

It's Not Where You Are, It's Where You Are Registered IoT Location Impact on MUD

Anat Bremler-Barr

David Hay

Bar Meyuhas

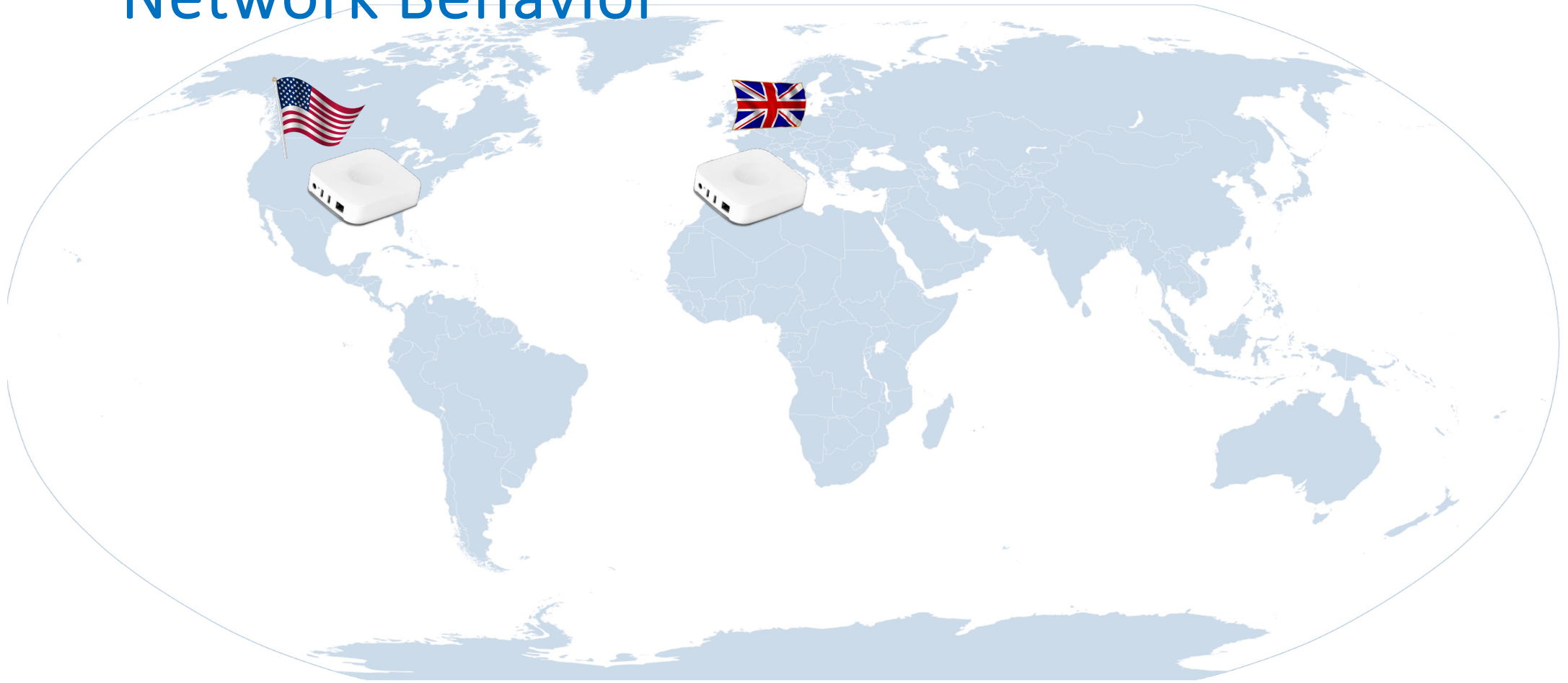
Shoham Danino



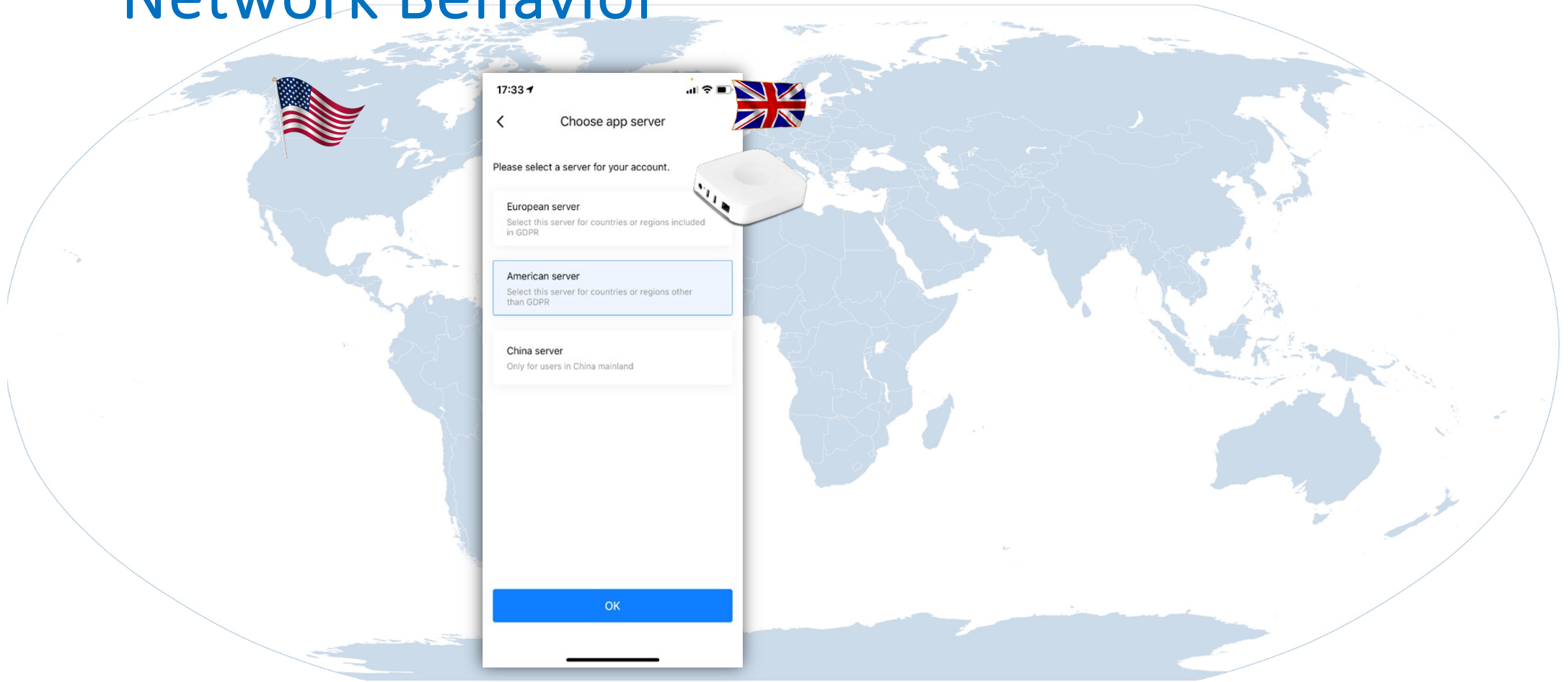
Partially supported by Cisco and Israel research authority

Applied Networking Research Workshop

IP-based Location Impact the IoT Network Behavior



User-defined location Impact the IoT Network Behavior



Motivations

Implication on:

- Network security framework (MUD RFC 8520)
- IoT Identification

→ Learning normal device behavior and then extracting rules and features is affected

Outline

- IP-based location < user-defined location
- Common user-defined location implementation
- Background MUD – IETF security framework
- The implication of user-defined location on the MUD
- Improving implementation using DNS ECS

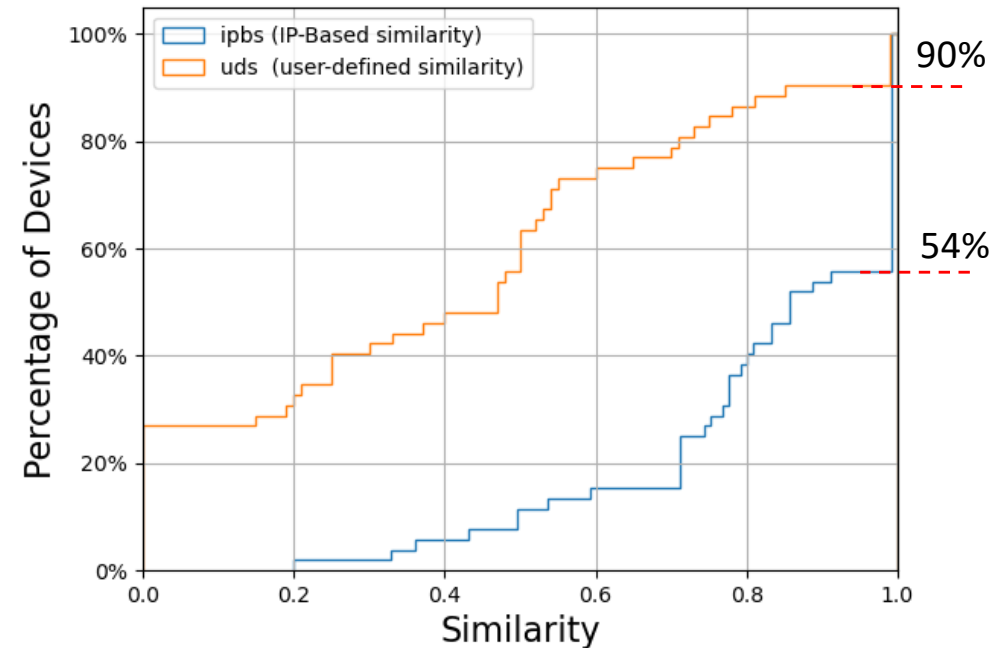
Location Impact is Very Common

The similarity measure of two set of domains for the same device d , at location i and location j is defined:

$$uds(d, il, ul, ul') = \frac{|\mathcal{D}(d, il, ul) \cap \mathcal{D}(d, il, ul')|}{|\mathcal{D}(d, il, ul) \cup \mathcal{D}(d, l, ul')|}$$

$$ipbs(d, ul, il, il') = \frac{|\mathcal{D}(d, il, ul) \cap \mathcal{D}(d, il', ul)|}{|\mathcal{D}(d, il, ul) \cup \mathcal{D}(d, il', ul)|}$$

CDF of MUD similarity measure values

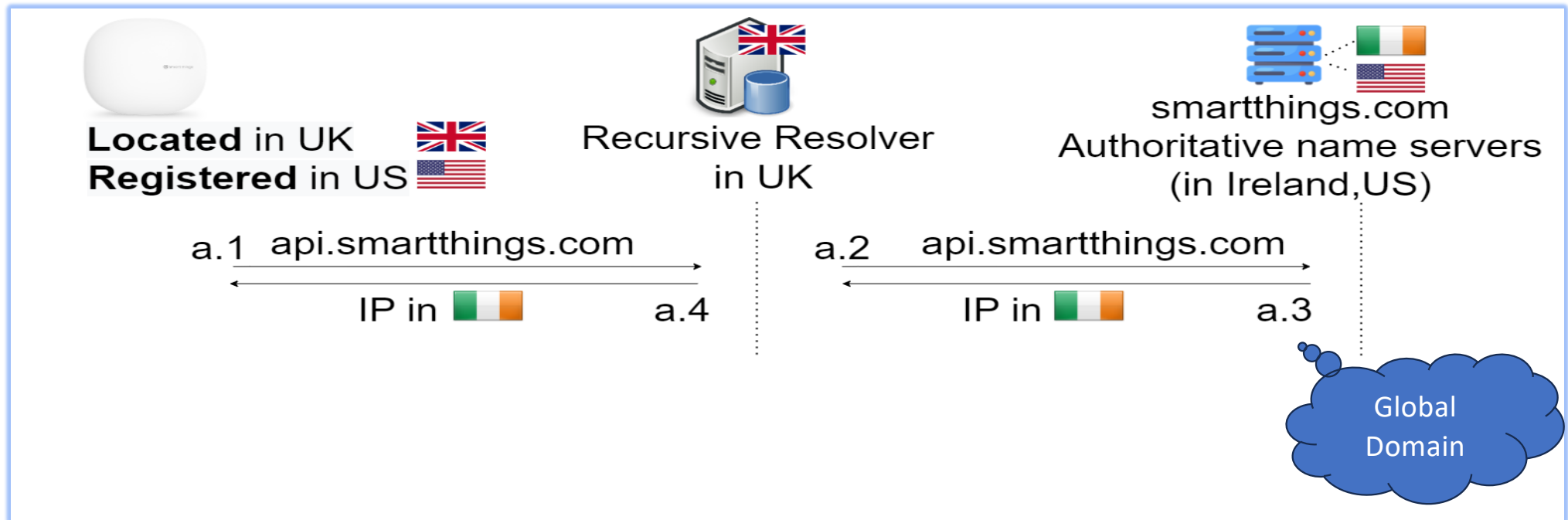


Why there is a difference in the domains?

- Different domain names allow different features and servers
 - For example, a camera facial recognition feature is available only in China
- However, there are other ways to implement different IPs for the same domain, for example using IP-based location

To allow USER-DECISION of location, the domain names must be different

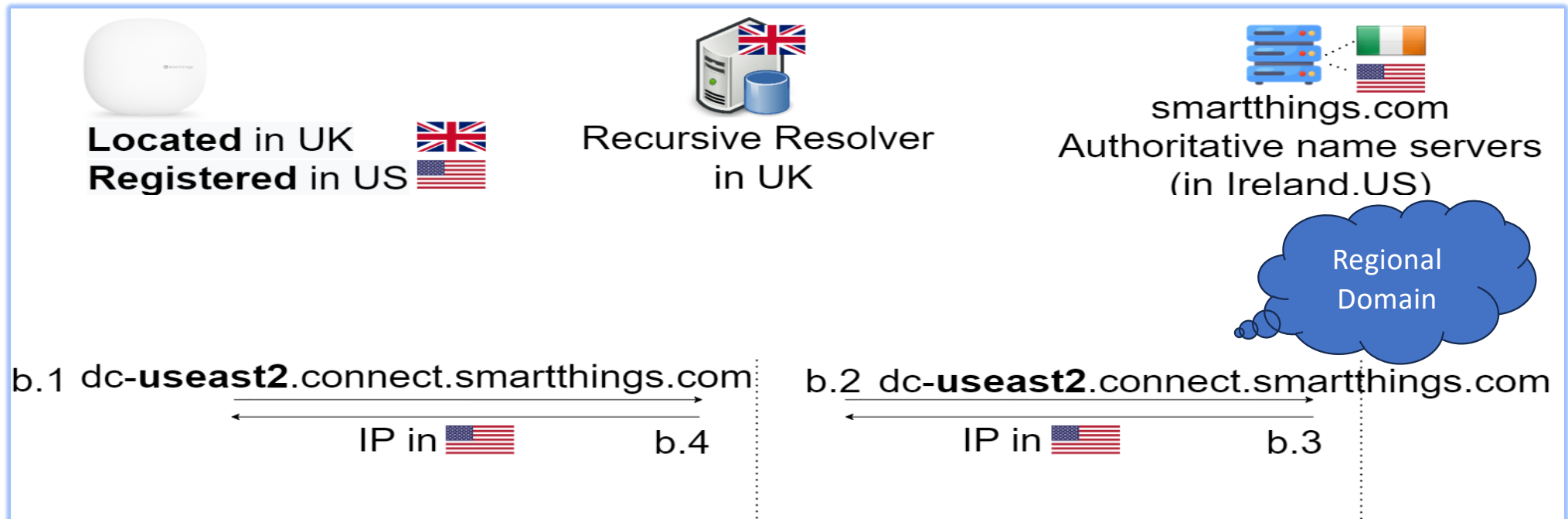
IP-Based Location Decision: DNS



User-Defined Location: **US**

IP Location: UK

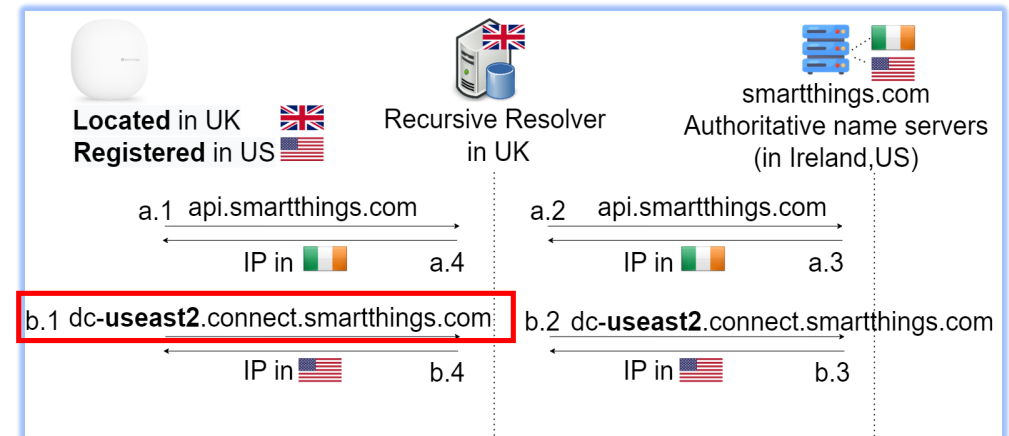
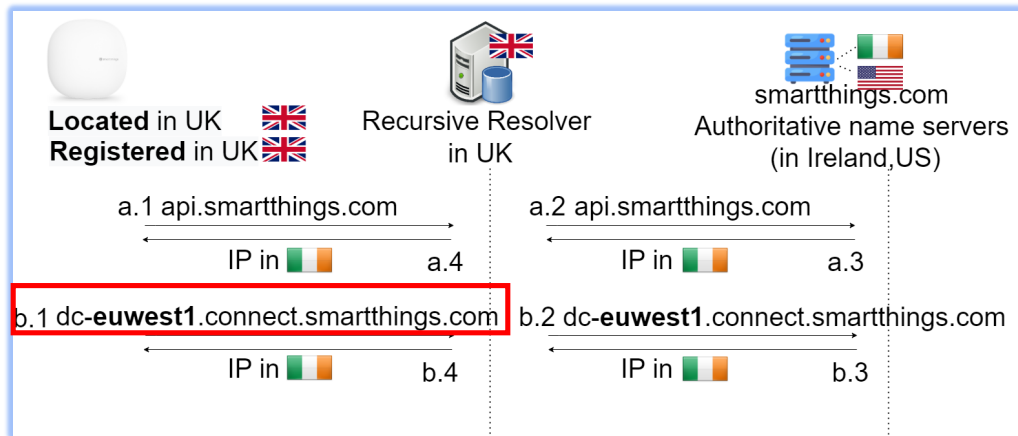
User-Defined Location Implementation



User-Defined Location: **US**

IP Location: UK

User-Defined Location Difference



User-Defined Location: **UK**

IP Location: UK

User-Defined Location: **US**

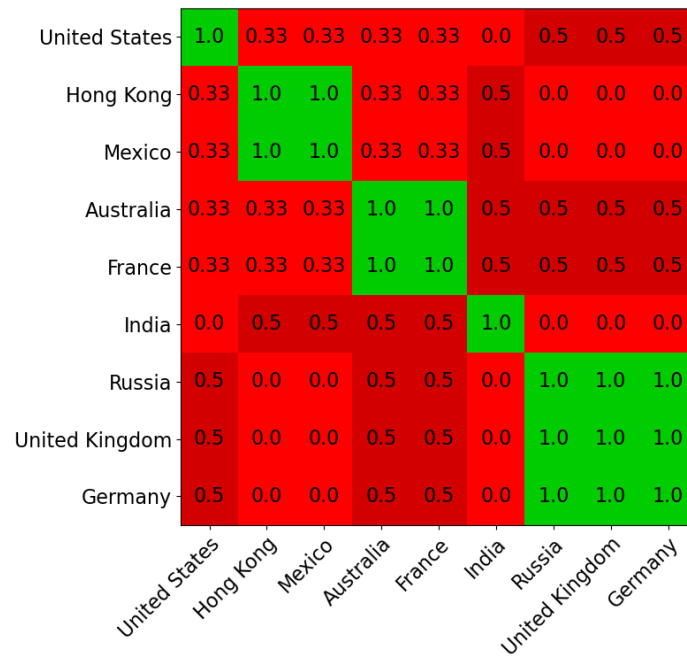
IP Location: UK

Regional domain changes: dc-**euwest1/useast2**.connect.smarththings.com

Global domain remains: api.smarththings.com

Correlation to Regions

Yi camera : similarity heat-map



Common case the differences in sub-domains

dc-**euwest1**.connect.smarthings.com
user-defined location in the UK

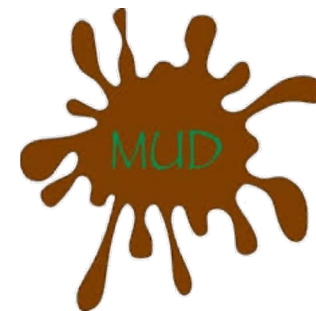


dc-**useast2**.connect.smarthings.com
user-defined location in the US



Only 9% of the domains present a difference in the Top-Level-Domain (TLD)


MUD Profile: network behavior formalization




- IETF Standard, RFC 8520
- MUD file 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
 - Allow-list 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"
        }
      }
    }
  ]
}
```


MUD Implication

Rule direction = from 
Rule details:
Protocol = TCP, **Domain** = api.smarthings.com
Source port = *, Destination Port = 443

Rule direction = from 
Rule details:
Protocol = TCP, **Domain** = euwest.connect.smarthings.com
Source port = *, Destination Port = 443

UK MUD file

Rule direction = from 
Rule details:
Protocol = TCP, **Domain** = api.smarthings.com
Source port = *, Destination Port = 443

Rule direction = from 
Rule details:
Protocol = TCP, **Domain** = useast.connect.smarthings.com
Source port = *, Destination Port = 443

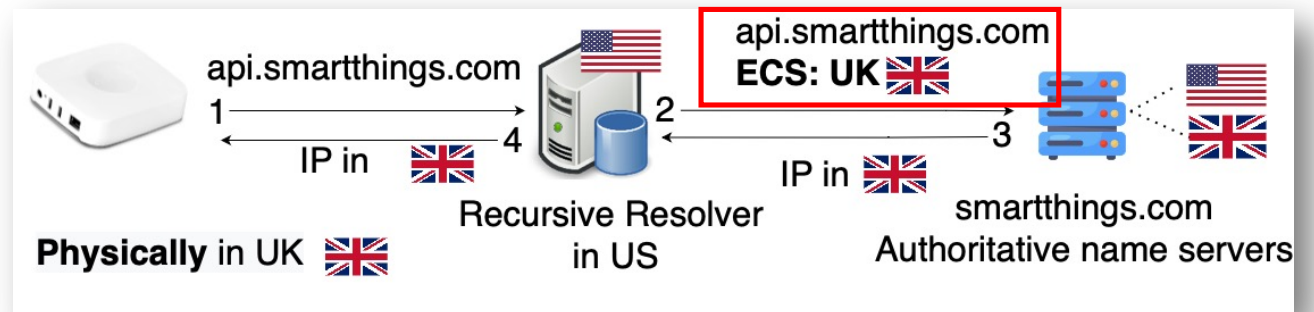
US MUD file

- Learning phase MUD
- Single large MUD vs separate MUD files
- Explainability & Maintenance

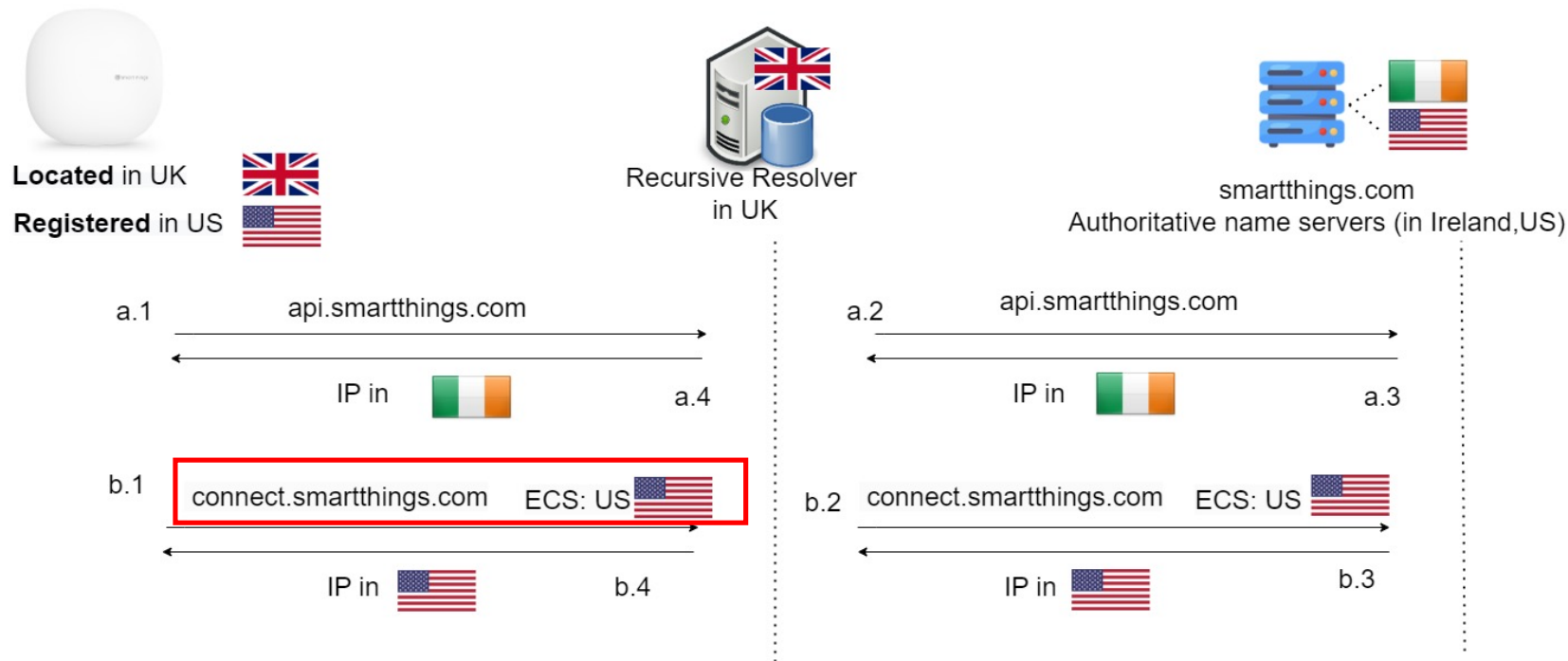
Extension DNS: ECS (Client Subnet)

- When using an open resolver, in which the resolver location is different than the client location. ECS can carry the client's IP.
- ECS RFC allows the end-point device to send an ECS field.

EDNS Client subnet -
Current implementation



Our proposal: using DNS ECS to carry the USER-DECISION



In our ECS-based user-defined location, the IoT device, and not the resolver, will add the ECS. Regional domains carry an ECS field while global domains do not.

MUD Using ECS

Rule direction = from



Rule details:

Protocol = TCP, **Domain** = api.smarthings.com
Source port = *, Destination Port = 443

Rule direction = from



Rule details:

Protocol = TCP, **Domain** = connect.smarthings.com
Source port = *, Destination Port = 443

- Learning phase MUD – easier
- Single MUD
- Explainability & Maintenance

Conclusion

User-defined location has an impact on IoT device network behavior

Dataset and security measurement should take location into account

User-defined can be implemented using the extension DNS

For more information on our IoT research

<http://www.deepness-lab.org/lotica>

Questions: meyuhas.bar@post.idc.ac.il

dhay@cs.huji.ac.il

mrdaninos@gmail.com

anatbr@tauex.tau.ac.il

