IoT Testbed and Demonstration of Attack

-Ronak Khandelwal (2013CS50295)
-Priyam Agrawal (2013CS10248)

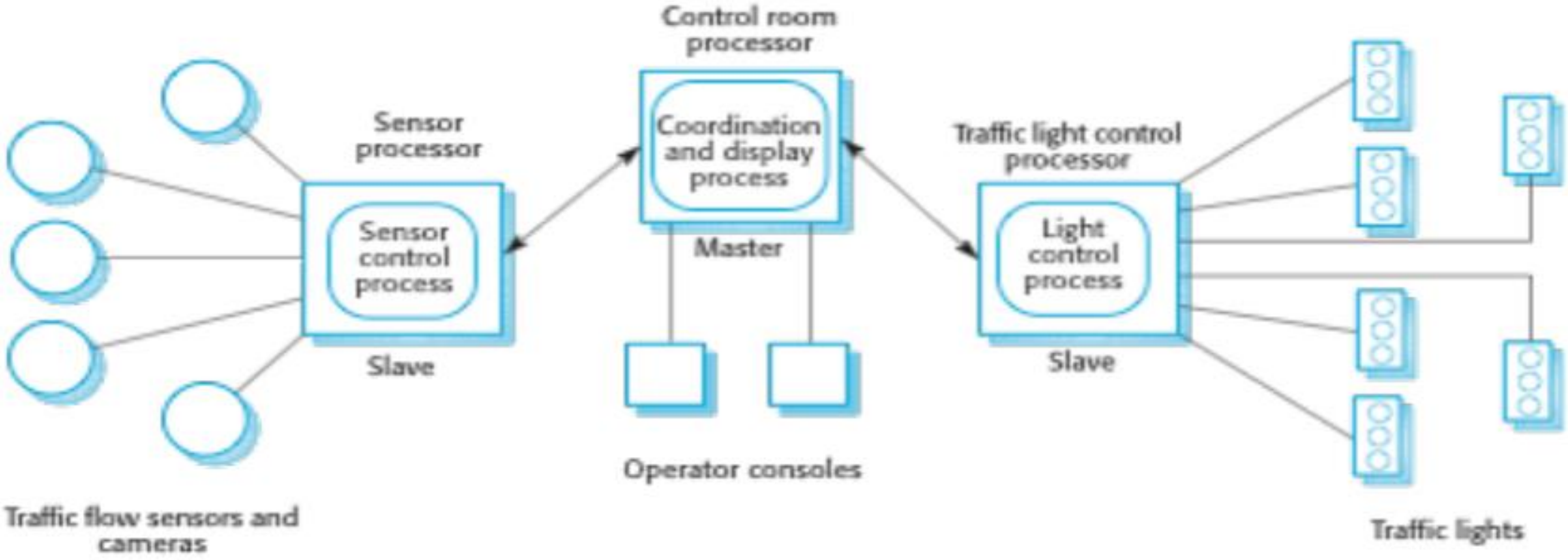
Motivation

- Many IoT devices in the market now-a-days like Google Home, smart buildings etc.
- An attacker can hack into these devices and can create problem
- Thus we need to prepare ourselves to analyze these attacks
    - Create a test-bed and simulate the attacks to further strengthen our communication protocol

IoT master slave architecture

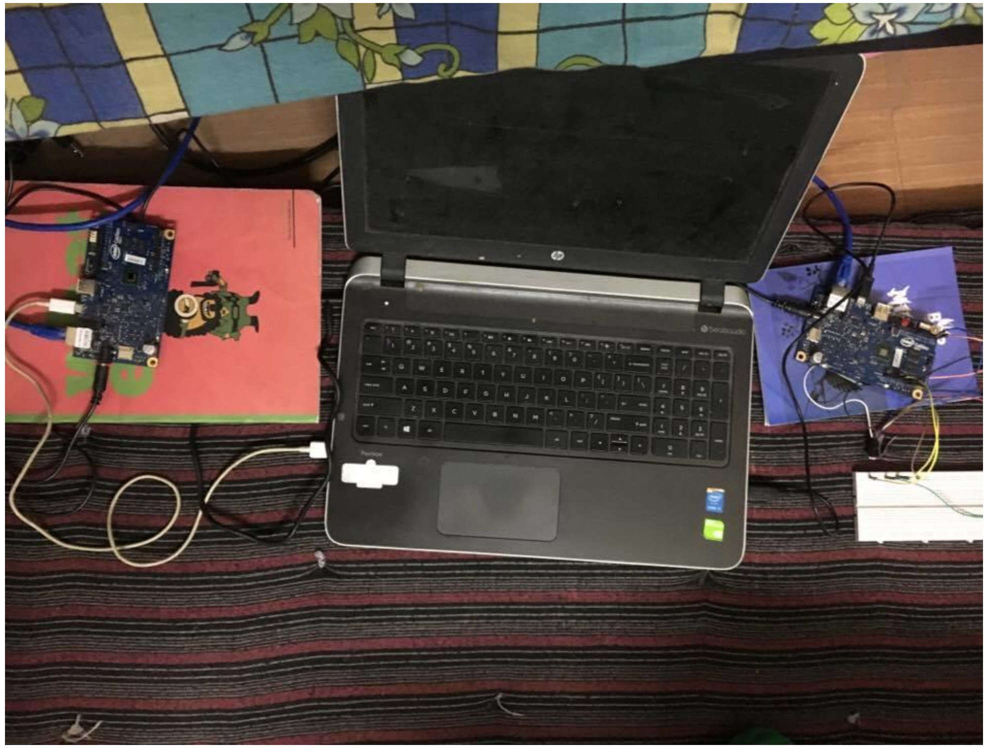
- Distributed systems architecture
- Consists of wireless sensor networks – sends data to server(s)
- Server
    - Receives data
    - Collates them
    - Does some computation and send the decision to the actuators
- Actuator control some devices based on signal received from server

Application – Traffic Management System

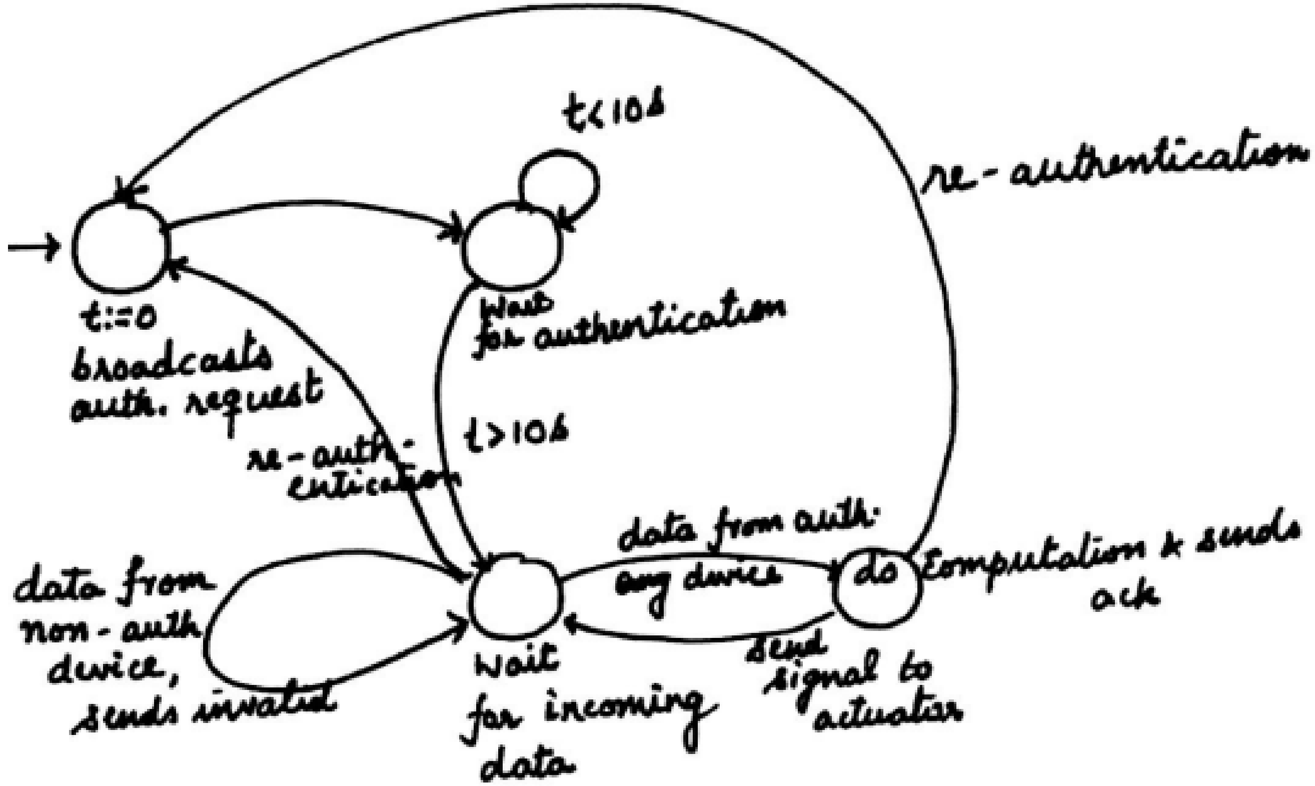


Outline of Testbed

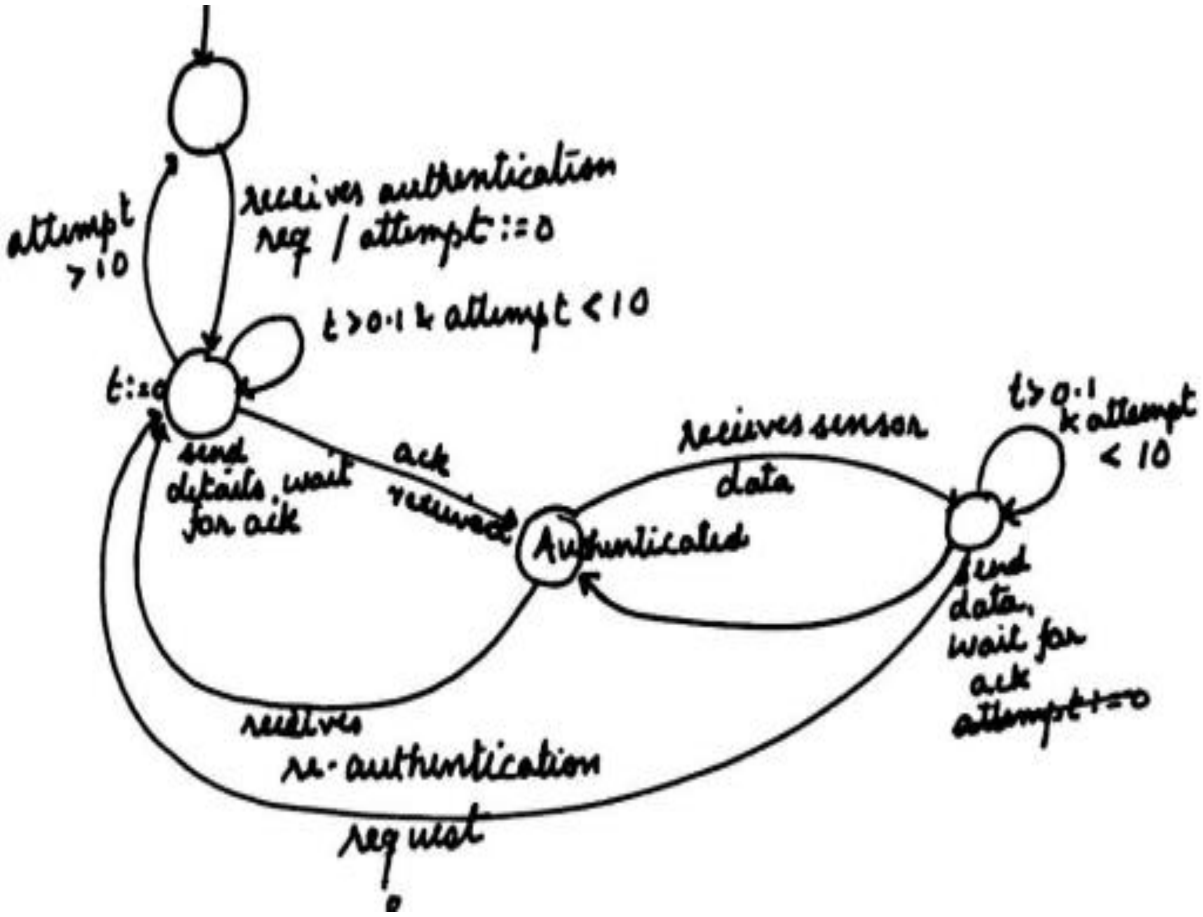
- Based on publisher-subscriber model which is quite common in IoT network
- Scenario considered – group of fire-sensors and door locks



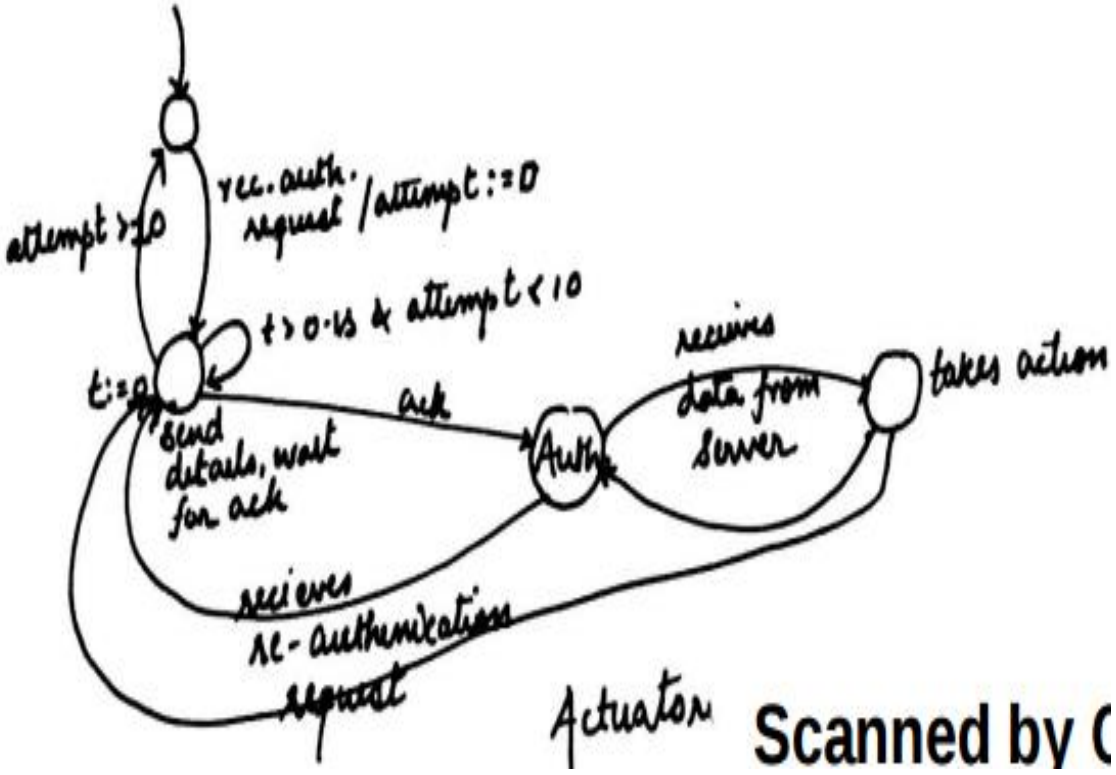
Communication Protocol



Server


attempt >10
receives authentication req / attempt:=0
t>0.1 & attempt<10
t:=0
send details, wait for ack
ack received
Authenticated
receives sensor data
t>0.1 & attempt < 10
send data, wait for ack attempt+=0
receives re-authentication request

Sensor


attempt >10
rec. auth. request /attempt:=0
t>0.15 & attempt<10
t:=0
send details, wait for ack
ack
Auth
receives data from server
takes action
recieves re-authentication request
Actuator
Scanned by C

Actuator

Assumptions and Simplifications

- All communication is happening through plain text.
- Network consists of only one server, sensor and actuator
- Used serial monitor in place of sensor

Attack on this protocol

- Assumption: attacker is already connected to the router of the network
- Takes use of the fact that server is broadcasting the authentication request
- Gets server's ip from the above and spoofs it
- Sends signal to all the devices on the subnet except server, thus disrupting the working of the network

Link to the videos: Showing testbed working and demonstrating the attack
Controlling Lock

Future aim of the project

- Generalize this testbed as much as we can
- To build a lightweight consensus protocol for IoT systems
- Analyze its convergence and security aspects using this testbed