ACSAC 2022

Stepping out of the MUD: contextual threat information for IoT devices with manufacturer-provided behavior profiles

Luca Morgese Zangrandi	TNO
Thijs van Ede	University of Twente
Tim Booij	TNO
Savio Sciancalepore	Technical University of Eindhoven
Luca Allodi	Technical University of Eindhoven
Andrea Continella	University of Twente

Motivation

Motivation

- Attackers actively compromise IoT devices

Motivation

- Attackers actively compromise IoT devices
- >50% devices deployed in home-like environments

Motivation

- Attackers actively compromise IoT devices
- >50% devices deployed in home-like environments
- No honeypots, monitors, intelligence

Motivation

- Attackers actively compromise **IoT devices**
- >50% devices deployed in **home-like environments**
- No honeypots, monitors, intelligence

→ Hard to gather threat information

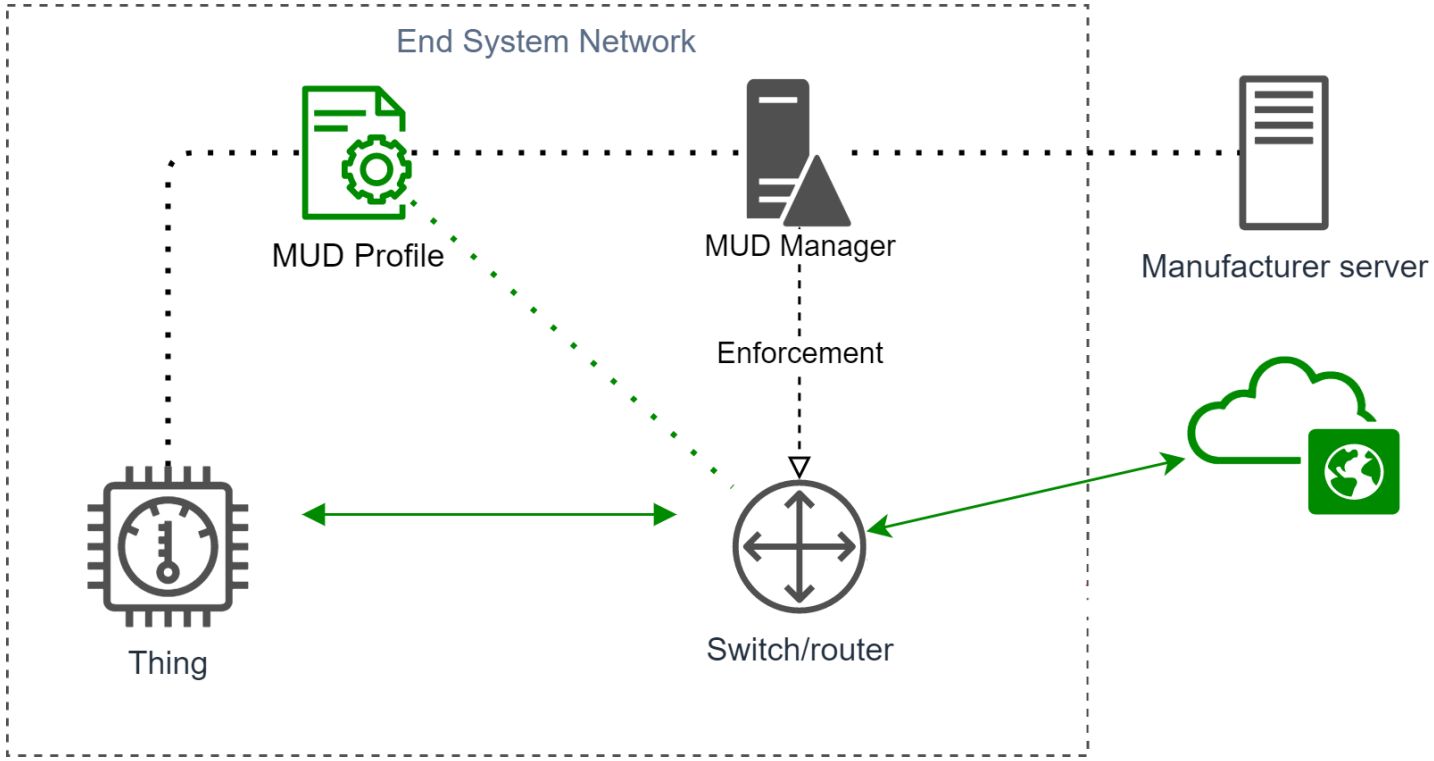
Goal

MUDscope

→ Monitor for IoT threat activities at home-like environments

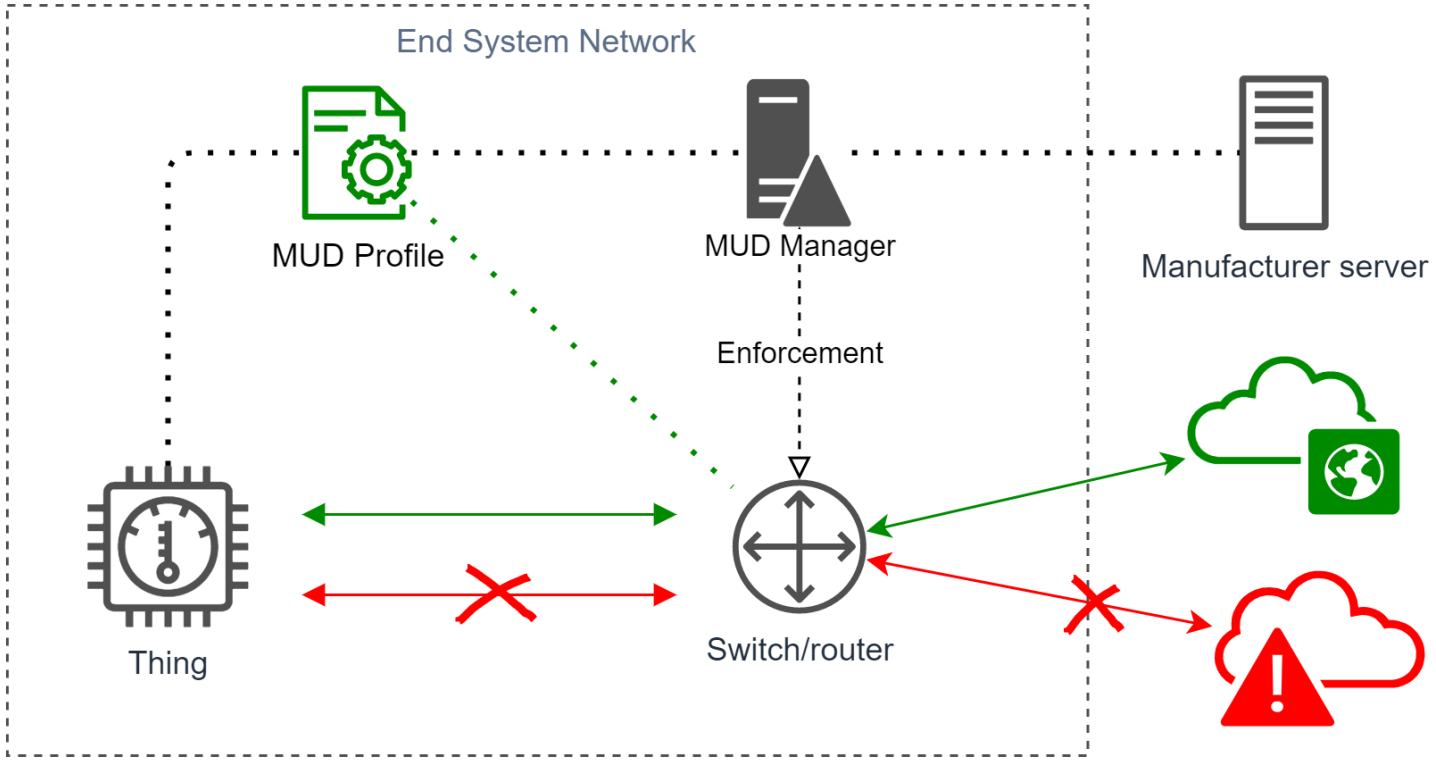
MUD profiles

- **Manufacturer-provided allow-lists**
- Manufacturer Usage Description (IETF RFC 8520)

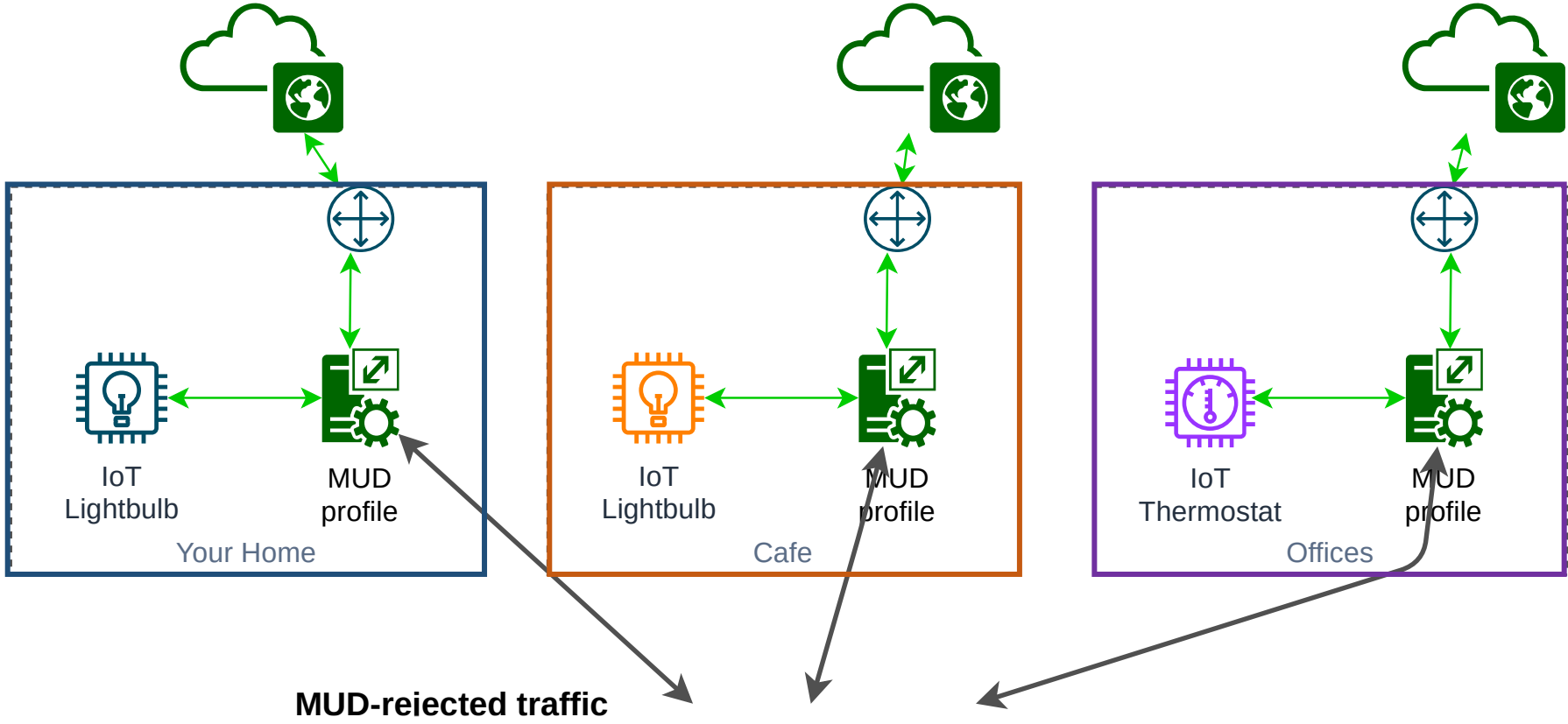


MUD profiles

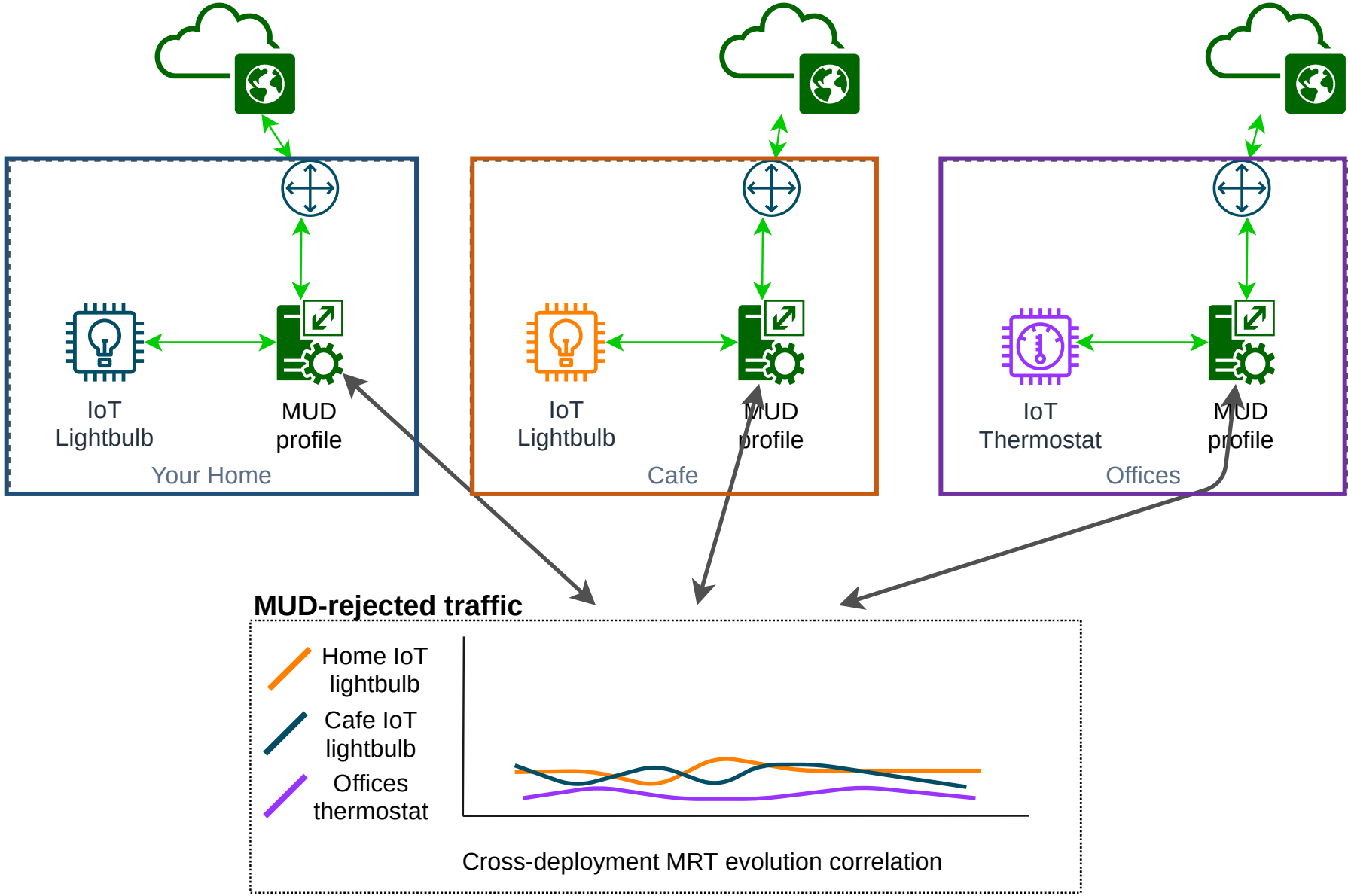
- **Manufacturer-provided allow-lists**
- Manufacturer Usage Description (IETF RFC 8520)



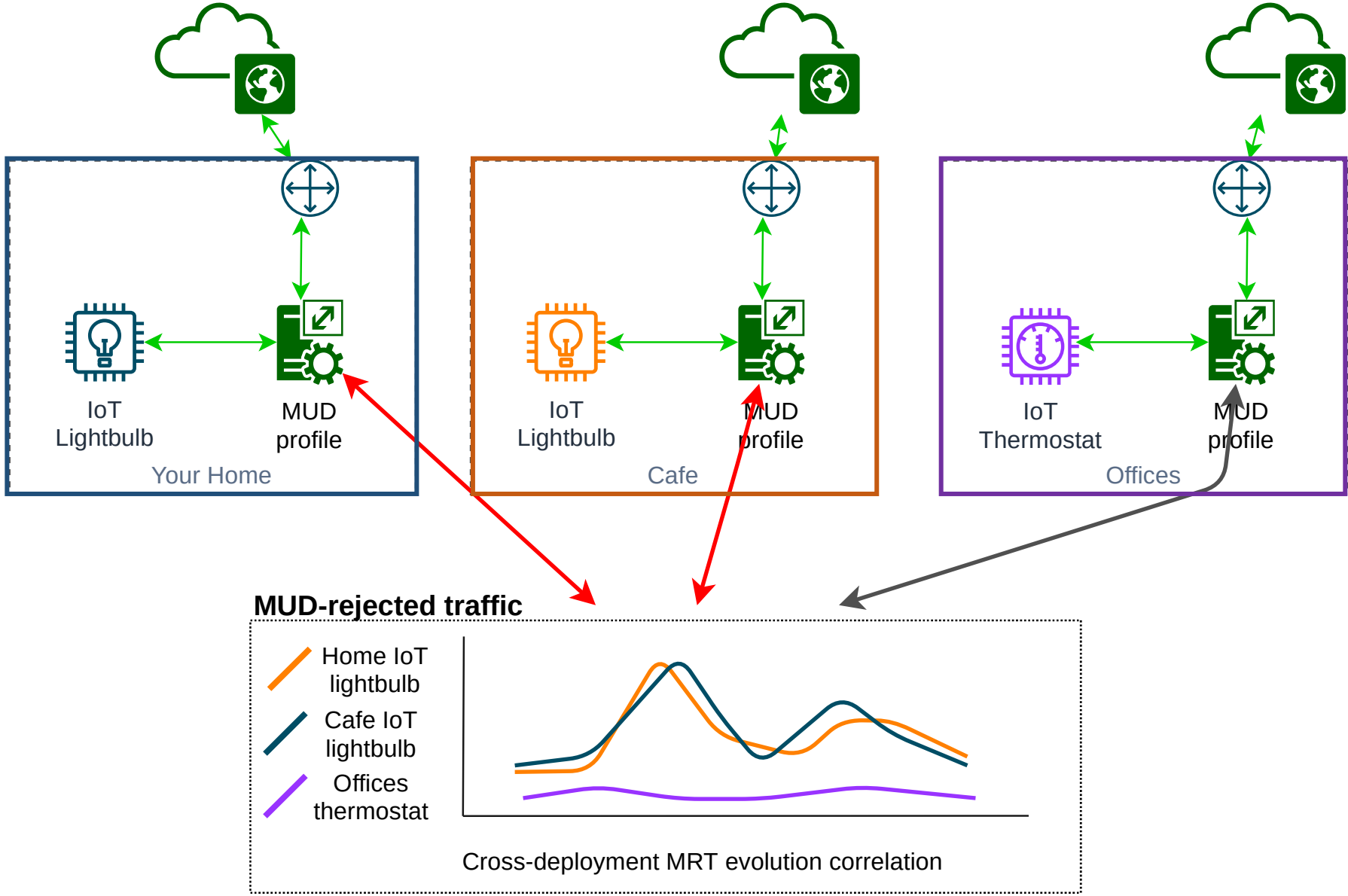
Key idea


IoT
Lightbulb
MUD
profile
Your Home
IoT
Lightbulb
MUD
profile
Cafe
IoT
Thermostat
MUD
profile
Offices
MUD-reiected traffic

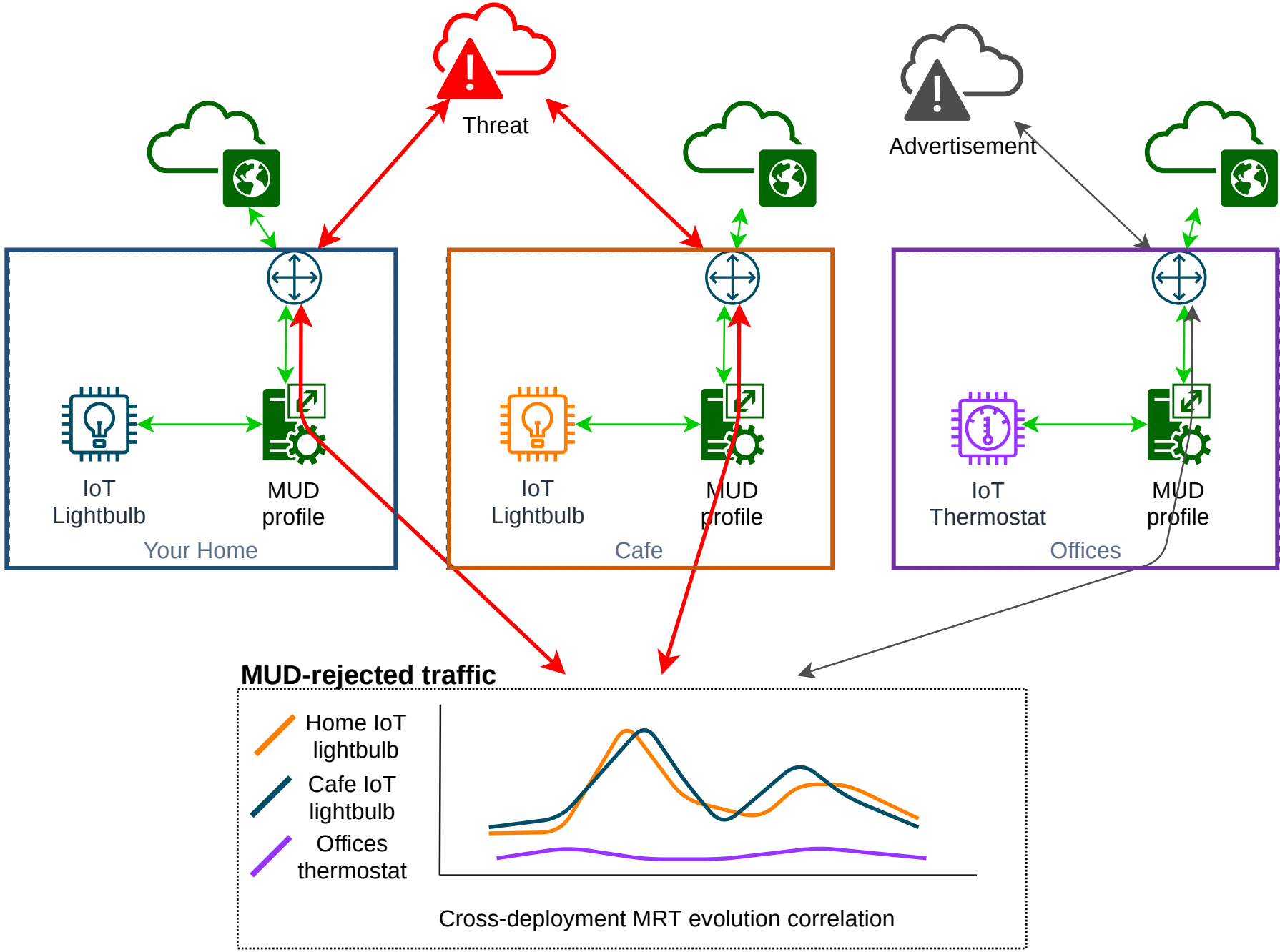
Key idea


IoT
Lightbulb
MUD
profile
Your Home
IoT
Lightbulb
MUD
profile
Cafe
IoT
Thermostat
MUD
profile
Offices
MUD-rejected traffic
Home IoT
lightbulb
Cafe IoT
lightbulb
Offices
thermostat
Cross-deployment MRT evolution correlation

Key idea


IoT
Lightbulb
MUD
profile
Your Home
IoT
Lightbulb
MUD
profile
Cafe
IoT
Thermostat
MUD
profile
Offices
MUD-rejected traffic
Home IoT
lightbulb
Cafe IoT
lightbulb
Offices
thermostat
Cross-deployment MRT evolution correlation

Key idea


Threat
Advertisement
IoT
Lightbulb
MUD
profile
Your Home
IoT
Lightbulb
MUD
profile
Cafe
IoT
Thermostat
MUD
profile
Offices
MUD-rejected traffic
Home IoT
lightbulb
Cafe IoT
lightbulb
Offices
thermostat
Cross-deployment MRT evolution correlation

Approach

Approach

0. MUD enforced (we used MUDgee)

1. Collect MUD-rejected traffic (MRT)

Device A

Approach

0. MUD enforced (we used MUDgee)

1. Collect MUD-rejected traffic (MRT)
2. Describe MRT

Device A

Approach

1. Collect MUD-rejected traffic (MRT)
2. Describe MRT

Device A

Device B

Device C

Approach

1. Collect MUD-rejected traffic (MRT)
2. Describe MRT

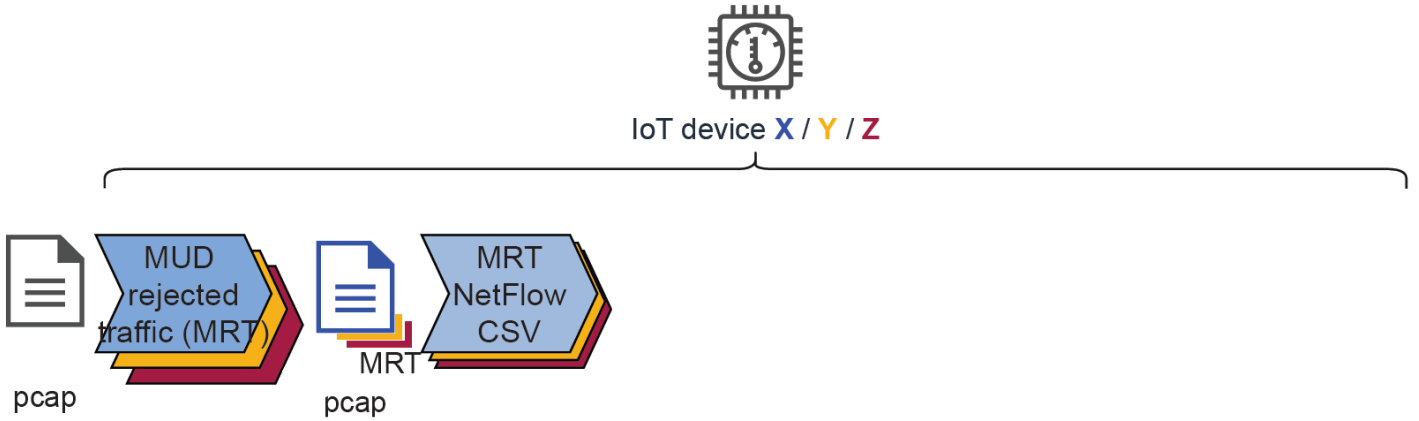
Device A

Device B

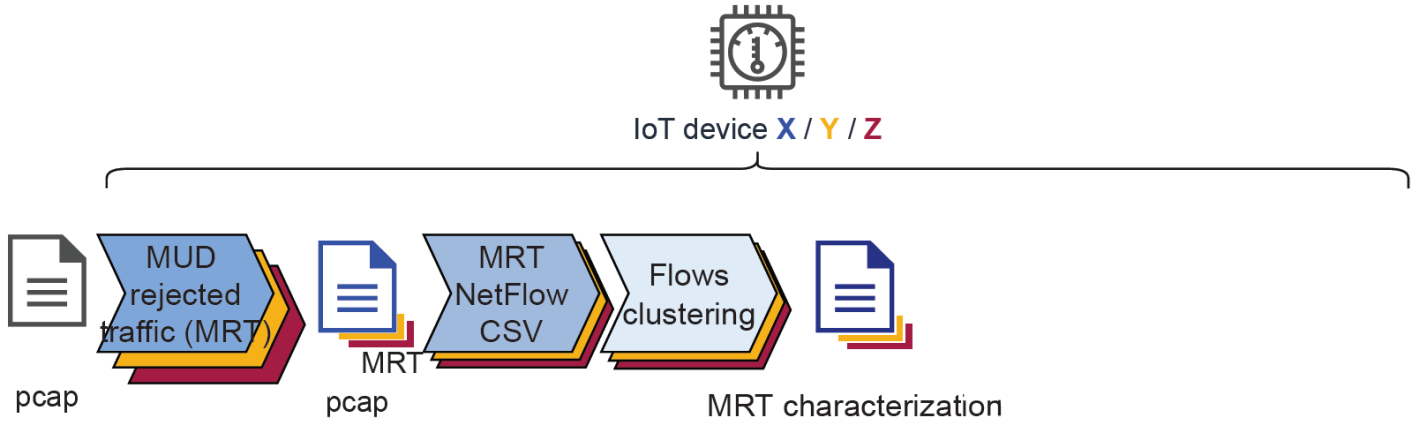
Device C

3. Compare MRT from many devices

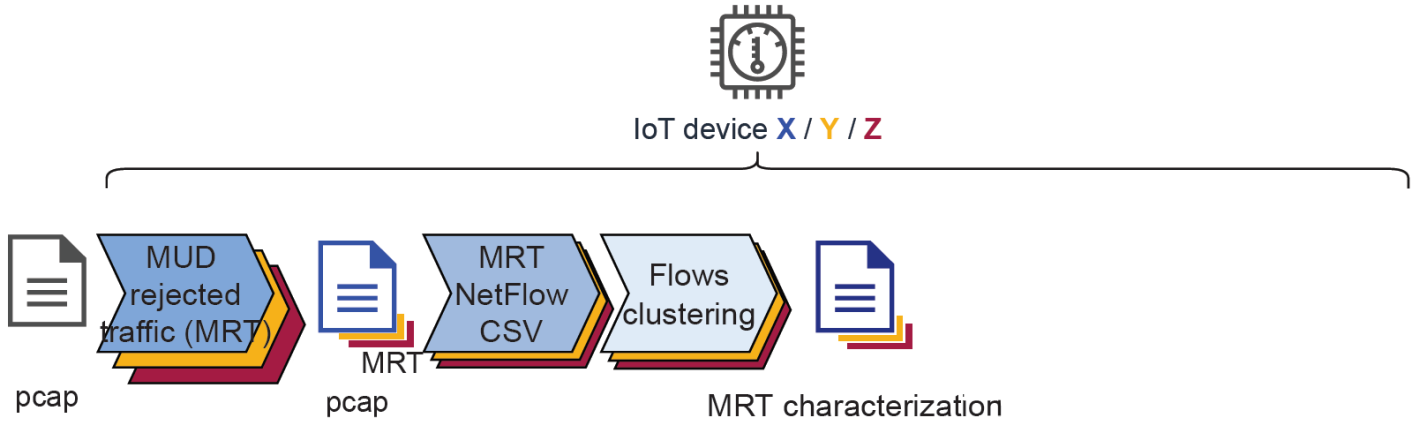
Approach – 1. Collect MRT

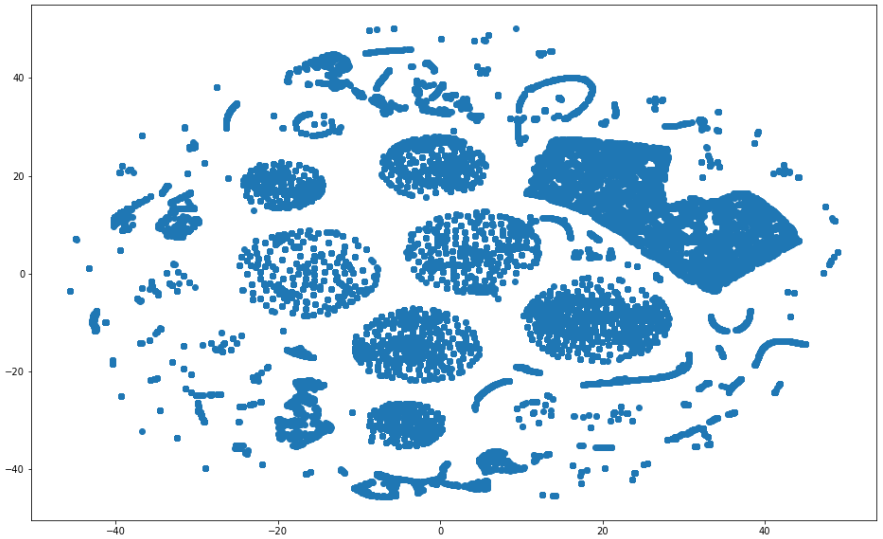


Approach – 2. Describe MRT

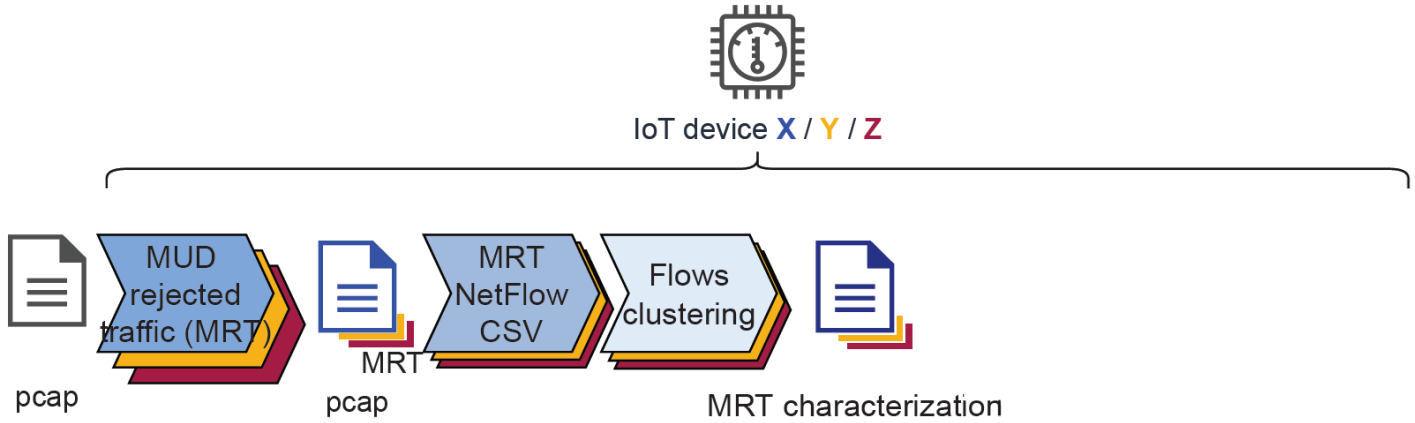


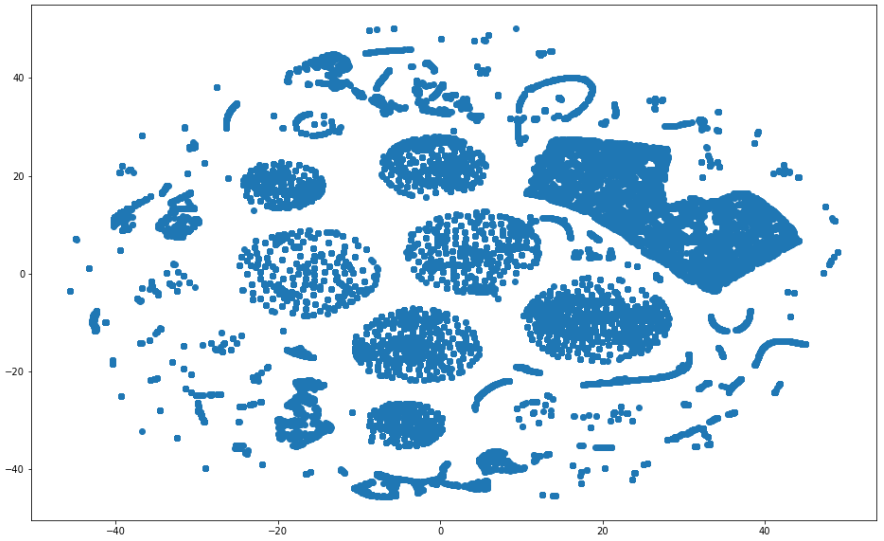
Approach – 2. Describe MRT

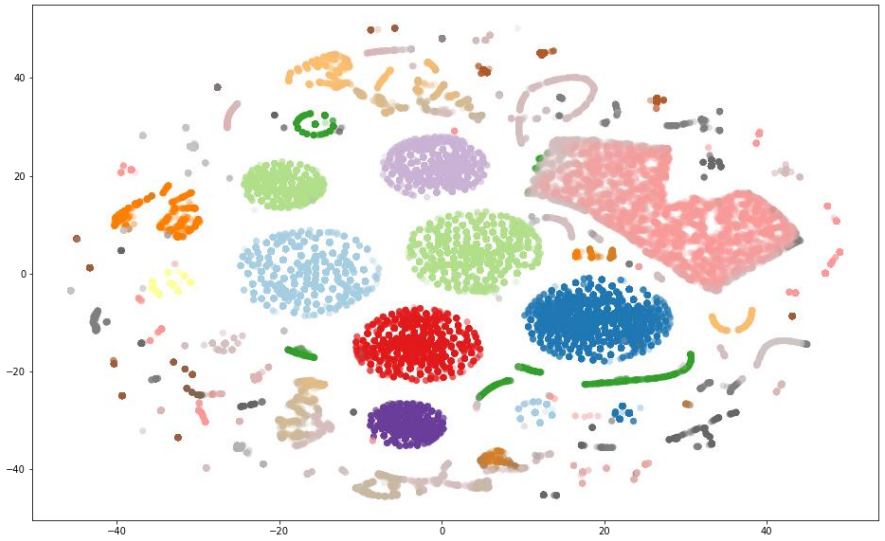




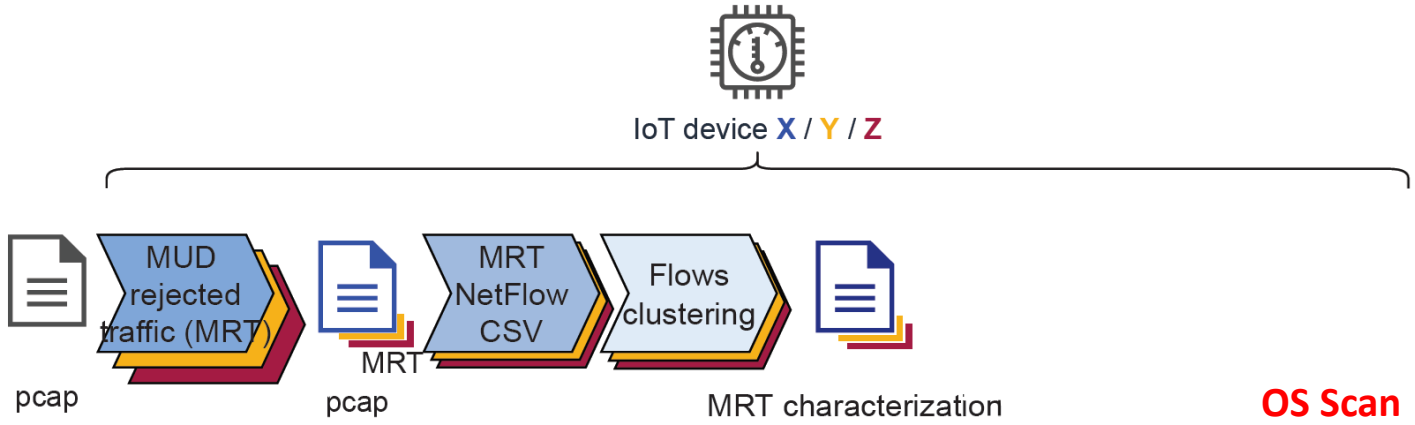
Approach – 2. Describe MRT

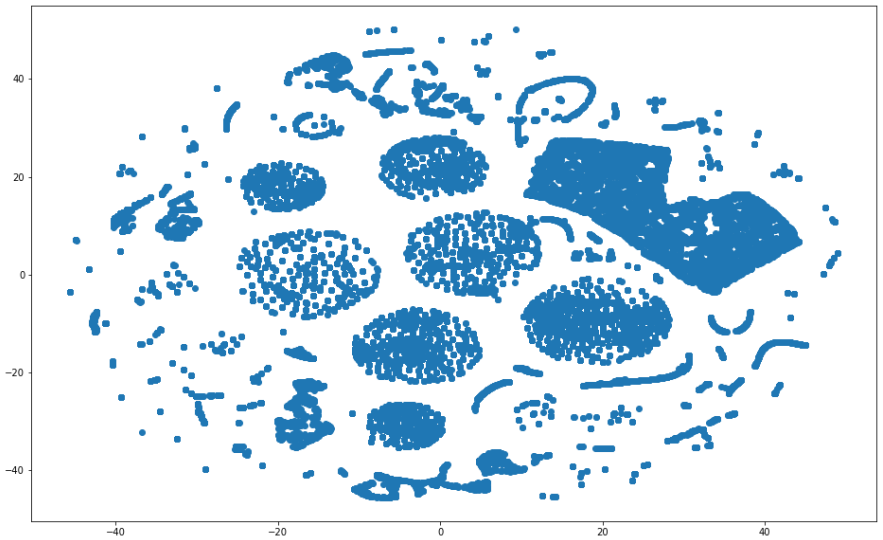


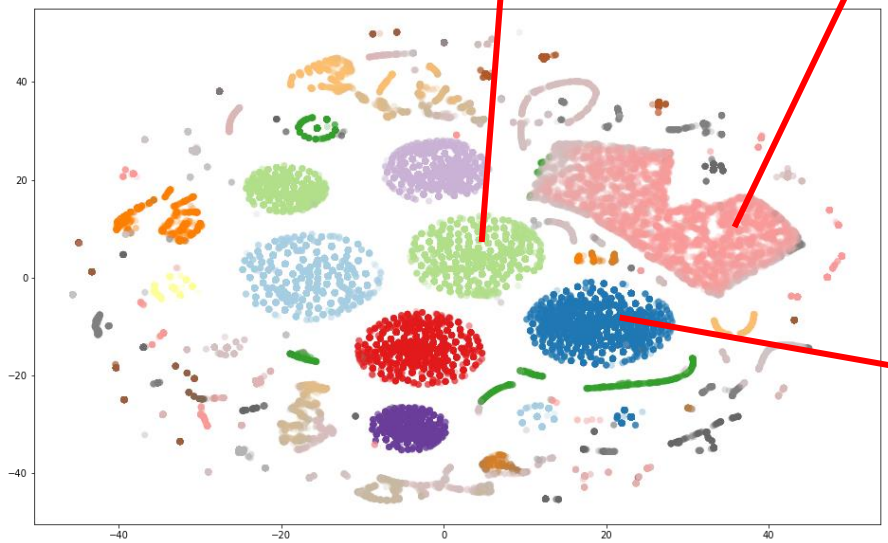




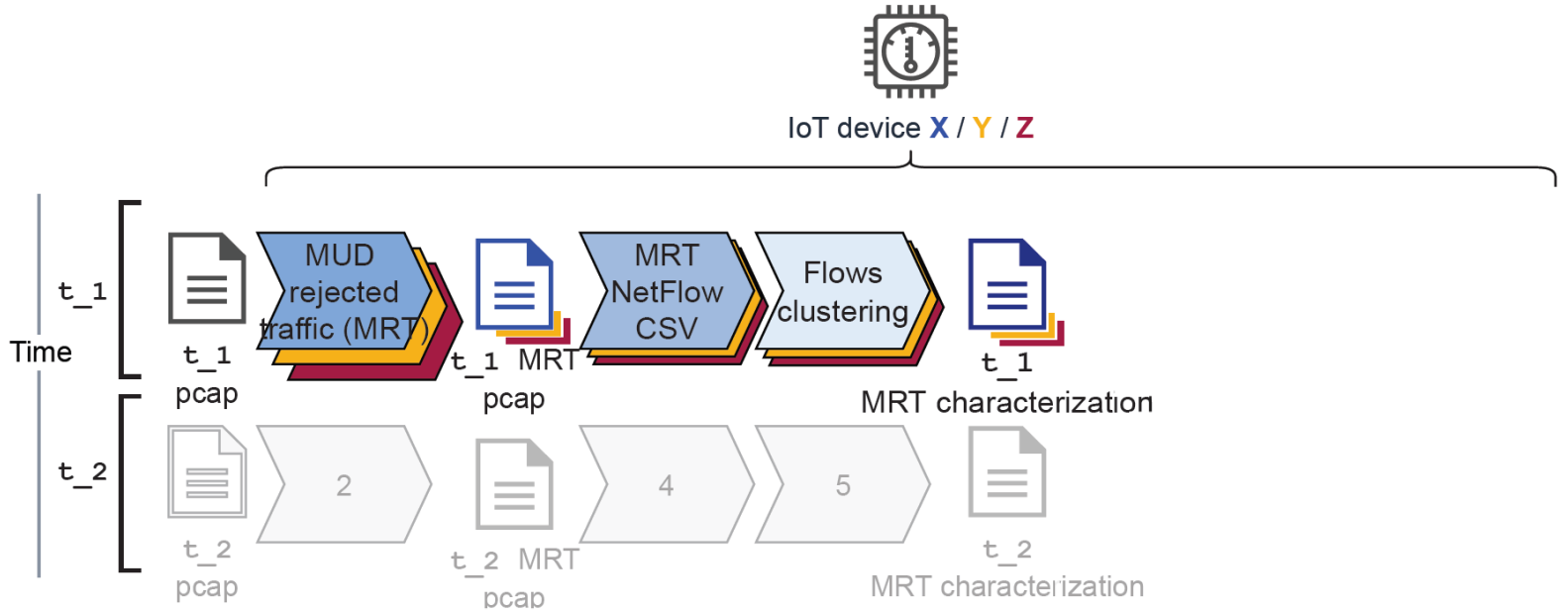
Approach – 2. Describe MRT



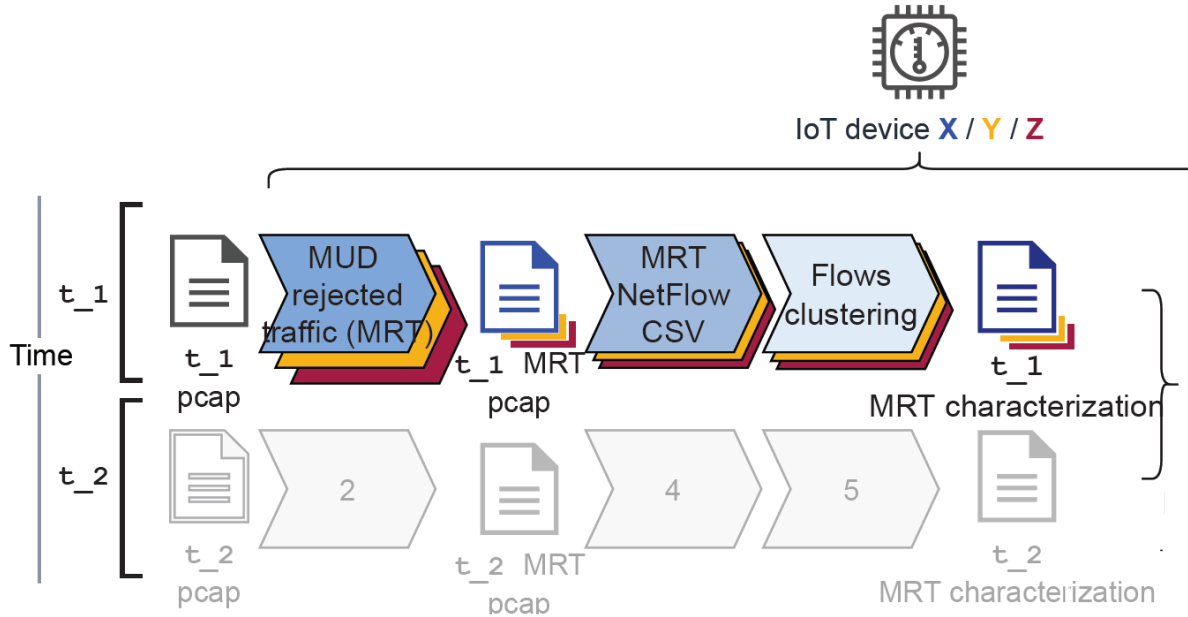


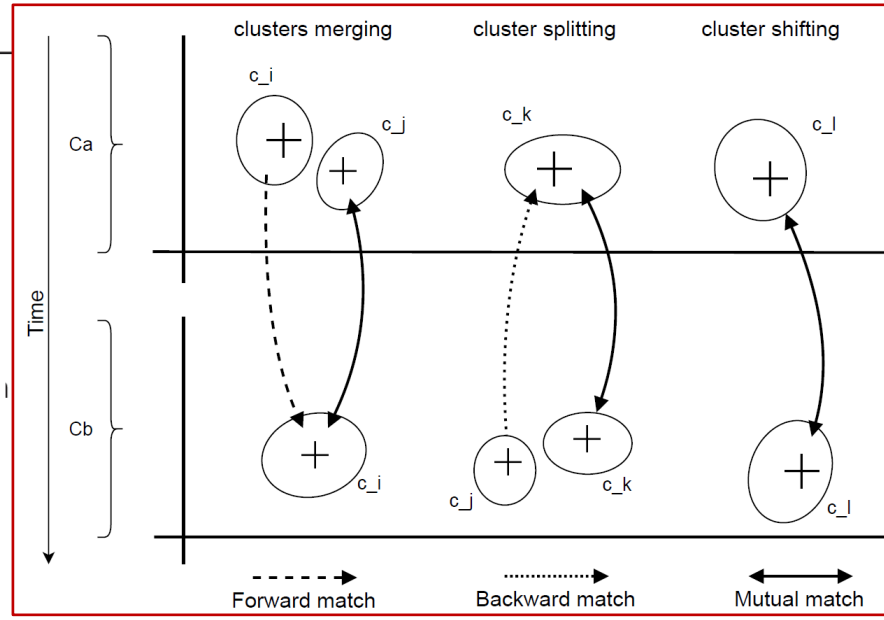


Approach – 2. Describe MRT

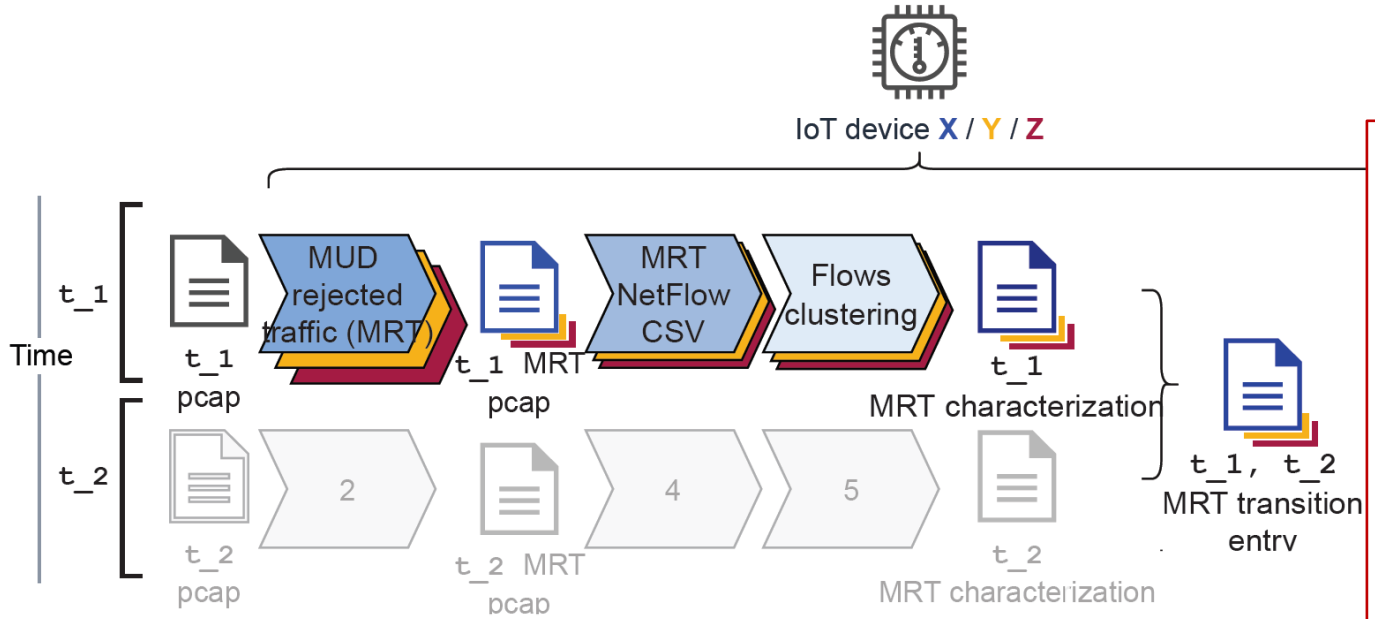


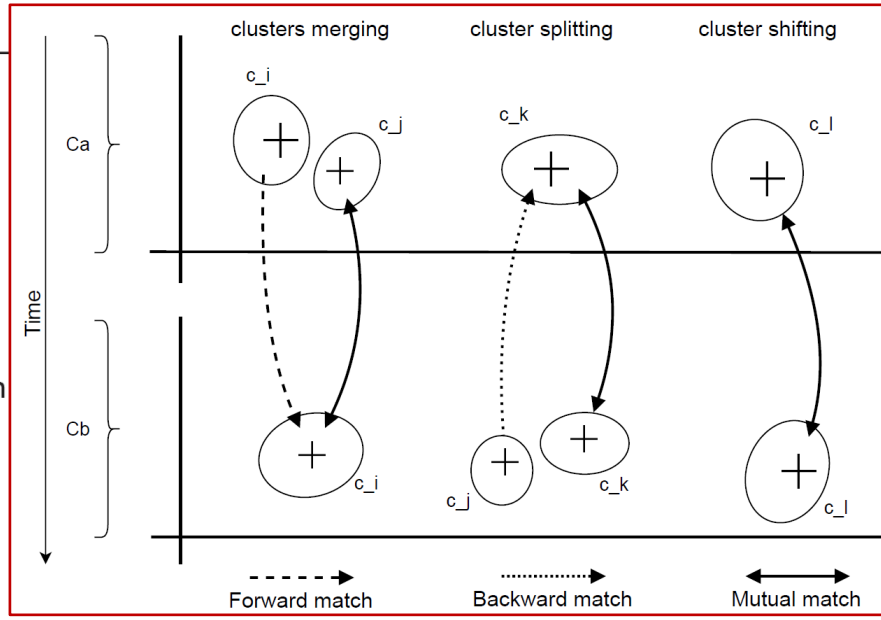
Approach – 2. Describe MRT





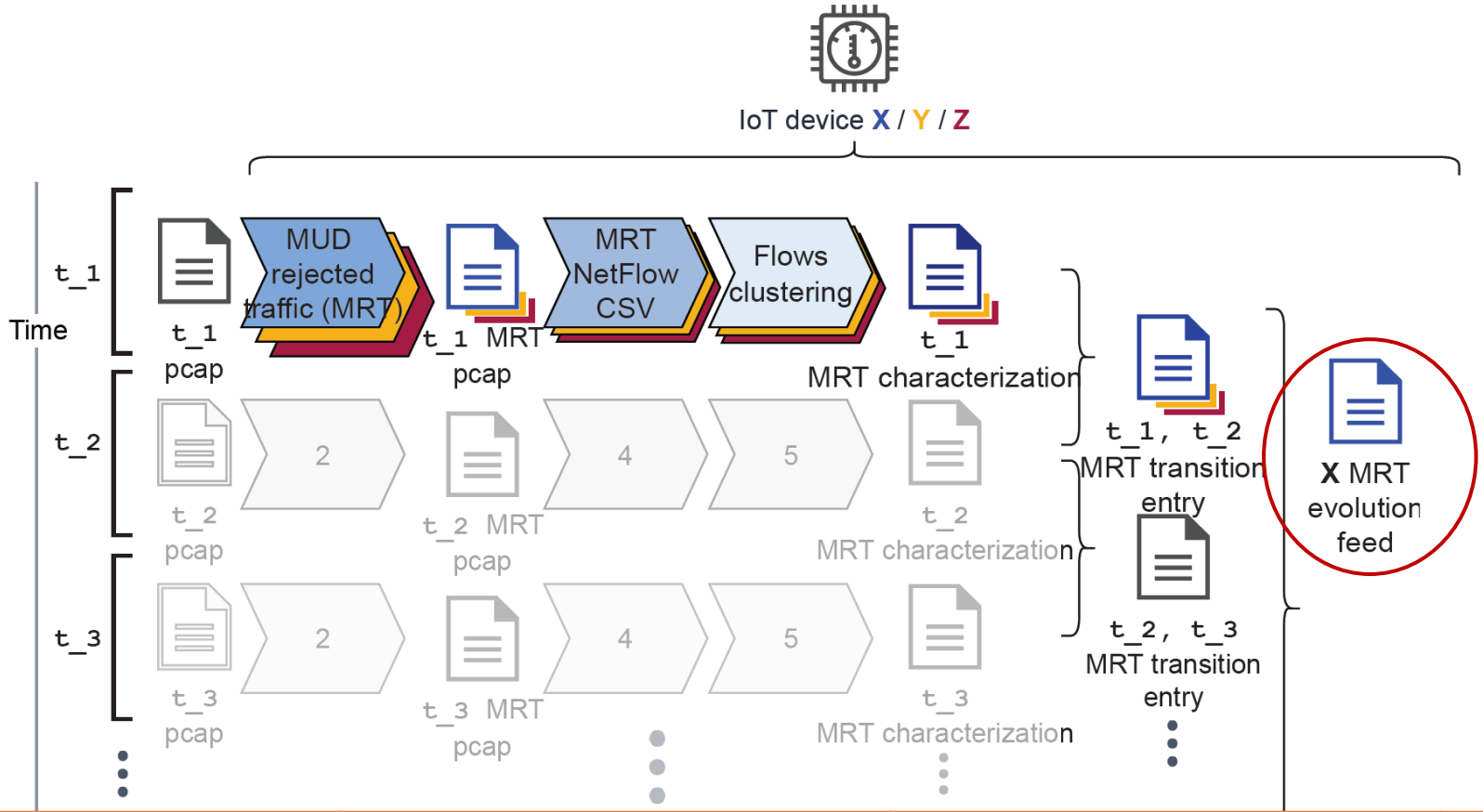
Approach – 2. Describe MRT





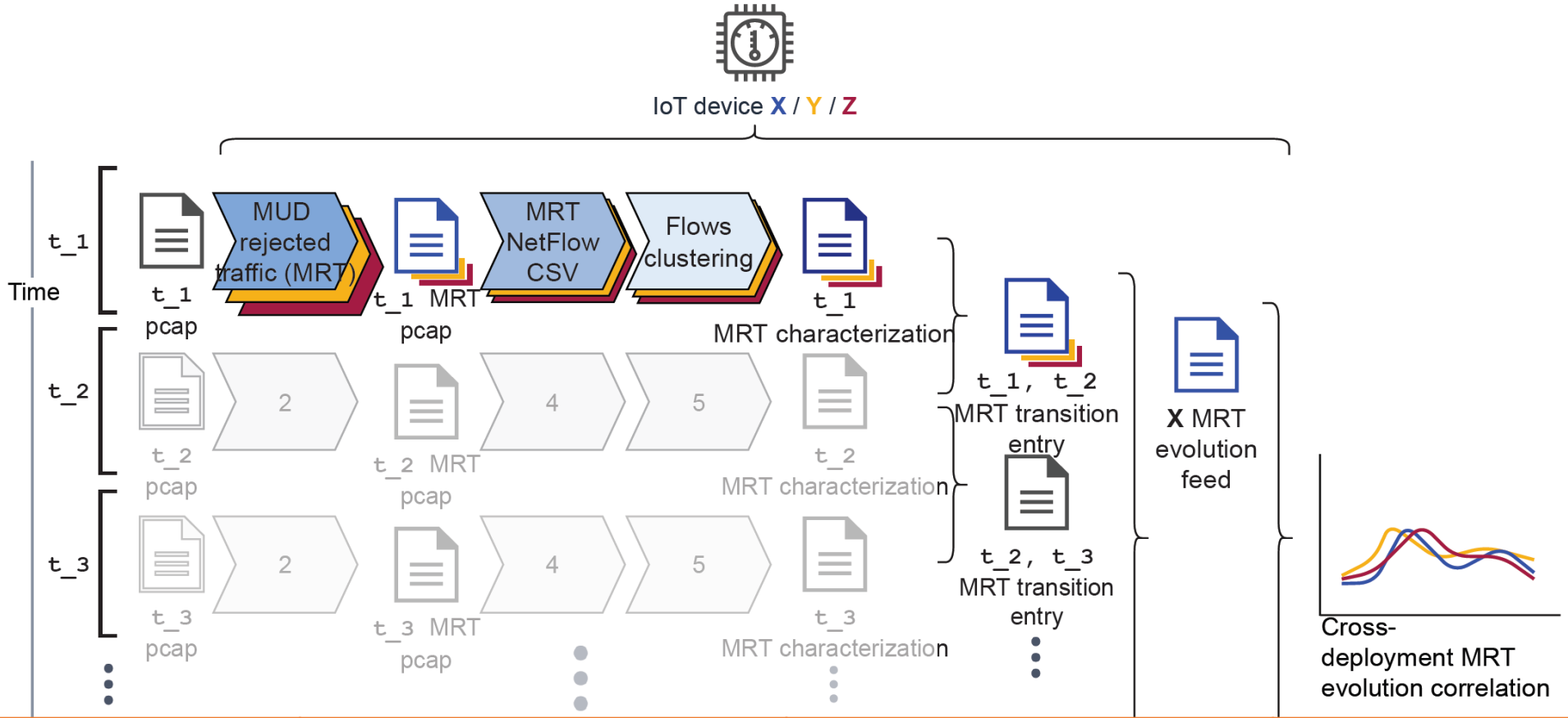
Clusters balance	clusters distances	Mutual/forward/backward matches	forward/backward agglomeration

Approach – 2. Describe MRT



Clusters balance	clusters distances	Mutual/forward/backward matches	forward/backward agglomeration
…	…	…	…
…	…	…	…

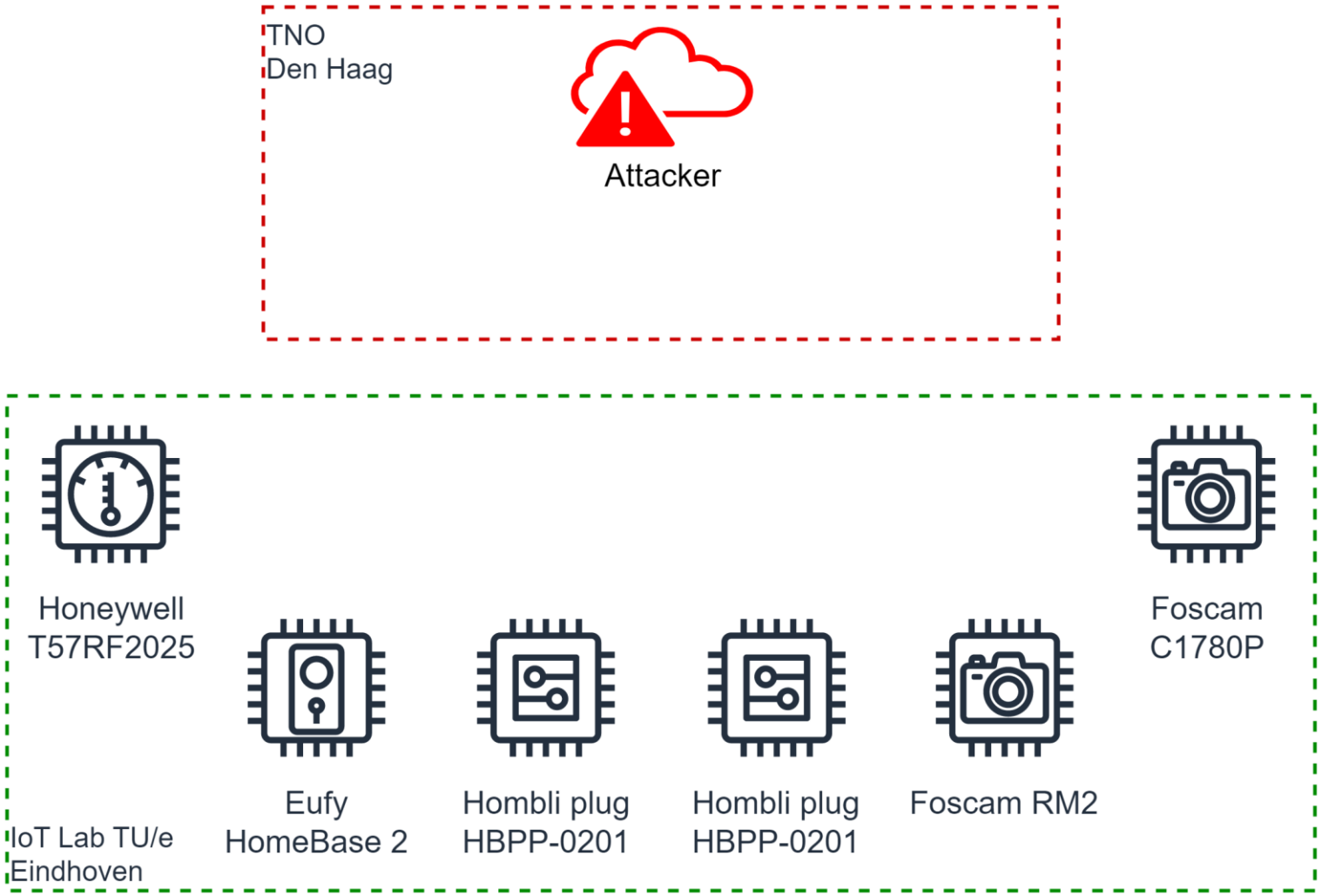
Approach – 3. Compare MRT



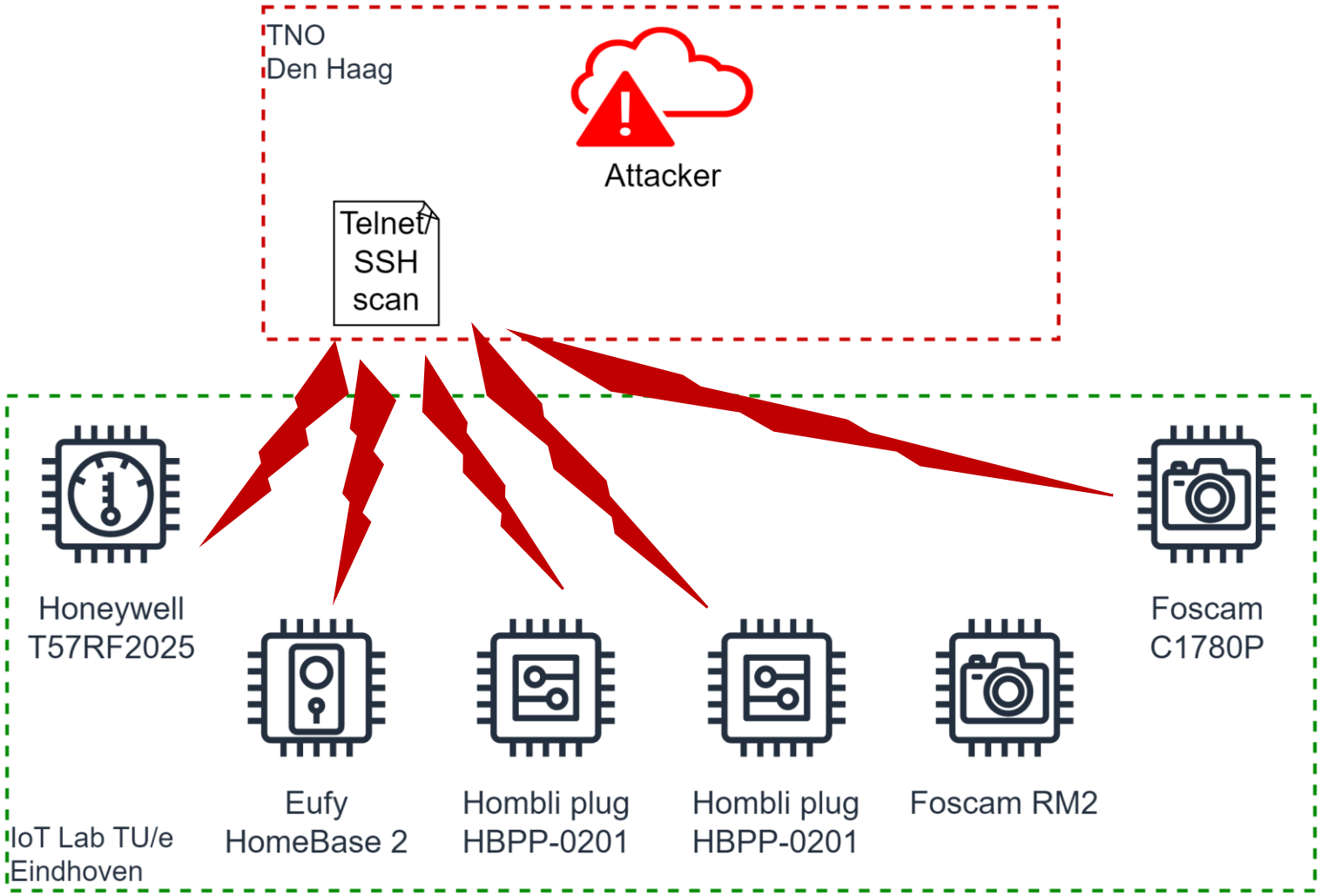
Clusters balance	clusters distances	Mutual/forward/backward matches	forward/backward agglomeration
…	…	…	…
…	…	…	…

Experiments

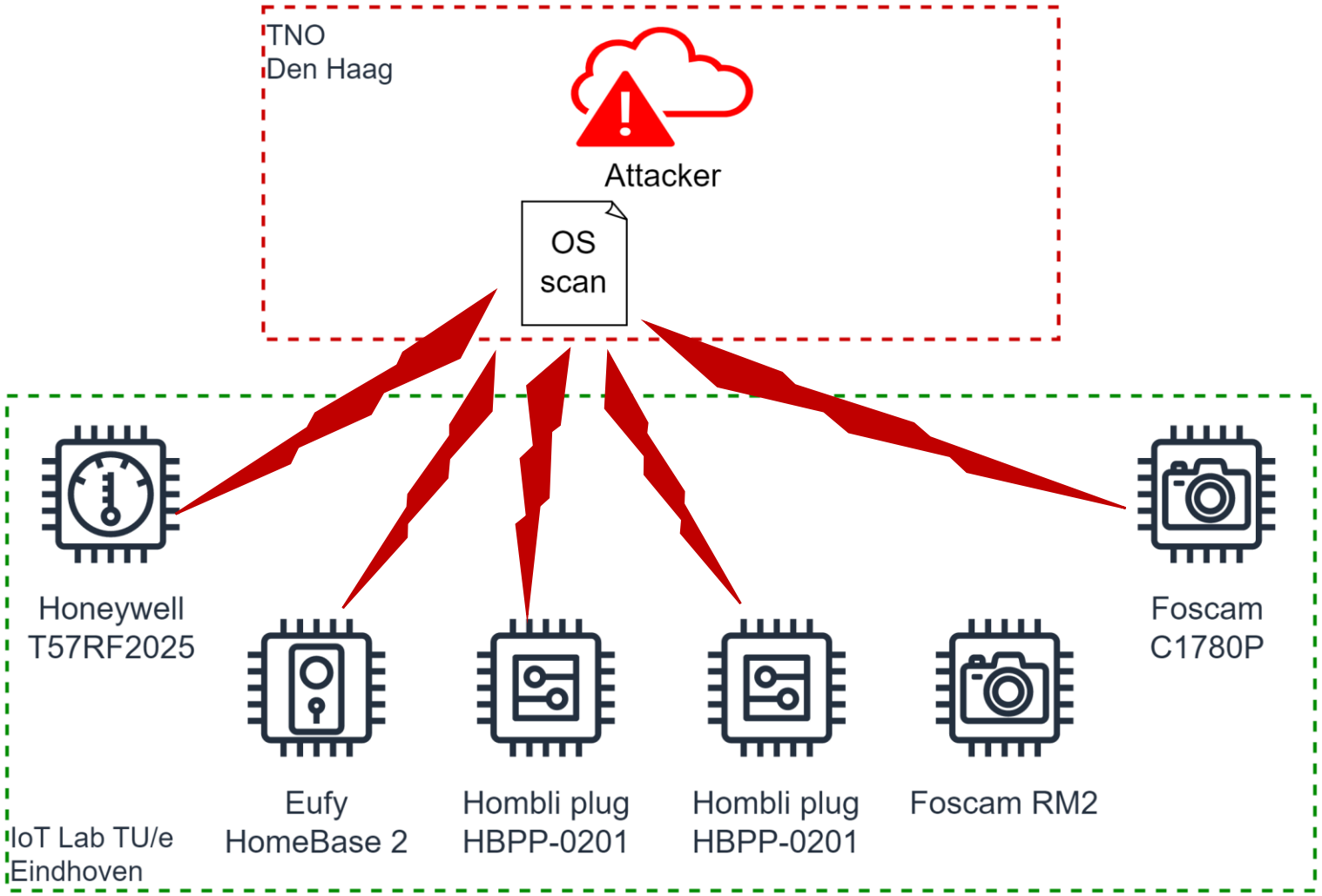
Experiments – same attacks



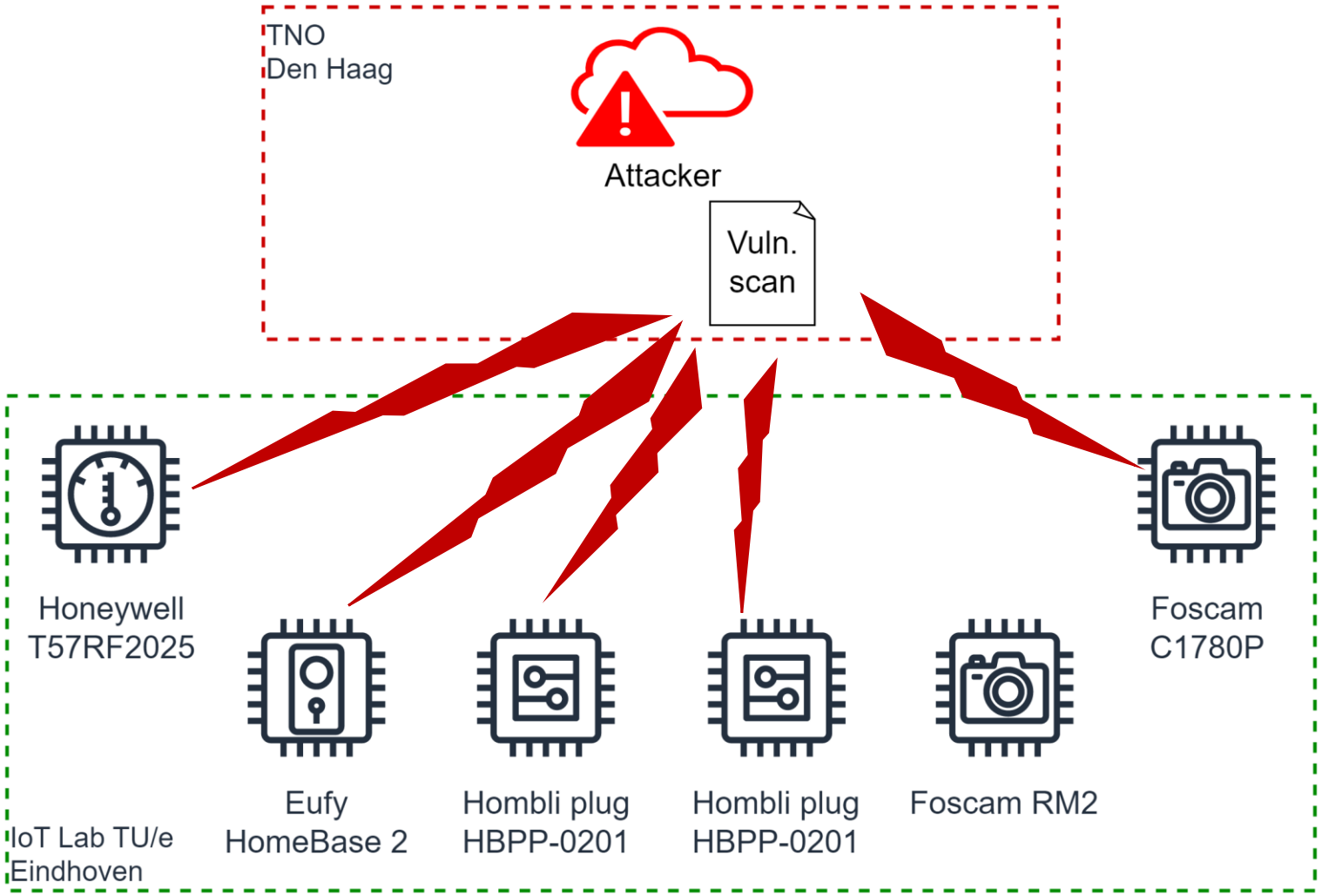
Experiments – same attacks



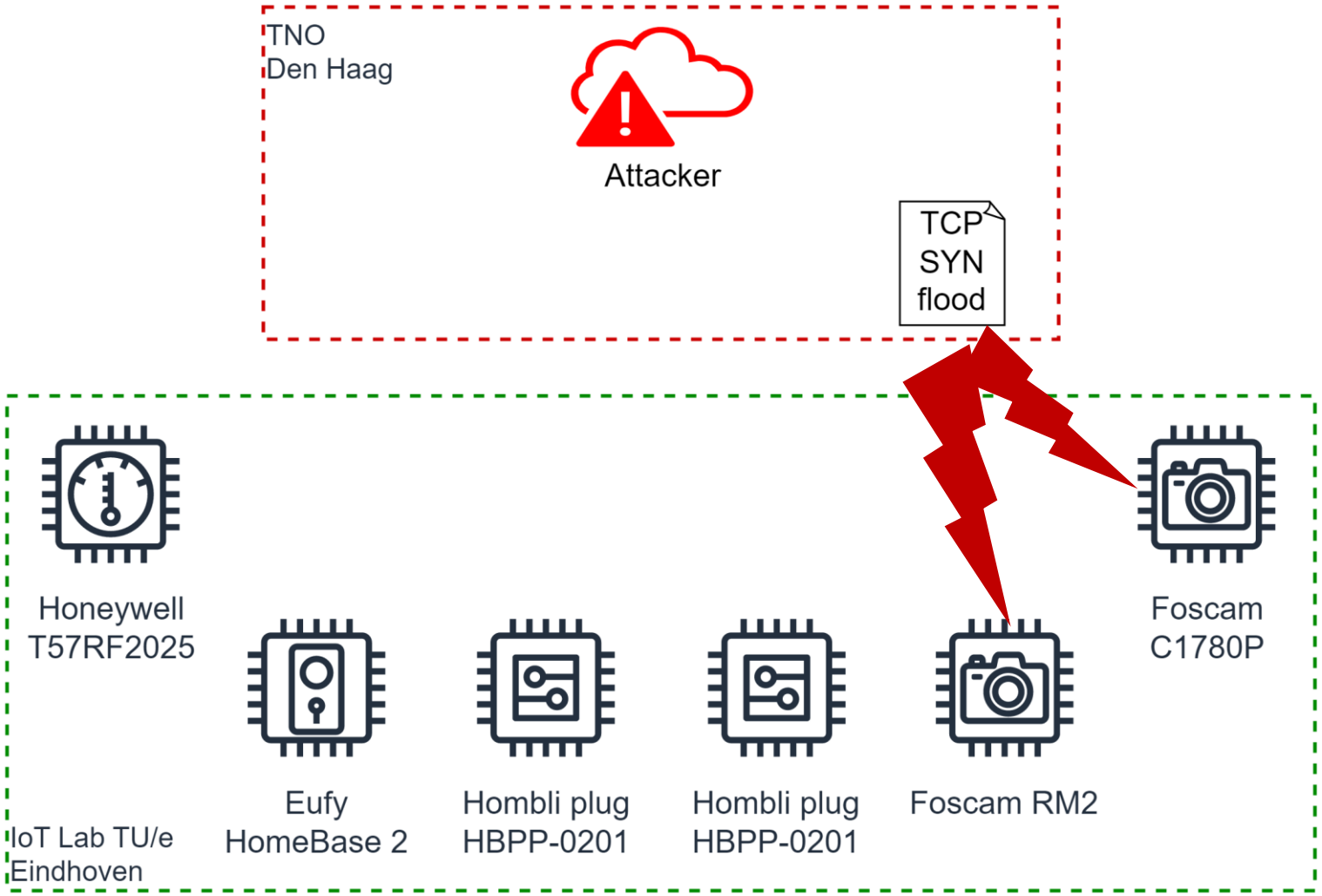
Experiments – same attacks



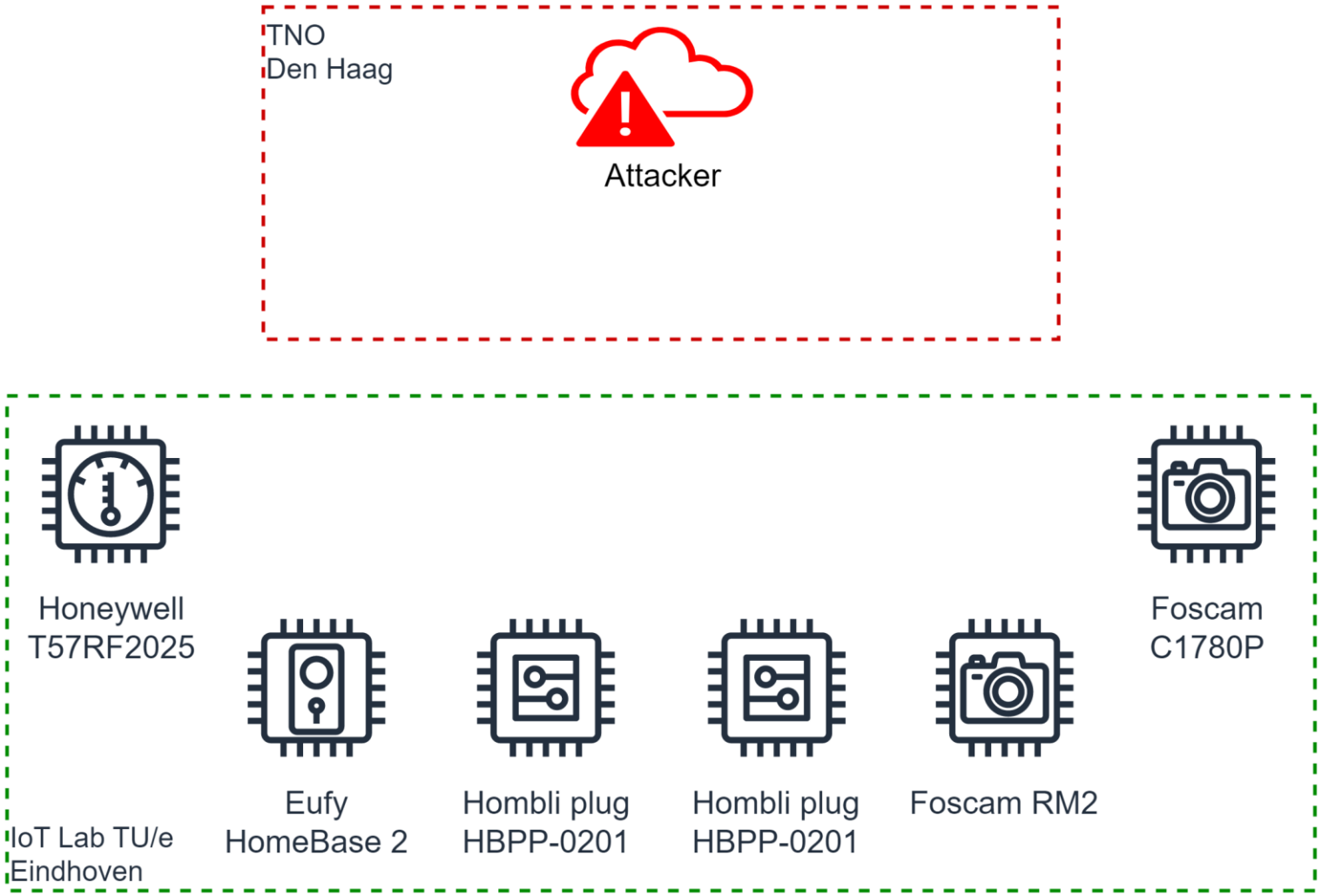
Experiments – same attacks



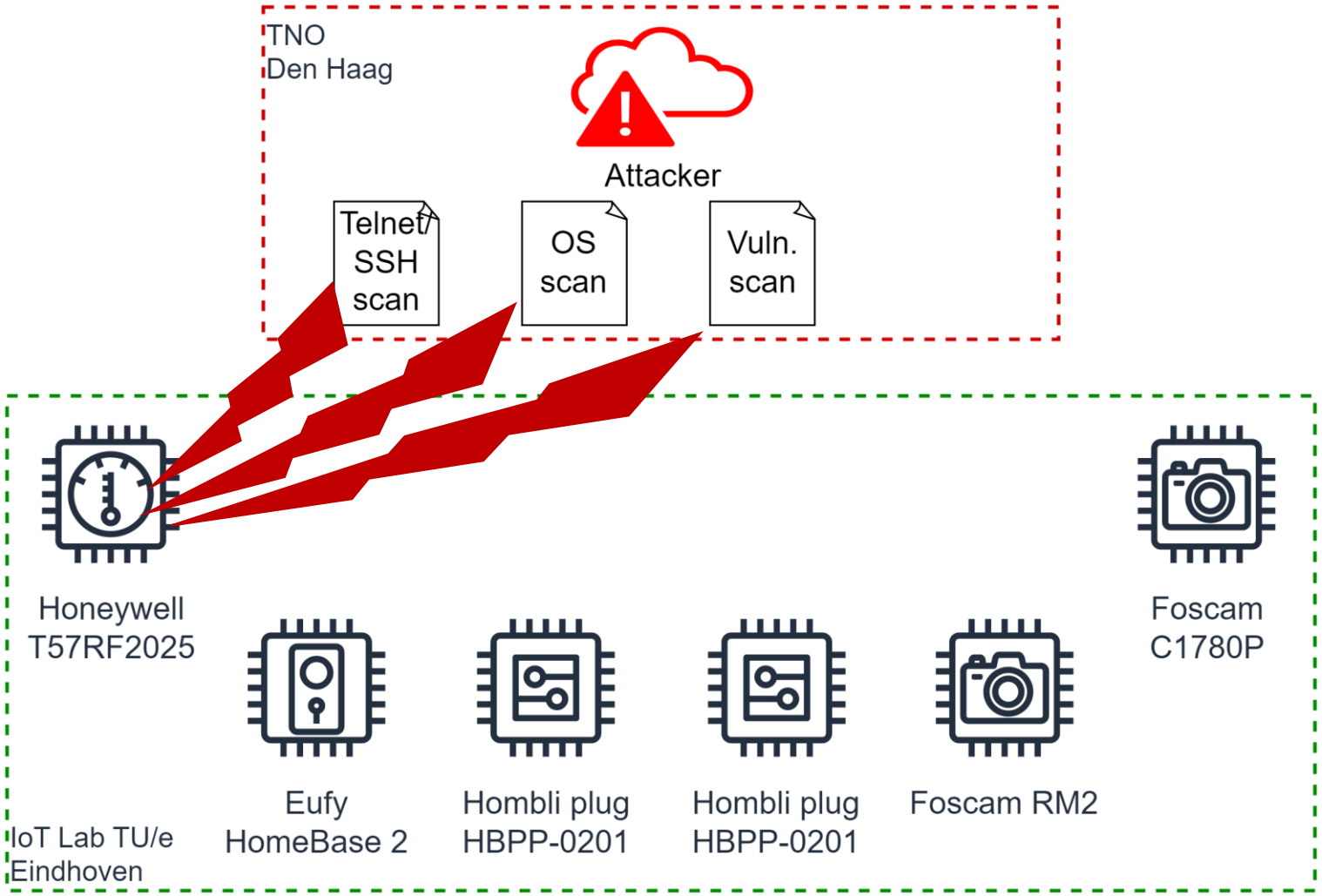
Experiments – same attacks



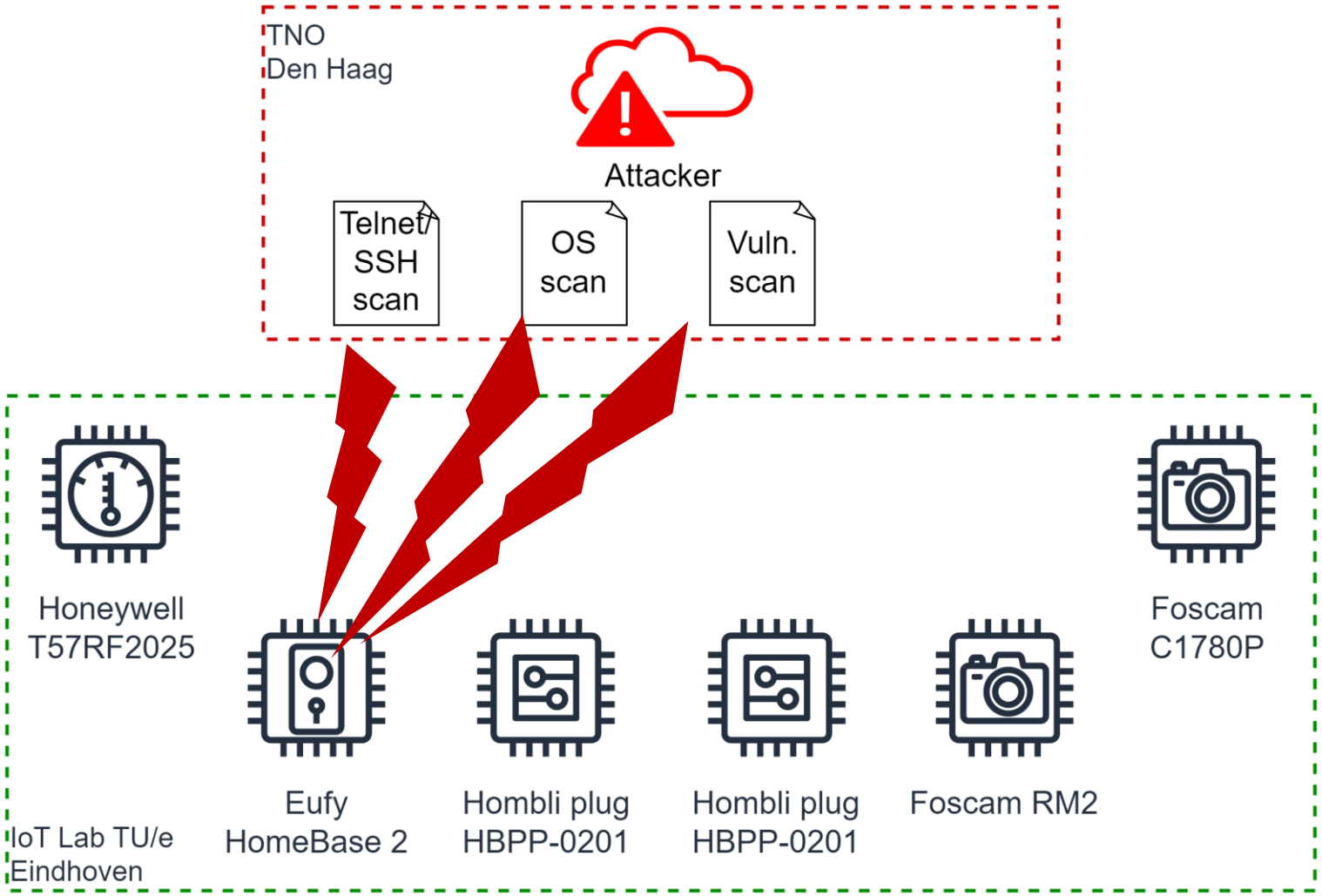
Experiments – different attacks



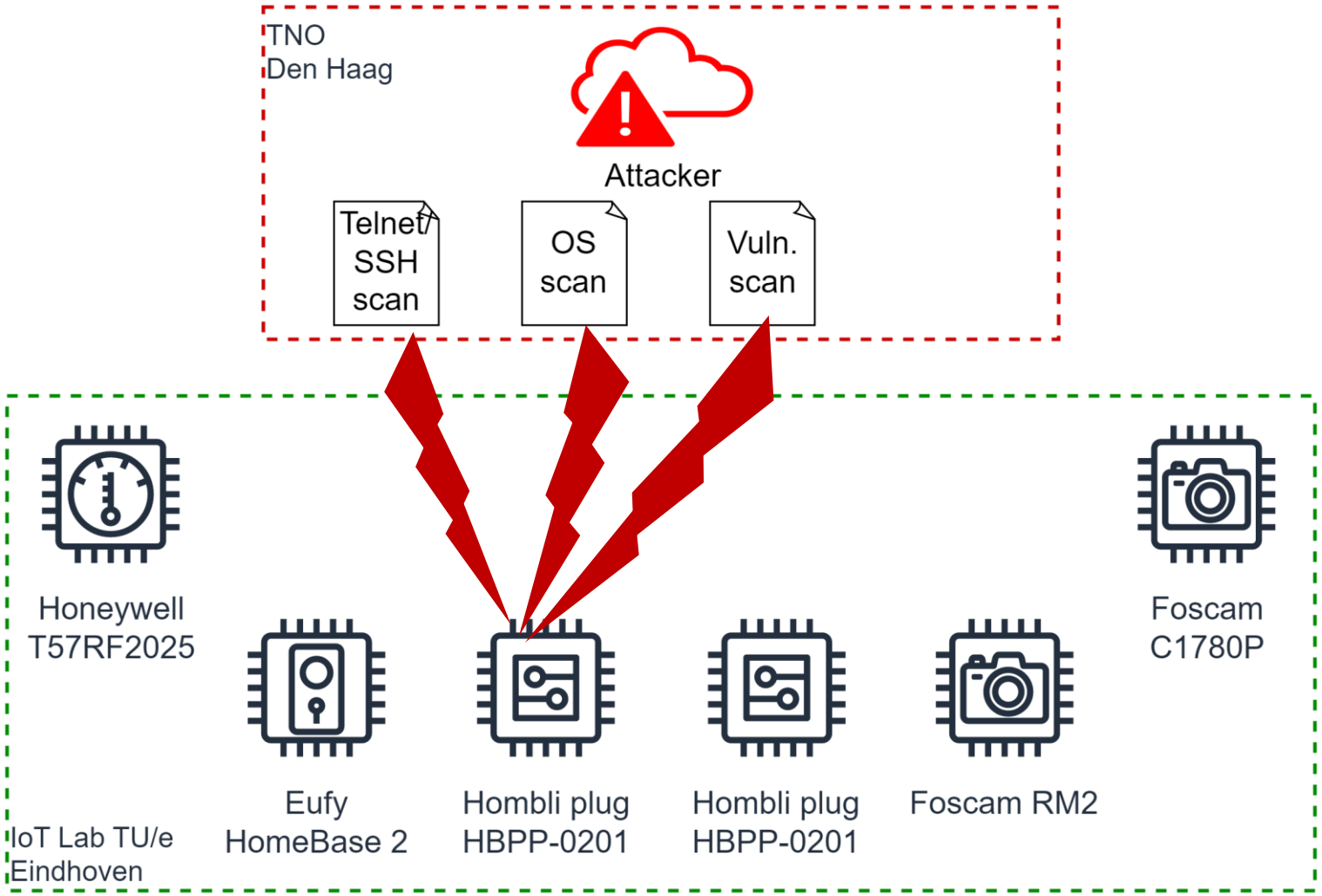
Experiments – different attacks



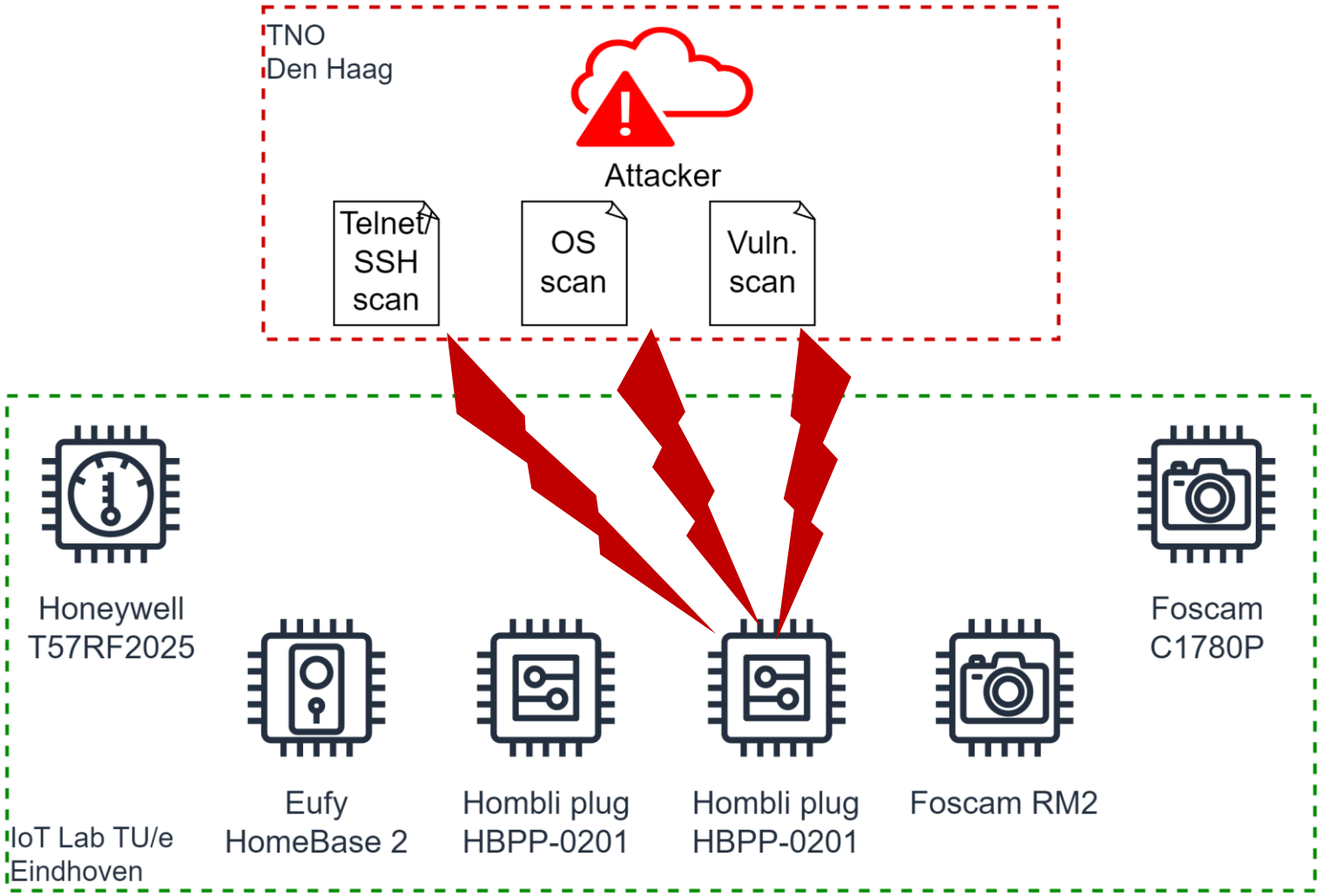
Experiments – different attacks



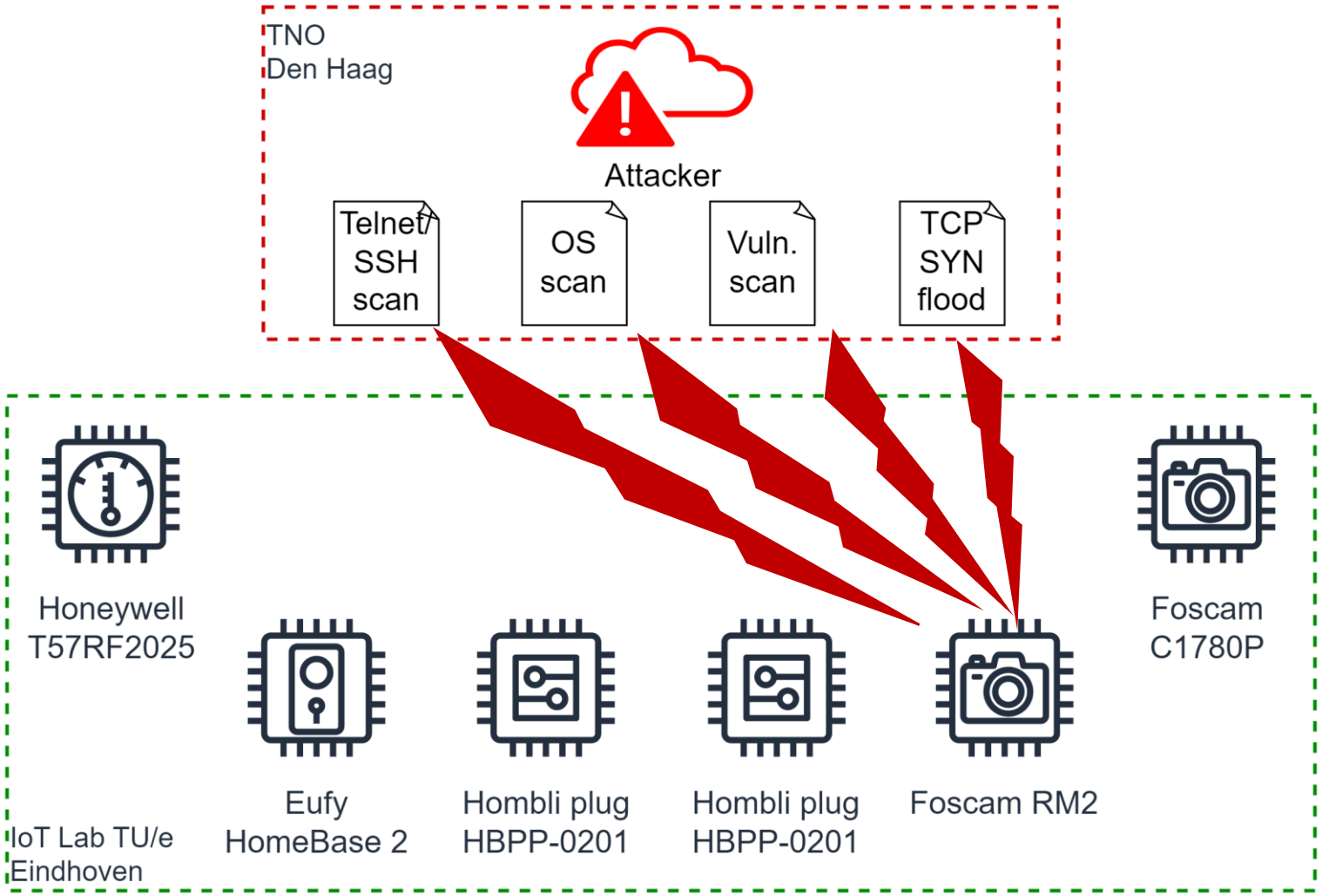
Experiments – different attacks



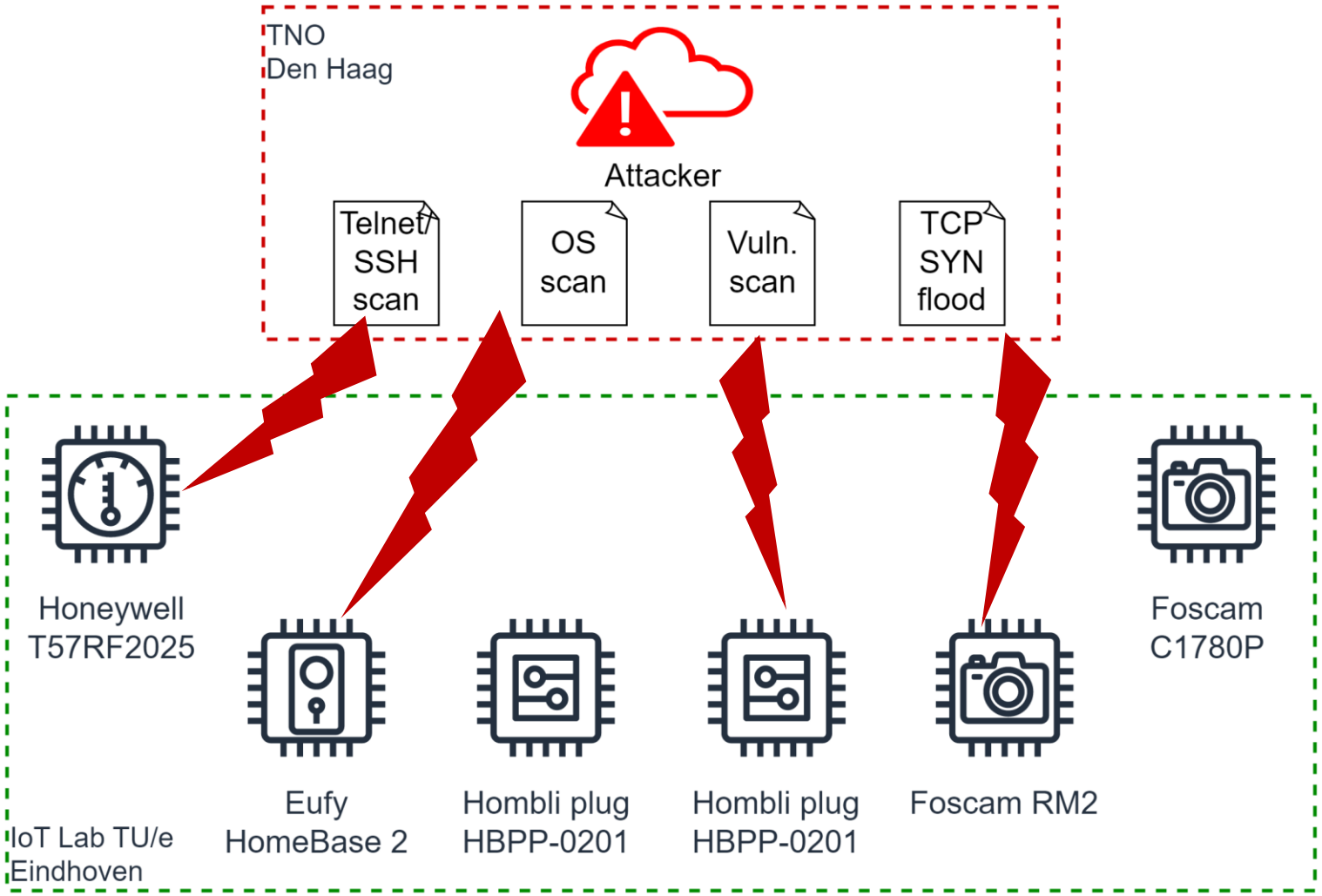
Experiments – different attacks



Experiments – different attacks



Experiments – different attacks



Results

Results – detecting attacks

(= with clusters fluctuations)

Attack	MRT entries	Anomalous entries	TP	TN	FP	FN	Accuracy	Precision	Recall	F1-score
Telnet/SSH port scan	130	15	15	115	0	0	100.00%	100.00%	100.00%	100.00%
OS scan	217	26	26	191	0	0	100.00%	100.00%	100.00%	100.00%
Vulnerability scan	310	48	45	259	3	0	98.06%	93.75%	100.00%	96.77%
TCP SYN flood DoS	170	22	16	142	6	0	96.47%	72.73%	100.00%	84.21%
Total	827	111	102	707	9	0	98.90%	91.89%	100.00%	95.77%

Results – detecting attacks

Attack	MRT entries	Anomalous entries	TP	TN	FP	FN	Accuracy	Precision	Recall	F1-score
Telnet/SSH port scan	130	15	15	115	0	0	100.00%	100.00%	100.00%	100.00%
OS scan	217	26	26	191	0	0	100.00%	100.00%	100.00%	100.00%
Vulnerability scan	310	48	45	259	3	0	98.06%	93.75%	100.00%	96.77%
TCP SYN flood DoS	170	22	16	142	6	0	96.47%	72.73%	100.00%	84.21%
Total	827	111	102	707	9	0	98.90%	91.89%	100.00%	95.77%

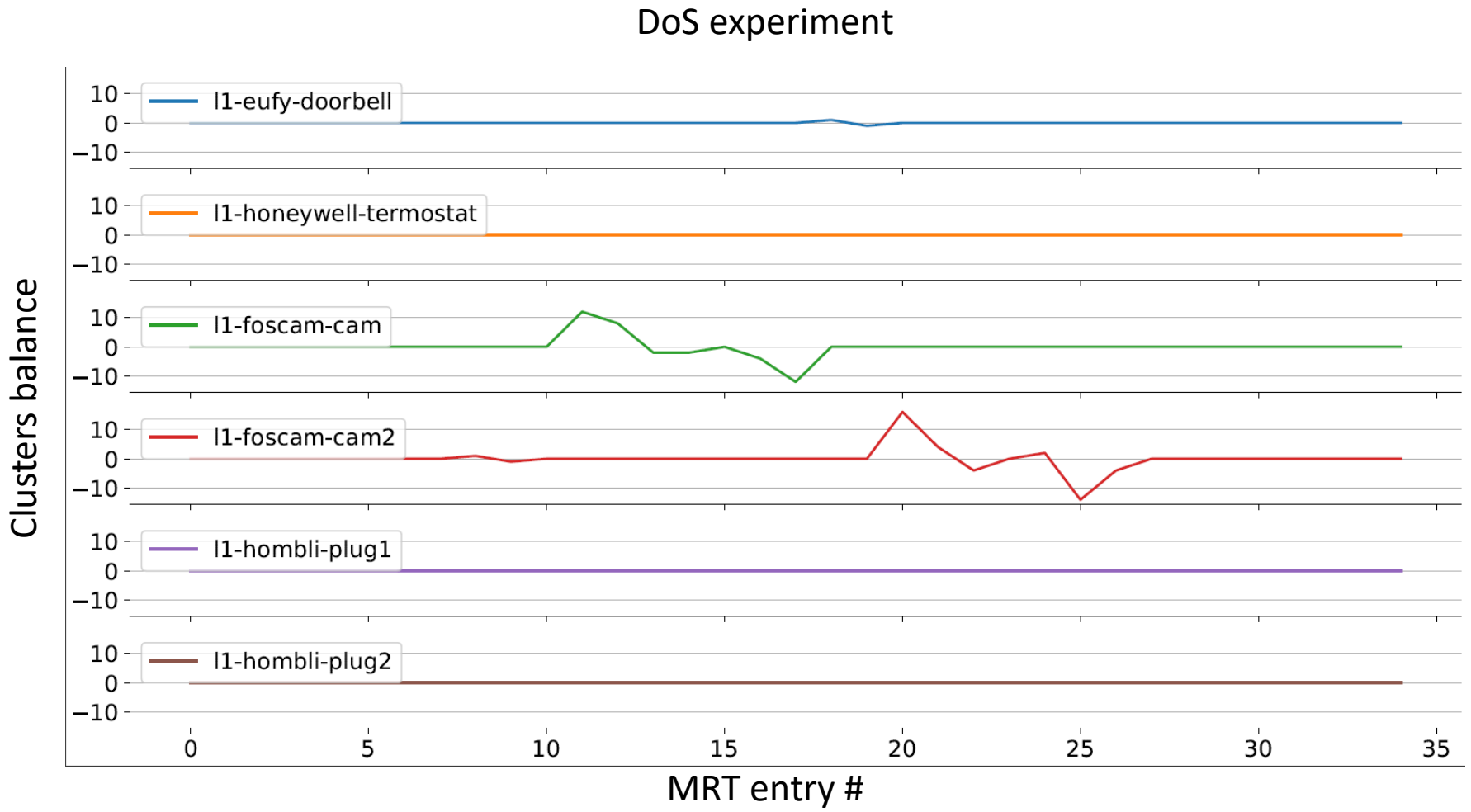
FPs because of non manufacturer's MUD

Results – identifying same attacks

Attack	Total signatures	Expected matches	TP	TN*	FP	FN	Accuracy	Precision	Recall	F1-score
Telnet/SSH port scan	5	10	10	N/A*	0	0	100.00%	100.00%	100.00%	100.00%
OS scan	5	10	6	N/A*	0	4	60.00%	100.00%	60.00%	75.00%
Vulnerability scan	5	10	8	N/A*	0	2	80.00%	100.00%	80.00%	88.89%
TCP SYN flood DoS	2	1	1	N/A*	1	0	50.00%	50.00%	100.00%	66.67%
Total	17	31	25	N/A*	1	6	78.13%	96.15%	80.65%	87.72%

same attacks identified as same

Results – identifying same attacks - example

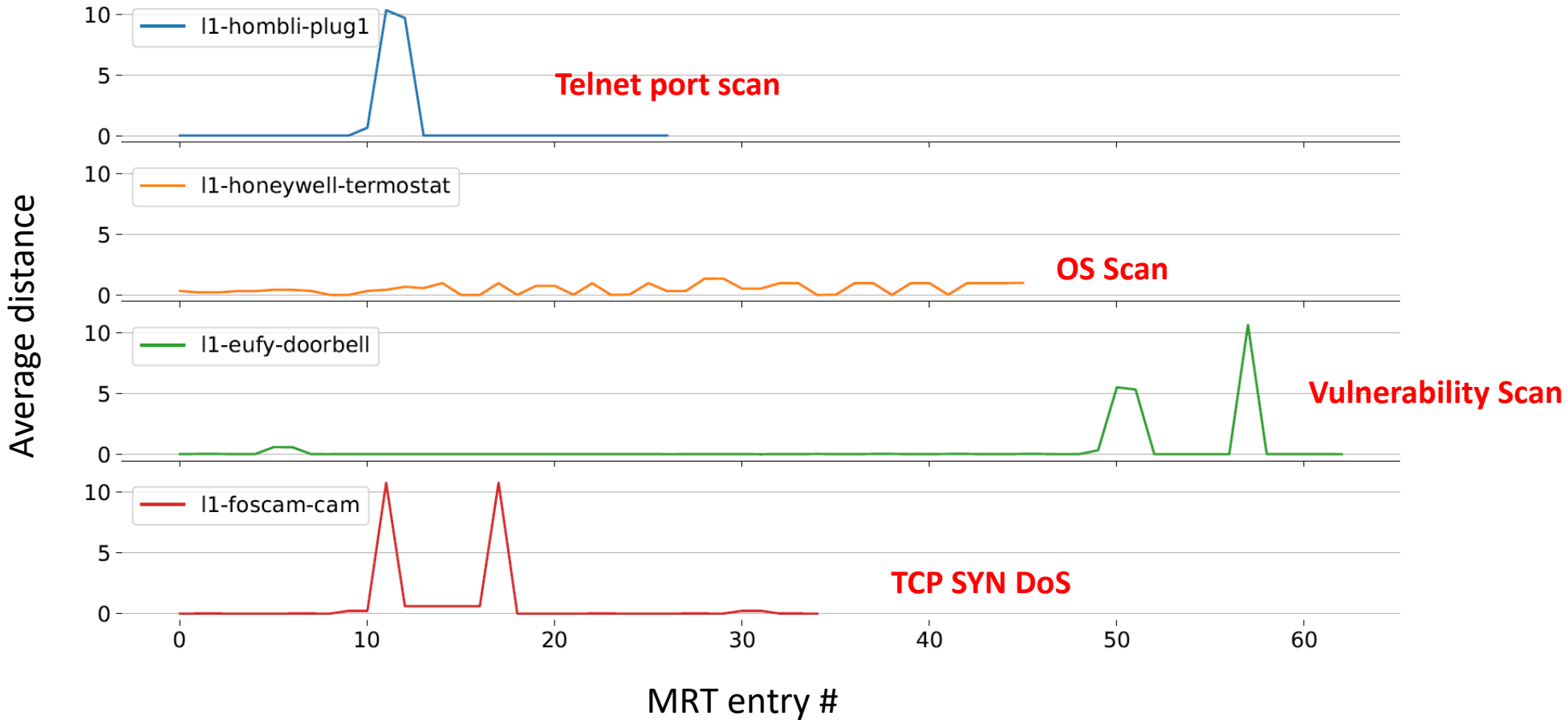


Results – discerning different attacks

Test	Device(s)	Compared MRT feeds	Incorrect matches Expected	Worst	Found
1	Eufy home-kit doorbell		0	3	0
2	Honeywell thermostat	Scans	0	3	0
3	Hombli plug 1	(Telnet/SSH, OS,	0	3	0
4	Hombli plug 2	Vulnerabilities)	0	3	0
5	Foscam camera C1780P	All	0	6	1
6	Eufy, Honeywell, Hombli, Foscam	All	0	6	0
Overall			0	18	1
Matches correctly discarded					**94.44%**

Comparisons correctly discarded

Results – identifying different attacks



Conclusions

Conclusions - results

Novel approach to gain visibility of IoT threats at home-like environments

95.77% F1 score for detection of attacks

96.15% of same attack cases identified as same

94.44% of different attack cases identified as different

Conclusions – discussion

Main limitations:

- MUD attack surface
- Low-volume attacks

Conclusions – discussion

Main limitations:

- MUD attack surface
- Low-volume attacks

Main future work:

- Distributed scenario → Test at-scale events

Conclusions – discussion

Main limitations:

- MUD attack surface
- Low-volume attacks

Main future work:

- Distributed scenario → Test at-scale events

Use-case:

- Security monitoring for vendors

Conclusions – open source!

MUDscope tool and Dataset

https://github.com/lucamrgs/MUDscope

Thank you

Stepping out of the MUD: contextual threat information for IoT devices with manufacturer-provided behavior profiles

https://github.com/lucamrgs/MUDscope

Luca Morgese Zangrandi

Questions?

luca.morgese@tno.nl