IoTurva: Securing Device-to-Device Communications in IoT Ecosystem

Ibbad Hafeez*, **Aaron Yi Ding**§, **Sasu Tarkoma***

* Department of Computer Science, University of Helsinki, Finland
§ Department of Informatics, Technical University of Munich, Germany

Motivation

- Growth in IoT installations in legacy networks
- Vision of smart home hindered by security issues
- Limited support from existing network hardware for inexpensive in-network monitoring
- Isolated and highly specialized security solutions
- IoT security nightmare turning into a reality
- Signature-based network attack detection mechanisms struggling to keep up with evolving attack models

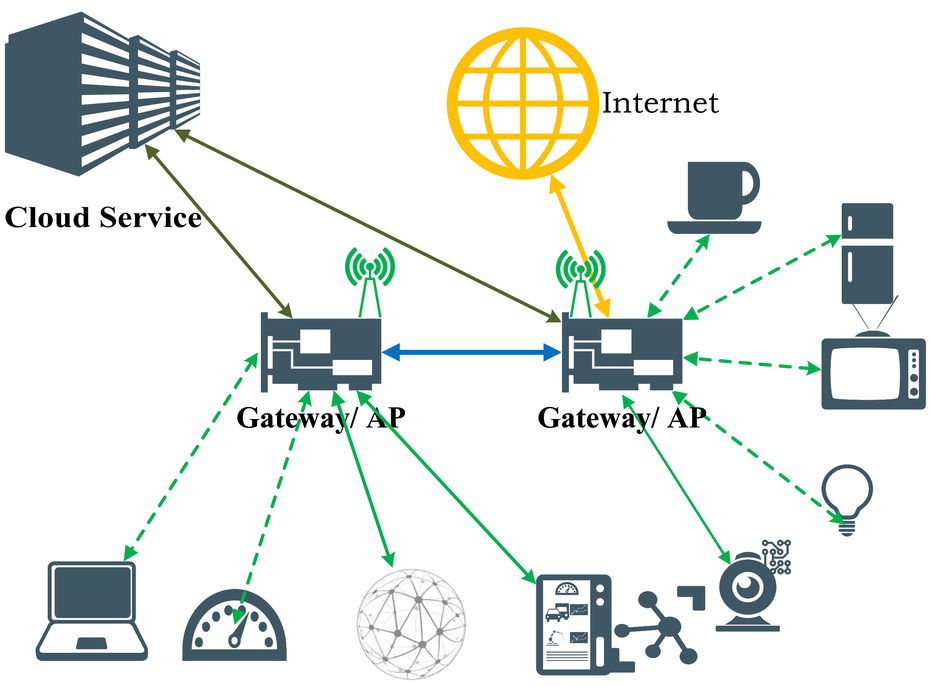
Challenges

- Heterogeneity of IoT ecosystem with variety of devices from various manufacturers
- Complex D2D interactions in IoT ecosystem
- Lack of ground truth for statistics and signature-based network security solutions
- Complex cross-device dependencies and interactions
- Need for automated rule generation and enforcement mechanism
- Classifying unseen device interactions as safe or attack

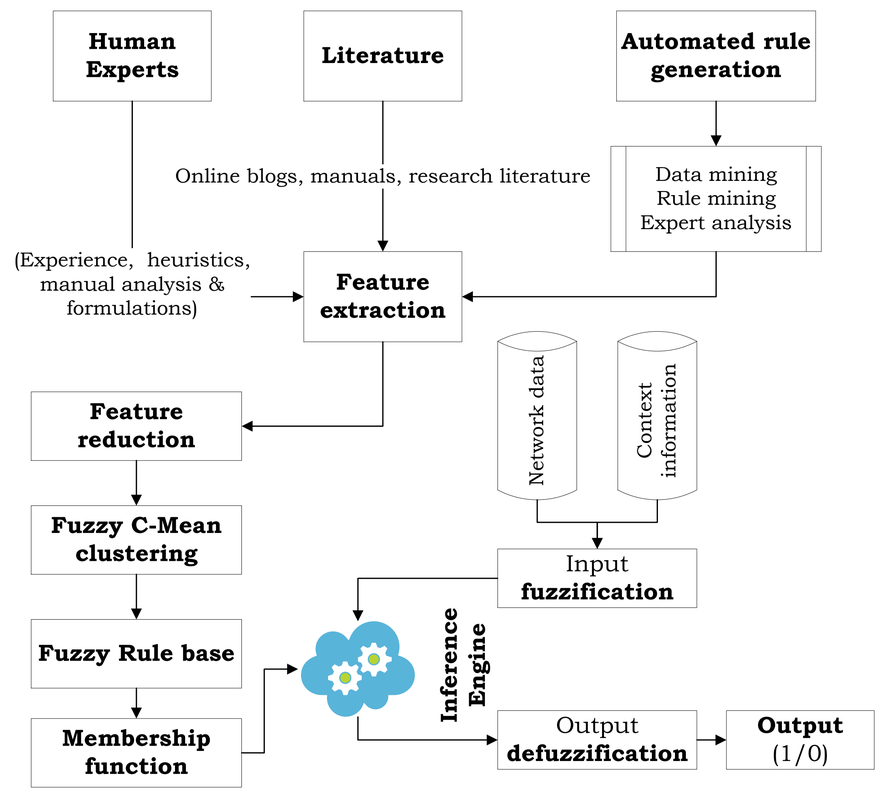
Research Questions

- How to efficiently collect ground truth?
  - Crowdsourcing, CVE, malware databases, Device manuals, testbeds
- What is the right tradeoff for putting intelligence in the edge?
- How to differentiate and handle direct and multilevel D2D interactions?
- What metrics and key aspects should be considered while developing a classifier for unseen D2D interactions based on ground truth available?
- How to incorporate context information in managing D2D communications?

System Design



Fuzzy model



Fuzzy rule generation and classification engine

Prototype Implementation

- Manual data collection for base rule generation
- Context information obtained from user devices
- Python based fuzzy engine for classification
- OF-enabled access point to monitor and control network communications

System Highlights

- Lightweight classification engine deployed at edge
- Cloud service responsible for data collection, updating rule base for classification engine
- Integrating contextual information for improved anomaly detection
- Shifting from signature based anomaly detection solution to handle ever evolving IoT interactions
- Supporting incremental design to support different solutions for performing classification

Future Work

- Improved data collection strategy
- Improve fuzzy classification model, using Q-Learning based techniques
- Evaluating fuzzy based solution against other machine learning models
- Support for agent based installation in legacy APs
- Developing agents deployed at gateway/AP for probing user devices to detect vulnerabilities.

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Technical University of Munich