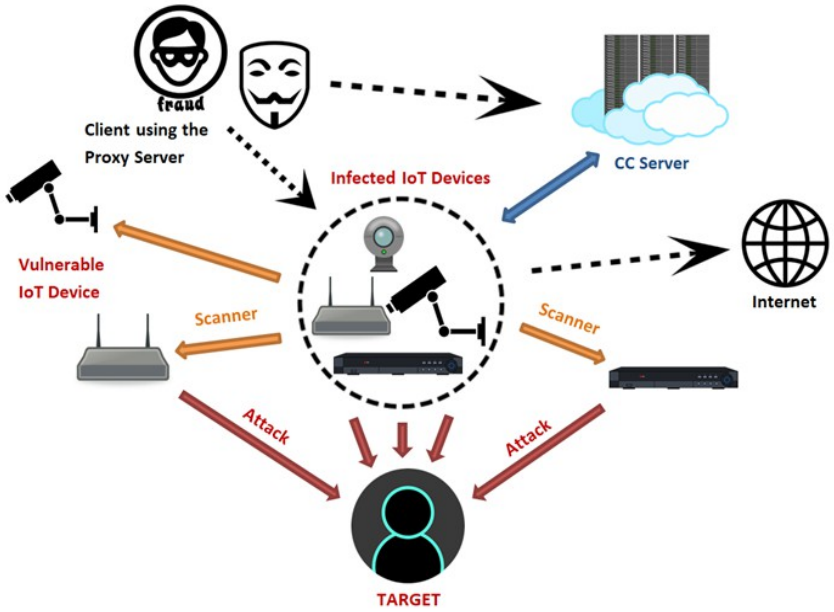
Institut Mines-Télécom

Machine Learning for IoT Network Monitoring

Mustafizur R. SHAHID & Gregory BLANC

Motivation

- 75B connected devices by 2030
- Diversity of IoT devices: security camera, smart bulb, smart plug, smart thermostat, smart car, …
- 600% increase in IoT attacks from 2016 to 2017 (ISTR Symantec 2018)
- Constantly evolving malware:
  - Mirai (2016)
  - Reaper (2017)
  - HideNSeek (2018)



IoT Botnet
Source: www.fortinet.com

Proposal

- **SoTA.** Extensive academic research on the use of ML for intrusion detection in general purpose networks: but few actual deployments in production

R. Sommer & V. Paxson : Outside the closed world, S&P'10

- **Key observation.** IoT devices perform very specific tasks making their networking behavior very stable and predictable

- **Constraints.** IoT devices may be resource-constrained so no monitoring on host

- Two types of monitoring methods are proposed:
  - IoT device identification: classification methods help enforce security, e.g. by applying device specific filtering rules.
  - Traffic anomaly detection: learning IoT signals to detect new and anomalous behaviors

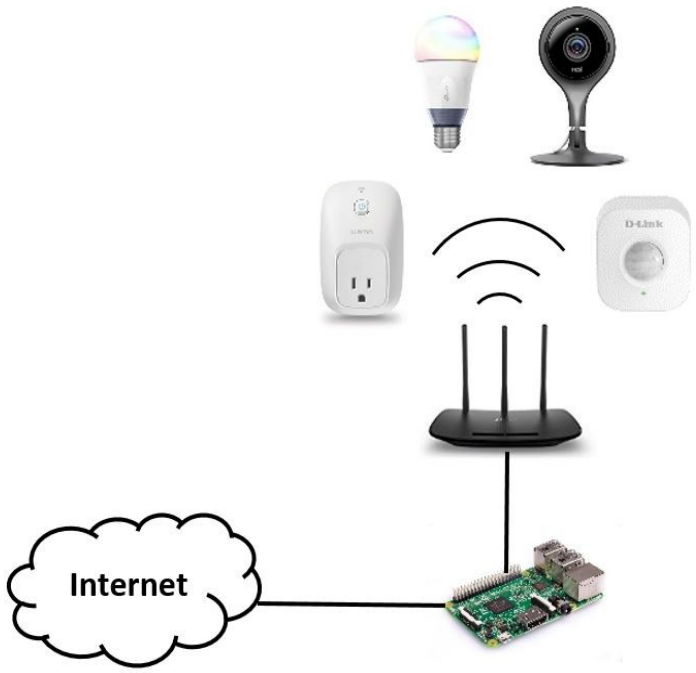
Platform

- Experimental smart home network composed of Nest security camera, D-Link motion sensor, TP-Link smart bulb and smart plug.

- Traffic collected for 7 days

- N = 10, timeout = 600 seconds

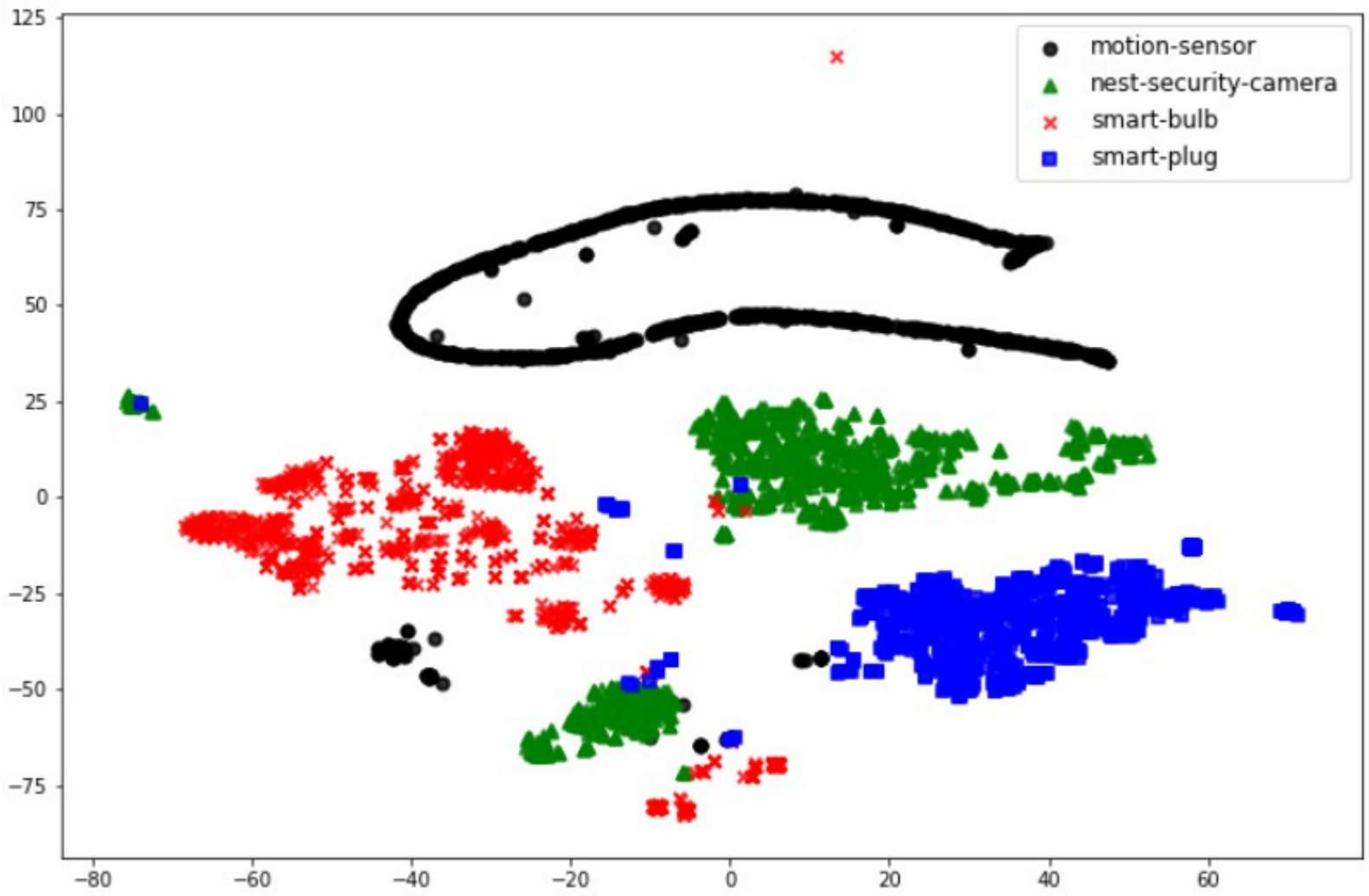
	train	test
Motion sensor	867	207
Security camera	839	216
Smart Bulb	821	219
Smart Plug	695	163
Total	**3222**	**805**



IoT Device Recognition

- Network Traffic Classification on TCP packet headers or flow metadata
- Assumption: 1 profile for each category of IoT device
- Training: 7 days of data, validation set of 25% to fine tune hyperparameters
- Focus on precision: need to accurately classify objects
- Tested algorithms: Random Forest, Decision Tree, SVM, k-Nearest Neighbors, Artificial Neural Network and Gaussian Naïve Bayes.

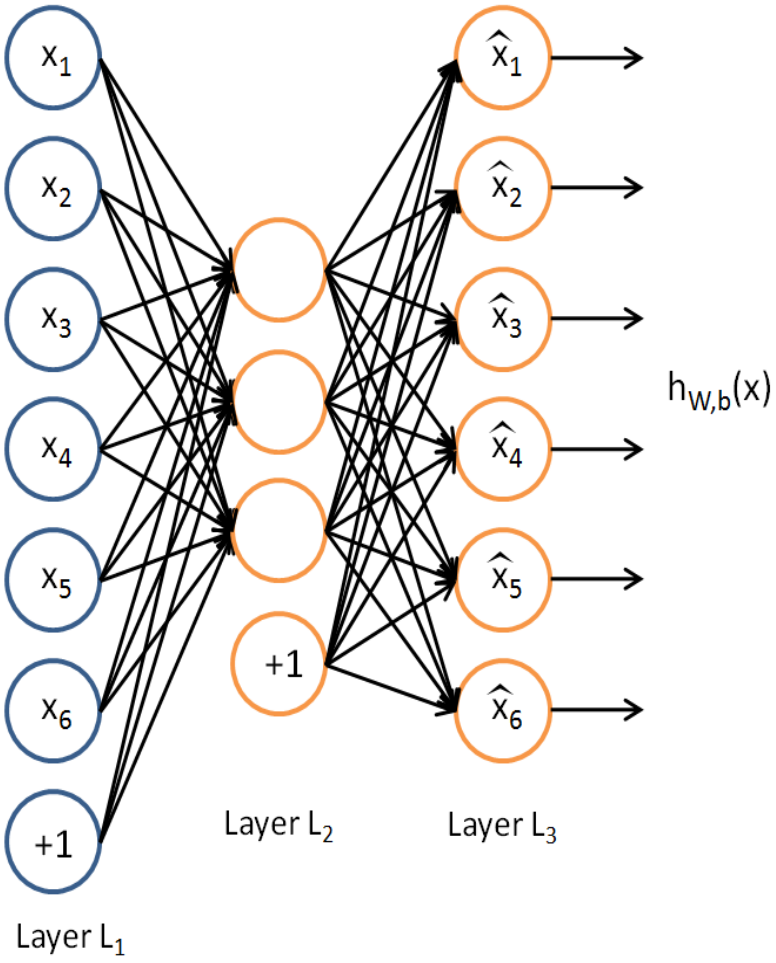
Features Visualization



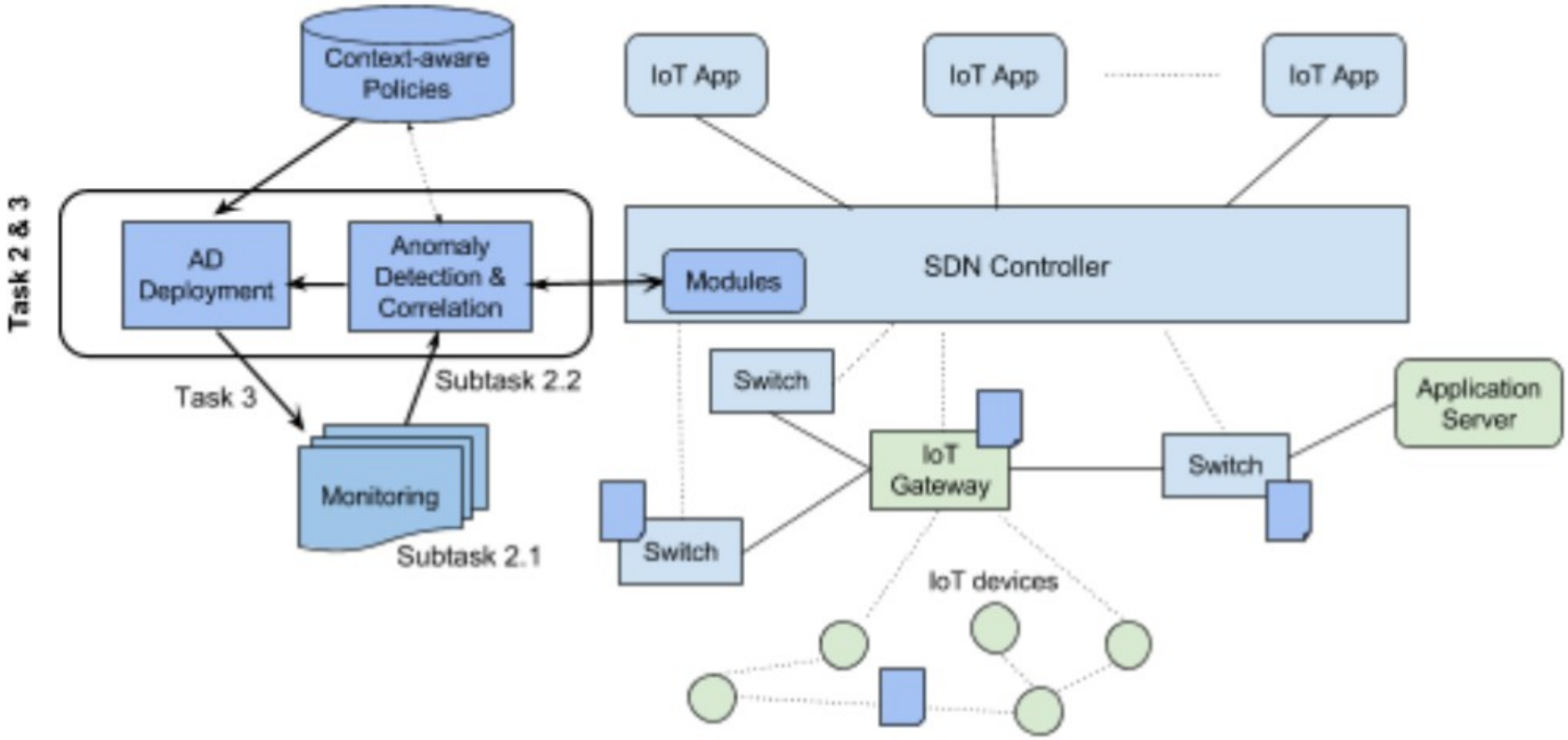
Institut Mines-Télécom

Anomaly Detection

- **Intuition:** create a model that faithfully reproduce normal traffic
- Model attempts to minimize the reconstruction error of the signal
- One anomaly detector per device



Future Work


Context-aware Policies
IoT App
IoT App
IoT App
Task 2 & 3
AD Deployment
Anomaly Detection & Correlation
Modules
SDN Controller
Task 3
Subtask 2.2
Switch
Application Server
IoT Gateway
Switch
Monitoring
Switch
Subtask 2.1
IoT devices