Secure Multiparty Computation Based Privacy Preserving Smart Metering System

Cory Thoma; University of Pittsburgh
Tao Cui, Dr. Franz Franchetti; Carnegie Mellon University

Carnegie Mellon

Motivation

The implementation of smart metering into the electric grid provides high resolution real-time data to the energy providers. This real-time data allows energy companies to engage in real-time pricing markets based on the current energy supply and demand. However, real-time data gives energy providers the ability to extract detailed information about consumer's daily lives, which can be seen as an invasion of privacy and can adversely effect demand.

Problem

The main problems being addressed in this work are:

- Ensure consumer privacy while allowing energy companies to monitor the load on the grid.
- Implement a private and secure supply and demand market that sets a price for energy.

Solution

Using *Secure Multiparty Computations* (SMC) in a *Zero-Knowledge* environment, we can make consumption data private and maintain real-time energy markets, while still giving energy companies the ability to effectively monitor the grid.

To keep data private, we use:

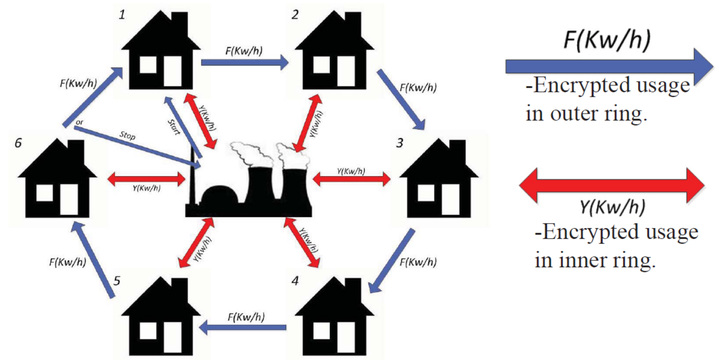
- Paillier cryptosystem to manage the load and aggregate the demand data privetly.
- Yao's Solution to the millionaire problem to check an individual consumer's demand and consumption.

Implementation

We use SMC to privatize consumer consumption data with real-time data in a simulated smart grid community. This community has consumers represented by a house as well as an energy supplier. The purpose of the simulation is to:

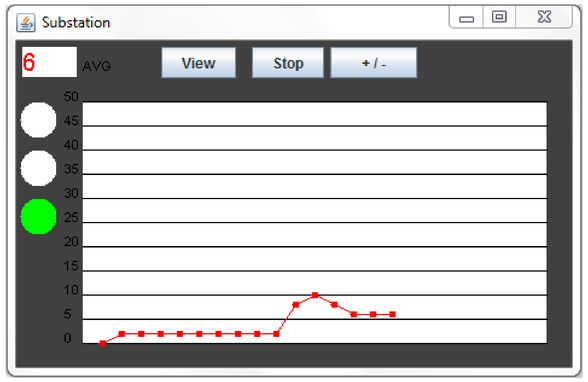
- Show data can be kept private
- Manage the load on the utility
- Properly bill each consumer
- Set pricing based on a secure SMC market

Simulation: Networking



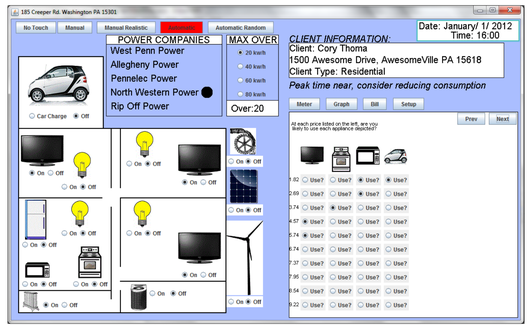
Ring and star network topology (on LAN or the Internet).

Simulation: Substation (Server)



The substation, acting as a server in the network. It computes the load, bills the consumers, and penalizes any consumer who uses too much energy during a peak time.

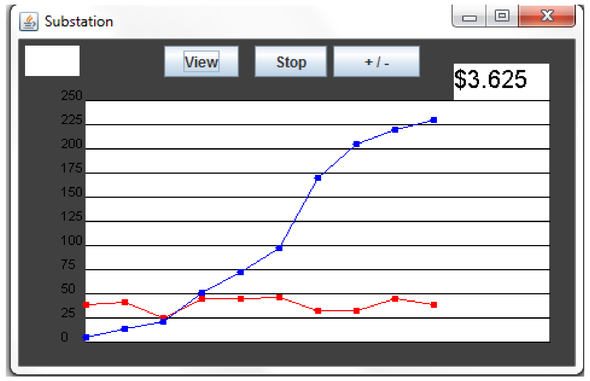
Simulation: Consumer (Client)



A typical house with appliances and an electric car.

Simulation: Market

Each consumer sets their demand through stating whether or not they will use an appliance given a certain price. The utility sets their price given the environmental variables, previous demand, and the ability to meet that demand. . A supply and demand curve is created and the market clearing price is calculated at the intersection of the supply and demand, all while remaining private.



Cryptography

SMC requires more than two parties be able to privately compute on some numbers. Paillier allows for homomorphic encryption such that the sum of the encryptions is the encryption of the sums. This allows the energy company to compute the average consumption, as well as compute the demand at each price over each consumer.

- **Encryption:** $encryption = g^M * r^n \mod n^2$
- **Decryption:** $decryption = \frac{L(e^\lambda \mod n^2)}{L(g^\lambda \mod n^2)} \mod n$

To maintain a zero-knowledge environment, the energy company may not know any information about any consumer. Using Yao's solution to the millionaire problem, the energy company can compute the bill, check the usage against a threshold, and compare prices from different utilities, all without knowing the actual values. Yao's solution uses iterative RSA encryption to hide the actual values.

Conclusions

SMC allows utilities to monitor the consumptions of consumers while maintaining the consumer's privacy. By adding a supply and demand market to the simulation we were able to have real-time pricing without any party knowing the actual consumptions.