ICRI-CARS
Secure Systems Group, Aalto University

Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, N. Asokan and Ahmad Sadeghi

DÏoT: A Self-learning System for Detecting Compromised IoT devices

Problem setting

Increase in IoT malware and botnets

- Mirai, Persirai, Reaper, Hajime, etc.

Existing intrusion detection methods are inefficient

- Heterogeneity of IoT devices
- Scarcity of communications
- Resource limitations / etc.

Require a self-learning system for security monitoring of IoT

DÏoT system overview

Self-learning device-type identification

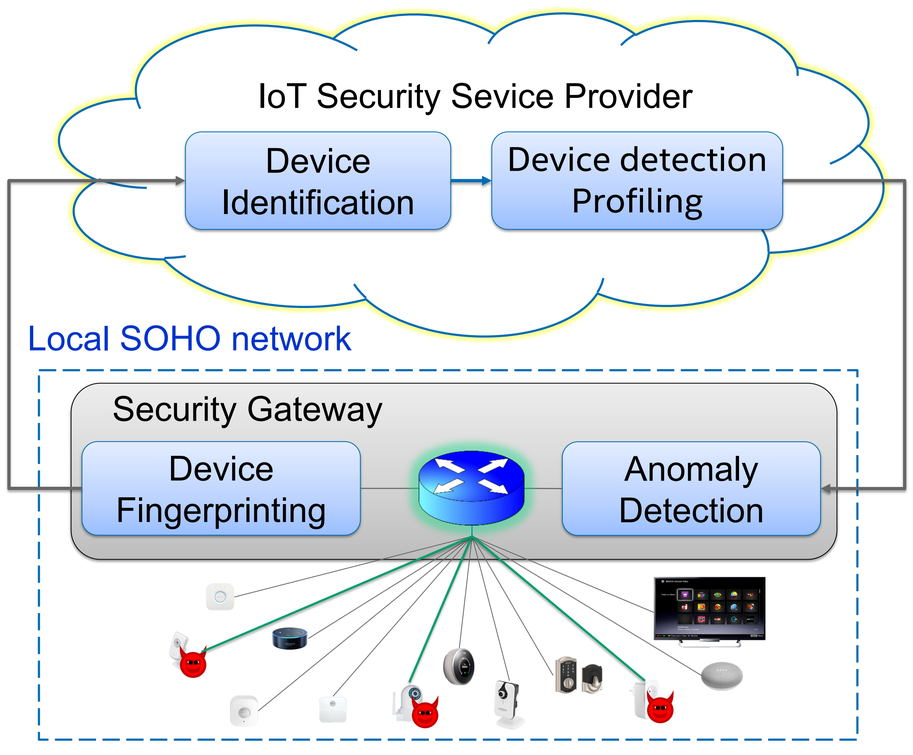
- Passive fingerprinting of periodic traffic
- Abstract device types: *type#12*

Self-learning anomaly detection system

- Gated recurrent unit (GRU) to model communications as a language
- Device-type-specific anomaly detection model
- Federated learning of AD models

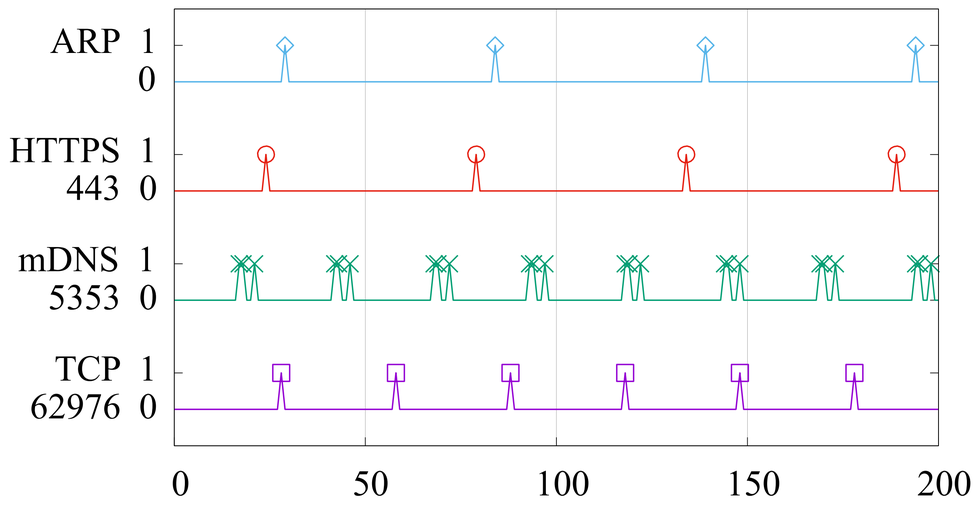
Distributed and collaborative system

- One IoT security service provider
- Several security gateways



Periodicity of communications

- Binarization of communication flows
- Fourier transform + signal autocorrelation



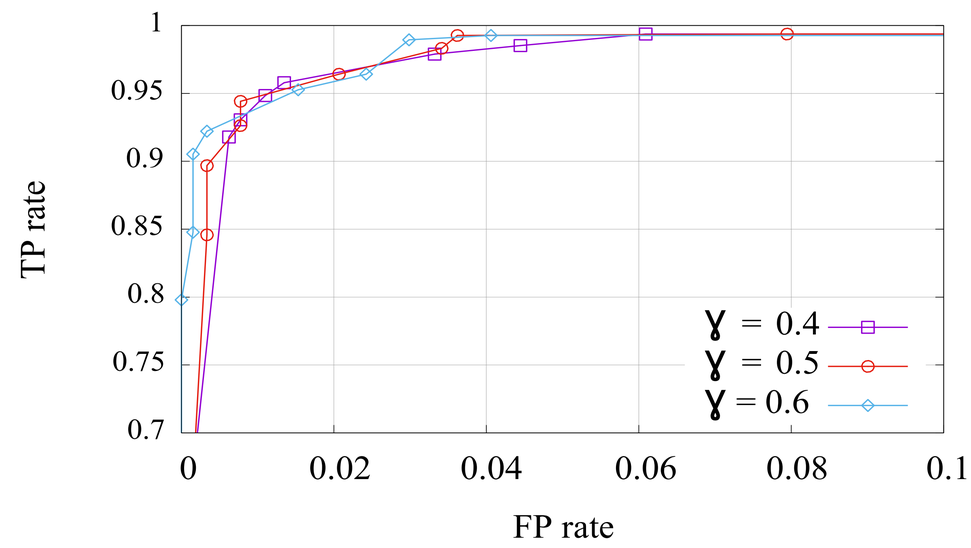
Evaluation (> 30 IoT devices)

Device-type identification

- 98% accuracy
- 30 minutes to identify a device's type

Anomaly detection

- Detects 94% of attacks from Mirai botnet
- Average detection time of 2 seconds
- No false positives (real-world deployment)



Attack	Packets/s.	Detection time (s.)	Detection rate
scan	292.2	0.4	100.0%
udp	84.4	1.7	100.0%
syn	752.6	0.2	100.0%
ack	123.8	1.1	94.6%
udpplain	1755.8	0.1	82.2%
vse	331.1	0.5	63.3%
dns	1292.6	0.1	100.0%
greip	167.8	0.7	100.0%
greeth	53.4	2.3	100.0%
http	10.9	15.4	100.0%
Average	**442.3**	**2.3**	**94.0%**

Aalto University
Research Institute for Collaborative Autonomous and Resilient Systems
TECHNISCHE UNIVERSITÄT DARMSTADT