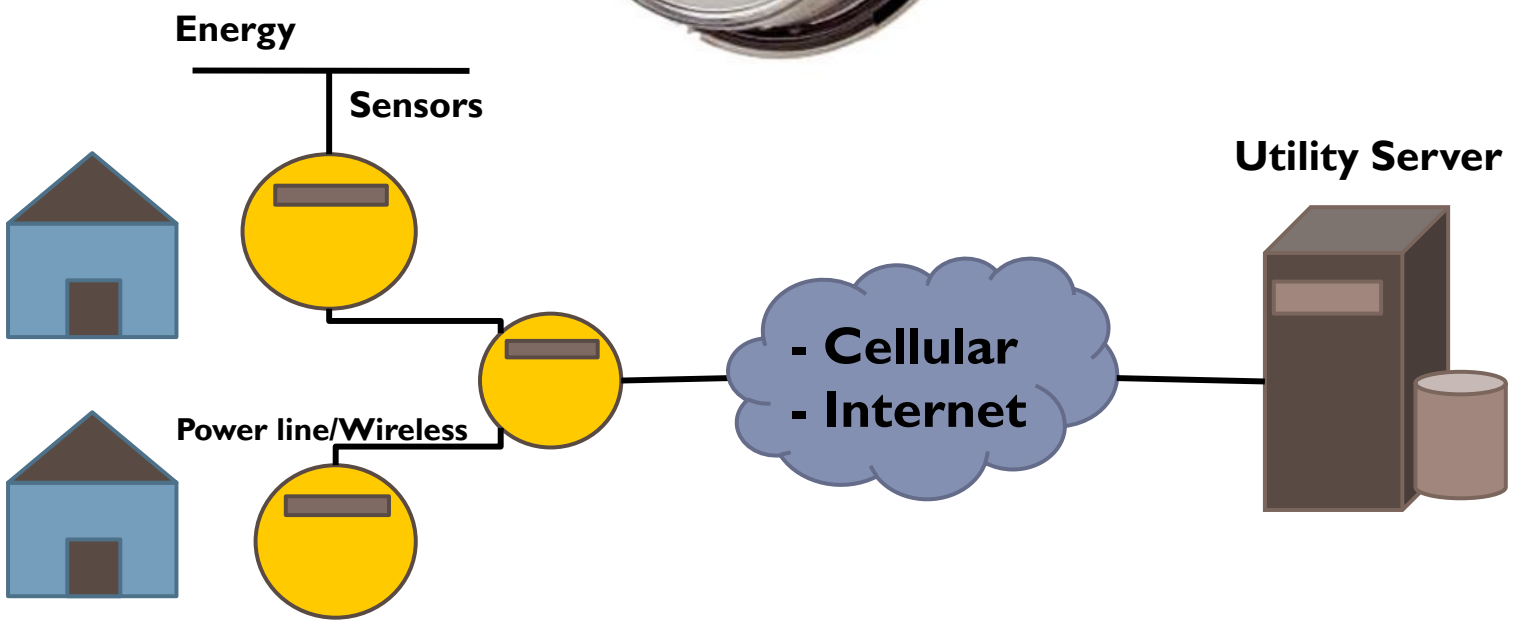
A Model for Security Analysis of Smart Meters

Farid Molazem, Karthik Pattabiraman
Electrical and Computer Engineering Department
University of British Columbia

Smart Meter


123456
iCON
20 000 004


Energy
Sensors
Power line/Wireless
- Cellular
- Internet
Utility Server

Global Status of Smart Meters

2009: 76 million

2010: 118 million

2012: 1 billion

Security

- Smart meters vs analog meters
  - Software attack
  - No need for physical presence
  - Everyone can do it
  - Hard to detect
  - The scale of the attack can be large

Analog Meter

Smart Meter

Security

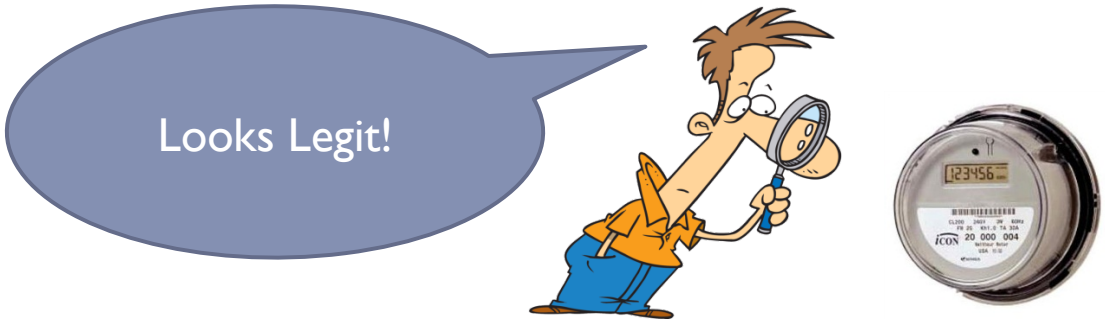
- Is it a concern?

Current Solutions

- Intrusion Detection (Berthier 2010)
  - Network-based (Berthier 2011)
  - Host-based
    - Low end devices
    - False negatives

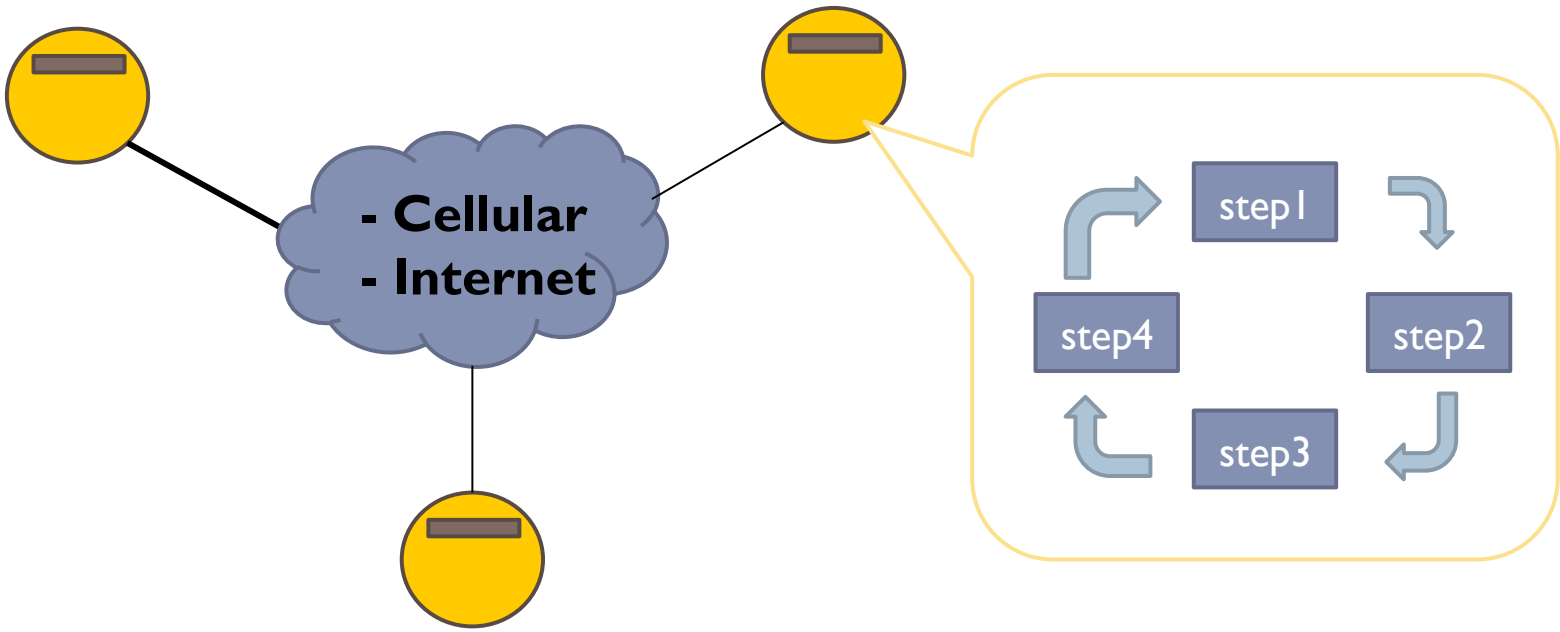
Current Solutions

- Remote Attestation (LeMay 2007, LeMay 2009)
  - Scalability
  - Security



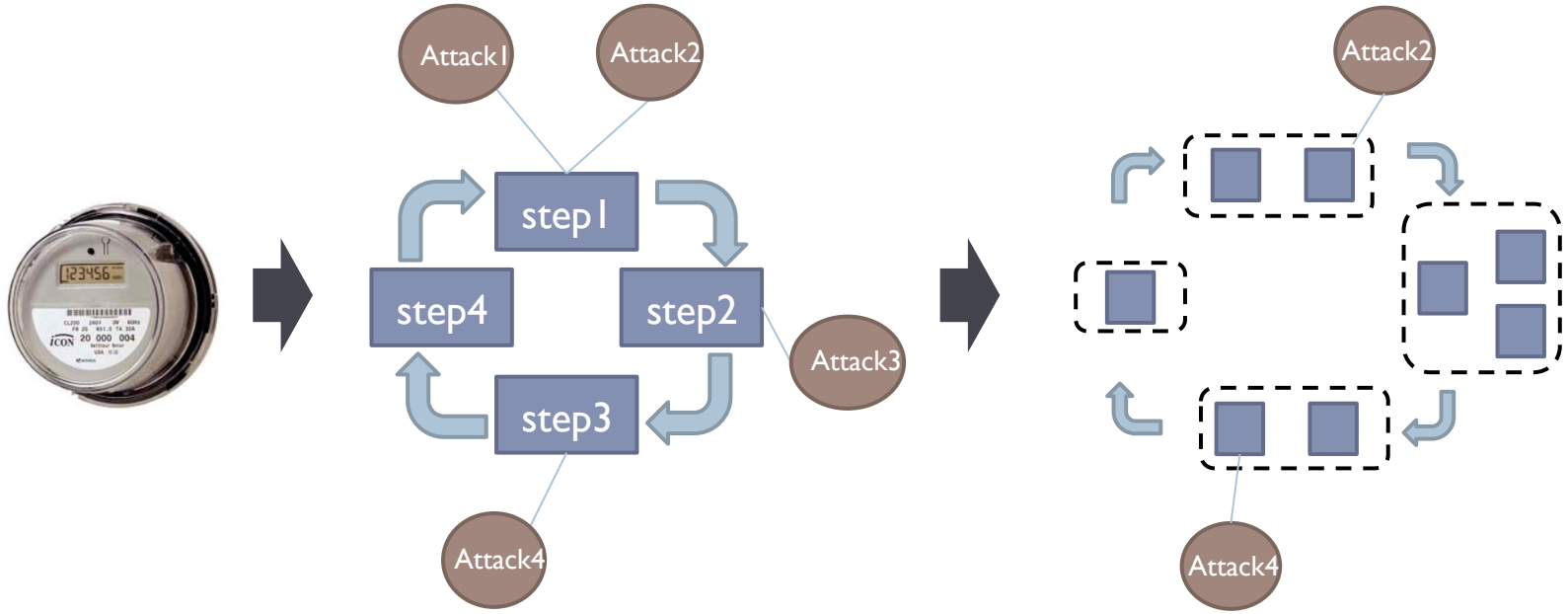
Goal

- Improve the security of the host (smart meter)



What did we do?

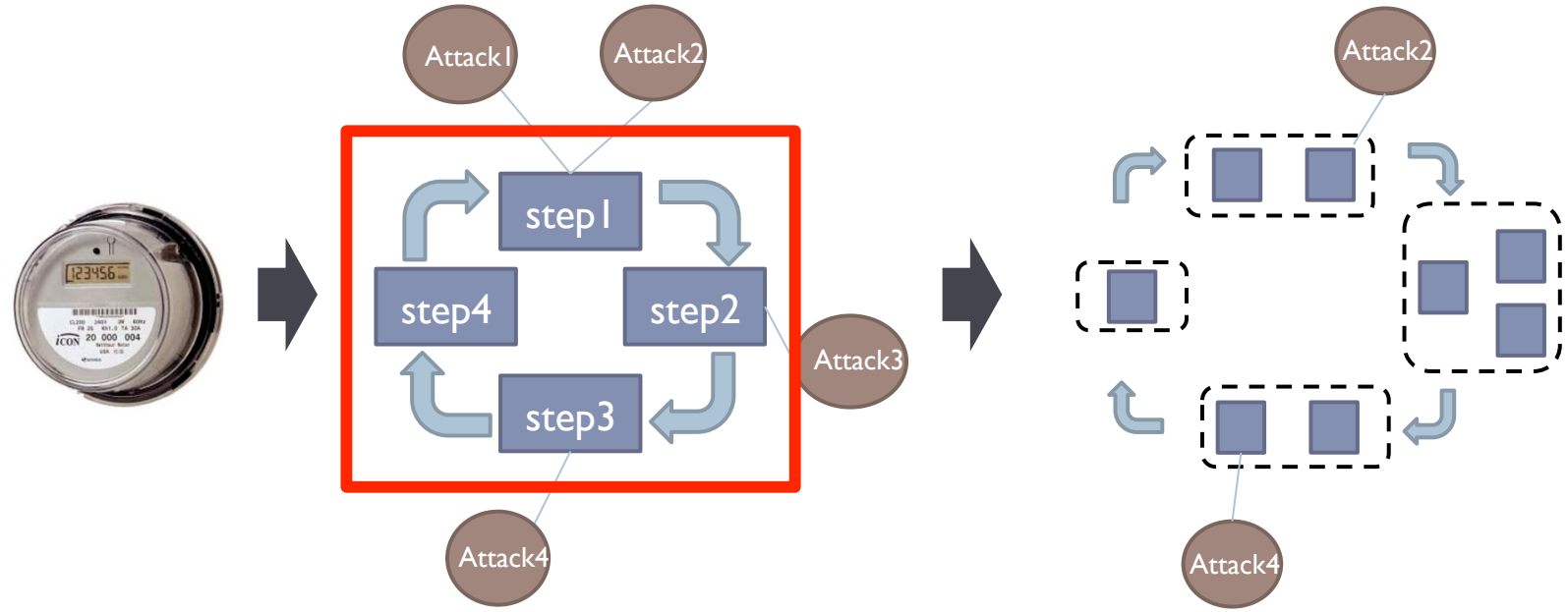
- Build a model of the meter software
  - Meters are designed to do specific tasks



Abstract Model

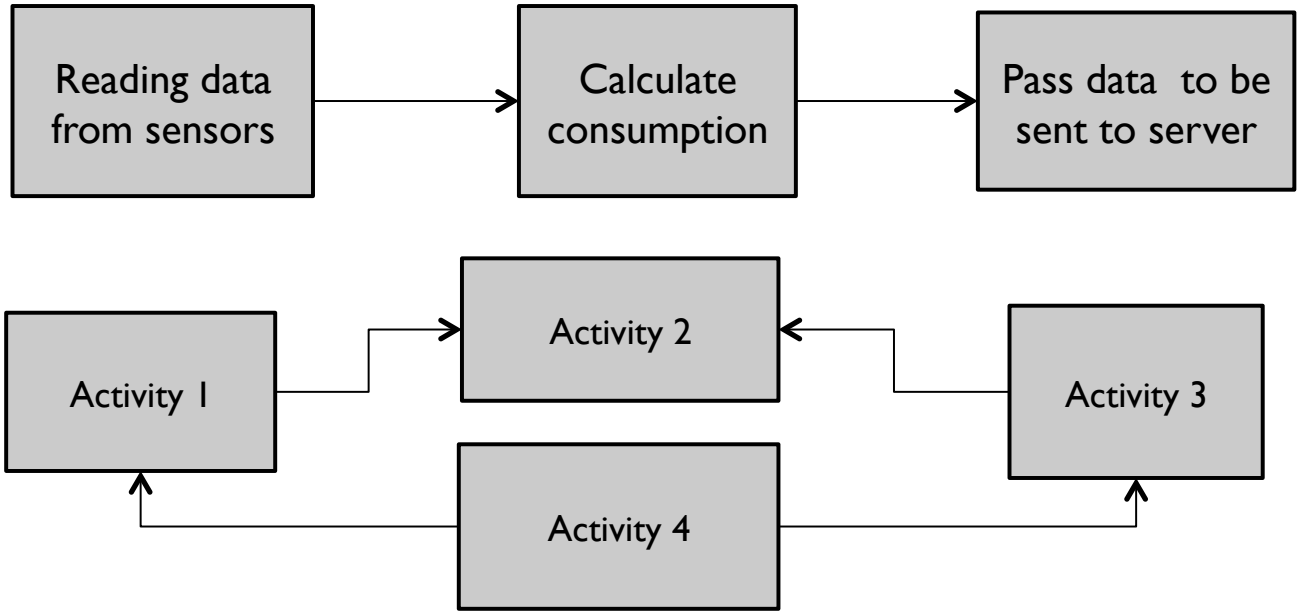
Concrete Model

Abstract Model

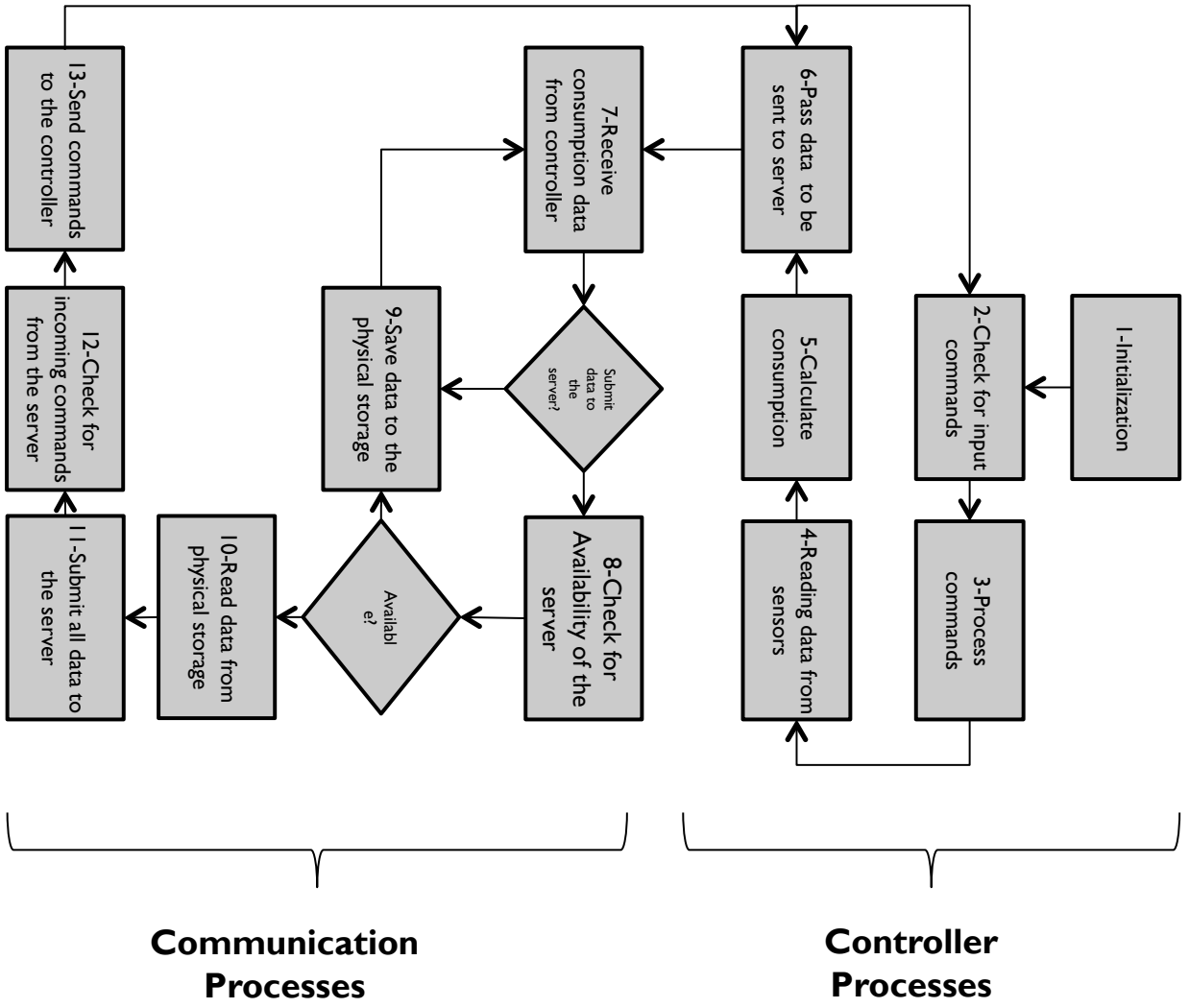


Abstract Model

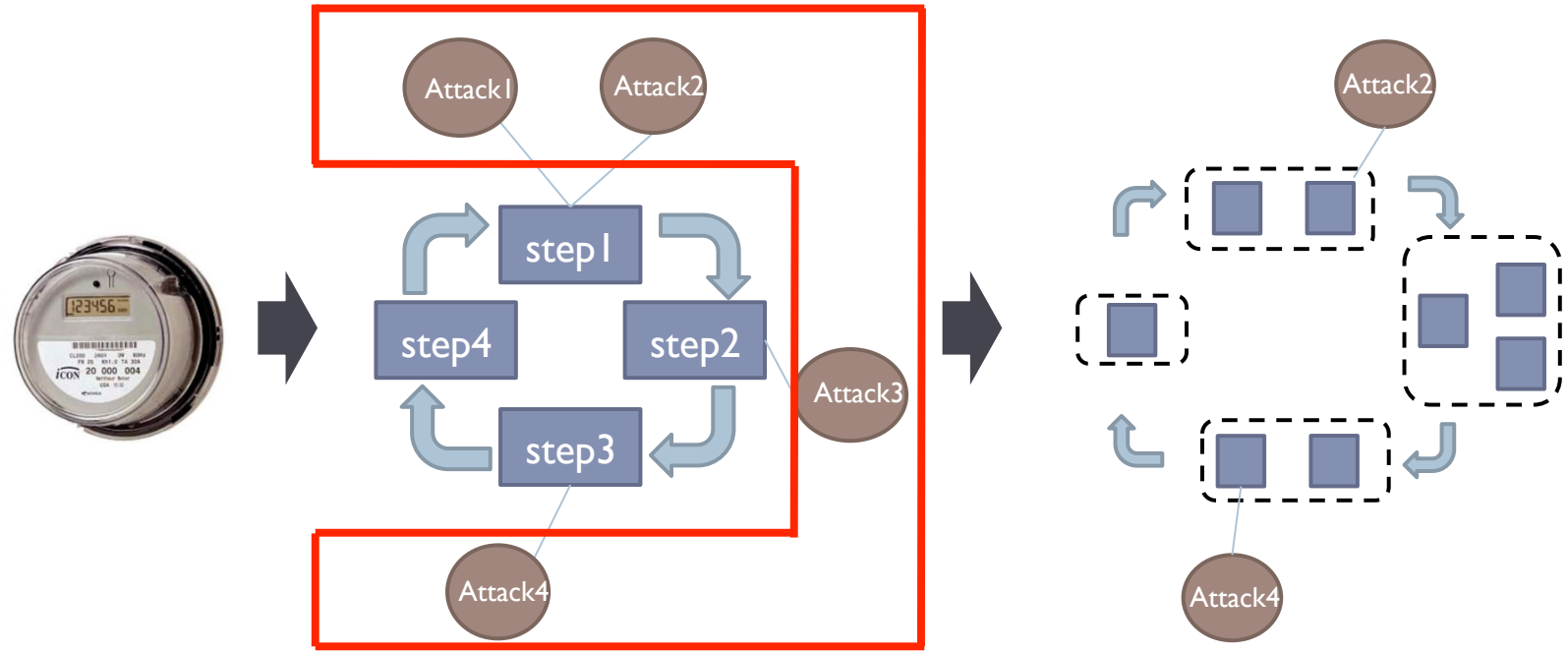
- Build an abstract model based on the common functionalities of all the meters



Abstract Model



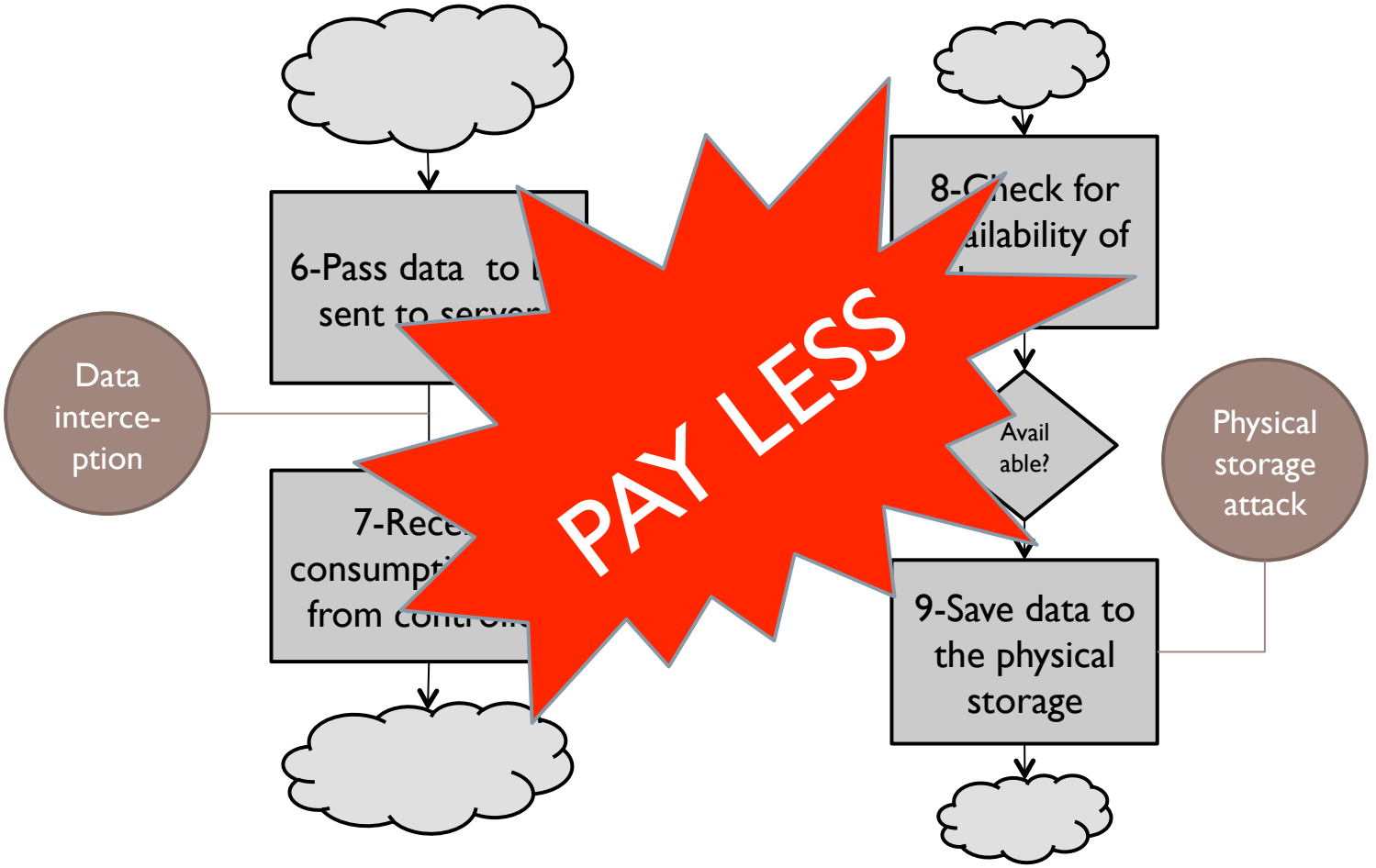
Attacks



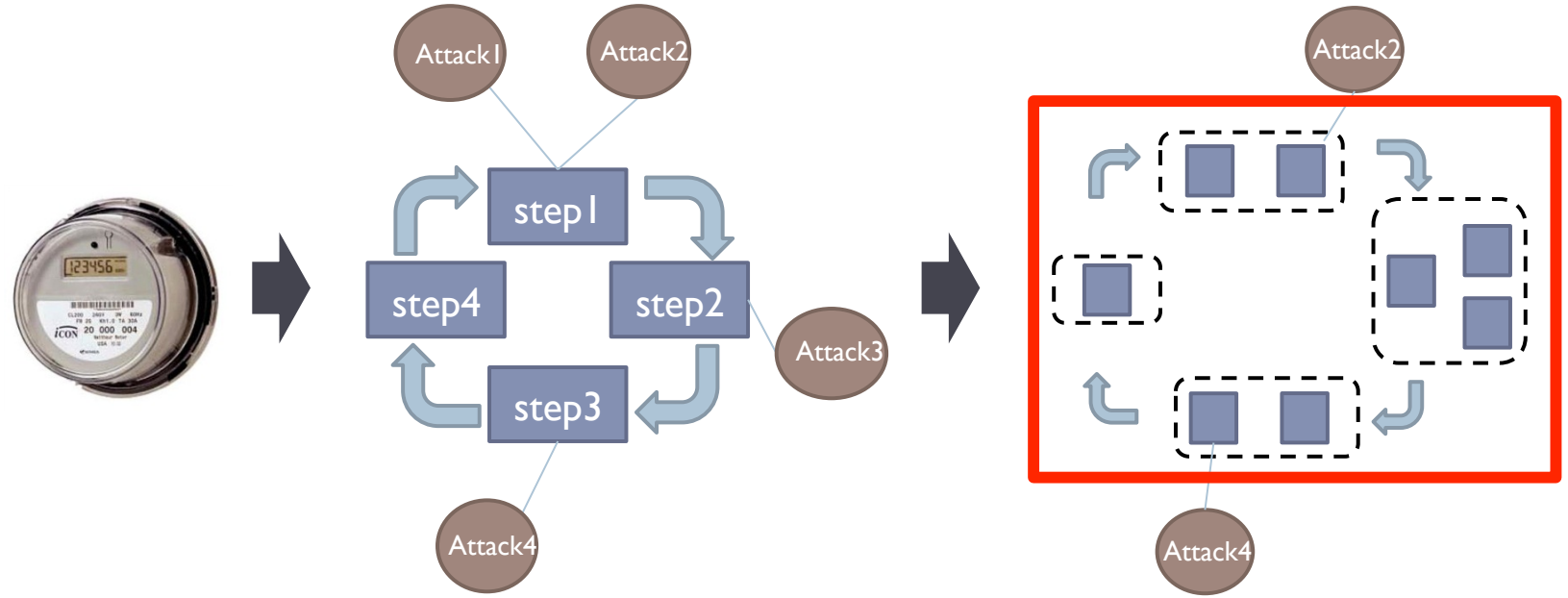
Abstract Model

Concrete Model

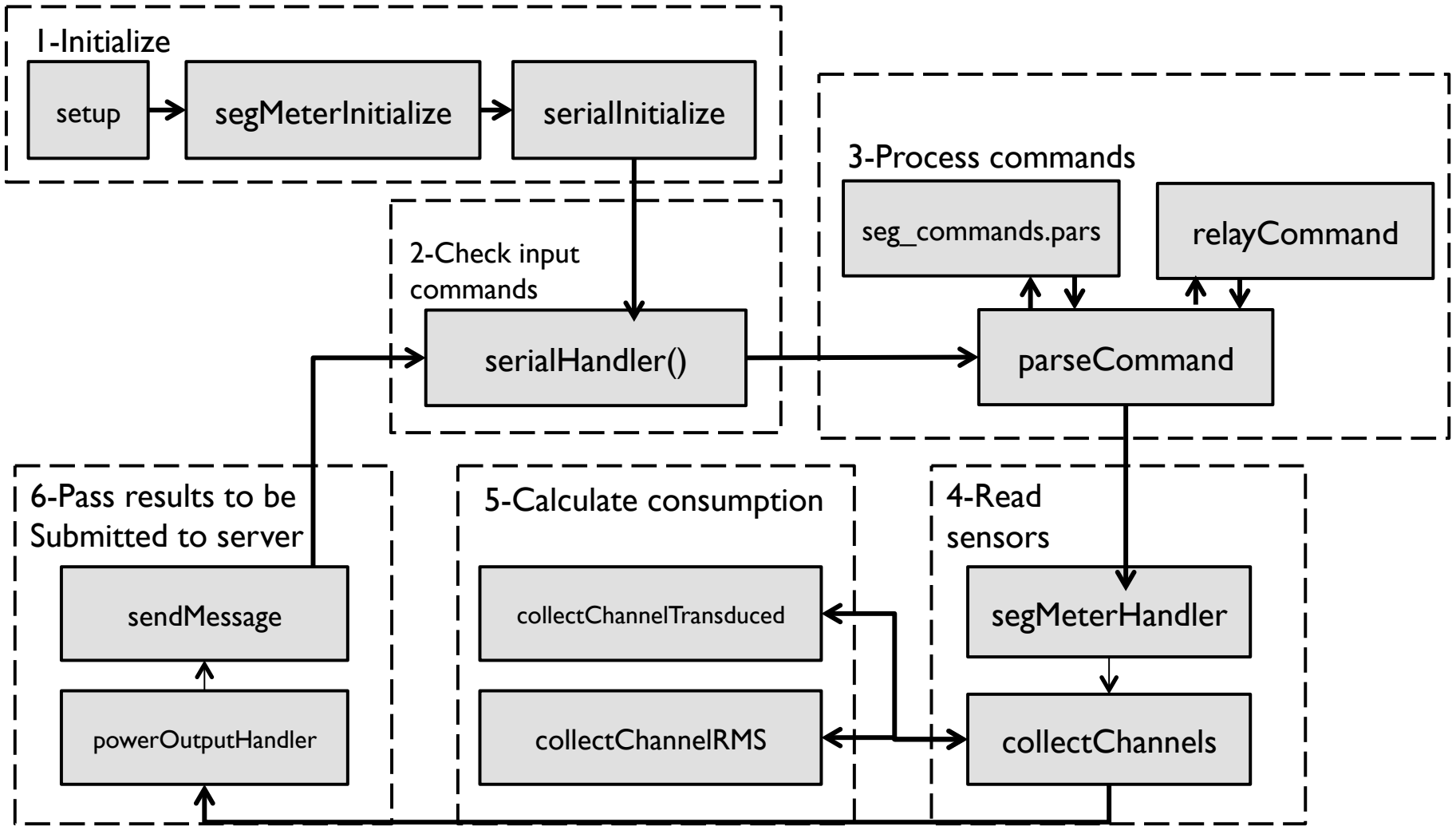
Example Attacks



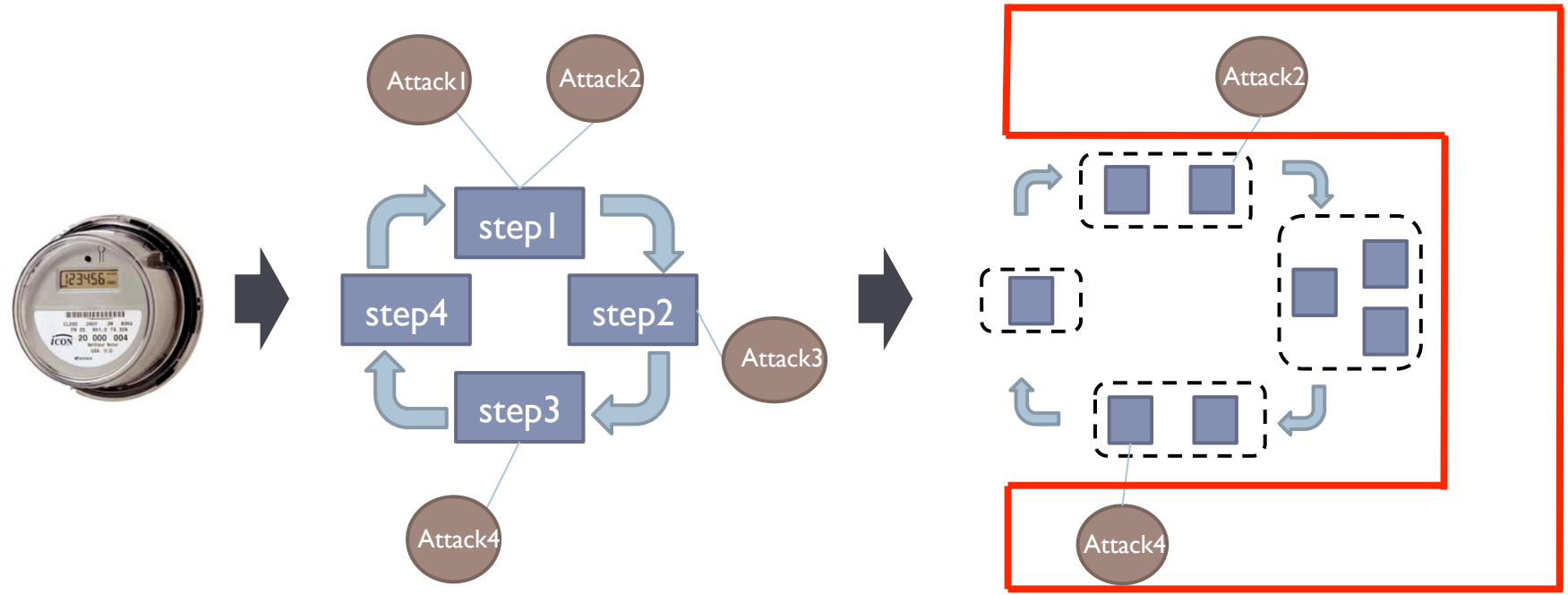
Concrete Model



Concrete Model



Mounting Attacks

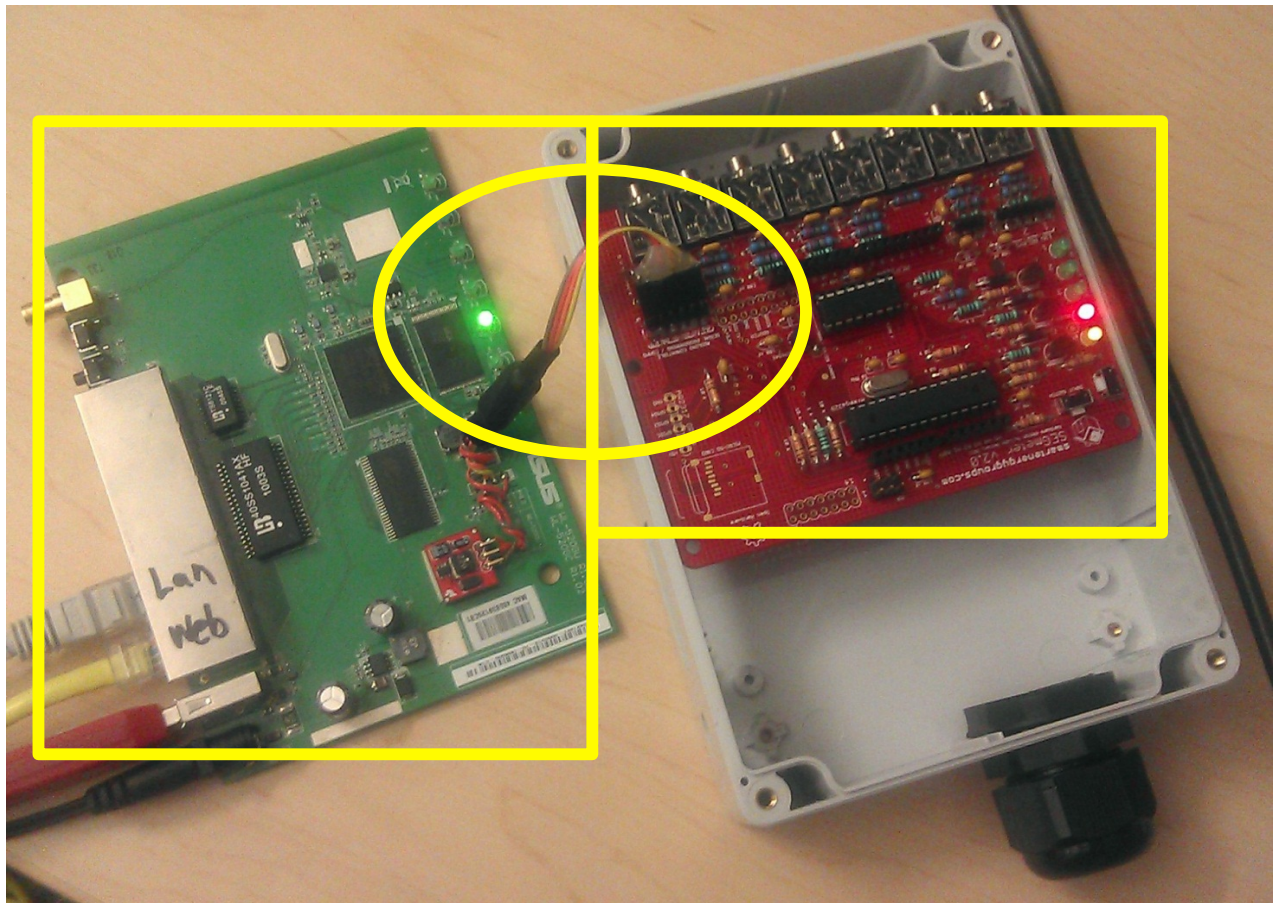


Abstract Model

Concrete Model

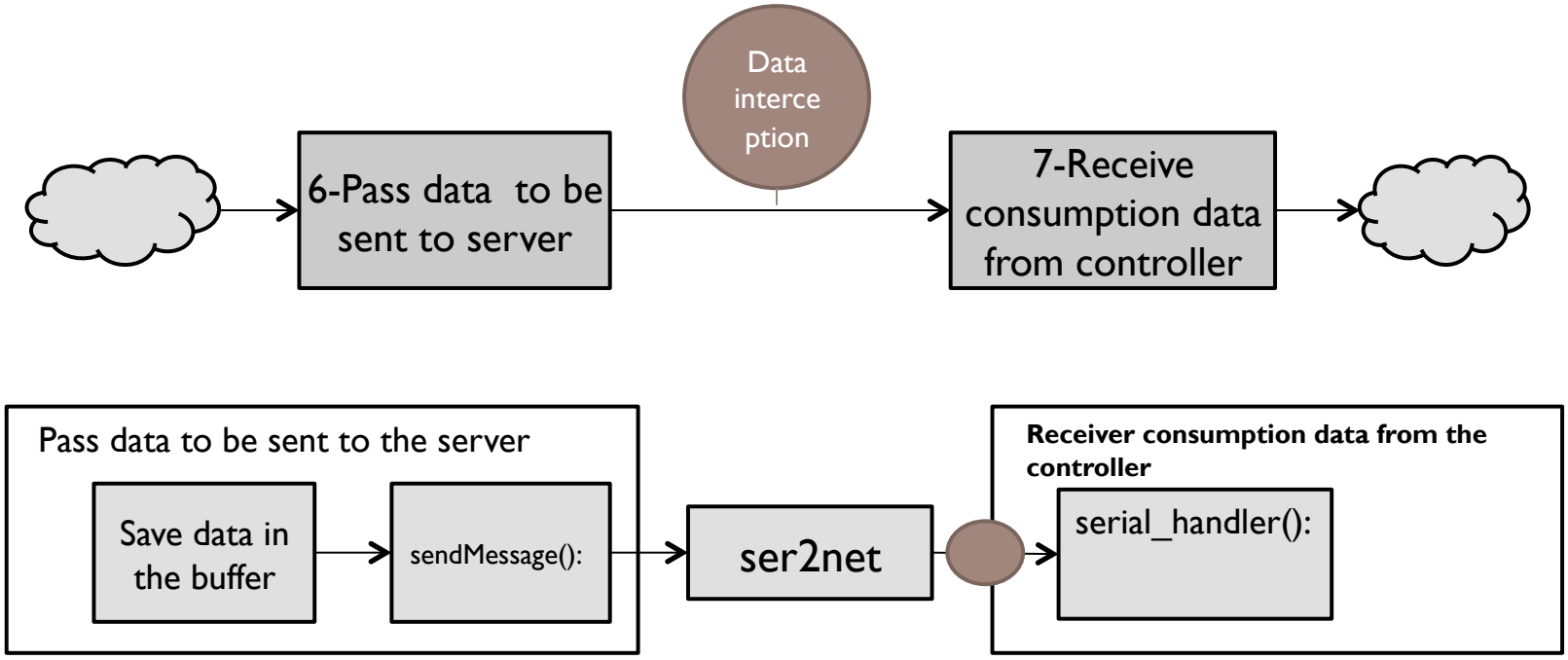
Implementation

- Open source smart meter from “Smart Energy Groups”



Attacks

- Communication interface attack



- 0% CPU overhead and 4% memory overhead

Conclusions and future work

- Systematic security analysis
  - Extendable
  - Captures design flaws
  - Platform for protection techniques

- Future Work
  - Building the Concrete Model
    - 4000 lines of code
    - Automation
  - Generalizing to other meters