# Formal Modeling of IoT Smart Spaces

Outline

In IoT Smart Spaces software is interacting with humans. Security becomes important from different perspectives, including:

- PRIVACY, to protect the dissemination of data a Smart Space inherently collects.
- SAFETY, to protect users from their autonomous mowers, workers from their robot colleagues, etc.
- SECURITY, to protect unwanted intrusion to the physical Smart Spaces.

An important tool for providing security is verification. It requires a formal modeling of an IoT Smart Space. I did diverse preliminary work into that direction already and would like to take this approach to the next level with you…
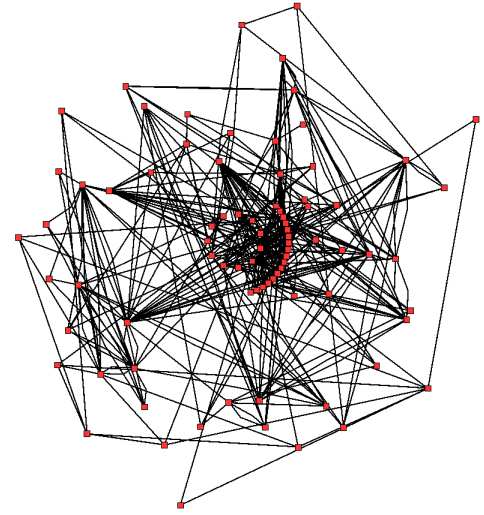
Possible Structure

- Analysis
    - o Technology review
    - o Review of service modeling and verification patterns
- Related work
    - o What do other projects do that answer related questions?
- Design
    - o Which components do you need?
    - o Security, dependability, scalability, …
    - o Which are options for the design? Why are your choices good?
- Implementation
    - o Frameworks used, screenshots, etc.
- Evaluation
    - o How well does it work?
        - ▪ Metrics!

Requirements

Curiosity, Joy to work in a team, Knowledge in Java.
Ability to write good code (including unit tests and documentation).

Contact

If you are interested, please send an email briefly explaining why you think to be the right person for this thesis to:

Marc-Oliver Pahl
pahl@net.in.tum.de
http://s2o.net.in.tum.de/

Image source:
https://upload.wikimedia.org/wikipedia/commons/a/a0/A_thaliana_metabolic_network.png

Distributed Smart 2pace Orchestration System

ds2os.org/