CPS: Market Analysis of Attacks Against Demand Response in the Smart Grid

Carlos Barreto, carlos.barretosuarez@utdallas.edu
Alvaro A. Cardenas, alvaro.cardenas@utdallas.edu
Nicanor Quijano, nquijano@uniandes.edu.co
Eduardo Mojica, eamojican@unal.edu.co

University of Texas at Dallas

December 11, 2014

Problem: Vulnerability of Smart Grid Devices

Smart Meters are being compromised for fraudulent purposes (Malta, Puerto Rico, etc.)

Malta customers who steal power won't face criminal charges

Posted by: Metering International | February 18, 2014 | Leave a Comment

As Enemalta, the state utility of Malta in southern Europe, begins to prosecute its employees for smart meter tampering, the government is reassuring consumers that they won't face criminal charges.

Last week, a former Enemalta employee, Paul Pantalleresco, was jailed for two years after he admitted to bribery and tampering 250 smart meters.

Another two employees were detained on Monday and more arrests are expected to follow.

Enemalta's Theft Control Unit identified 1,000 smart meters that had been rigged to record a small percentage of the household's energy consumption, amounting to revenue losses of €30m a year.

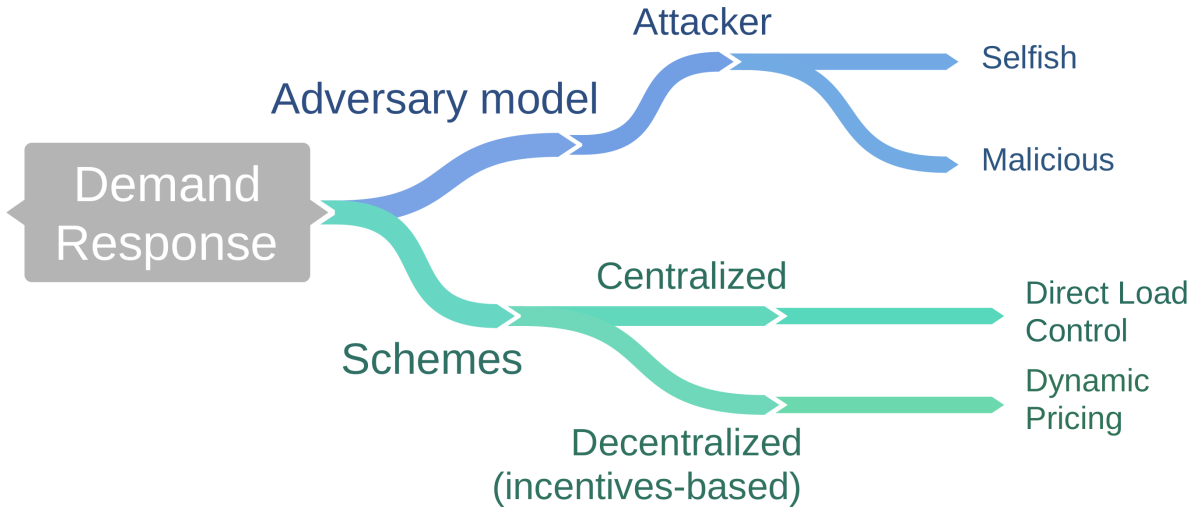
- What about vulnerabilities of new consumer services—such as **Demand Response (DR)**.
- By attacking DR, in addition to fraud, attackers can damage the power grid.

Previous Work on DR Security

Vulnerability of Demand Response (DR) to attackers that compromise control signal: [Tan et al., CCS'13].

- They ignore the fact that DR is essentially a **market** problem. So we need to include an economic analysis to this problem.
- They consider parametric attackers (scaling and delay attacks). A realistic attacker will not be constrained to only these two options. It can fake arbitrary signals.
- They only consider one type of DR (dynamic pricing).

Contributions



We address the limitations of previous work by using a DR market model based on Game Theory.

- We model two demand response programs with different fundamental characteristics: direct load control and dynamic prices.
- We analyze the resiliency of these demand response programs against two different types of attackers: selfish and malicious.
- Created an open-source toolbox to solve evolutionary games. [Available at: github.com/carlobar/PDToolbox_matlab]

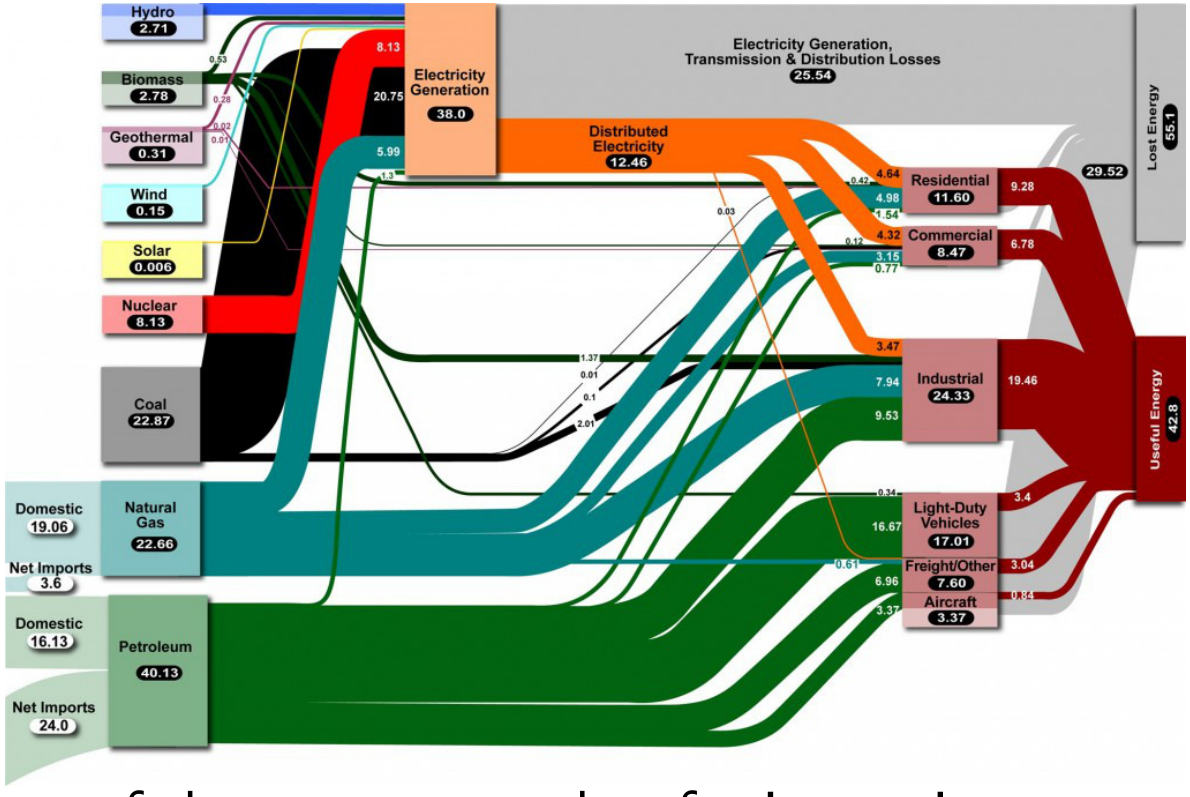
Outline

The Smart Grid

The electricity system is being modernized to improve:

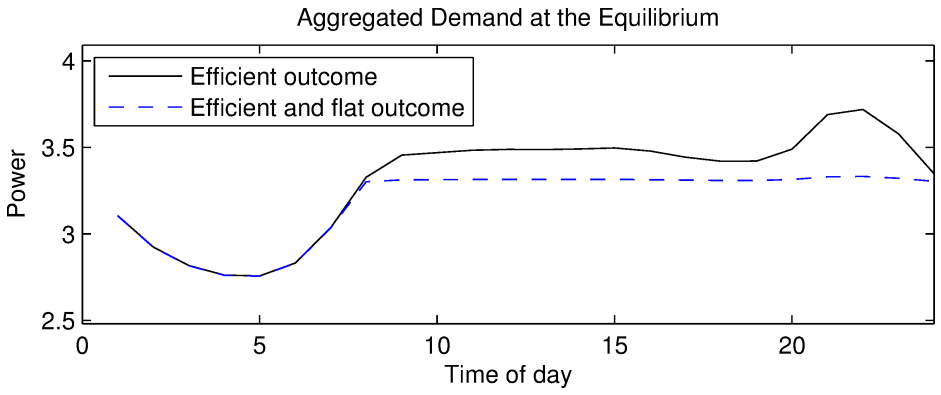
- Efficiency
- Reliability
- Consumer Choice

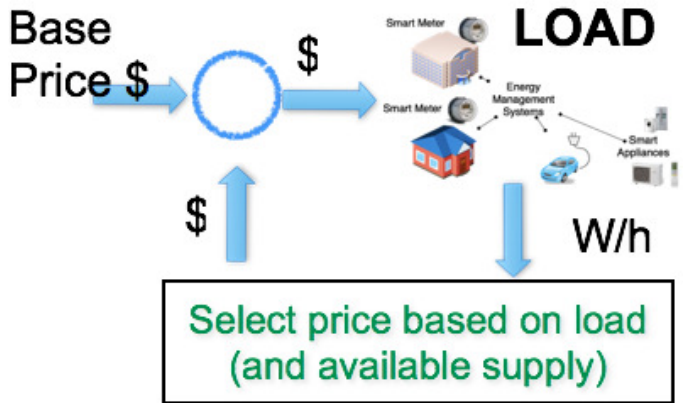
Diagram Source: LLNL



Demand Response is one of the new approaches for improving efficiency, reliability and consumer choice.

What is Demand Response (DR)?

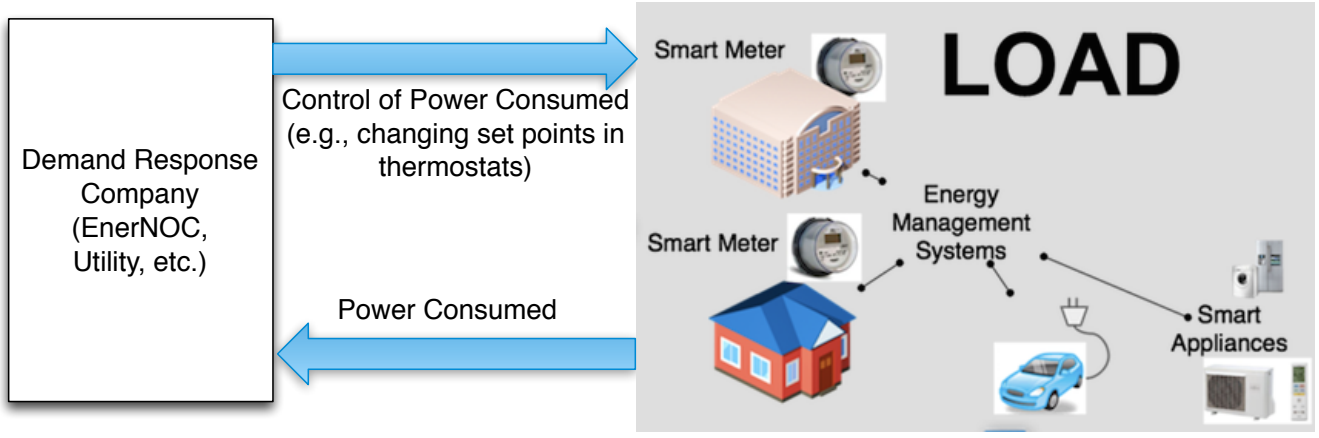




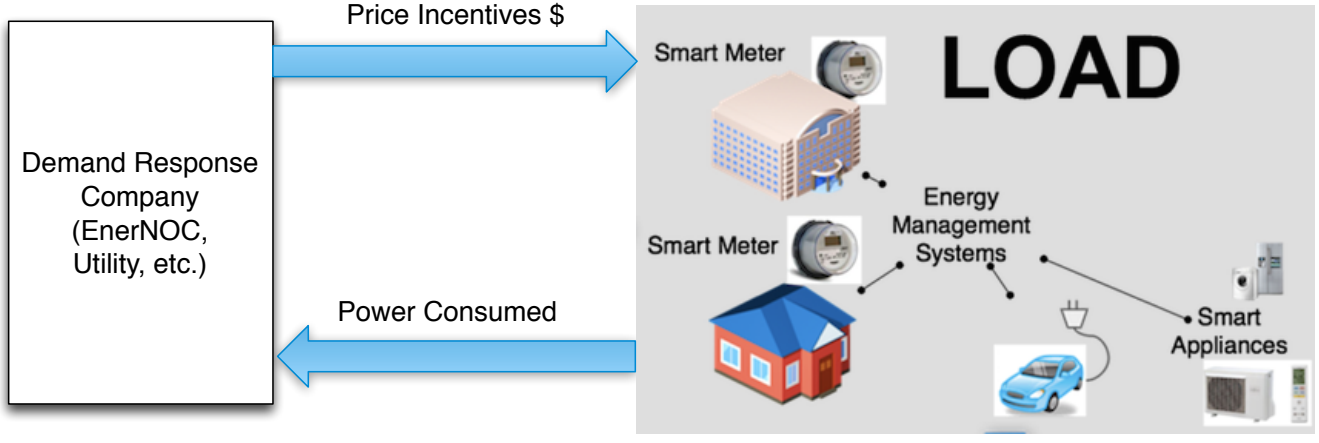
- Time varying demand creates three problems:
  1. It creates an inefficient market: bulk power market changes significantly, while consumers (retail market) pay fixed rates
  2. Over Provisioning
  3. It puts the grid in a vulnerable state: if load cannot be met
- Demand Response (DR) is a new approach to control the load. Gives consumers incentives to reduce consumption when
  - Generating more electricity is expensive
  - Demand cannot be met

Demand Response Programs

Direct Load Control (DLC): Central agent controls electricity load.



Dynamic Prices (DP): Central agent sends prices to consumer.



Models Capturing Market Dynamics

[Roozbehani et al. IEEE Trans. Power Systems 2012]

Direct Load Control (DLC): Central agent controls electricity load.

Global optimization problem (Pareto efficient)

$$\begin{aligned} \underset{\boldsymbol{q}}{\text{maximize}} \quad & \sum_{i=1}^{N} U_i(\boldsymbol{q}) \\ \text{subject to} \quad & q_i^t \geq 0. \end{aligned}$$

$U_i(\boldsymbol{q})$: Utility of the i^{th} agent.
$\boldsymbol{q}$: Population's consumption profile.
$i = \{1, \ldots, N\}, t = \{1, \ldots, T\}$

Dynamic Prices (DP): Central agent sends prices to consumer.

Selfish optimization problem

$$\begin{aligned} \underset{\boldsymbol{q}_i}{\text{maximize}} \quad & U_i(\boldsymbol{q}_i, \boldsymbol{q}_{-i}) + I_i(\boldsymbol{q}) \\ \text{subject to} \quad & q_i^t \geq 0. \end{aligned}$$

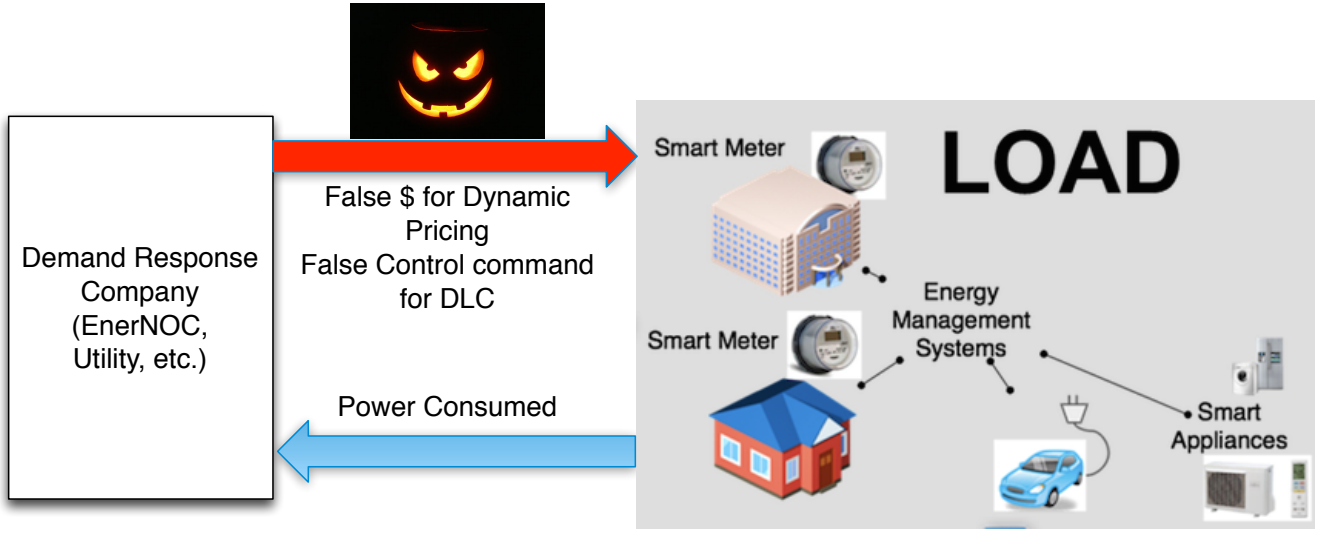
$I_i(\boldsymbol{q})$: Incentives for the i^{th} agent.

Remark

Using mechanism design, $I_i(\cdot)$, can force selfish users to the Pareto efficient equilibrium.

Outline

Adversary Model



Fraudster

- Defraud the system (pay less for electricity) without damaging the power grid.
- If attacker tampers with smart meter, then the attack can be easily attributed. By attacking DR, the attack is difficult to attribute.

Malicious

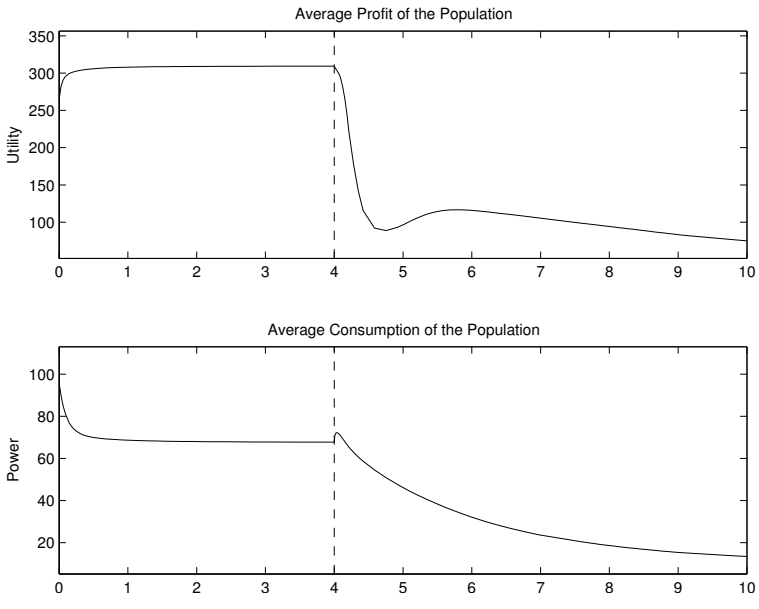
- Attempts to damage the power grid (e.g., create an unanticipated load spike)

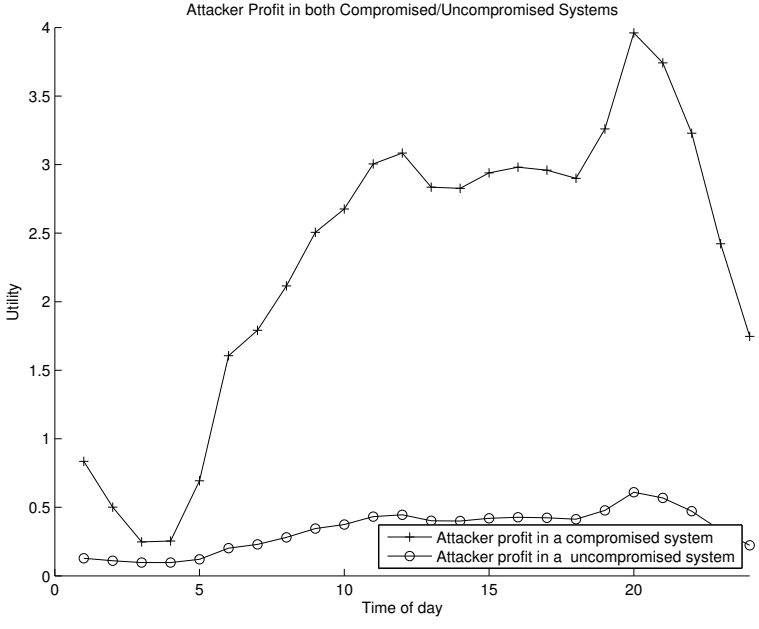
Fraudster Attacker in Direct Load Control (Attributable)

Attacker's objective is to maximize its own profit, that is

$$\begin{aligned} \underset{\boldsymbol{q}_i, \boldsymbol{q}_{-i}}{\text{maximize}} \quad & U_i(\boldsymbol{q}_i, \boldsymbol{q}_{-i}) \\ \text{subject to} \quad & q_i^t \geq 0. \end{aligned}$$

In a DLC scheme the attacker can manipulate the consumption made by other users to cause price reductions to consume more power.





Fraudster Attacker in Direct Load Control (Unattributable)

However, in order to keep undetected she might regulate the impact of the attack considering the following objective

$$\begin{aligned} \underset{\boldsymbol{q}}{\text{maximize}} \quad & \lambda \sum_{h \in \mathcal{S}} U_h(\boldsymbol{q}) + \sum_{h \in \mathcal{V}} U_h(\boldsymbol{q}) \\ \text{subject to} \quad & q_i^t \geq 0, \end{aligned}$$

where $\lambda \geq 1$ represents the severity of the attack and $\mathcal{V}$ and $\mathcal{S}$ are sets of victims and safe customers, respectively. We find the following relation between the attacker utility $U_s(\cdot)$ and the victims utility $(U_v(\cdot))$:

$$\frac{U_s(x_s)}{U_v(x_v)} = \frac{1}{\lambda} \frac{1-\gamma}{\gamma}, \tag{1}$$

γ is the proportion of safe customers.

Remark

An attacker must decrease her benefits in order to camuflage her actions.

Fraudster attacker under Dynamic Prices (Unattributable)

The subtle attack can be implemented in a decentralized system with dynamic prices by modifying the incentives as follows:

$$l_j(\boldsymbol{q}) = \left(\sum_{h \in \mathcal{V}-j} q_h + \lambda \sum_{h \in \mathcal{S}} q_h \right) \left(\frac{N}{N-1} p(||\boldsymbol{q}_{-j}||_1) - p(||\boldsymbol{q}||_1) \right),$$

for all $j \in \mathcal{V}$ and

$$l_i(\boldsymbol{q}) = \left(\frac{1}{\lambda} \sum_{h \in \mathcal{V}} q_h + \sum_{h \in \mathcal{S}-i} q_h \right) \left(\frac{N}{N-1} p(||\boldsymbol{q}_{-i}||_1) - p(||\boldsymbol{q}||_1) \right),$$

for $i \in \mathcal{S}$.

Remark

Note that the attacker should be able to identify the consumption of each agent.

DLC is more vulnerable than Dynamic Pricing: Adversary Gains

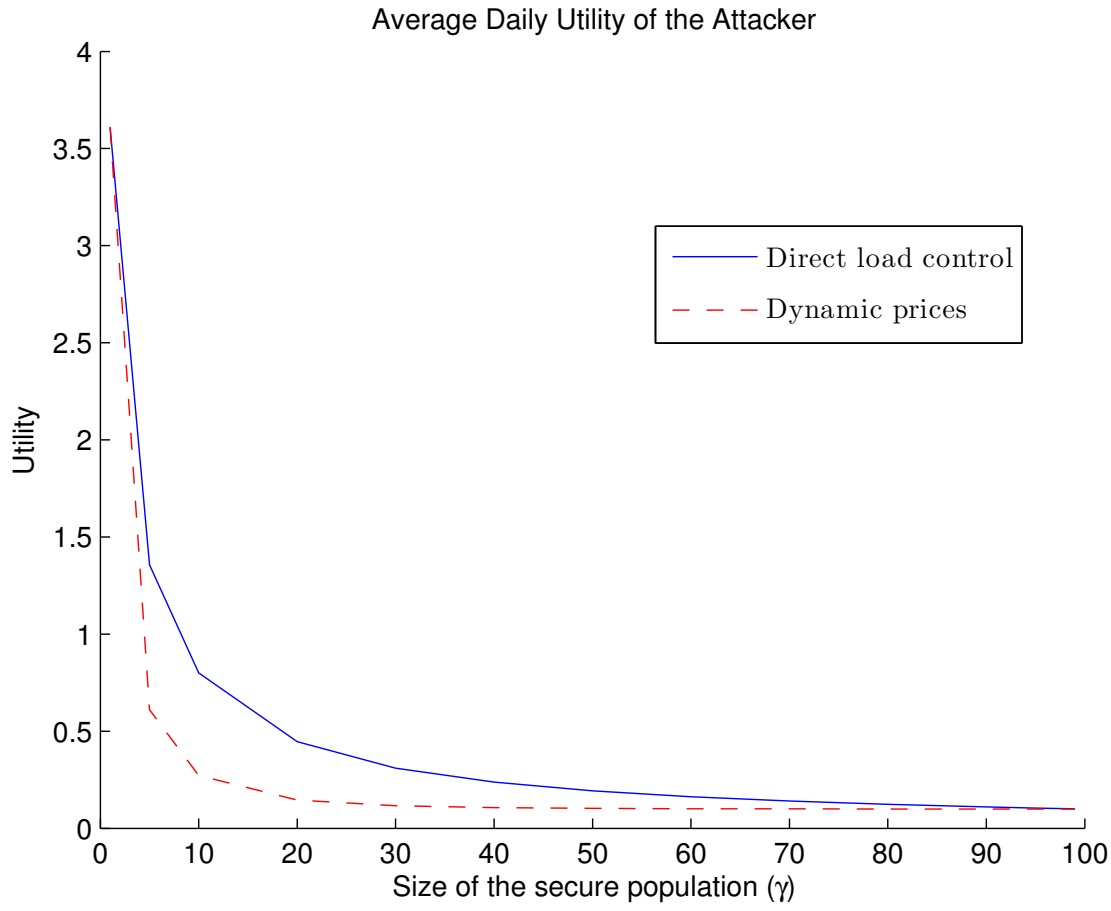


Figure 1: Fraudsters obtain more benefits from attacking DLC systems when compared to dynamic pricing.

Consumers Suffer More With DLC but the Utility has More Expenses With Dynamic Pricing

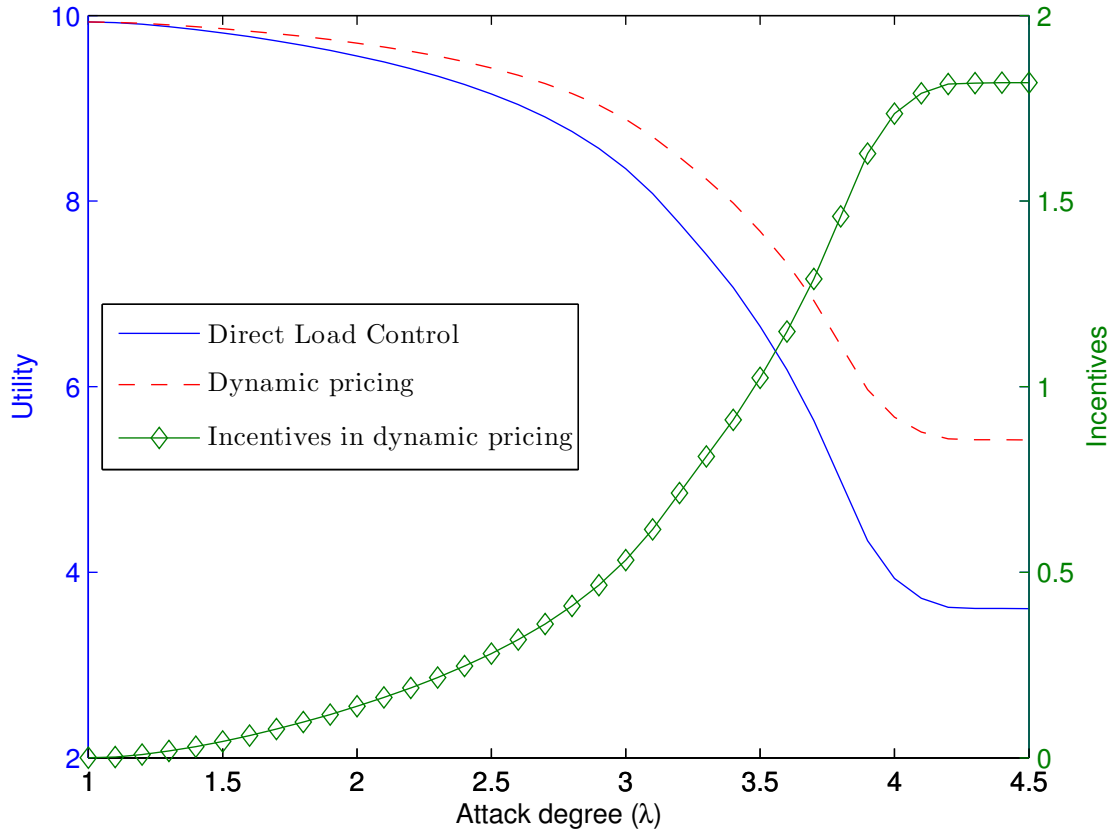


Figure 2: Impact of the attack in the social welfare utility and global incentives as a function of the attack severity λ for both the DLC and dynamic pricing schemes with $\gamma = 0.01$.

Malicious Attacker (DLC)

The objective of the malicious attacker might be represented as:

$$\begin{aligned} \underset{\boldsymbol{q}}{\text{maximize}} \quad & -\sum_{i=1}^{N} U_i(\boldsymbol{q}) \\ \text{subject to} \quad & q_i^t \geq 0, i = \{1, \ldots, N\}, t = \{1, \ldots, T\}. \end{aligned} \tag{2}$$

the malicious attacker causes a power overload in the system, because the minimum wellfare happens when the consumption is high.

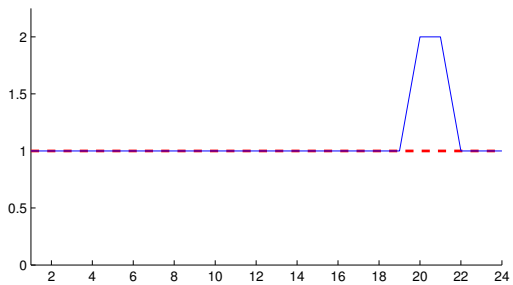
Remark

Since this goal requires full information, it can be implemented only with DLC.

Malicious Attacker (Dynamic Prices)

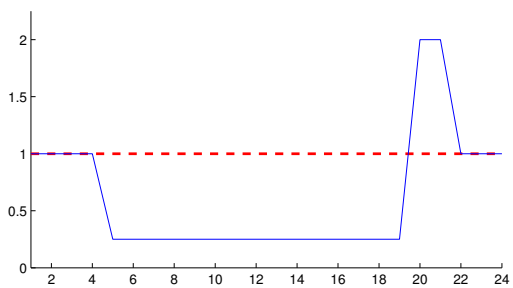
We assume that the attacker is able to compromise the incentives and send some fake signal. Here we consider two attacks:

Naive attack Incentive inre consumption through price reductions.



$$l_i^m(\boldsymbol{q}) = \begin{cases} l_i(\boldsymbol{q}^t) + \sigma_1 ||\boldsymbol{q}||_1 & \text{if } t = t_{attack}, \\ l_i(\boldsymbol{q}^t) & \text{otherwise,} \end{cases}$$

Strategic Attack Attempts to reduce the consumption before the attack to cause a larger overpeak.



$$l_i^m(\boldsymbol{q}) = \begin{cases} l_i(\boldsymbol{q}^t) + \sigma_1 ||\boldsymbol{q}||_1 & \text{if } t = t_{attack}, \\ l_i(\boldsymbol{q}^t) - \sigma_2 ||\boldsymbol{q}||_1 & \text{if } t \in [t_a, t_b], \\ l_i(\boldsymbol{q}^t) & \text{otherwise,} \end{cases}$$

Simulations

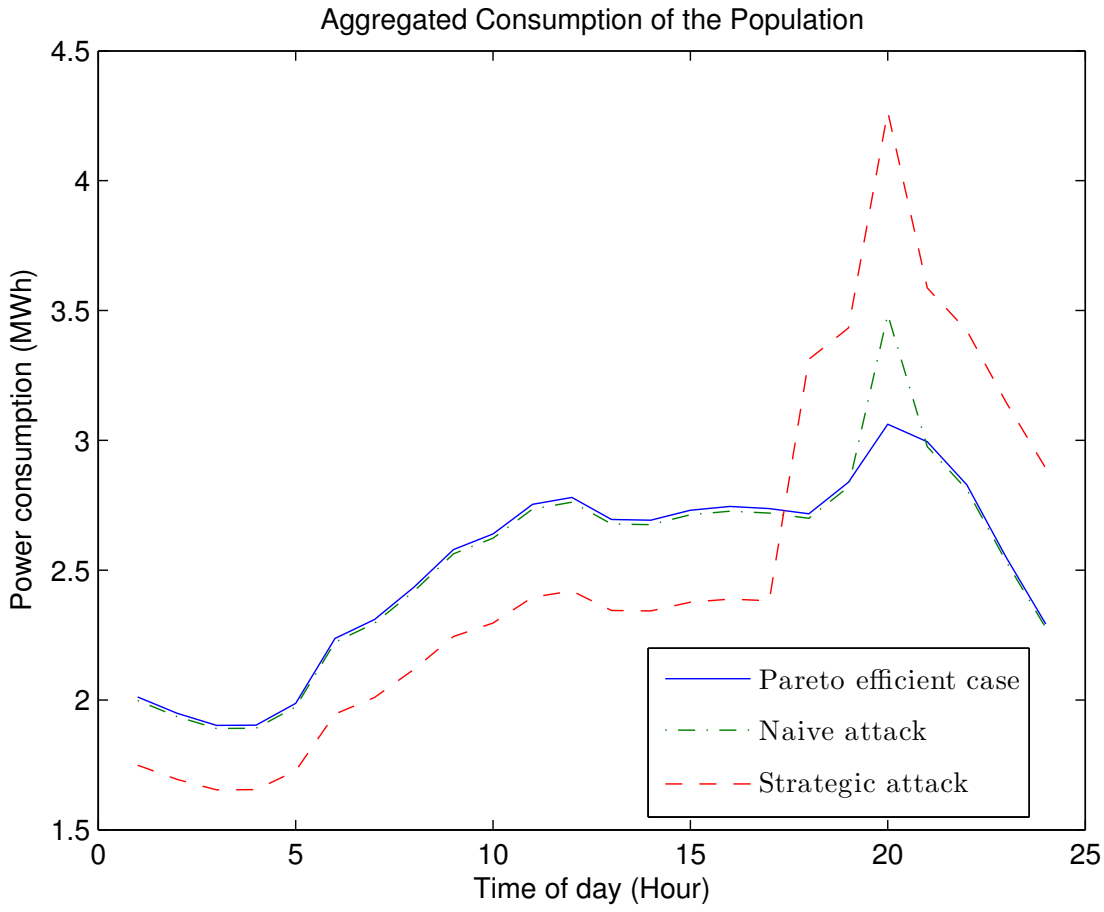


Figure 3: Impact of a malicious attack on the populaiton demand for two different attacks 1) attack on a single hour and 2) coordinated attack on various hours of the day.

Conclusions and future work

- We introduced a formal mathematical model of attackers using game theory and proved the optimality of attacks (details in paper) for general utility functions.
- We created a simulation toolbox available online to model population dynamics in game theory.
- Attacker has higher benefits with Dynamic Pricing than with DLC
- Society (consumers) suffers more with DLC than with Dynamic Pricing
- Utility has to pay more in Dynamic Pricing than with DLC.
- Future work: detection of attacks.