Intrusion detection for IoT based on physical communication profiling

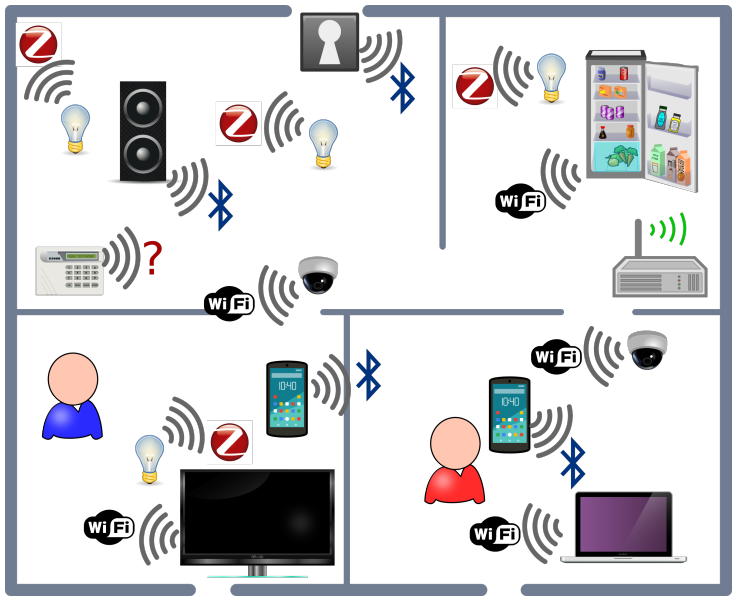
Jonathan Roux, Eric Alata, Guillaume Auriol,
Mohamed Kaâniche, Vincent Nicomette

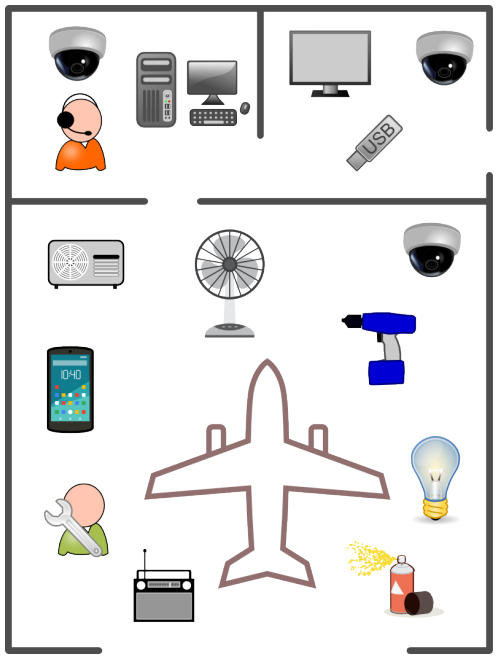
LAAS CNRS

Research group on Dependable Computing and Fault Tolerance

73rd IFIP WG 10.4 meeting, GoA, 12-13 January 2018

Smart homes – Smart spaces

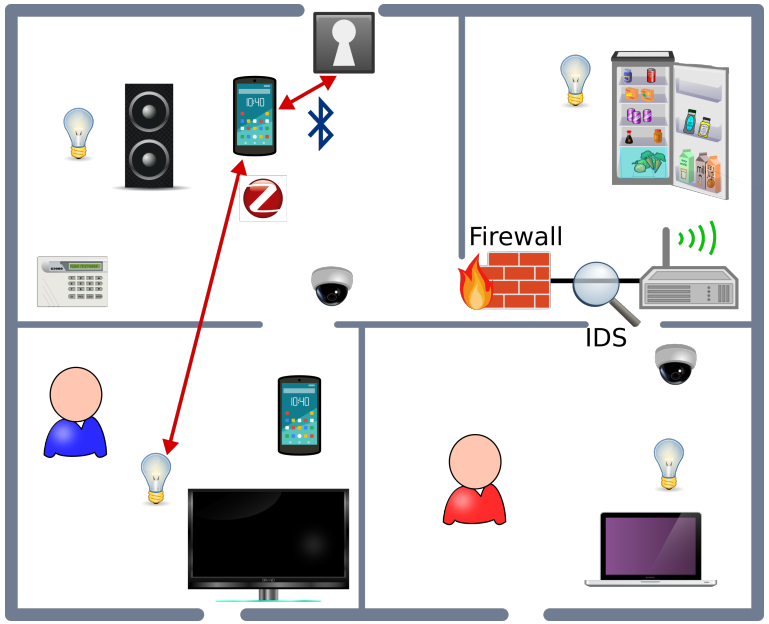


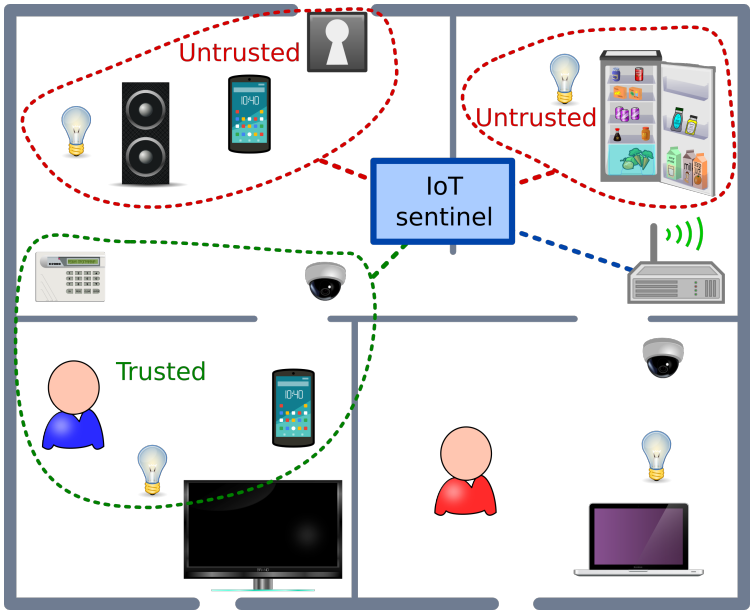


- Multiple and heterogeneous protocols
  - standards/proprietary
- Many deployed devices have security vulnerabilities
  - Mirai, BASHLITE, Remaiten, …
  - Patches often not available, difficult to deploy automatically
  - Too limited resources to implement security mechanisms

IoT- State of the art solutions

- Traditional techniques
  - Firewall, IDS
    - Limited scope
- Dedicated solutions
  - IoT Sentinel [ICDCS17]
    - IoT device identification & isolation
    - Only WIFI/Ethernet

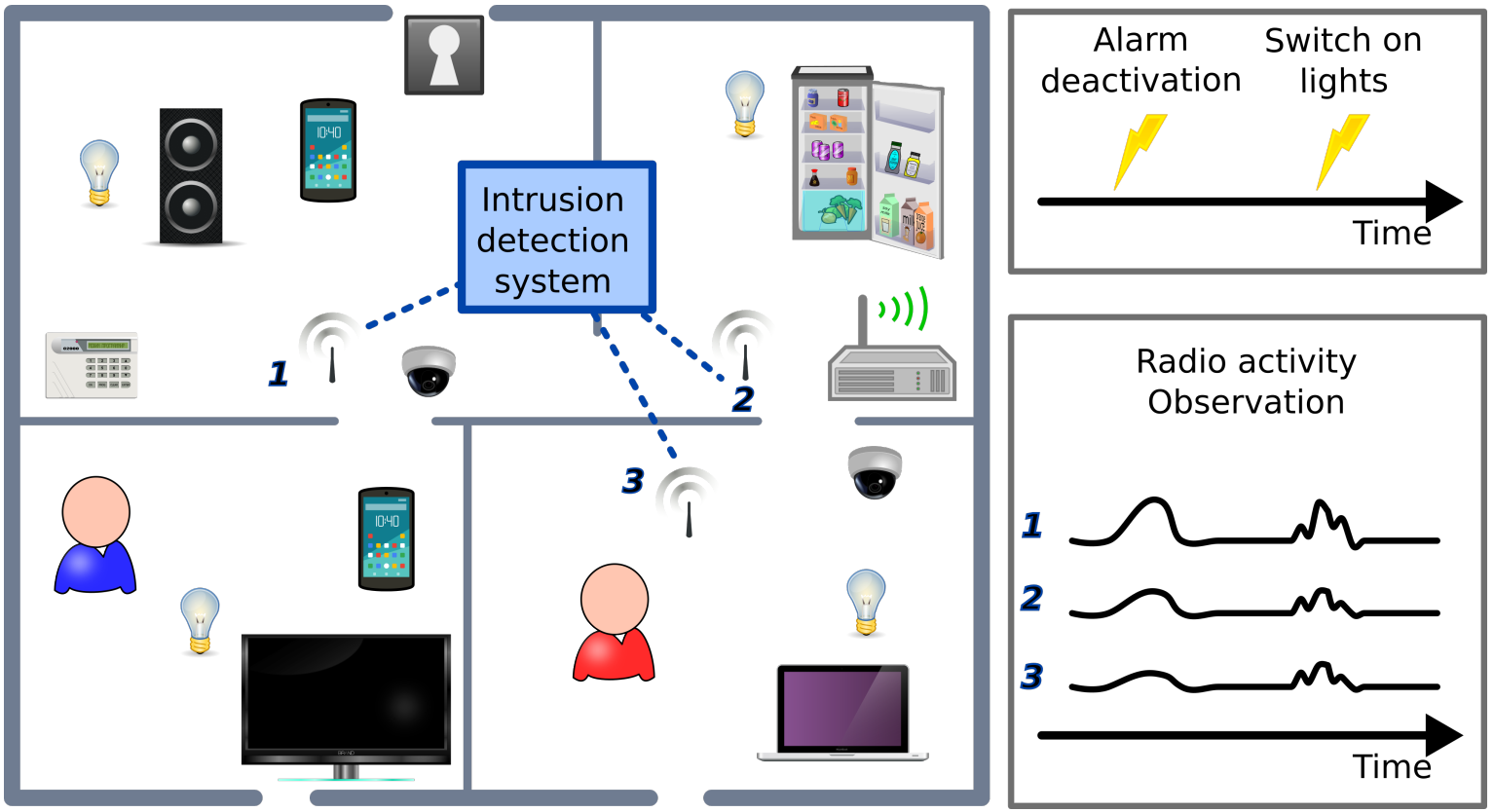




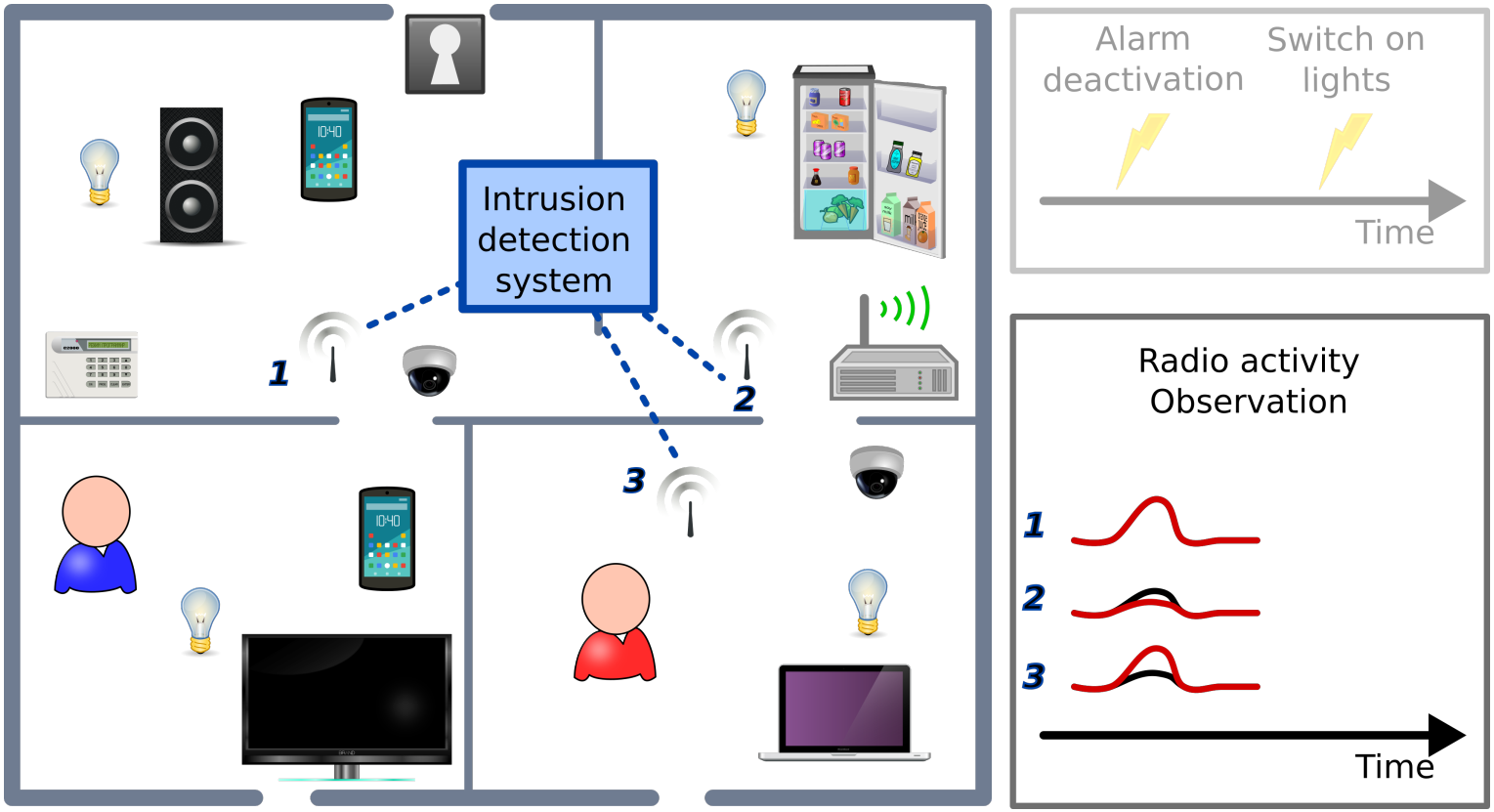
Approach

- Objectives
  - Protocol agnostic
  - Behavioral anomaly detection system
  - Nonintrusive
- Monitoring radio communication
  - Measure radio activities
  - Space and time analysis
- Machine learning techniques
  - Model users legitimate behavior
  - Detect potential deviations

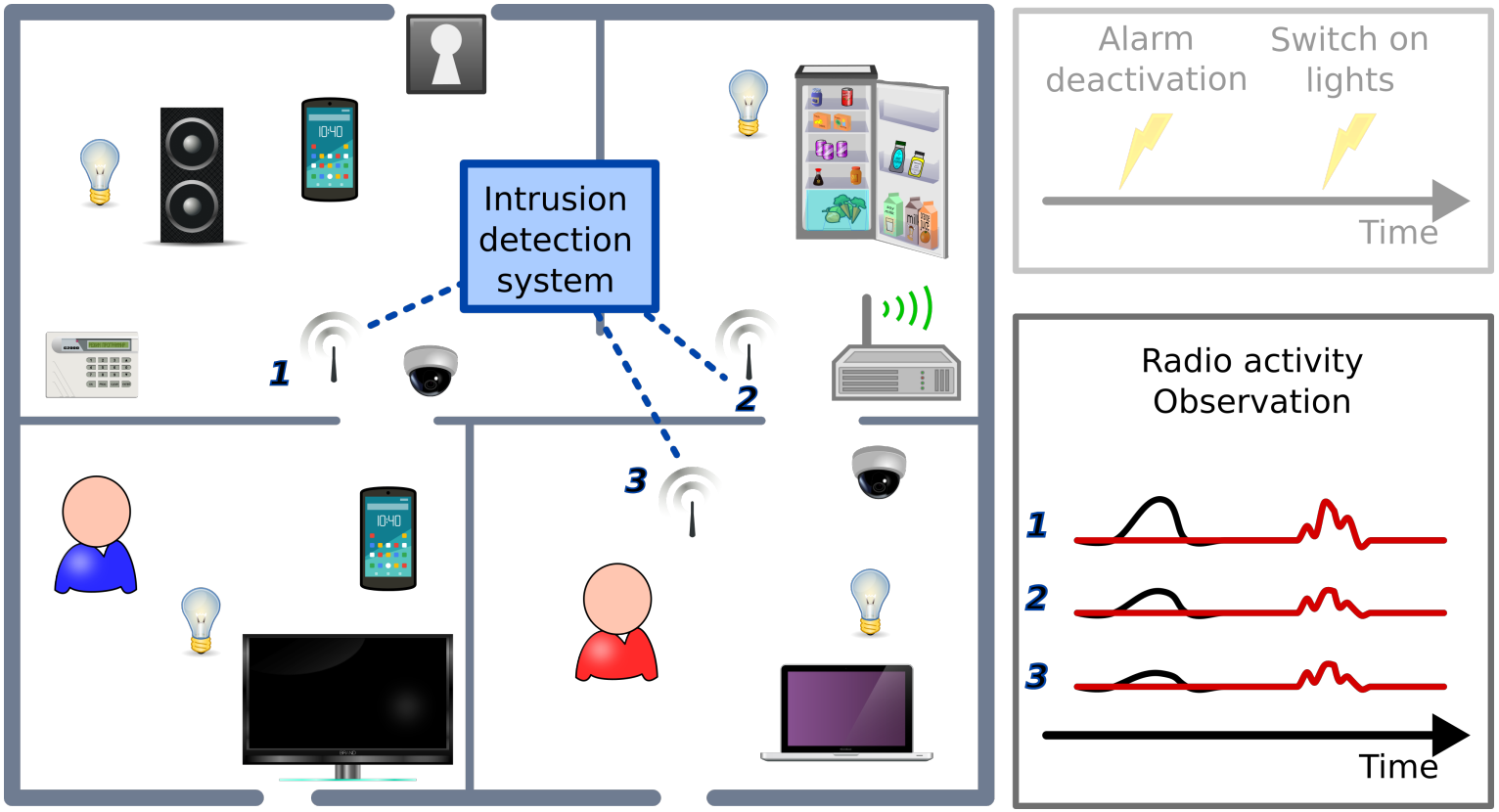
Approach


Intrusion detection system
1
2
3
Alarm deactivation
Switch on lights
Time
Radio activity Observation
1
2
3
Time

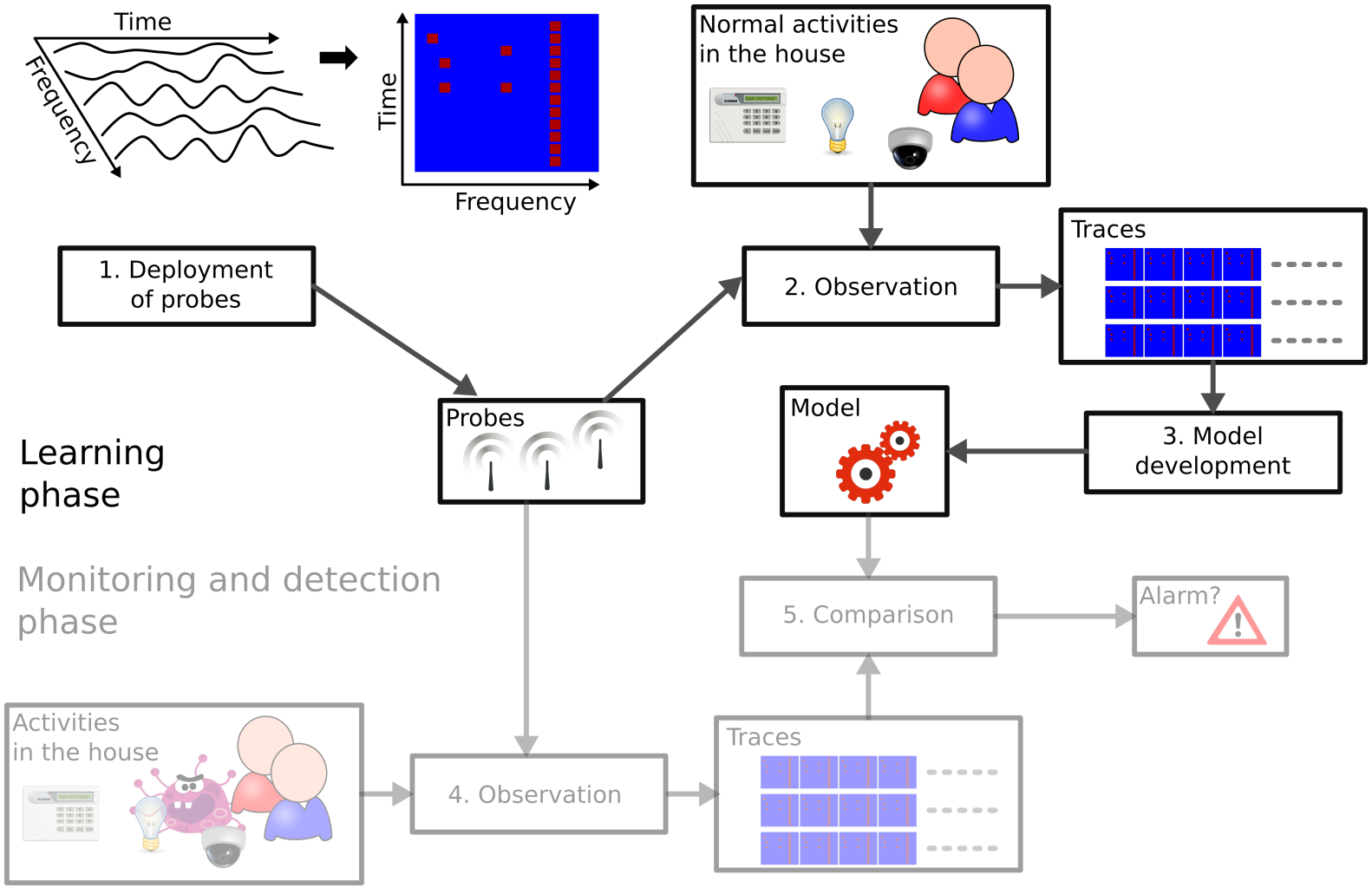
Approach


Intrusion detection system
1
2
3
Alarm deactivation
Switch on lights
Time
Radio activity Observation
1
2
3
Time

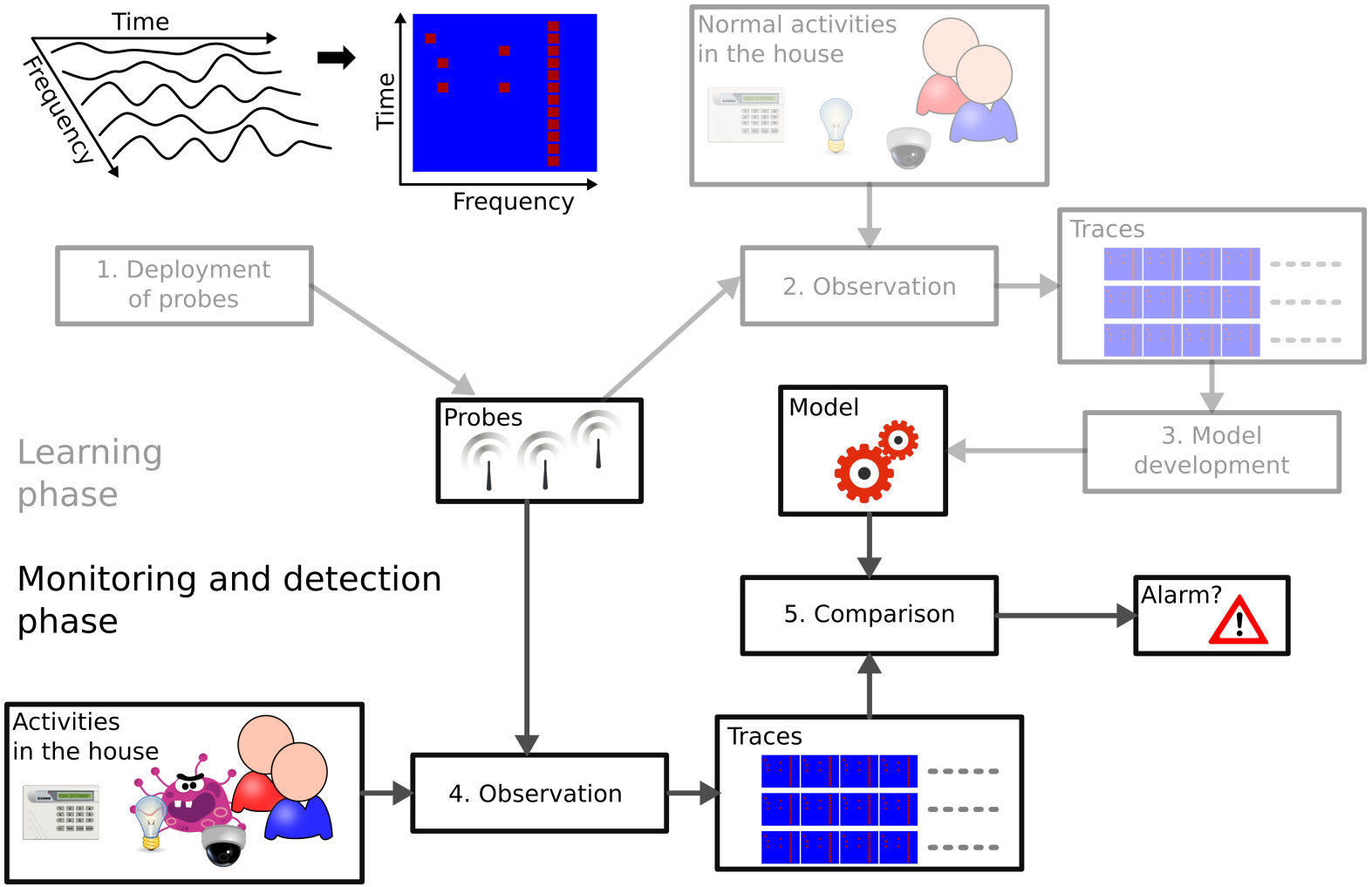
Approach


Intrusion detection system
1
2
3
Alarm deactivation
Switch on lights
Time
Radio activity Observation
1
2
3
Time

Main Steps


Time
Frequency
Time
Frequency
Normal activities
in the house
1. Deployment
of probes
2. Observation
Traces
Probes
Model
3. Model
development
Learning
phase
Monitoring and detection
phase
5. Comparison
Alarm?
Activities
in the house
4. Observation
Traces

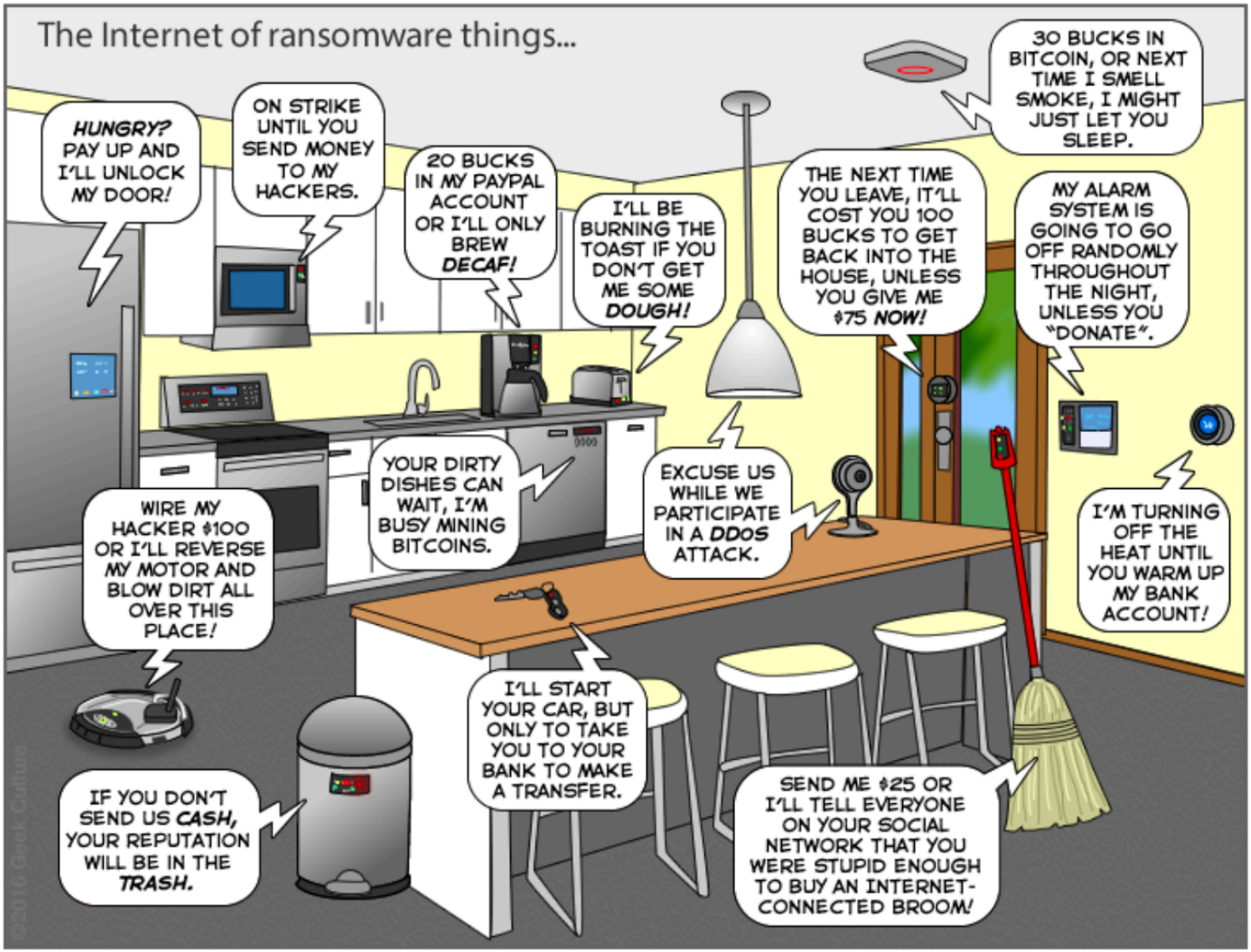
Main Steps


Time
Frequency
Time
Frequency
Normal activities in the house
1. Deployment of probes
2. Observation
Traces
Probes
Model
3. Model development
Learning phase
Monitoring and detection phase
5. Comparison
Alarm?
Activities in the house
4. Observation
Traces

Ongoing work

- Deployment in a smart home and first experiments
- Usage scenarios and data collection
- Comparative analysis of machine learning algorithms
- IDS assessment
  - Simulated attacks
  - False positives / false negatives
- Fingerprinting of IoT devices
- Isolation strategies
- Complementarity with other solutions

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com