One MUD to Rule Them All

IoT Location Impact

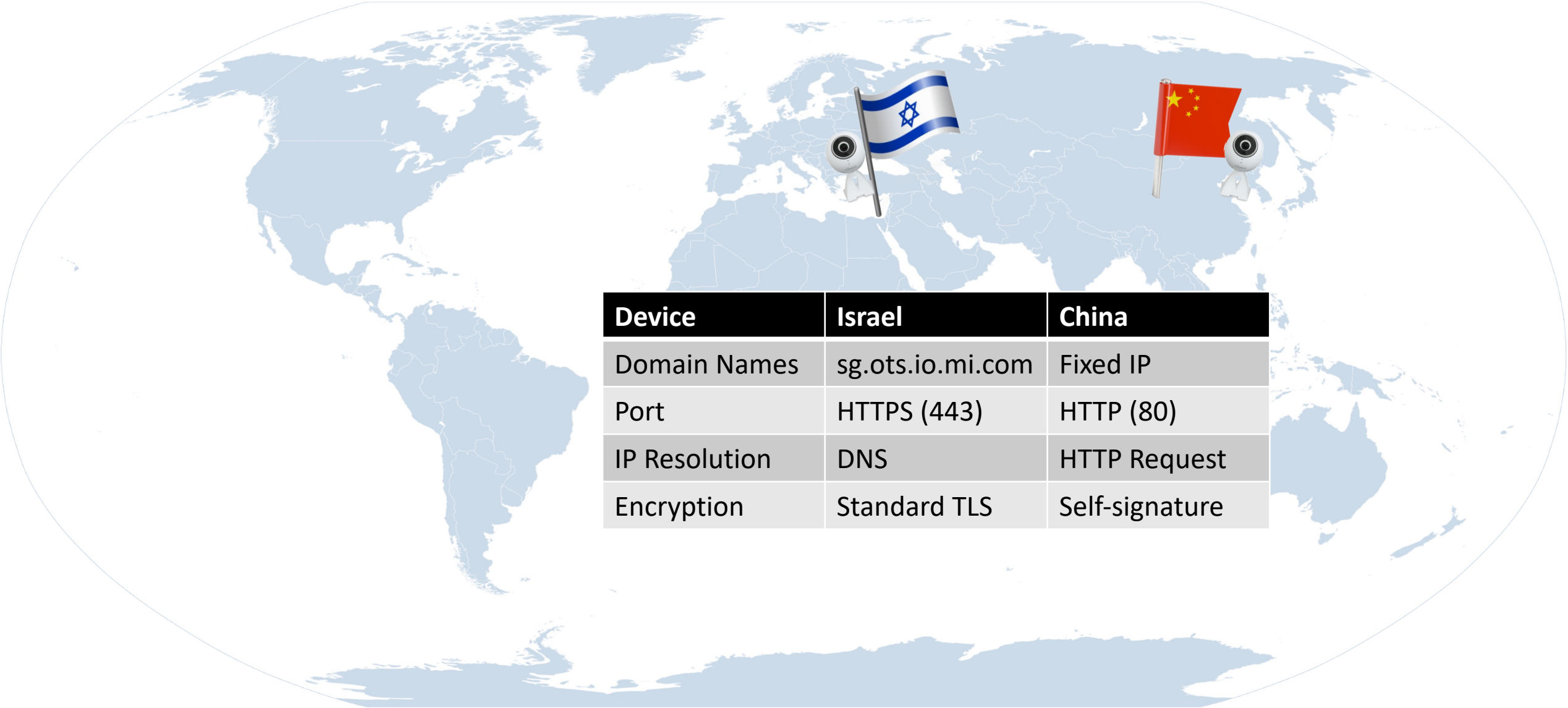
Bar Meyuhas

Anat Bremler-Barr, Ran Shister

Reichman University

Partly supported by Cisco grant

Same IoT device with the same firmware, behaves differently across the globe



Device	Israel	China
Domain Names	sg.ots.io.mi.com	Fixed IP
Port	HTTPS (443)	HTTP (80)
IP Resolution	DNS	HTTP Request
Encryption	Standard TLS	Self-signature

Outline

- Research goal and motivation
- MUD background
- Experiments
  - Dataset
  - 4 observations - location has an impact!
- Logical location support in MUD
- MUDIS: MUD Inspection System
- MUD Generalization: One MUD to Rule Them All

Research Goal: understanding the impact of the IoT device's location on its networking behavior

- Motivation:
  - MUD – Network security framework
  - IoT Identification
  - Learn normal device behavior and then extract rules and features

MUD Profile: network behavior formalization

- IETF Standard, RFC 8520

- MUD is an Access Control List (ACL), a set of Access Control Entries(ACEs)
  - *ACE = (Legitimate Endpoint, protocol, source port, destination port, direction)*
  - Legitimate endpoint is usually a **domain name** (or IP ,MAC)

- Reduce attack surface
  - Allowlist IoT Network Behavior
  - Firewall allows only known network behavior

```
{
  "ace": [
    {
     "name": "from-ipv4-xiaomi-camera-Israel",
     "ipv4": {
       "protocol": 6,
       "ietf-acldns:dst-dnsname": "sg.ots.io.mi.com"
     },
     "tcp": {
       "destination-port": {
          "operator": "eq",
          "port": 443
       },
       "ietf-mud:direction-initiated": "from-device"
     }
    },
    {
     "actions": {
       "forwarding": "accept"
     }
    }
  ]
}
```

Experiment

- Dataset
  - Traffic Logs (PCAP) -> MUD files ([1])
  - 31 IoT devices (plugs, bulbs, cameras, streamers..)
  - User accounts in up to 14 countries:

Virtually connected to different locations (VPN)

Physically connected to different locations [2]

[1] - Hamza, Ayyoob, et al. "Clear as MUD: Generating, validating and applying IoT behavioral profiles. ” *Proceedings of the 2018 Workshop on IoT Security and Privacy*.
[2] - Ren, Jingjing, et al. "Information exposure from consumer iot devices" .*Proceedings of the Internet Measurement Conference* 2019.

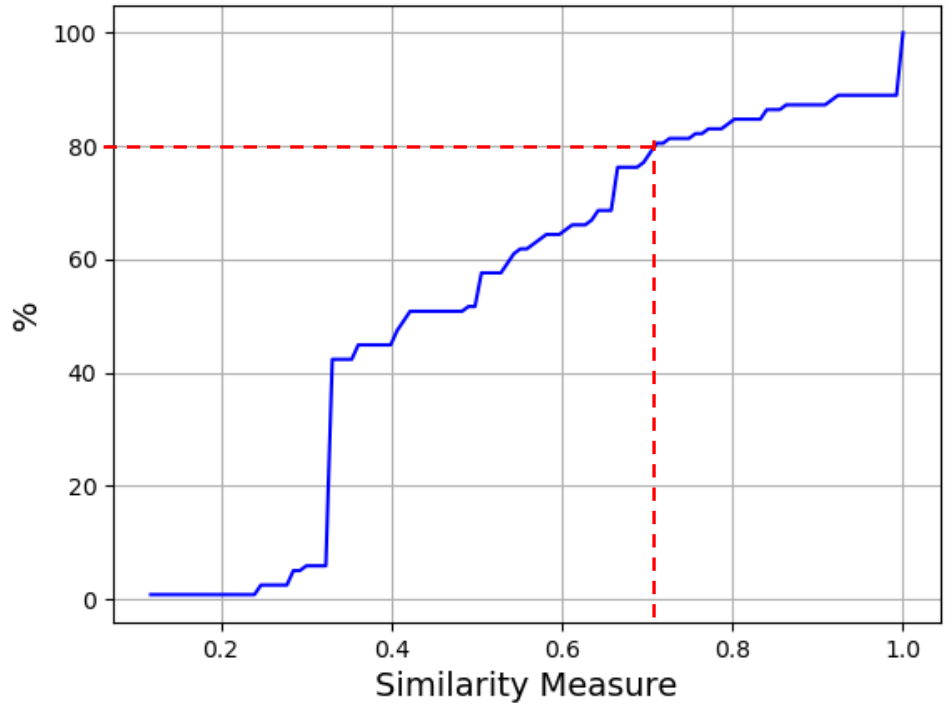
Observation 1: Location impact is very prevalent

- Similarity measure of two MUDs for the same device d, at location i and location j is defined :

$$Similarity_d(MUD_i^d, MUD_j^d) = \frac{|MUD_i^d \cap MUD_j^d|}{|MUD_i^d \cup MUD_j^d|}$$

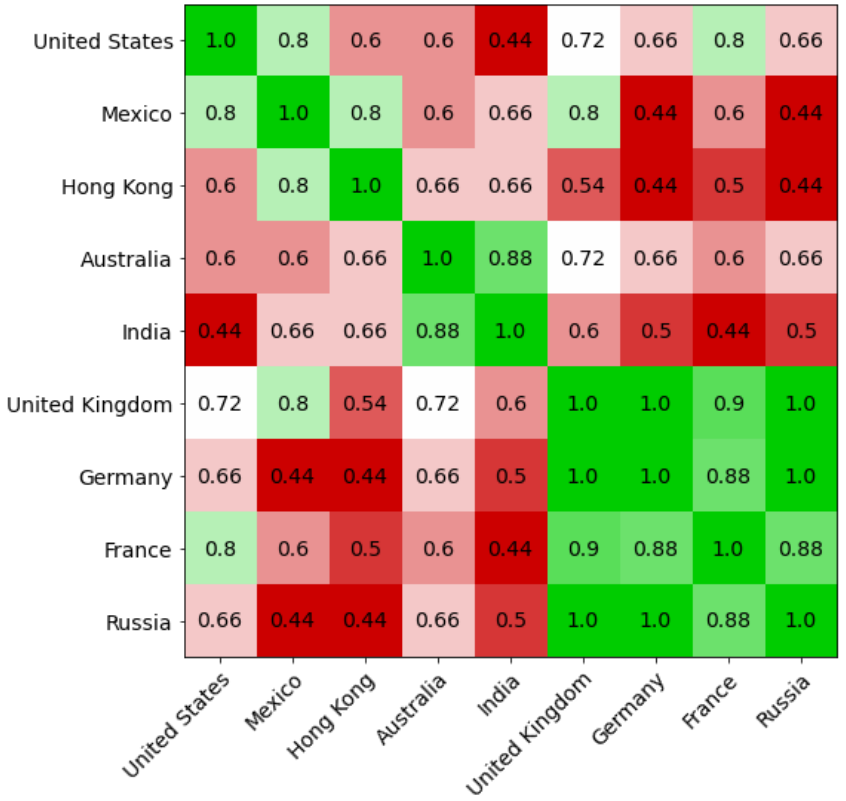
- 80% of the MUD comparisons show similarity measure lowers than~0.7

CDF of MUD similarity measure values



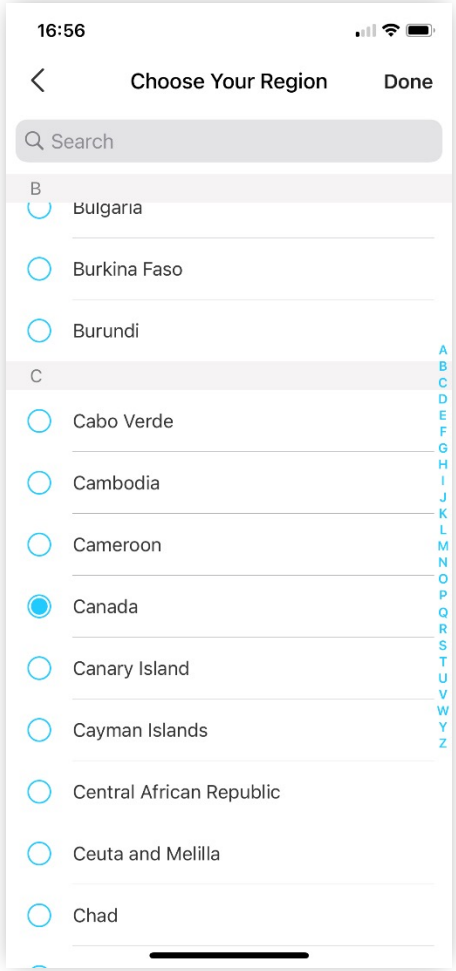
Observation 2: Correlation to Regions (Cloud Regions)

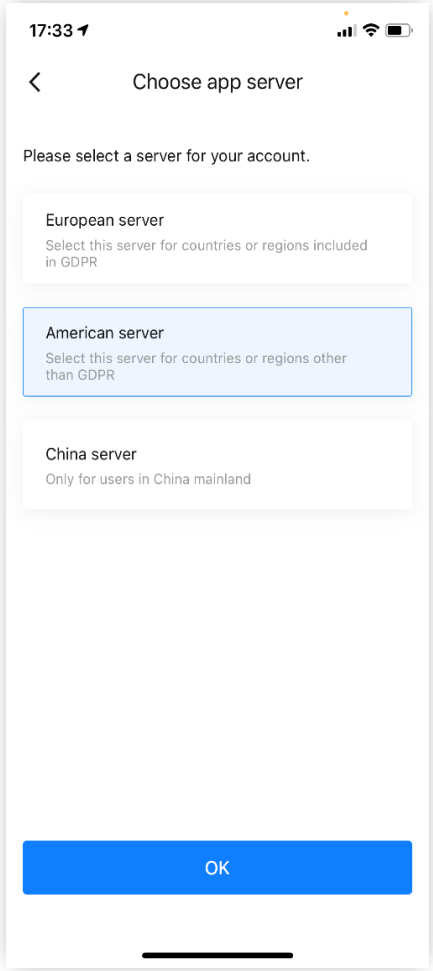
Yi camera : similarity heat-map

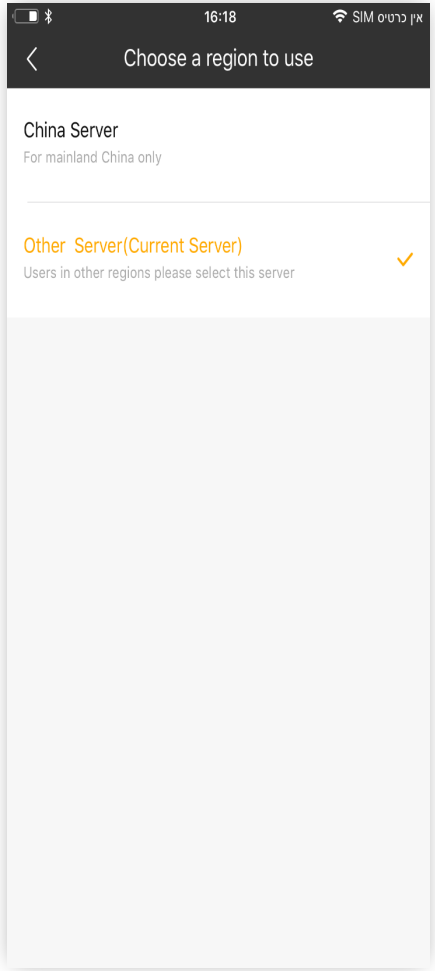


Countries are ordered according to geographical regions

Observation 3: Network behavior is affected by the logical location and not by the physical location (Geo-IP)







Observation 4: In most cases, the differences are in the domains

ru.ot.io.mi.com in Russia vs *de.ot.io.mi.com* in UK

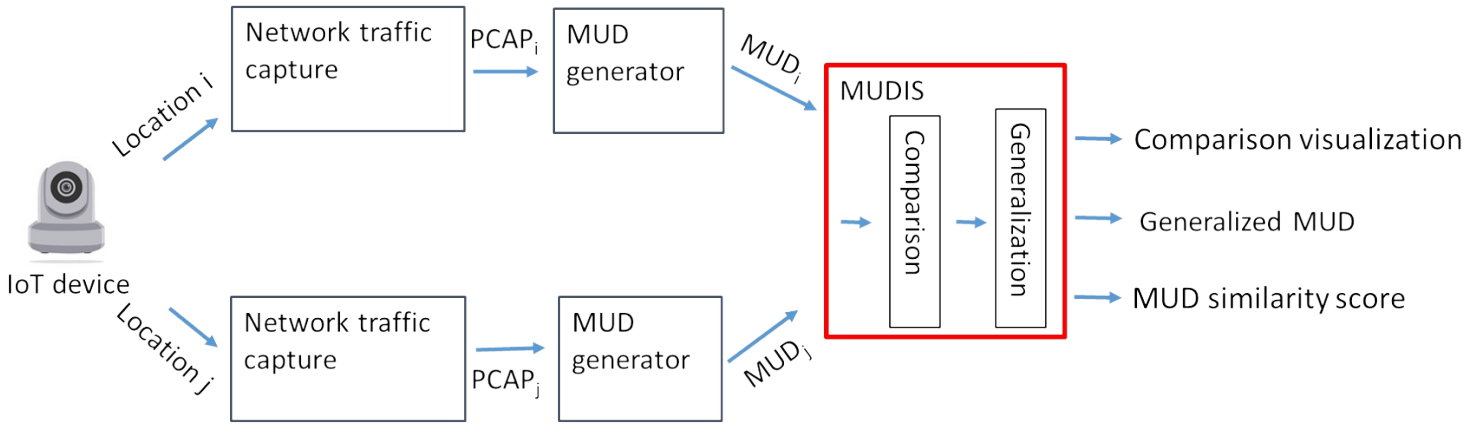
Generalization: **.ot.io.mi.com*

Logical location support in MUD

- Two options:
  1. Single global MUD:
     a. Naïve – unify all ACEs
     b. Generalized ACEs (**.ot.io.mi.com*)
  2. Different MUD per location:
     - User-defined location
     - Add information to the MUD URL should be defined as a result of the user's decision

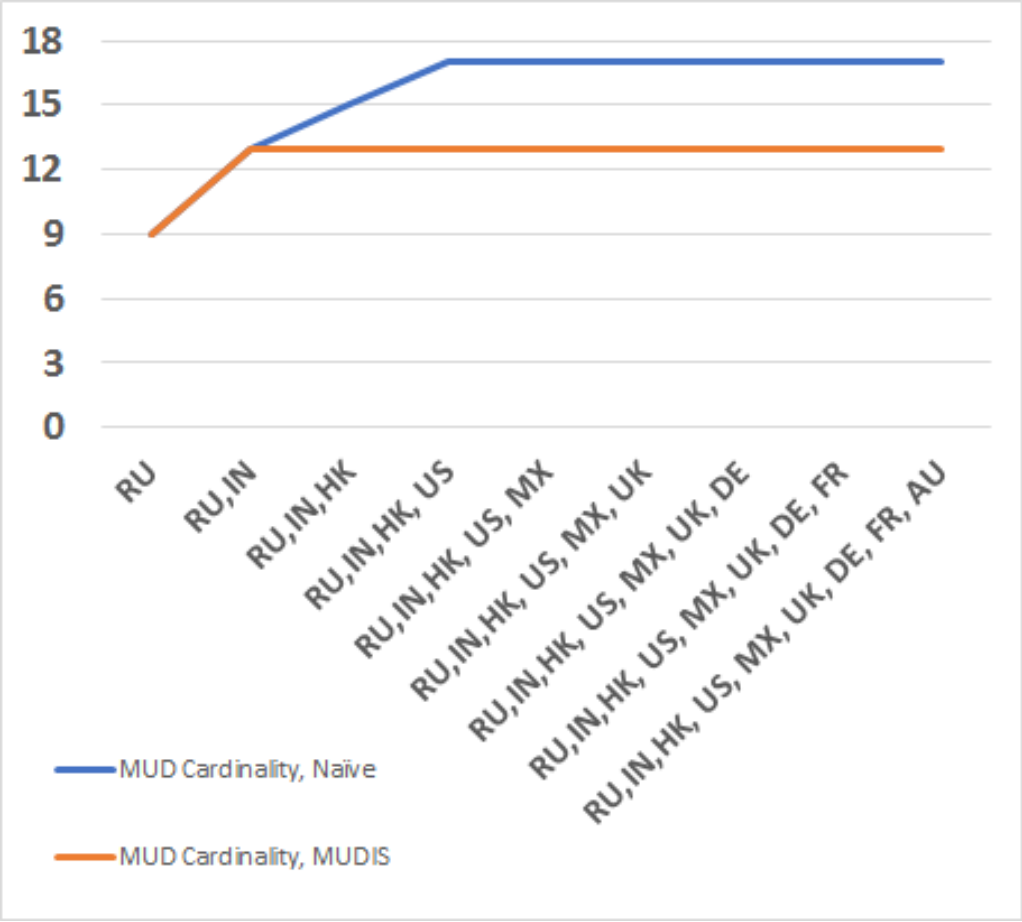
MUDIS: MUD Inspection System [1]

- We need a tool that helps us to compare and generalize MUDs:
  - Matching ACEs – find similar entries that can be combined or generalized into a generic rule.
  - Export generic MUD – Create a generic MUD out of input MUD files.
  - MUD similarity score – find out the impact of device location (or any other environmental variable) on the MUD.



[1] – Bremler-Barr, Shister, et al. "MUDIS: MUD Inspection System." *Demo Session NOMS 2022*.

One MUD to Rule Them All



MUD per location is not a feasible task

Naïve Unify of ACEs into a single MUD creates a bigger (by ~50%), unexplainable file

MUDIS generalization algorithm outcome is one MUD to rule them all

For more information on our IoT research

http://www.deepness-lab.org/Iotica

Questions: bremler@idc.ac.il

ran.shister@post.idc.ac.il

meyuhas.bar@post.idc.ac.il

SCAN ME