SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 21: Privacy Issues in CPS

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

Privacy Issues in CPS

- Smart Grid CPS
- Vehicle CPS
- Smart Building CPS

Privacy Issues in CPS

Privacy is about personal data

- How to collect, store and share it?
- Privacy vs Security

Some CPSes will collect data that relates to people -> This may raise privacy issues

- Smart Grid CPS;
  - Smart meter data – about people's power usage
- Vehicular CPS;
  - Electric Vehicles charge locations
- Smart Building CPS;
  - People's location for HVAC control purposes

Smart Grid CPS

Three components of Smart Grid

- Physical system (electricity flow)
- Communication network to send and receive data; Sensor data to be collected from field and Control data to be sent to actuators
- Control center (SCADA)

Power data is collected from various devices

Before control decisions are made, the system observation is needed

- State Estimation
  - This is computed each time and adjustments are made accordingly through control system

Smart Grid Communication Network

Mainly three major components

- Home Area Networks/Building Area Networks
- Neighborhood Area Networks/Field Area Networks
- Wide Area Networks

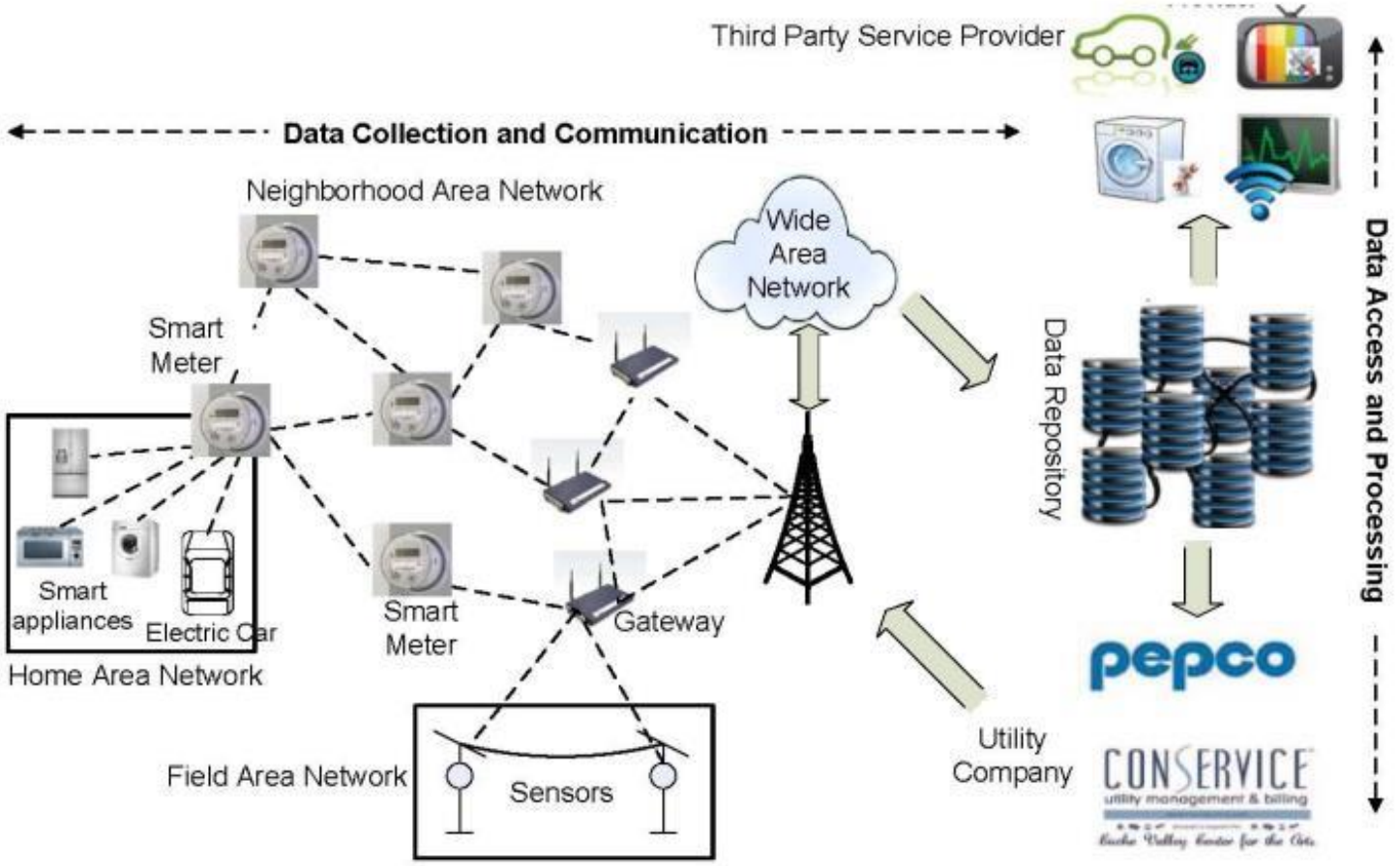
Implementation: A blend of wired and wireless

- Various wireless technology: Wireless LAN, wireless mesh network, Zigbee, cellular network
- Various wired technology: common wired (Ethernet), fiber optic, Power Line Communication (PLC)

Privacy issues arises in Advanced Metering Infrastructure (AMI)

- Uses Neighborhood Area Networks (NAN)

AMI


Third Party Service Provider
Data Collection and Communication
Neighborhood Area Network
Wide Area Network
Smart Meter
Data Repository
Data Access and Processing
Smart appliances
Electric Car
Home Area Network
Smart Meter
Gateway
pepco
Utility Company
CONSERVICE
utility management & billing
Field Area Network
Sensors

Privacy Issues in AMI

Huge amount of data will be generated by Smart Meters

- For real time dynamic pricing, real time demand forecasting
- Higher frequency data (6 seconds/15 minutes/1 hour)

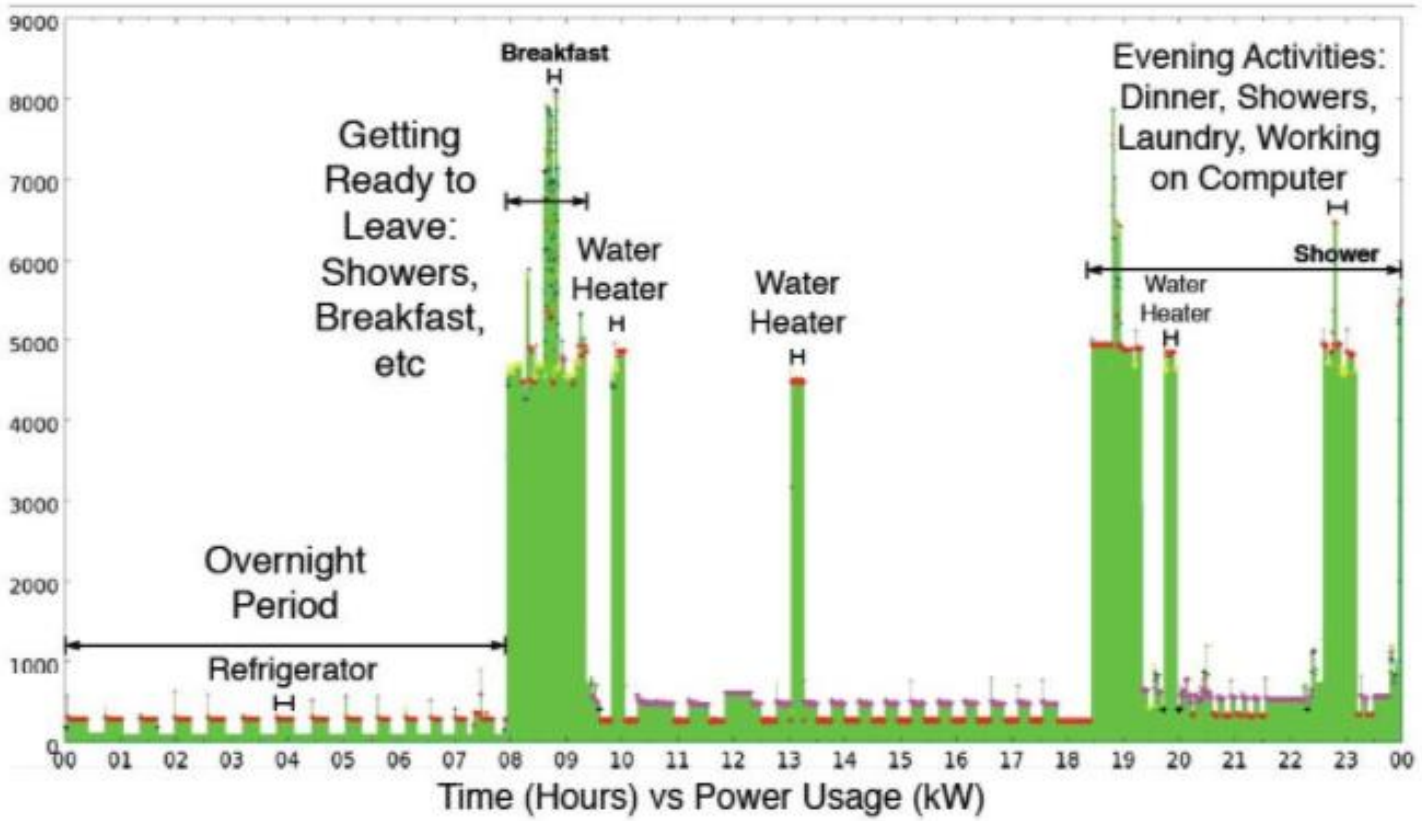
When aggregated over time, this near real-time data can be used to infer the number of people occupying a home, their habits, and the rhythm of their movements!!

One (Law enforcement, thieves, marketers, neighbors, press, insurance companies, landlords, etc.) can deduce

- Avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics of the customer or the household

Smart Meter's Power Data

Without detailed knowledge of appliance signatures, intuitive observation with power consumption variations indicates human activity



Privacy Concerns

The customers eventually may NOT

- Want to participate in smart grid programs
- Even want to share the data with the utility companies

Ideal Solution:

- Nobody will have access to individual readings including utility
- Utility will be able to do billing, state estimation, demand management
- Possible?
  - Fully Homomorphic Encryption systems

Possible Solutions

Anonymization: Disassociation of customer ID and data

- Need third party and large structural changes in the system

Power Data Reshaping: hiding the actual use

- Need a power router and battery at home

Data Aggregation: Instead of individual data, collect neighborhood data

- Still exposes individual readings of smart meters in transmit

Power Data Masking: obfuscation of readings

- Scalability and implementation issues
- Adding noise!

Noise/Obfuscation

How does this impact any state estimation?

In our case, smart meter data may be used for distribution state estimation

Then the issue comes to adding noise to power readings

- How can be state estimation done?

Privacy vs Control Optimality tradeoff

Privacy Preserving via Obfuscation

The goal:

- To preserve the privacy of the consumer
- At the same time give the utility the opportunity to state estimation of the grid

Privacy Preserving State Estimation

Security Goals

Attack 1: The utility company misuses fine-grained meter data it obtains to analyze consumer behavior or shares the data with a third party for this purpose

- Security Goal 1: Obfuscate the collected fine-grained meter data to protect it from misuse by the utility company or related third party

Attack 2: An eavesdropper monitors the communication channel to capture meter data in messages between a targeted Smart Meter (SM) and the utility company to determine the behavior of its consumer

- Security Goal 2: Protect communications containing SM readings

Security Goals

Attack 3: An intruder impersonates a SM or captures the messages from a SM. The intruder may send fabricated readings or obfuscation values or modify captured messages or obfuscation values to disrupt monitoring activities

- Security Goal 3: Provide sender authentication and integrity to verify the sender and contents of messages

Attack 4: A malicious user may capture the obfuscated values and replay them to change the state or billing

- Security Goal 4: Prevent the replay of messages through timestamping

Vehicular CPS

Vehicles communicate each other for safety and traffic optimization

Traffic optimization is of interest for CPS

- Gather vehicle data
- Make computations for efficient traffic optimization
- Ask vehicles to take the computed routes

Vehicular CPS

The privacy issue here -> Vehicle location and tracking

- If this information is not shared, traffic optimization accuracy will degrade

Current standard IEEE 1609.2 (Standard for Wireless Access in Vehicular Environments) provides pseudonyms

- Vehicle IDs
- Changed frequently
- Tracking a vehicle can be eliminated

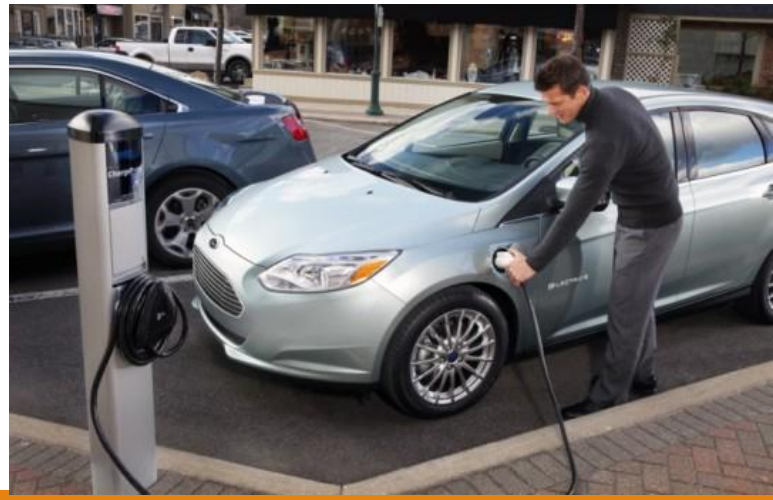
How about Electric Vehicle CPS?

Plug-in Electric Vehicles (EVs) are becoming widely available

- Due to environmental, economic, and energy benefits

Major Issue: Charging – physical system interaction

- Requires twenty times more power than supporting a typical North American home
  - Gets worse if the loads are aggregated and yet uncoordinated
  - Can stress the power grid at certain locations



Charging Coordination

However, this can also be an opportunity to use PEVs as a distributed energy storage system

- Battery storage of a vehicle is about 50kWh
  - Can supply energy of a home for several days

PEVs could buffer renewable power such as wind power by storing excess energy produced during windy periods and providing it back to the grid during high load periods

Communication to Grid (V2G)

Charging times need to be communicated to the:

- Utility (Home Charging: Vehicle to Home)
  - Can use AMI to talk to the Utility
- Charging stations (Aggregators)
  - Vehicles connect to the Charging stations via Vehicular communications
  - These PEVs will be equipped with wireless communication capabilities (e.g., DSRC or LTE)
- Vehicles (V2V charging)
  - In the future (wireless charging?)

Privacy Concerns

EV charging requires the exchange of considerable information that could expose vehicle owners to intrusions of privacy

- Short driving range of EVs (e.g., ~100-200miles)
  - Vehicles need to charge often; the frequency of charging will be much more than the frequency of filling gas in gasoline cars

Frequent EV charging exposes not only the location information to track an individual vehicle but also

- Charging time,
- Amount of battery charge available on the vehicle (State of Charge (SOC)),
- The amount of power EV charges each time
  - Track the users and learn their behavioral habits

Privacy-preserving Power Charging Coordination

Challenge:

- Privacy preservation usually aims to hide information but charging coordination schemes need enough data
- Privacy-utility trade-off
  - Would this impact control?
  - Grid coordination

If privacy concerns cannot be addressed, this may affect the wide-spread adoption of EVs

- Customer trust etc.
  - I have nothing to hide.. So I don't mind..

Attack Model

The attackers can be

- The Aggregator, the Charging Controller (CC), EVs
- Eavesdroppers; They may passively eavesdrop on the communications to figure out sensitive information

The aggregator and eavesdroppers should **not** know

- Whether EV owner needs to charge or not
- Whether driver is at home or not
- The charging requests' data, such as completion time, remaining amount

The CC should know enough data to run the charging coordination scheme

- But it should not be able to link the data to particular EVs

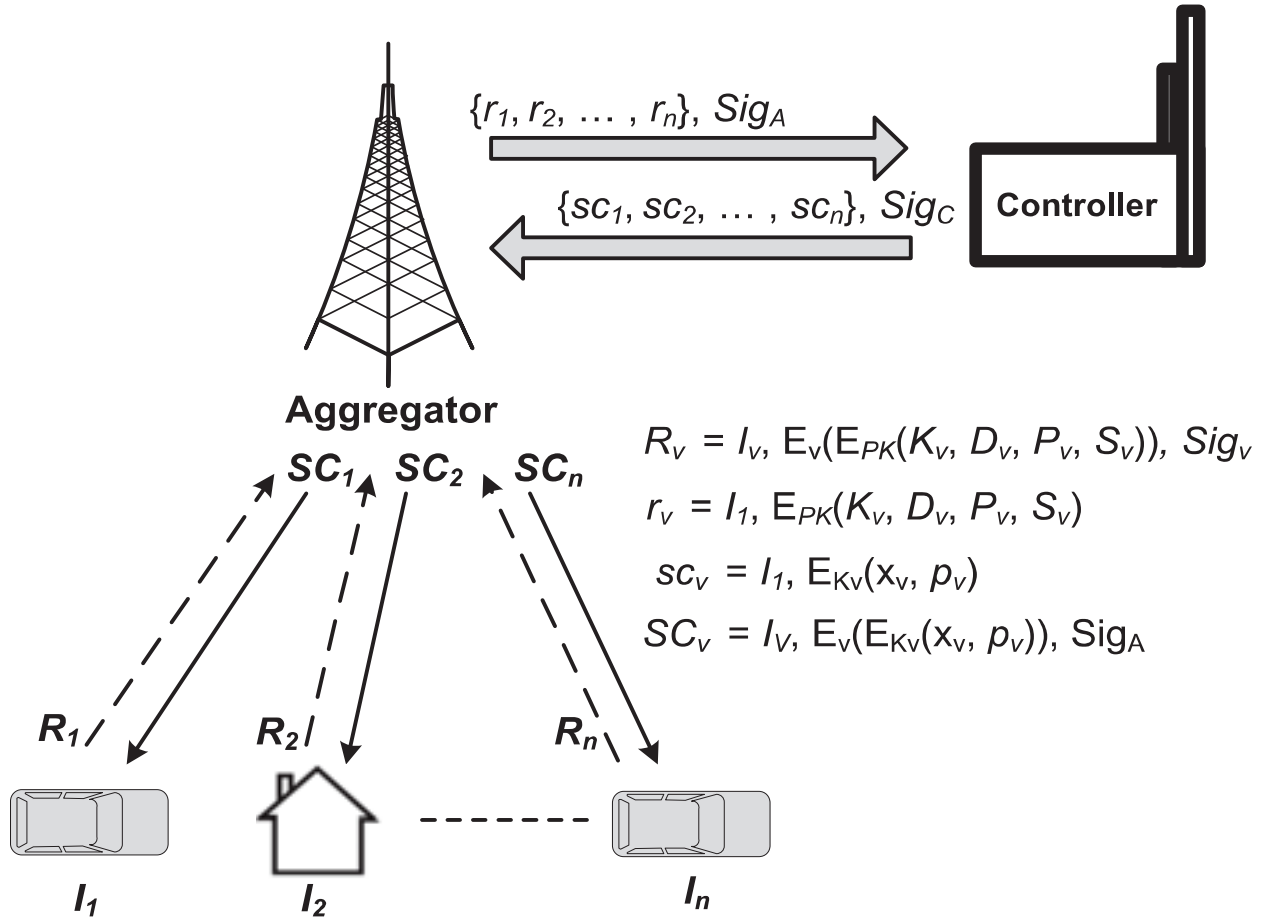
Hiding Private Data

Each EV should send a charging request to an aggregator

- The request does not reveal any private information to the aggregator

Via Aggregator:

- The aggregator forwards the requests to CC after shuffling and signing them
- CC can see the data but cannot linked data to a particular vehicle



Smart Building CPS

The goals of smart buildings are user's comfort, access control and security, and building management

- Also need to be energy efficient, cost saving
- Need to know the present of occupant and their behaviors to provide the desirable services

Where is the CPS?

- Mainly HVAC, lighting
- Collect data about the occupancy
- Make control decisions for cooling and heating based on that information
  - E.g. If the room is empty, then turn off lights and increase the temperature
- Continuously monitoring occupancy behavior to adjust control actions

Privacy Issues in Smart Buildings

When collection occupancy information, privacy leakages may occur

- User location and tracking
- User behavior pattern

Source of the location information:

- Various technologies used in the smart building (Building Devices):
  - Sensors, RFID, video surveillance, WiFi, etc.
- Electronic devices used by the occupants (Personal Devices)
  - Cellular phone, personal notebook, wearables, etc.

Privacy Issues in Smart Buildings

Lots of research to hide location and provide privacy

- Anonymization : strive to disassociate user identity and the private information
- Location Data Masking : strive to obscure the collected private information

Anonymization would be a solution that will not impact the accuracy of locations

- E.g., change the MAC address of your device regularly

Privacy Approaches

The other case is more relevant to control

- Distortion or obfuscation of the location information
- Or even not reporting any location information

Such reduced accuracy in location would affect the quality of the control

- Inefficient control
- No or random control
- So eventually no savings in energy
- Again privacy-utility tradeoff

Location Data Masking Example

Strive to decrease the location accuracy

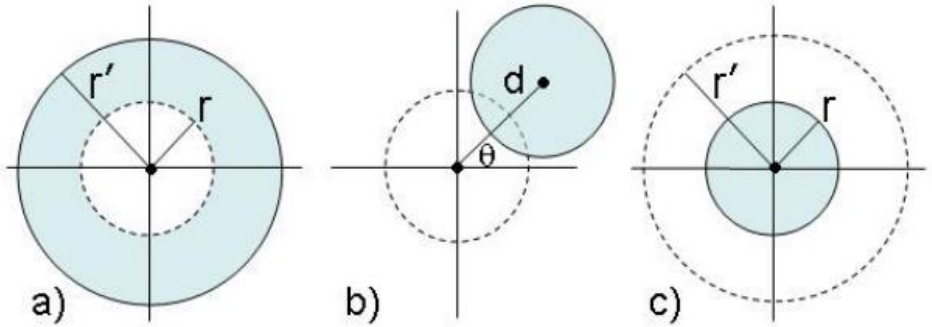
Uses a trusted middleware installed on the client devices to manage the location information sent to the applications

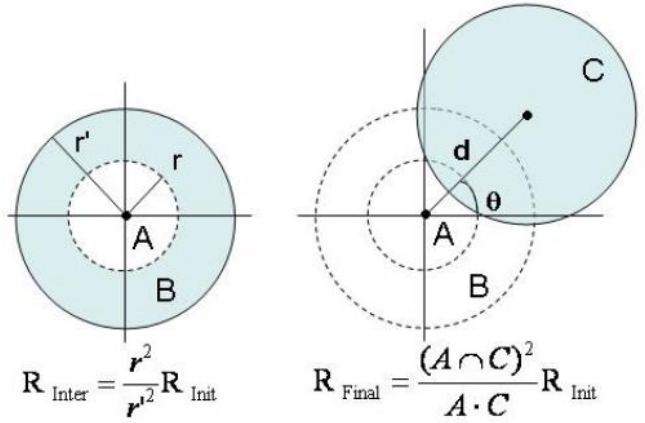
Spatial obfuscation;

- Enlarging the radius,
- Shifting the center,
- Reducing the radius

Combination of the basic techniques

- E.g. Enlarge and Shift





$$R_{Inter} = \frac{r^2}{r'^2} R_{Init}$$

$$R_{Final} = \frac{(A \cap C)^2}{A \cdot C} R_{Init}$$