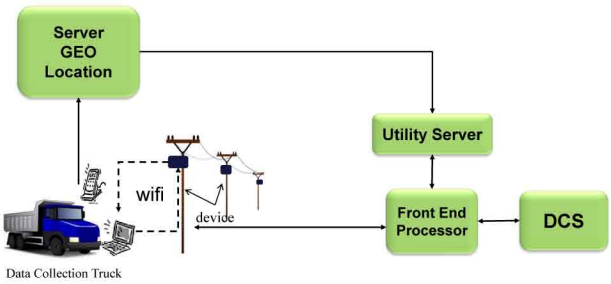
Password Changing Protocol

Rehana Tabassum and Klara Nahrstedt

Goal

- Distribution uses devices such as sensors and capacitor banks.
- These devices measure frequency, voltage, and current from power line
  - to determine health and stability of power line, and
  - to find fault locations due to damage (e.g., storm).
- These devices need to be maintained in the field, and measurements are collected by data collection trucks driven by operators.

The operator does the following steps to collect data:
1) Drives his or her truck under the pole (in the range of Wi-Fi)
2) Logs into the sensor device with a **common password**
3) Collects necessary readings from the device using Wi-Fi
4) Moves to next pole



Current data collection protocol

- Access to devices (sensors, capacitor banks) on electric poles requires password-based authentication.
- Change of password is required to make it resilient against intruder attacks.
- ***Cases:***
  - **Time Domain** (maintenance person doesn't log in on time)
    and/or
  - **Space Domain** (someone tries to log in where he or she is not supposed to)

Research Challenges

- Multiple users and multiple servers, but single password!
  - How can operations deal with thousands of electric poles with the same password?
  - Weak password (it's something easy to remember).
  - Long duration of same password (can't be changed very frequently – large number of users).
- Password can be stolen by someone easily!
- Operators don't know how to solve password-related problems!

➢ Our goal is to provide a **secure password changing protocol** considering:
  - ➢ **Identification** of data collection truck,
  - ➢ Physical **location** of the truck, and
  - ➢ Activity **timestamp** (timestamp of a truck at different poles).

➢ Cost effectiveness!

Research Motivation

- A **truck is stolen** or someone uses a **snooping tool** and gets the password!
  - ➢ Thieves know the password, can access readings from sensor devices.
  - ➢ Get the power to change the telemetric measurements.
  - ➢ Report wrong measurements to the utility companies.

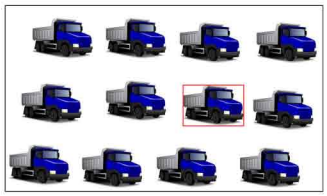
- **Need to make sure that an intruder can't access devices or change readings even he or she breaks the password.**

Research Plan

- Approach is to design Password Changing Protocol considering:
  - Cyber information (password)
  - Physical information (I.D., location, time, etc.)
- Simulation and validation.

Broader Impact

- Allow secure access at devices in the field level.
- Secure data inside the devices.
- Responsible operators can be identified in case of attacks.
- Accurate billing without data alteration.
- Good situational awareness.



Identifying attackers among all operators

Accurate billing

Interaction with Other Projects

Trustworthy Framework for Mobile Smart Meters

Future Efforts

- Explore current authentication protocols.
- Comparative study of different password changing protocols.
- Talk to industry people:
  - understand different scenarios
  - requirements
- Design a secure password changing protocol for our system and validate it.
- Cost-effective.