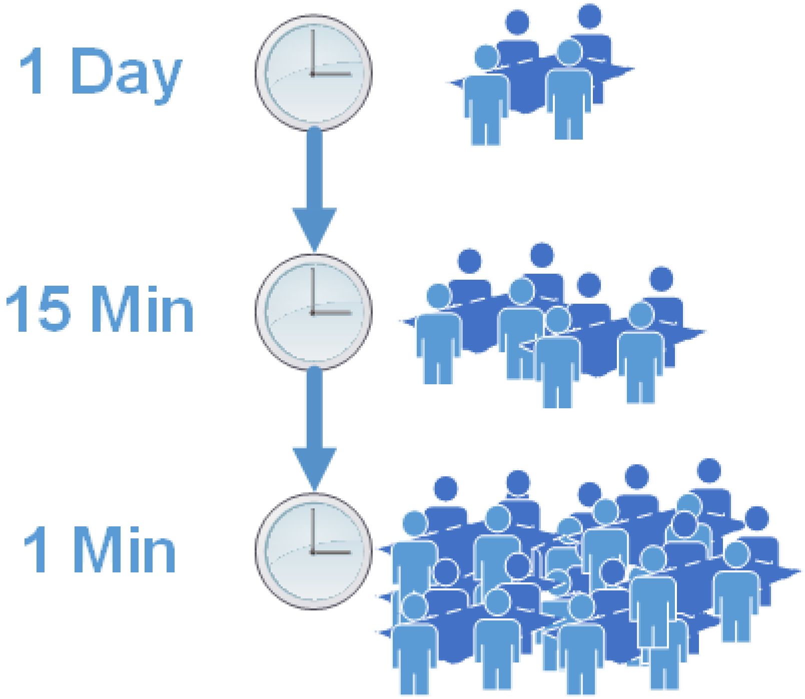
Renewables and Smart Grids

Vs.



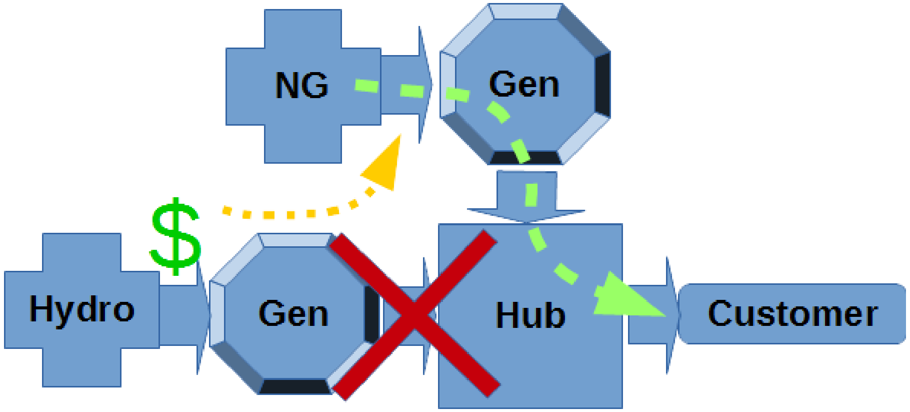
Power Markets

- Purpose
  - – Optimize generation
- Deregulation
  - – Price negotiation
- Smart grid
  - – Negotiation speed
- Renewables
  - – Real-time necessity

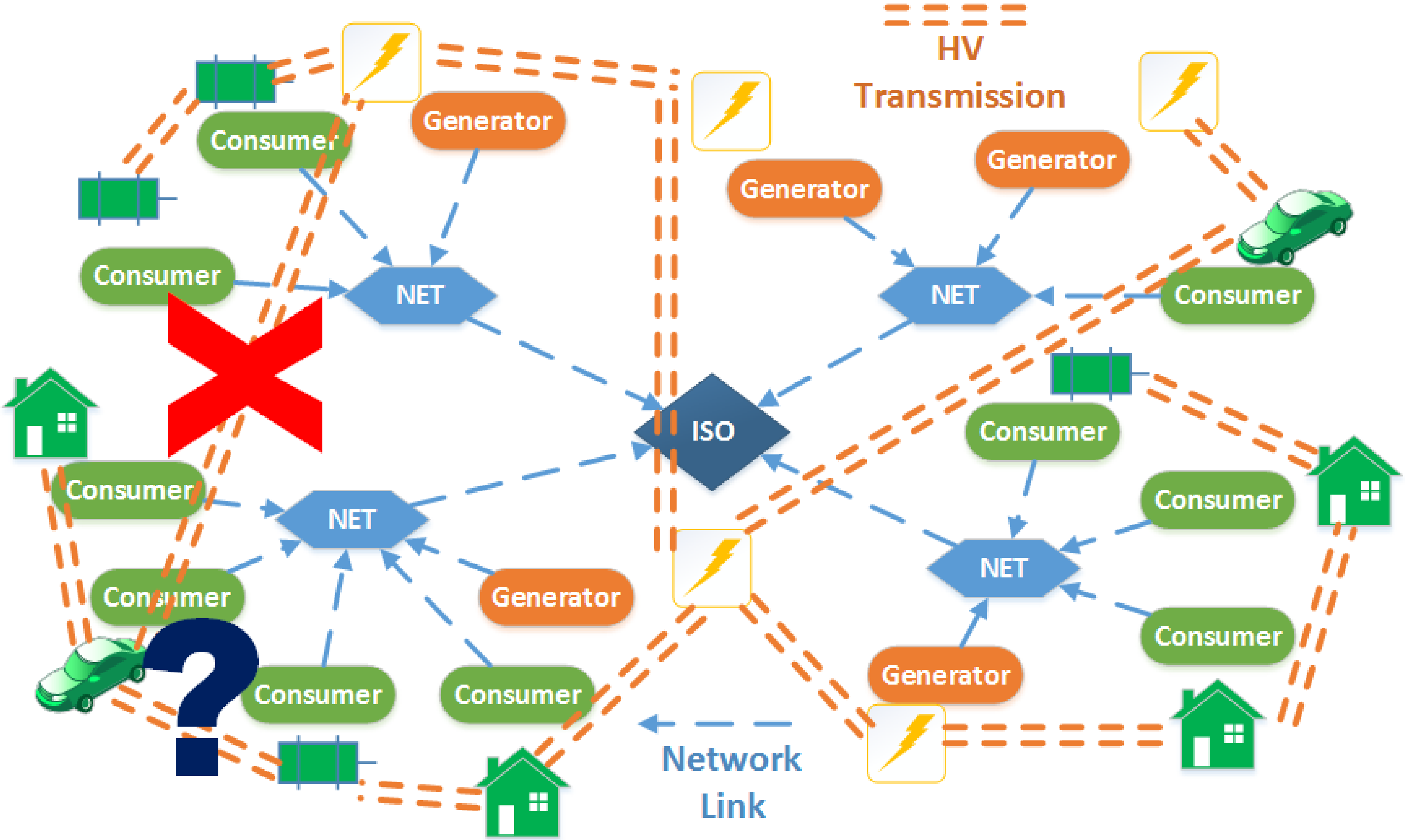


Profitable Attack Vector

- Fungible resource
  - Buy low, sell high
  - Eliminate competitors
- Incentive tracking
  - Market winners
    - Adversary
  - Market losers
    - Defenders
- Exclusions
  - Natural faults, random attacks, political motives



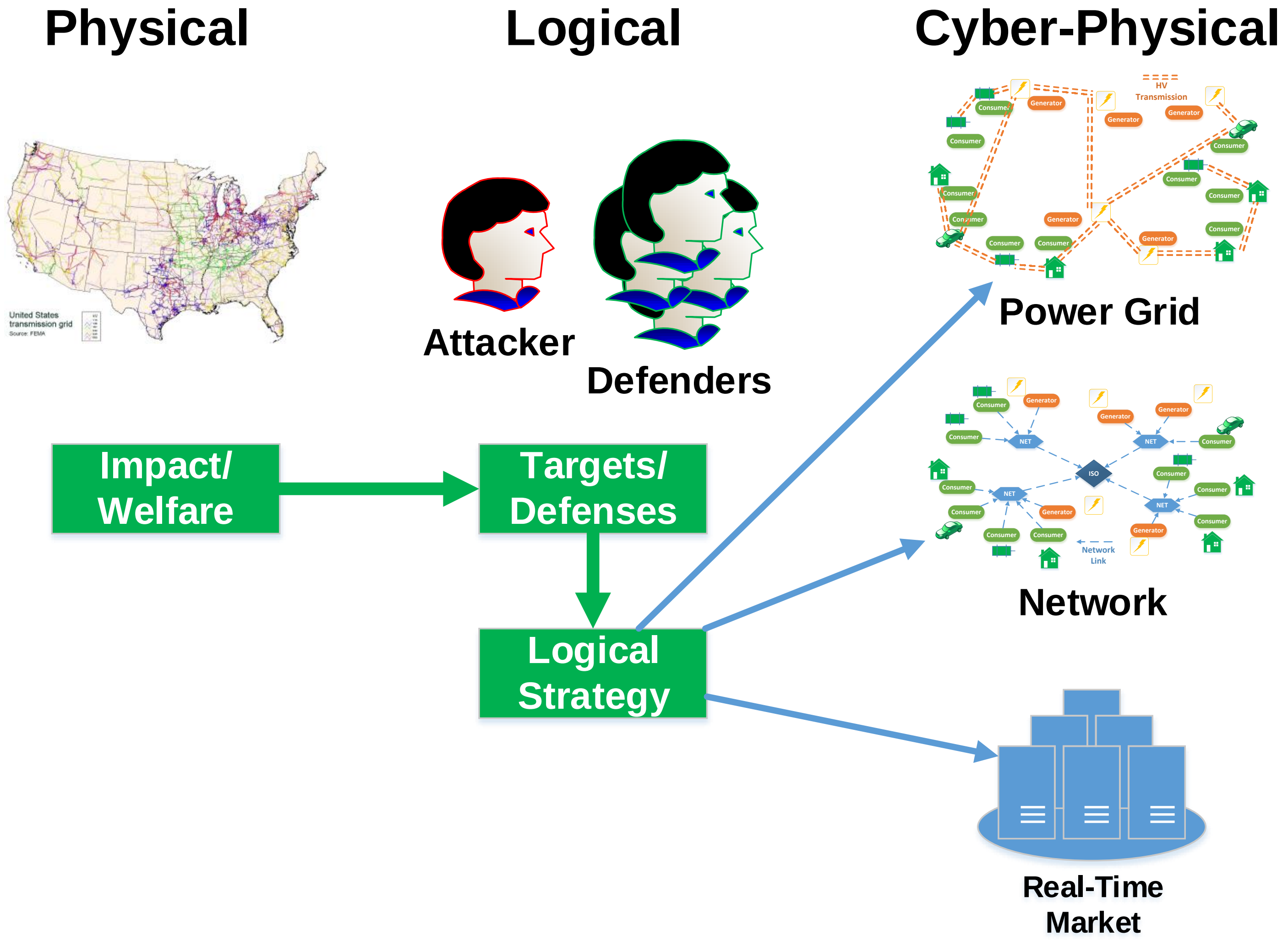
Power Infrastructure Attacks



Dependability Improvement Roadmap

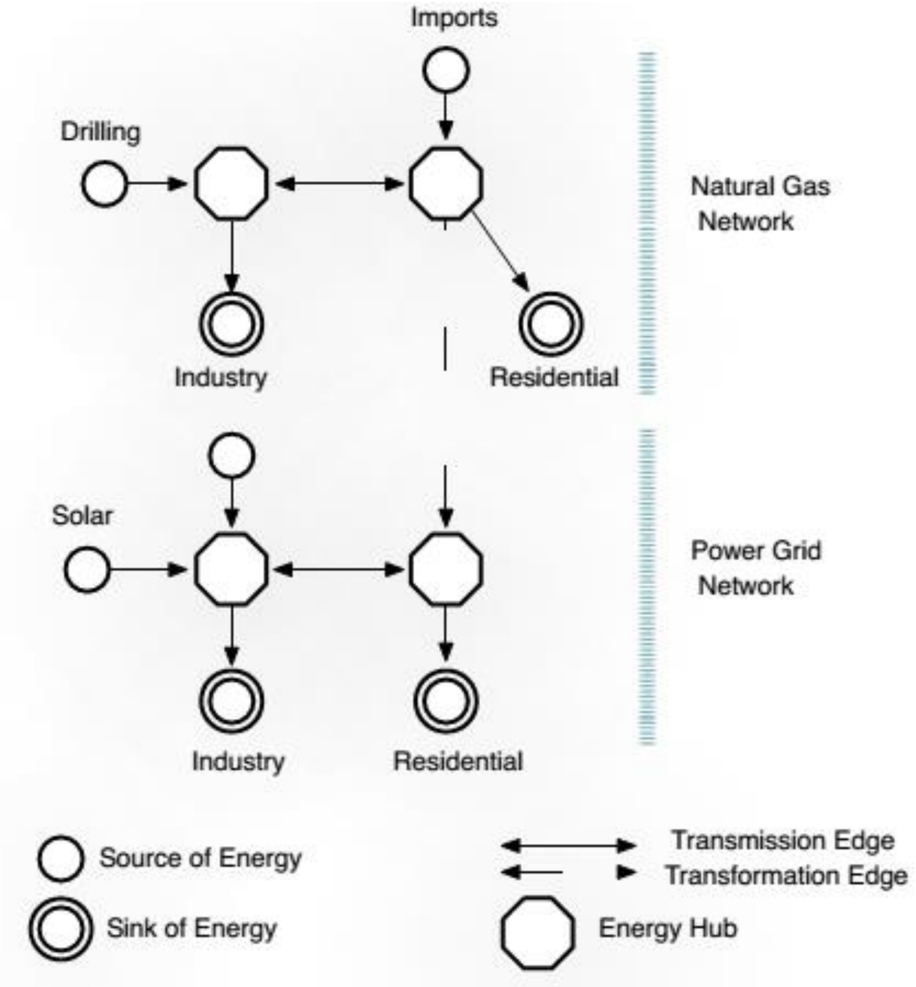
- Track the flow of money
  - What happens during an attack, who profits?
  - Where are attacks likely?
- Stop the flow of money with defenses
  - Which assets are targets, what do I protect?
  - Optimizing defensive investments
- Interdependent aspects
  - How can interdependent market players improve defenses?

Modeling Attacks and Defenses

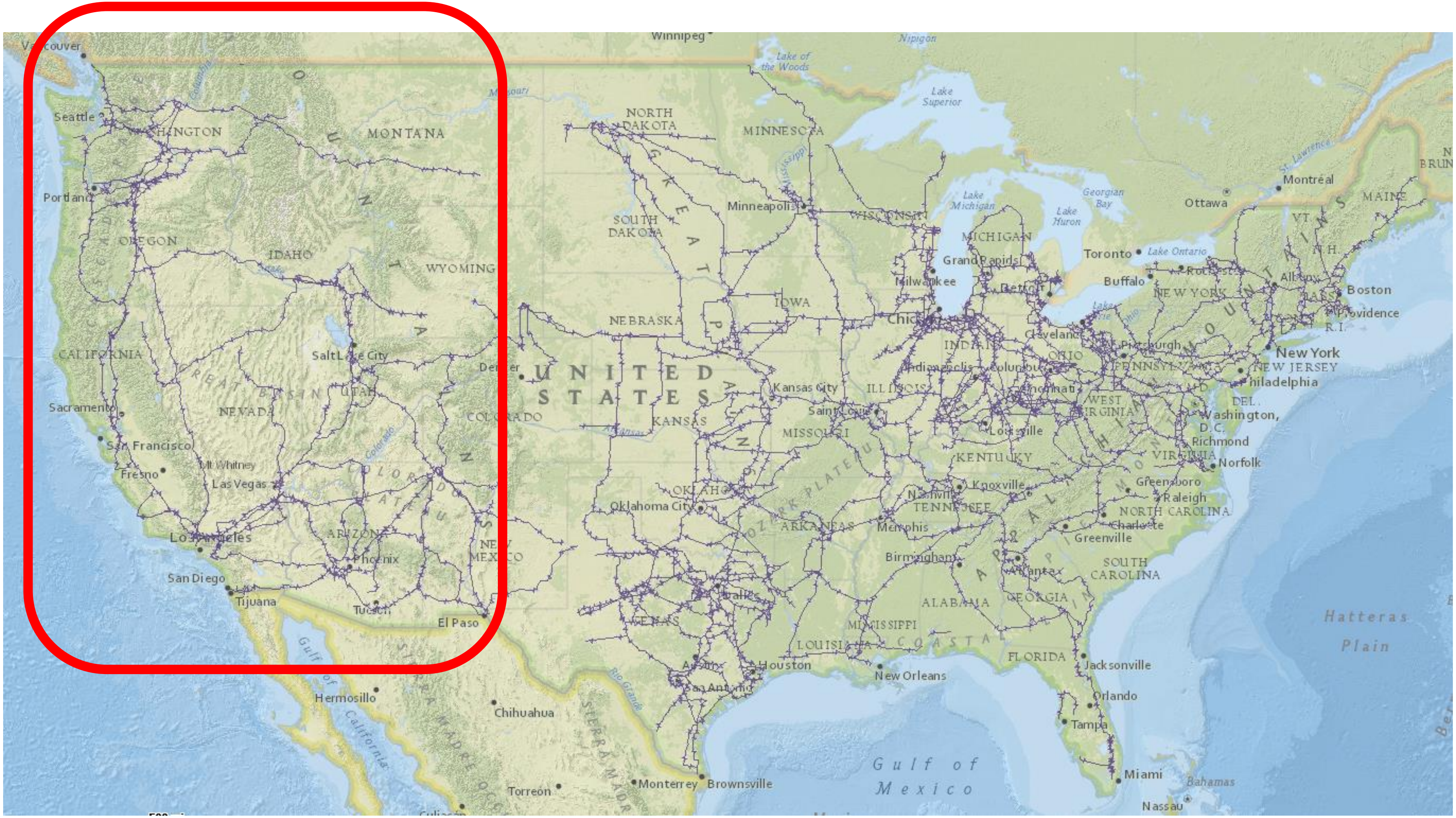


Physical System as a Graph

- Physical (Logical) assets
  - – Generators (Sources)
  - – Wells (Sources)
  - – Transmission (Edges)
  - – Consumers (Sinks)
- Ownership
  - – Actors own assets
- Constraints
  - – Capacity
  - – Losses
- Costs



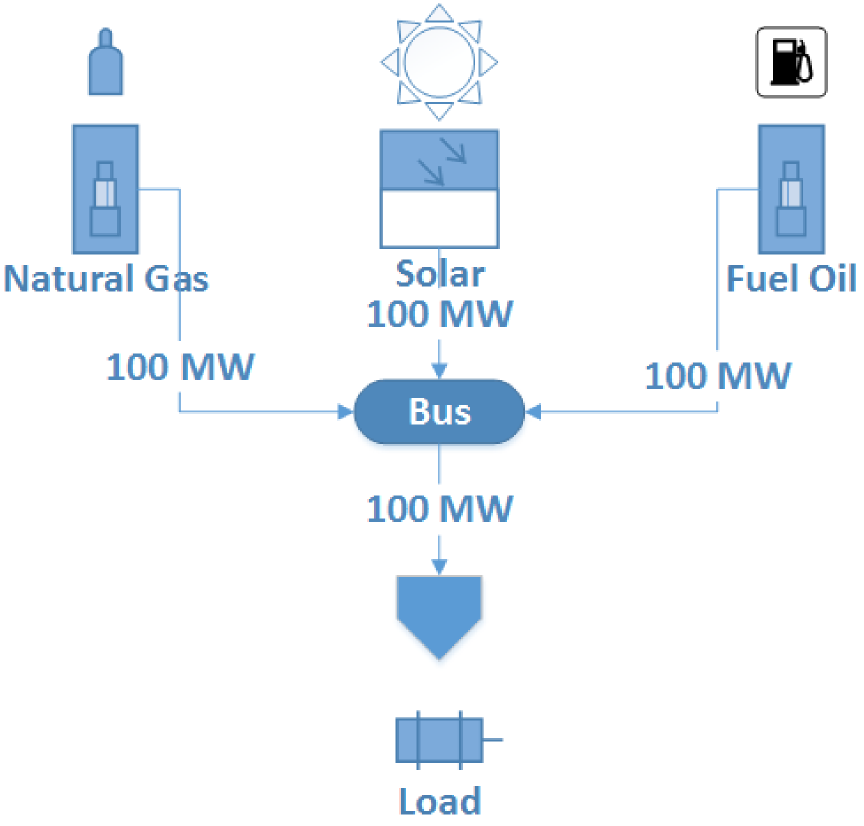
Capturing a Test Market



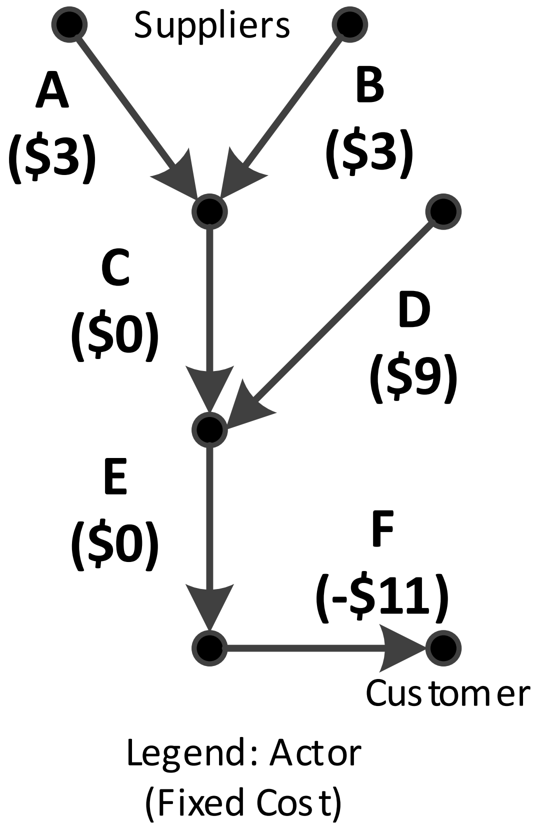
Data Source: U.S. Energy Information Agency (Public)

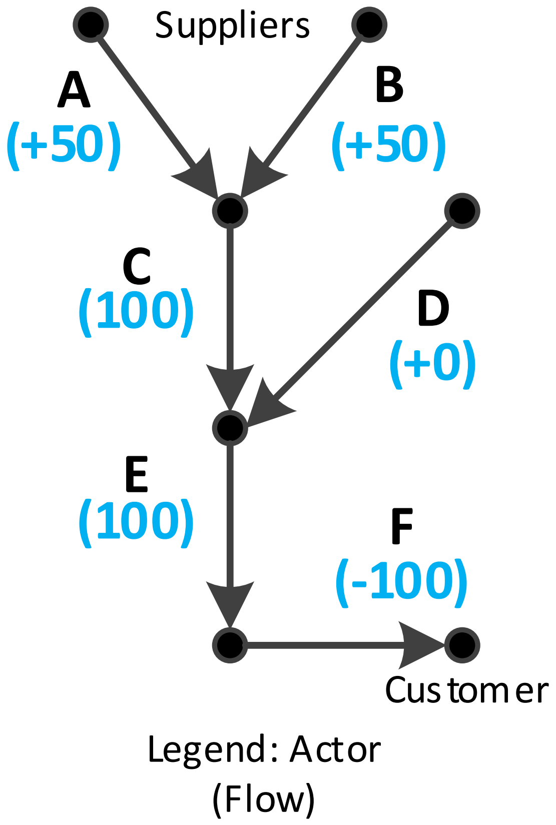
Optimal Power Flow (OPF)

- Single company
- Wide area negotiation
  - Locational Marginal Price (LMP)
- Regulated consumer
- Goal:
  maximize social welfare
  - Minimize costs
  - Maximize revenues



OPF Example



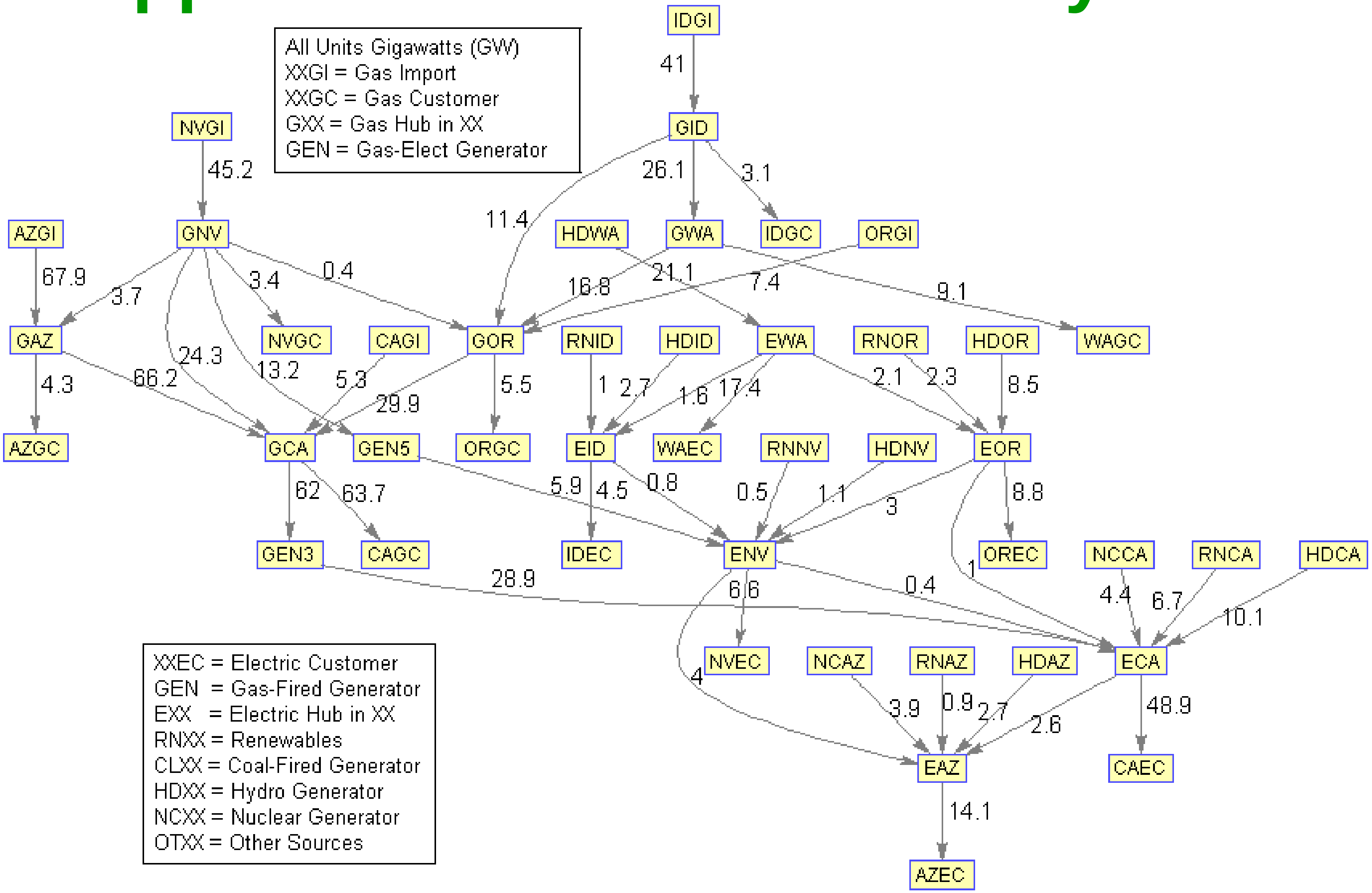


All Capacity=100 units

Profit = $1100-$300 = $800

Solvable with Linear Programming (LP)

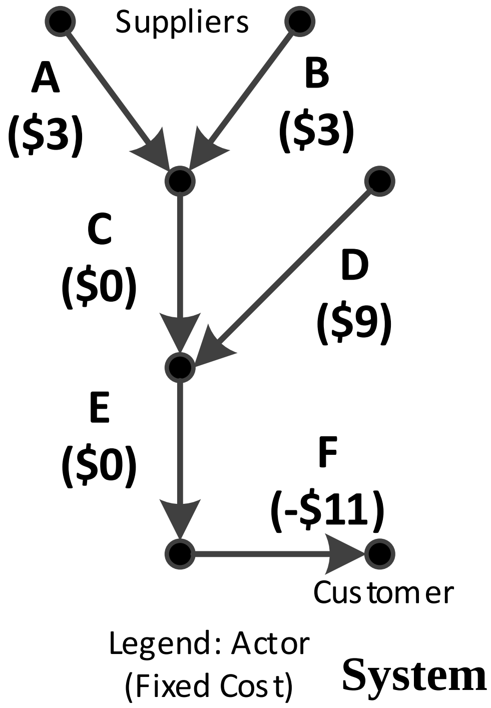
Application of OPF to Test System

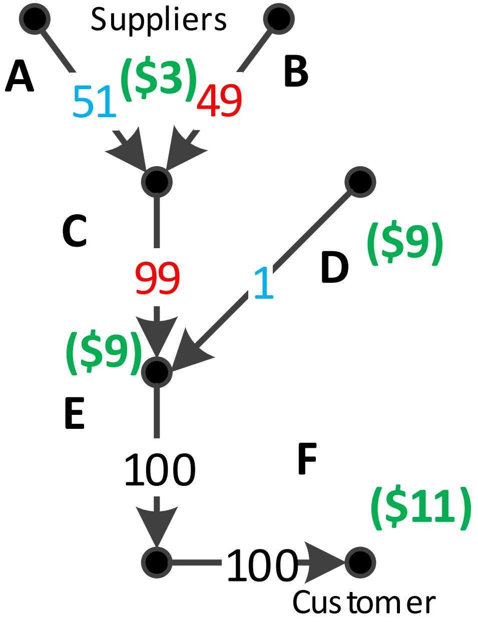


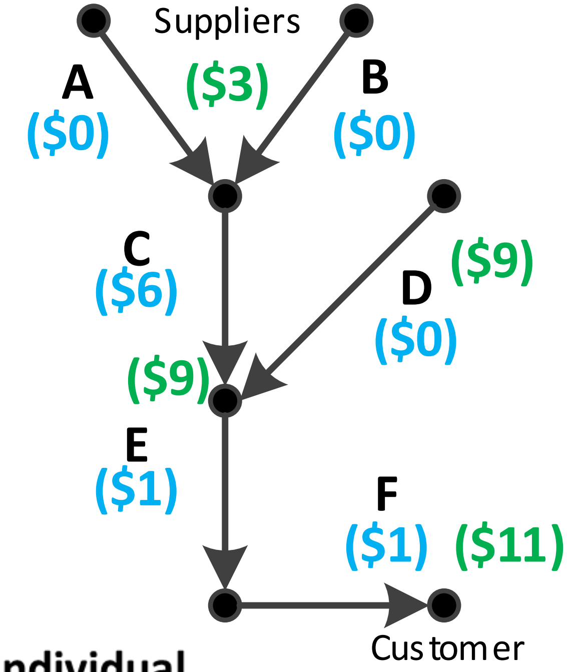
All Units Gigawatts (GW)
XXGI = Gas Import
XXGC = Gas Customer
GXX = Gas Hub in XX
GEN = Gas-Elect Generator

XXEC = Electric Customer
GEN = Gas-Fired Generator
EXX = Electric Hub in XX
RNXX = Renewables
CLXX = Coal-Fired Generator
HDXX = Hydro Generator
NCXX = Nuclear Generator
OTXX = Other Sources

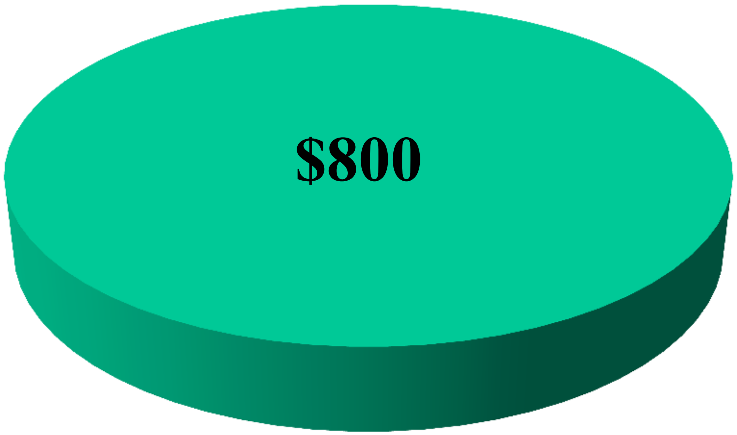
Multiple-Actor Negotiation



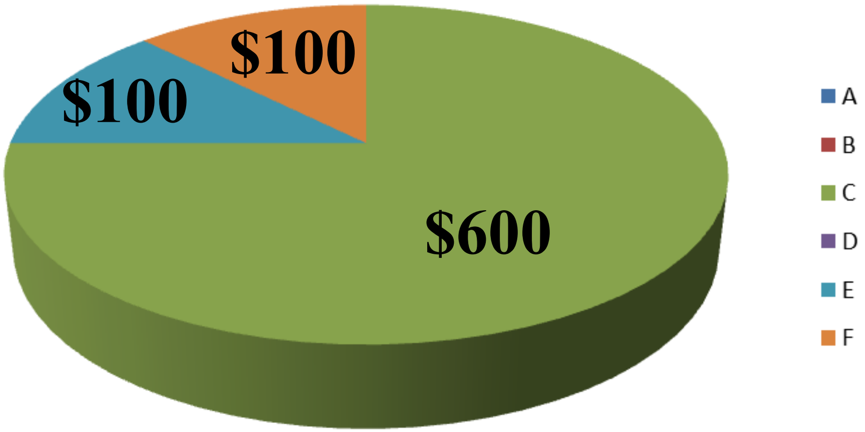




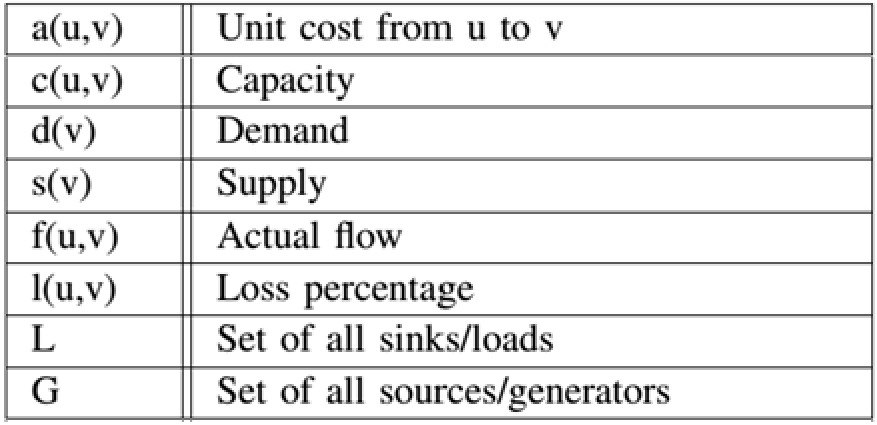
System



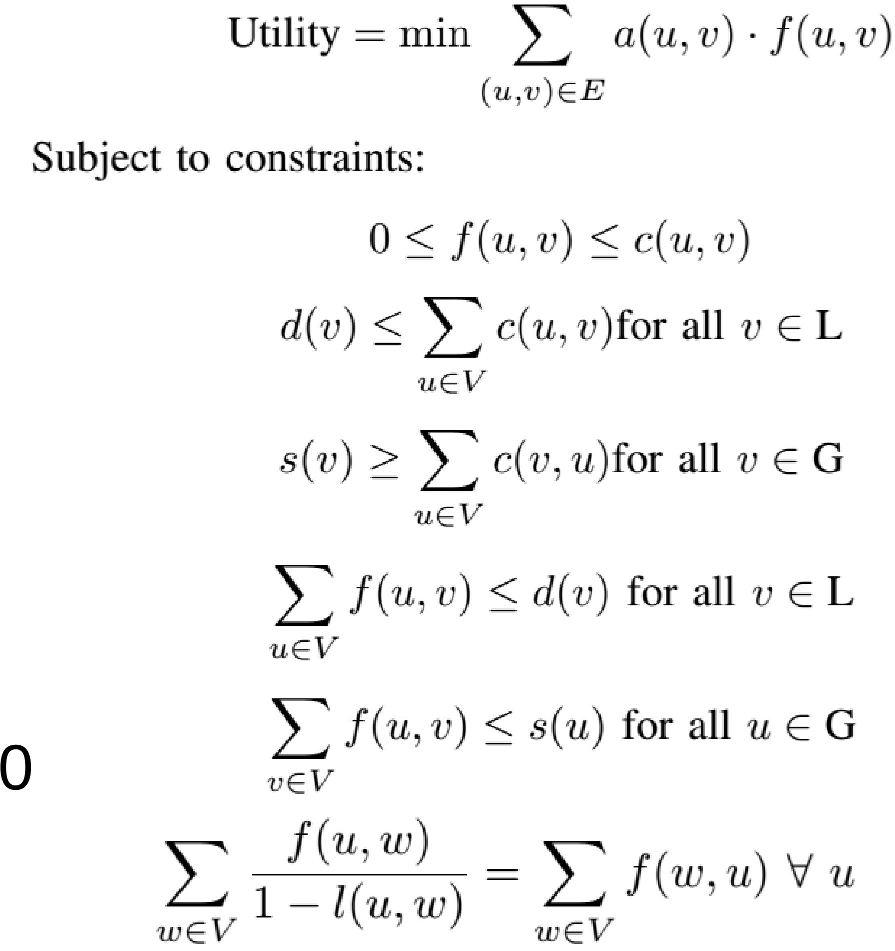
Individual



Multiple-Actor Negotiation Algorithm



a(u,v)	Unit cost from u to v
c(u,v)	Capacity
d(v)	Demand
s(v)	Supply
f(u,v)	Actual flow
l(u,v)	Loss percentage
L	Set of all sinks/loads
G	Set of all sources/generators



$$\text{Utility} = \min \sum_{(u,v)\in E} a(u,v)\cdot f(u,v)$$

Subject to constraints:

$$0 \le f(u,v) \le c(u,v)$$

$$d(v) \le \sum_{u\in V} c(u,v) \text{for all } v \in \mathrm{L}$$

$$s(v) \ge \sum_{u\in V} c(v,u) \text{for all } v \in \mathrm{G}$$

$$\sum_{u\in V} f(u,v) \le d(v) \text{ for all } v \in \mathrm{L}$$

$$\sum_{v\in V} f(u,v) \le s(u) \text{ for all } u \in \mathrm{G}$$

$$\sum_{w\in V} \frac{f(u,w)}{1-l(u,w)} = \sum_{w\in V} f(w,u) \ \forall\ u$$

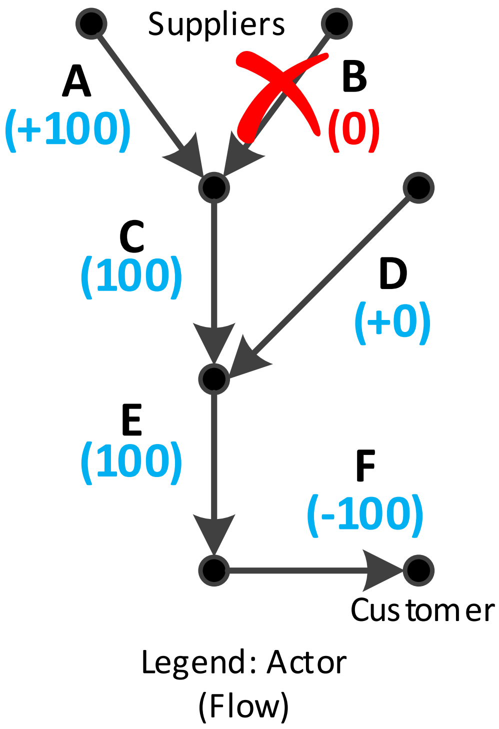
Solve via Linear Programming

Multi-Actor Algorithm:
a’=a+margin s.t. f’=f, Utility -> 0

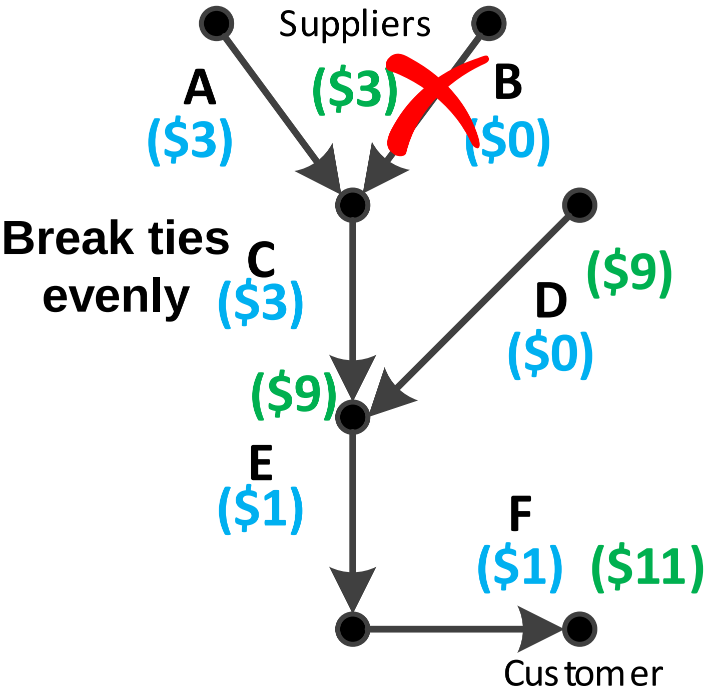
Targets and Impacts

- Logical target
  - Capacity reduction
  - Increased loss
  - Increased costs
- Real manifestation
  - PLC hack
  - Network DoS
  - (Physical disruption)

- Impact measurement
  - cost',loss',capacity'
  - Change in profit



Impact Calculation



Suppliers

A ($3)

($3)

B ($0)

Break ties evenly

C ($3)

D ($0)

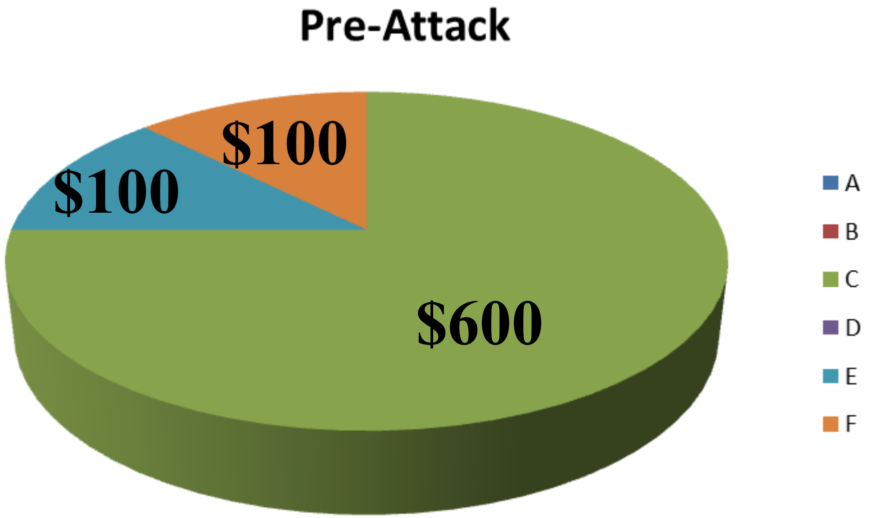
($9)

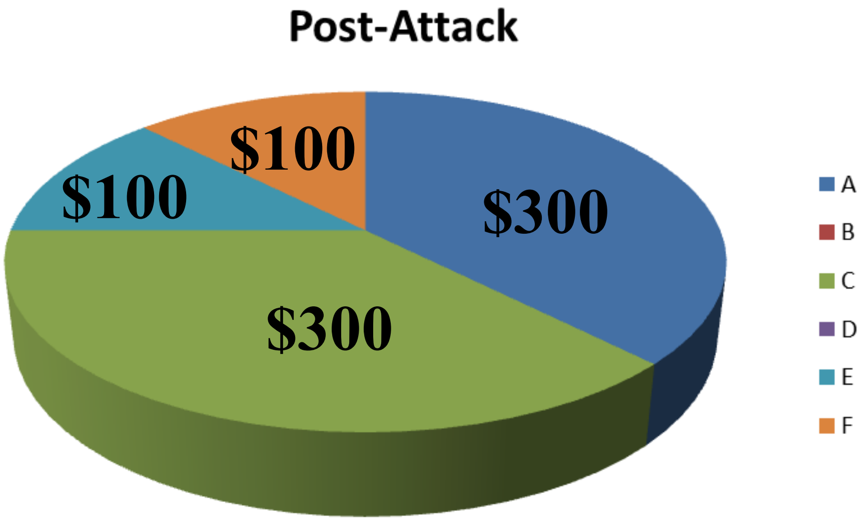
($9)

E ($1)

F ($1) ($11)

Customer



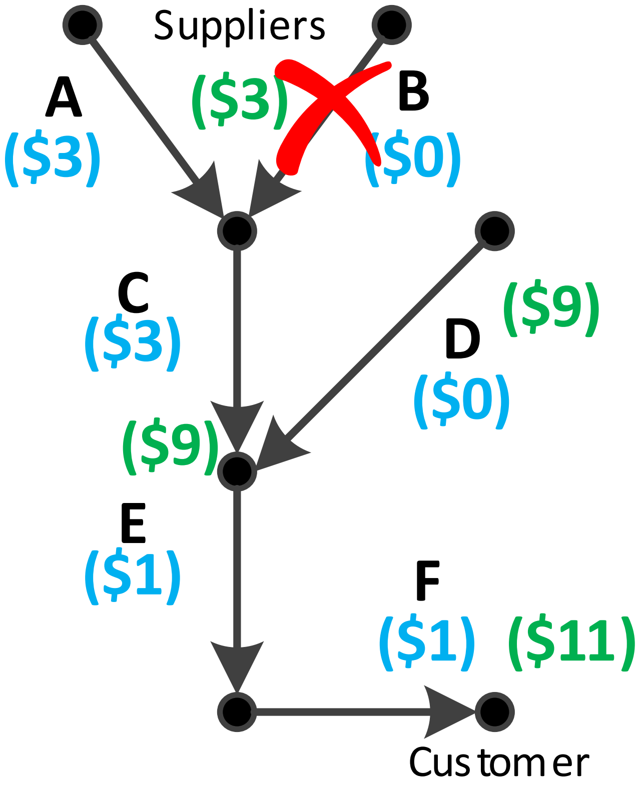


A motivated to attack B

Impact Matrix

	T-A	T-B	T-C	T-D	T-E	T-F
A	0	**300**	0	0	0	0
B	300	**0**	0	0	0	0
C	-300	**-300**	-600	100	-600	-600
D	0	**0**	100	0	0	0
E	0	**0**	-50	-50	-100	-100
F	0	**0**	-50	-50	-100	-100
Total	**0**	**0**	**-600**	**0**	**-800**	**-800**

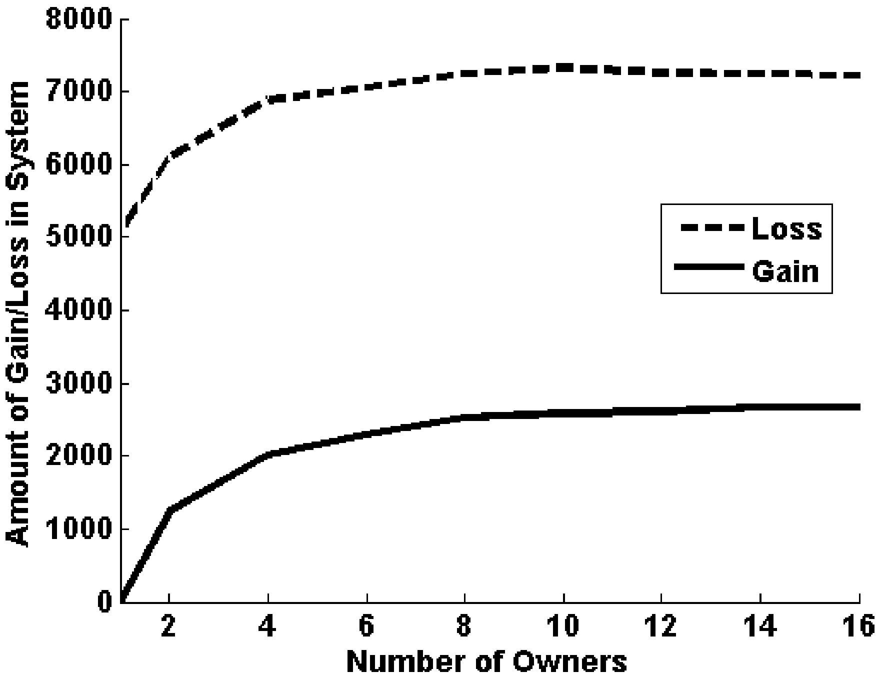
- Likely targets
  - A,B
- Likely defended
  - C
- A/B redundant
  - Low-value with single actor profit model



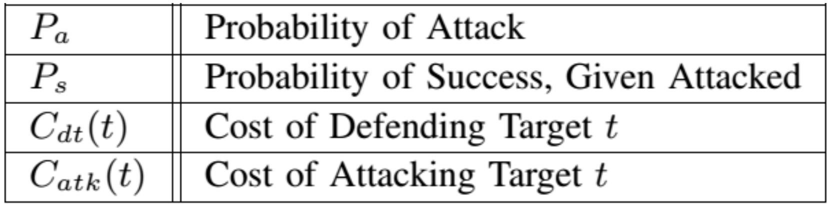
Multi-Actor Impact

Interdependence →

- Total gain/loss summed across all actors
- Multi-actor model creates profit elements
  - Diminishing impact as actor count approaches # competition points



Strategic Adversary



P_a	Probability of Attack
P_s	Probability of Success, Given Attacked
$C_{dt}(t)$	Cost of Defending Target t
$C_{atk}(t)$	Cost of Attacking Target t

$$\max_{T,A} \sum_{i \in T} \left(-C_{atk}(i) + \sum_{j \in A} IM[j,i] \cdot T(i) \cdot A(j) \cdot P_s(i) \right)$$

- Actor selection
  - Financial stake
  - May be adversary itself
- Optimize
  - Targets (binary)
  - Actors (binary)
- MILP formulation
  - Budget constraint

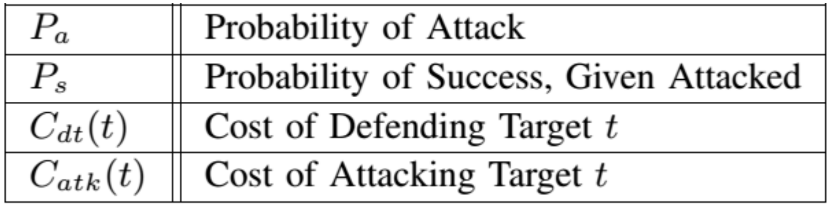
Defender Strategy

	T-A	T-B	T-C	T-D	T-E	T-F
A	0	**300**	0	0	0	0
B	300	**0**	0	0	0	0
C	-300	**-300**	-600	100	-600	-600
D	0	**0**	100	0	0	0
E	0	**0**	-50	-50	-100	-100
F	0	**0**	-50	-50	-100	-100
Total	**0**	**0**	**-600**	**0**	**-800**	**-800**

$$C_c d(a,t) = \frac{C_d(t) \cdot IM[a,t]}{\sum_{i \in CD(t)} IM[i,t]}$$

$$\max_{D} \sum_{i\ \in T} \left(\sum_{j \in CD(i)} \left(P_a(j,i) \cdot IM[j,i] \cdot (1 - D(i))\right) \right.$$
$$\left. - C_d(i) \cdot D(i) \right)$$

- Defender
  - Envisions attacker
    - Prob. of attack
  - Cooperation
    - CD(t)
    - Mutually beneficial
  - Selfish defense
    - CD(t) = 1
- MILP formulation



P_a	Probability of Attack
P_s	Probability of Success, Given Attacked
$C_{dt}(t)$	Cost of Defending Target t
$C_{atk}(t)$	Cost of Attacking Target t

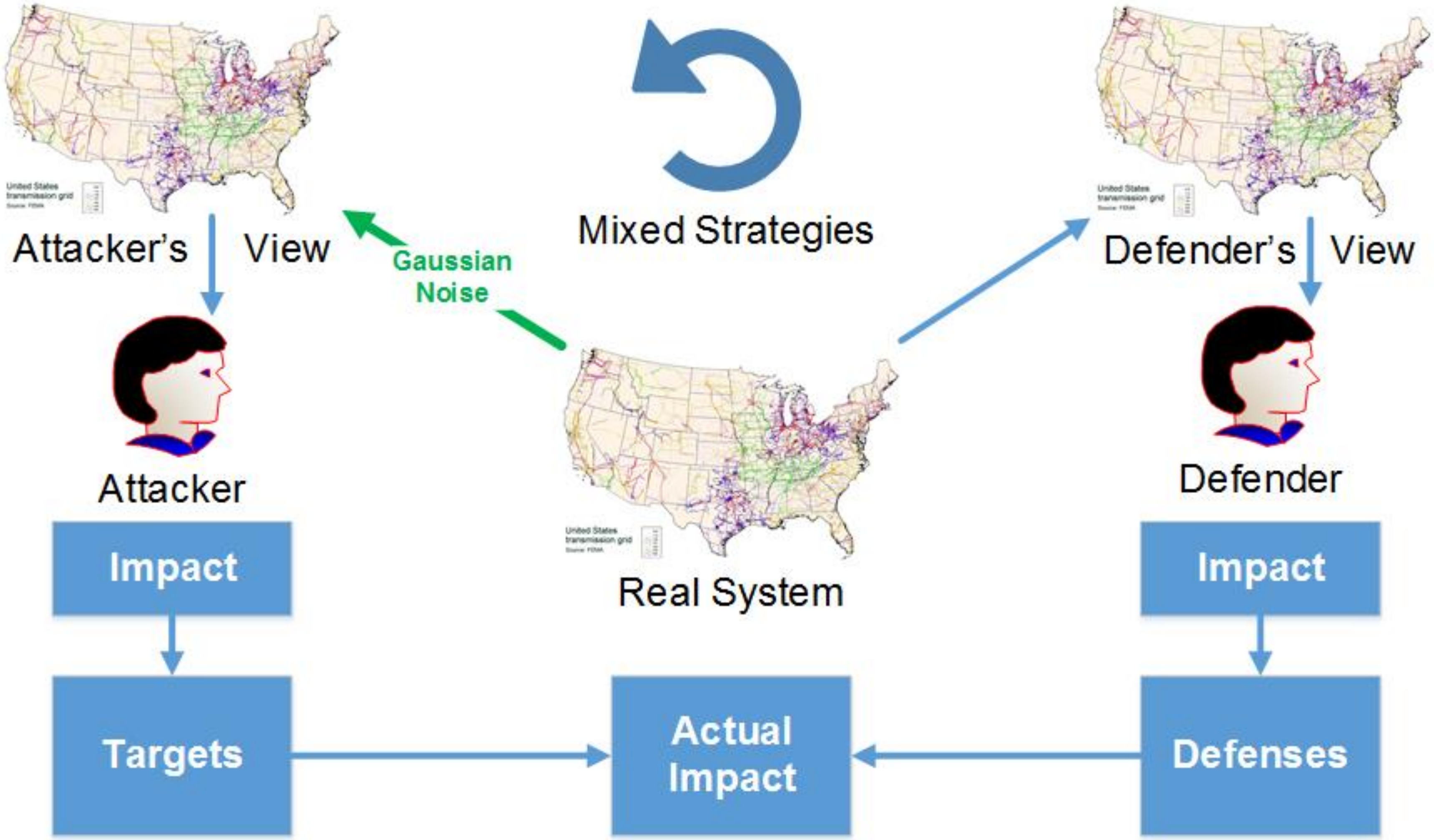
Overall Strategies

- Attacker
  - Set of targets
  - Maximized expected profits

- Defender
  - Set of defenses
  - Minimize expected loss

Pure strategy!

Knowledge Levels



Mixed Strategies

Attacker's View

Gaussian Noise

Defender's View

Attacker

Defender

Real System

Impact

Targets

Actual Impact

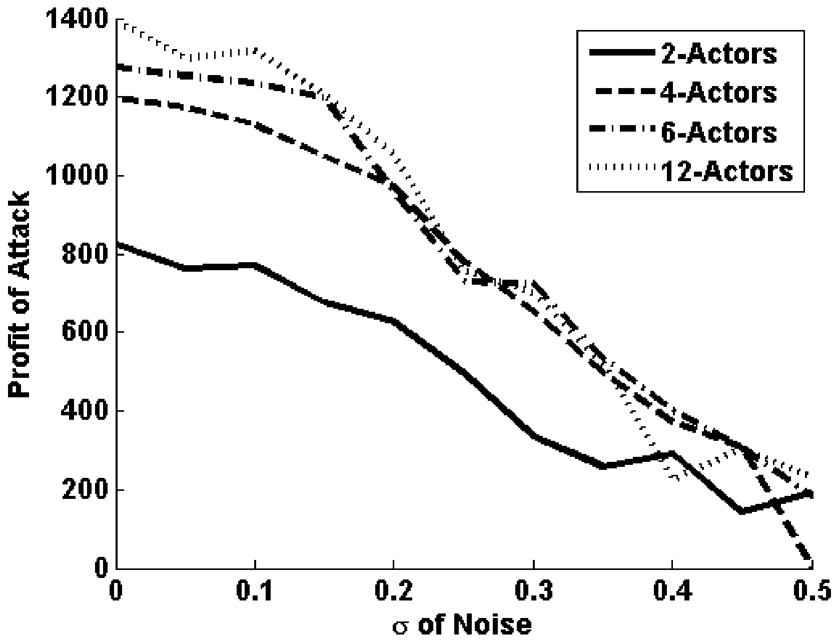
Impact

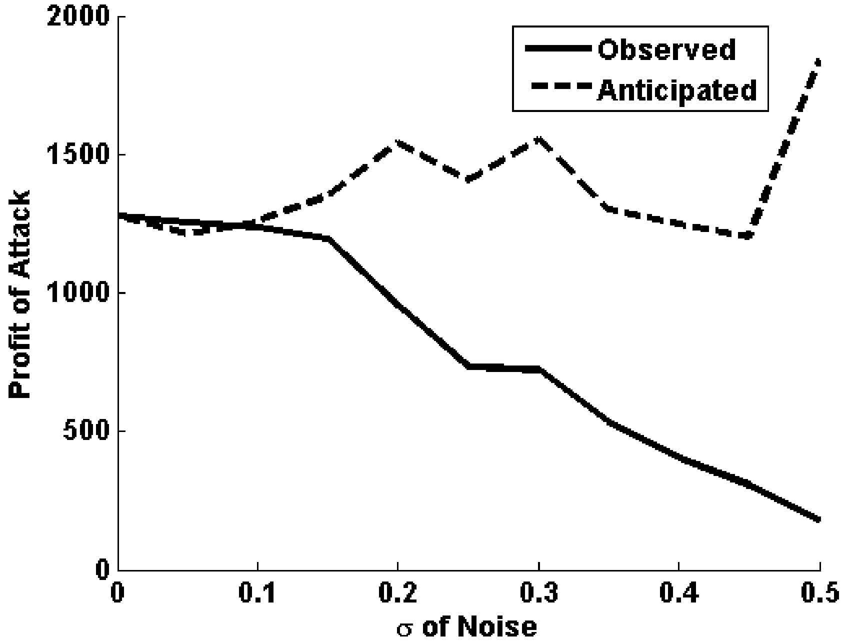
Defenses

United States transmission grid
United States transmission grid
United States transmission grid

Limited-Knowledge Attacker

- Attacker's view of model perturbed
  - Gaussian noise added to flow graph model

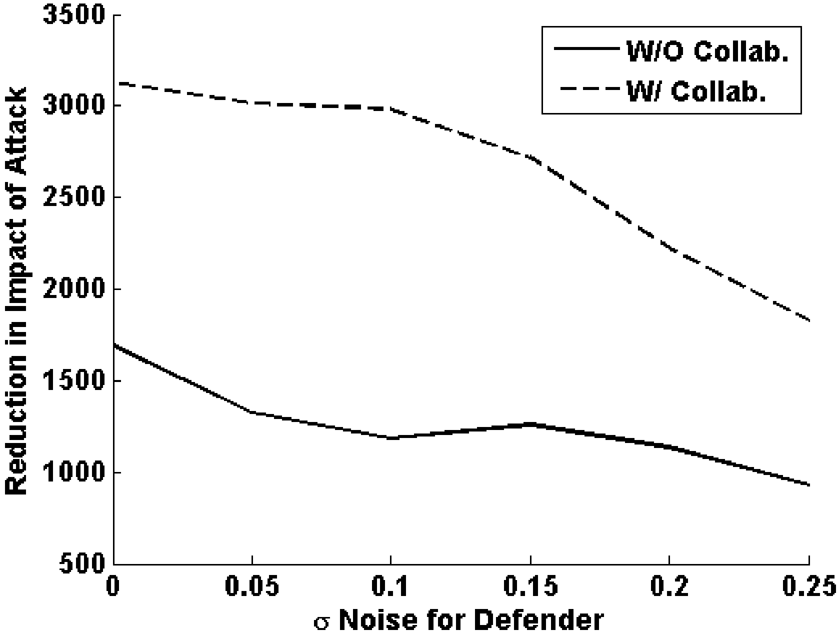




- Anticipated return misleading
  - Deception potential

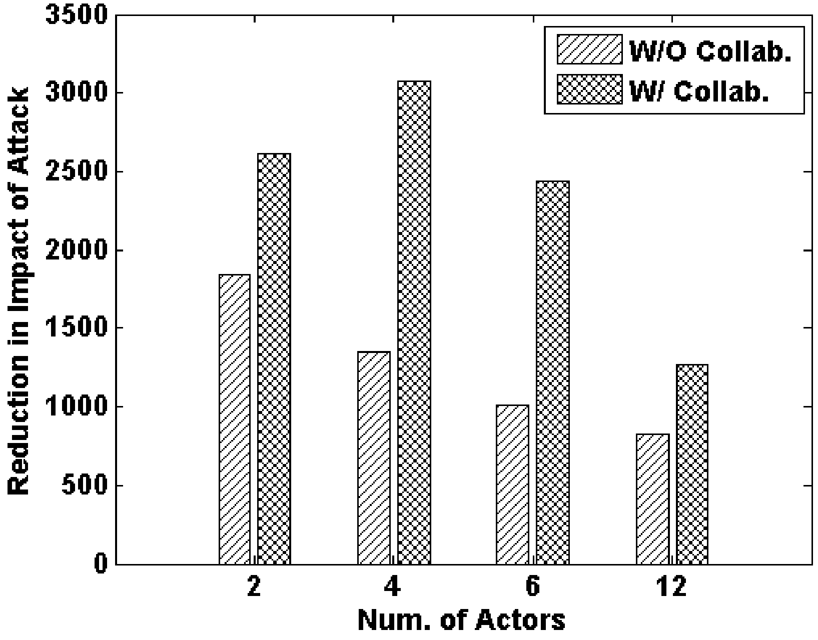
Attacker/Defender Games

- Attacker
  - Selects profitable targets
    - Subset of actors
- Defender
  - Pretends to be attacker
    - Uses probability of attack to drive defenses
- Mixed strategies
  - Equilibrium reached with probabilistic strategy



Collaborating Defenders

- Defenders have fixed resources to expend
- Collaboration
  - – Proportional cost-sharing
    - No conflict of interest
- Defenders save money
  - – Overall effectiveness decreases as number of actors increase



Contribution: Optimizing Defense under Strategic Adversary

Strategic Adversary Model

- Translation of physical system into graph model
  - High-speed computation
- Profit distribution method
  - Competitor's advantage
- Attacker motivation
  - Profit-seeking via competitor elimination

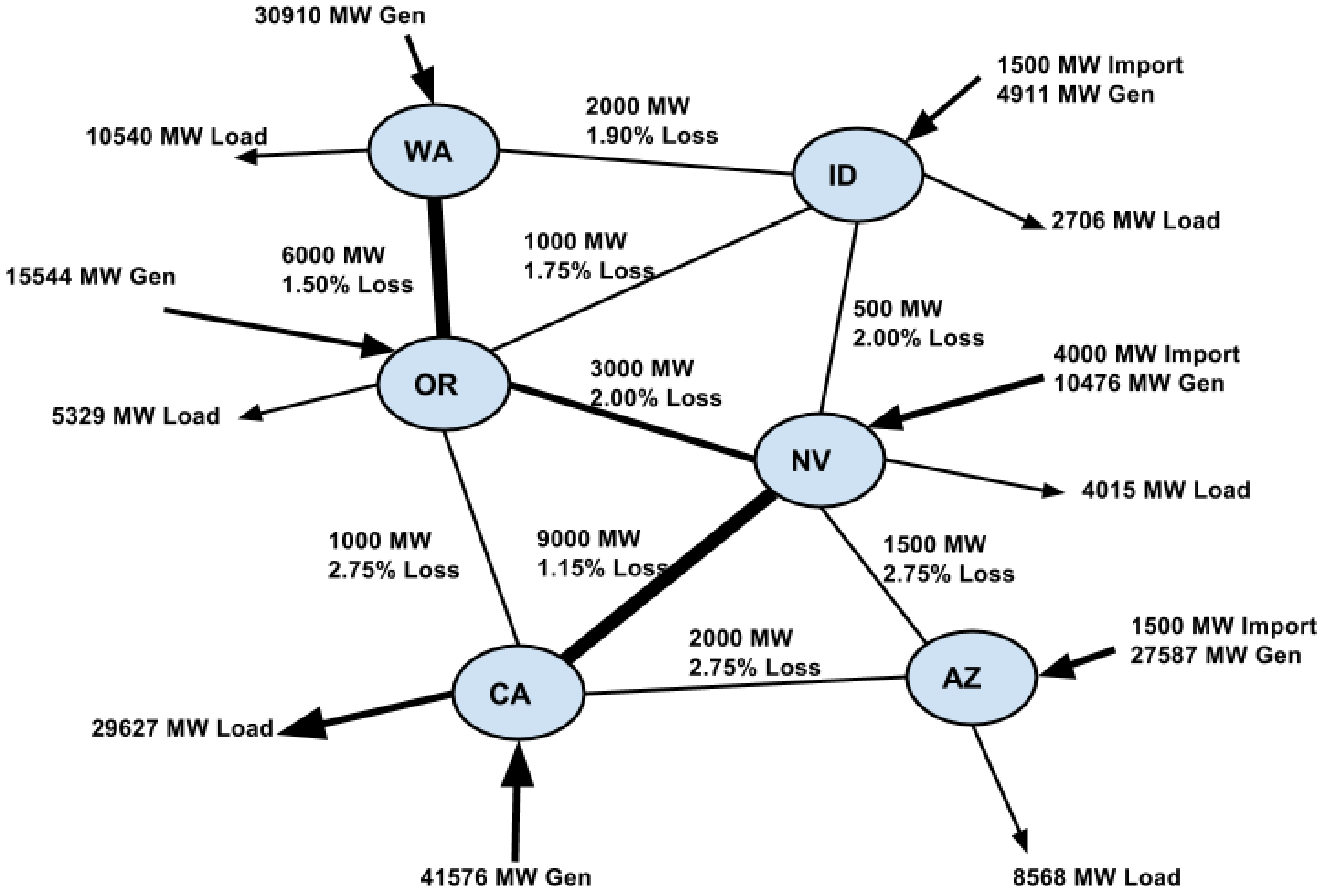
Defensive Investment Games

- Asset selection
  - Target values, selection in the face of adversary
- Knowledge levels
  - Model for independent actors and deception

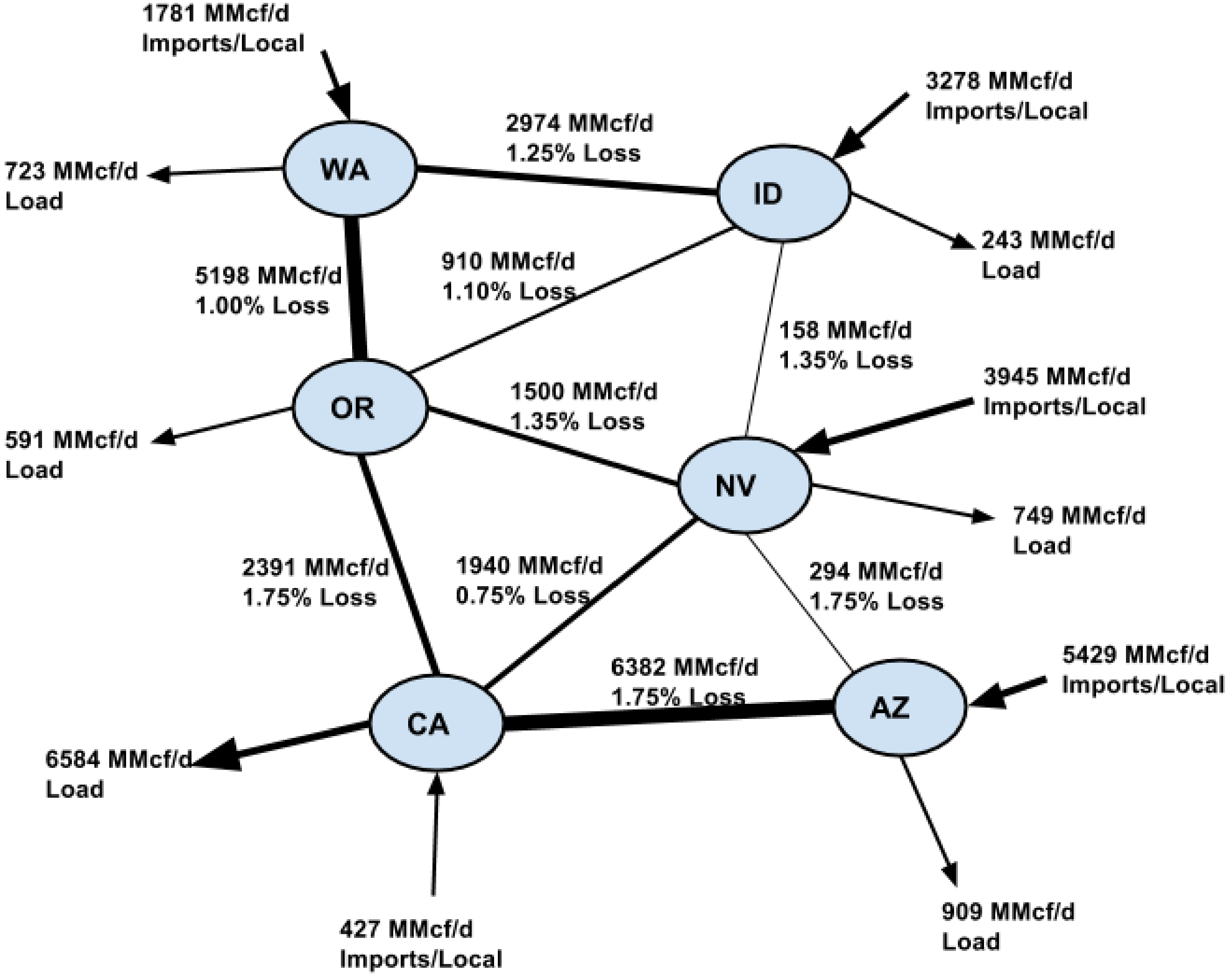
Future Work

- Strategies with online market algorithms
  - Distributed dynamic market mechanisms
  - Price negotiation over WAN
- Market algorithm resilience
  - Communication faults and market impact
  - Graceful degradation of market pricing
- Strategy application to architecture changes
  - Changes to communication infrastructures
  - Architecture planning and support

Test System: Electric



Test System: Gas


1781 MMcf/d Imports/Local
WA
723 MMcf/d Load
2974 MMcf/d 1.25% Loss
3278 MMcf/d Imports/Local
ID
243 MMcf/d Load
5198 MMcf/d 1.00% Loss
910 MMcf/d 1.10% Loss
158 MMcf/d 1.35% Loss
3945 MMcf/d Imports/Local
OR
591 MMcf/d Load
1500 MMcf/d 1.35% Loss
NV
749 MMcf/d Load
2391 MMcf/d 1.75% Loss
1940 MMcf/d 0.75% Loss
294 MMcf/d 1.75% Loss
6382 MMcf/d 1.75% Loss
5429 MMcf/d Imports/Local
CA
AZ
6584 MMcf/d Load
427 MMcf/d Imports/Local
909 MMcf/d Load