Protecting Consumers: The Smart Grid and Your Data

Cory Thoma, Washington & Jefferson College
Advisors: Dr. Holland-Minkley, W&J; Dr. Franchetti, Carnegie Mellon University

Motivation

The Smart Grid is the future of power distribution. It gives us the ability to make and conserve power and utilize the growing renewable energy industry. But the technology that makes the Smart Grid so powerful can also makes it intrusive way. The smart meters employed in homes have the ability to relay very specific data about the power consumption, some of which may be surprising:

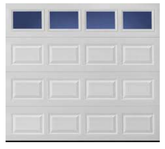
...know when you are cooking.

...change the temperature of your house.

...know the shows you have watched.

I have the ability to...:

...know when you have left your house.



...know when the lights are on or off.

...know how much you drive your electric car.

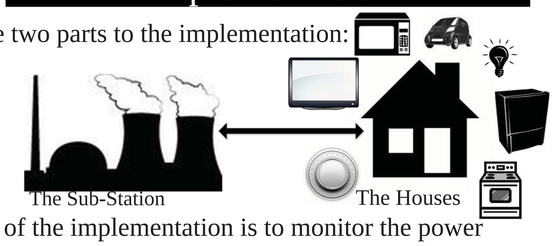
Formal Statement

Problem: Allow the users of the Smart grid to keep their usage data private while allowing the power companies to monitor the grid effectively and to bill the users properly.

Solution: Implement a zero-knowledge data sharing environment. In a zero-knowledge environment, all participants can compare and compute any usage data among themselves without giving individual data information away.

Implementation

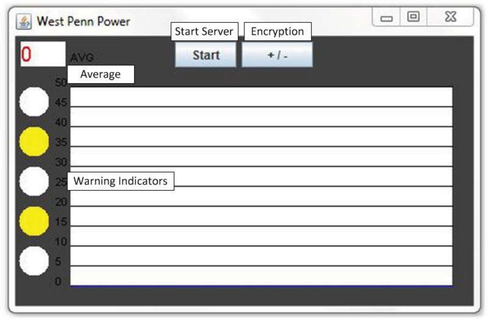
There are two parts to the implementation:

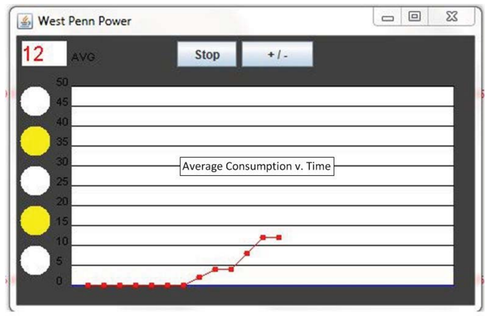


The Sub-Station The Houses

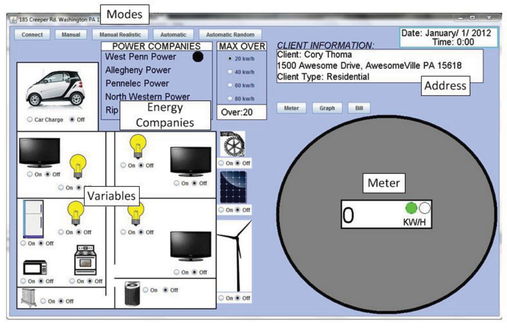
The goal of the implementation is to monitor the power consumption of each house. Without knowing the actual consumptions of individual houses', the sub-station computes the average consumption based on the usage of the appliances in each house.

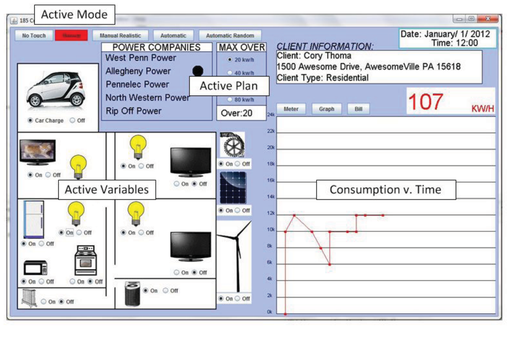
Sub-Station



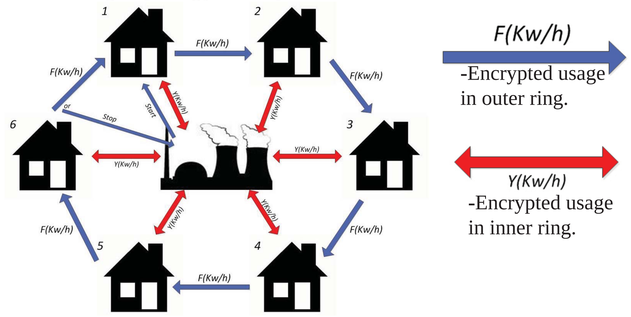


House

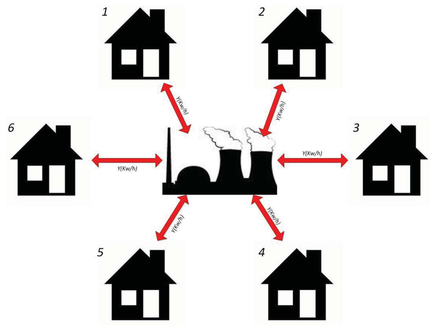




The implementation runs on a server-client network, in which the substation or power station is the server, and each user is a client. It runs over a ring topology as depicted below.



The blue ring computes the average with the encryption function F which based on either the Paillier encryption scheme or random number arithmetic. If the average consumption exceeds C_{max} or does not reach C_{min}, then the sub-station uses the network depicted below to compare each consumption individually using the algorithm described below, as represented by $Y(Kw/h)$ in the graph.



- **Step 1.** Bob (room) picks a random n-bit integer called x (Alice (controller) will later use a $n/2$ bit prime, so the length of the integer is important). Bob first calculates c as the RSA encipherment of x using Alice's public key.
- **Step 2**. Bob transmits $c - b + 1$ to Alice.
- **Step 3.** Alice generates a series of numbers $y_1, y_2, \ldots, y_k$ such that y_i is the RSA decipherment (using her private key) of $c - b + i$.
- **Step 4.** Alice now generates a random $n/2$ bit length prime p. Alice then generates $z_1, z_2, \ldots, z_k$ by calculating $z_i = y_i \bmod p$. Note that p must be chosen so that all the z_i differ by at least 2.
- **Step 5.** Alice now transmits the prime p to Bob, and then sends k numbers u_i. The first few u_i are $u_1 = z_1$, $u_2 = z_2, \ldots, u_a = z_a$ with a being Alice's worth in millions. Then Alice adds 1 to all the remaining $k - a$ values u_i to be sent and sends $u_a+1 = z_a+1 + 1, \ldots, u_k = z_k + 1$.
- **Step 6.** Bob receives p and $u_1, \ldots, u_k$. He computes $g = x \bmod p$. If the $u_b = g$ then Alice is equal or greater in wealth ($a \geq b$). If the $u_b \neq g$ then Bob is wealthier than Alice ($a < b$).

Further Work

- Allow the consumer to bid for power, and allow the power companies to offer prices to the consumer.
- Allow each house to provide energy for itself through solar panels, and other forms of renewable energy which could result in power being sold back to the companies.
- Make the application more interactive to simulate real users.