UNIVERSITY OF CAMBRIDGE

A step towards building resilient, robust and trustable IoT ecosystem

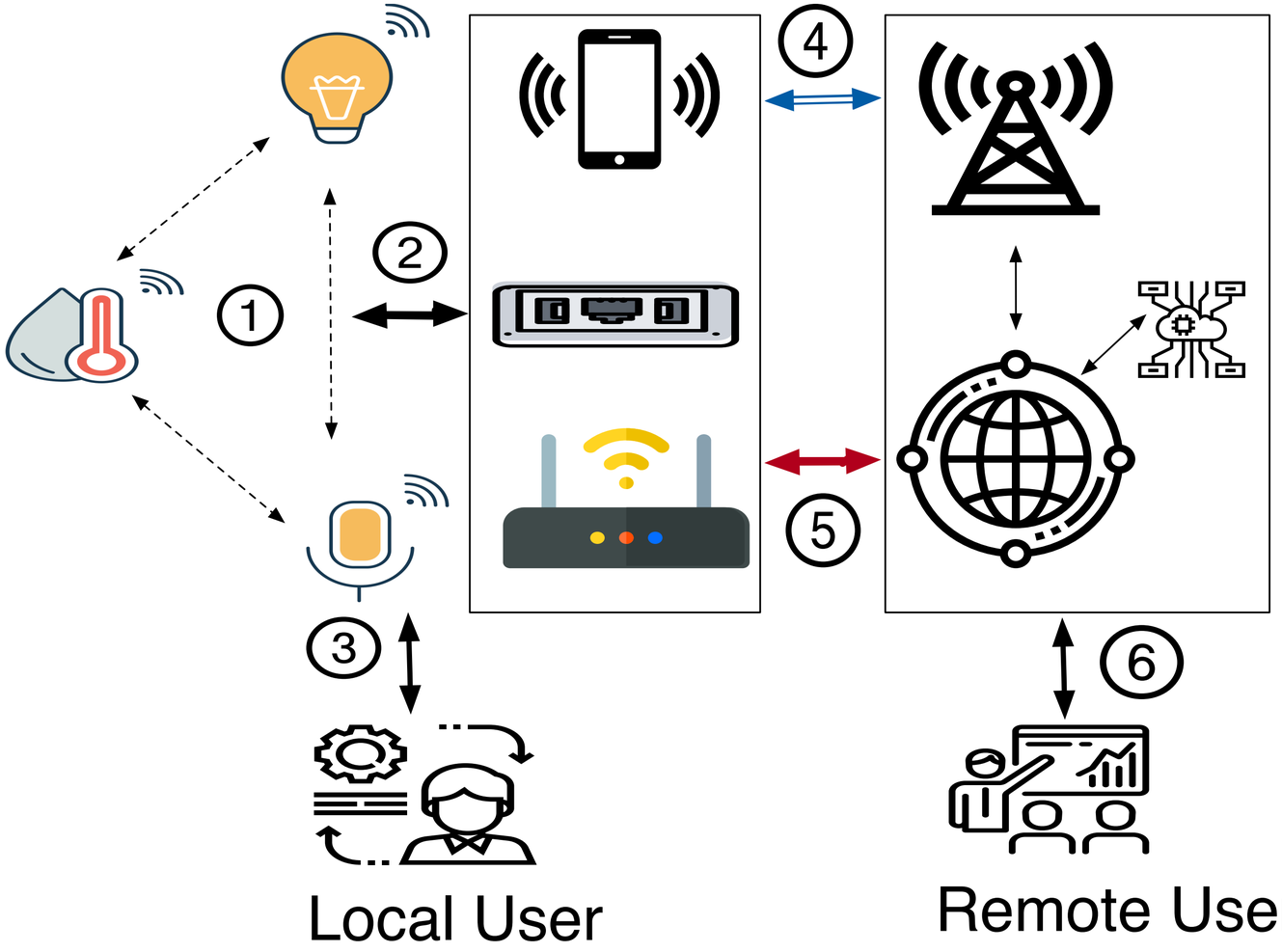
Poonam Yadav and Richard Mortier

MSN 2019

This project was supported by a mini-projects award from the Centre for Digital Built Britain and Innovate UK under Grant 90066, and by EPSRC EP/N028260/1 and EP/R03351X/1.

Networks & Operating Systems
SRG, Computer Laboratory

IoT Ecosystem



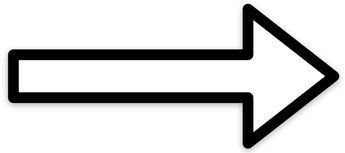
1. Interdevice communication
2. Device-gateway
3. Device-local user
4. Gateway-cellular
5. Gateway-broadband
6. Gateway-remote user

Challenges

- Heterogeneity
  - Devices, Comm, Apps, Users (and their Data)
- Scalability
- Lack of Standardisation
- Interpretability

Challenges

- Heterogeneity
  - Devices, Comm, Apps, Users (and their Data)
- Scalability
- Lack of Standardisation
- Interpretability



Messy interactions in the end-to-end ecosystem

Challenges

Messy interactions

Unreliable and untrustworthy systems

Image source: http://www.ltktechnologies.com/how-iot-influence-everyday-life/

Untangling …

Messy interactions

Understand by profiling a set of interactions

Extended profiling from crowdsourced interactions

Machine Learning Based Profiling

Image source: http://www.ltktechnologies.com/how-iot-influence-everyday-life/

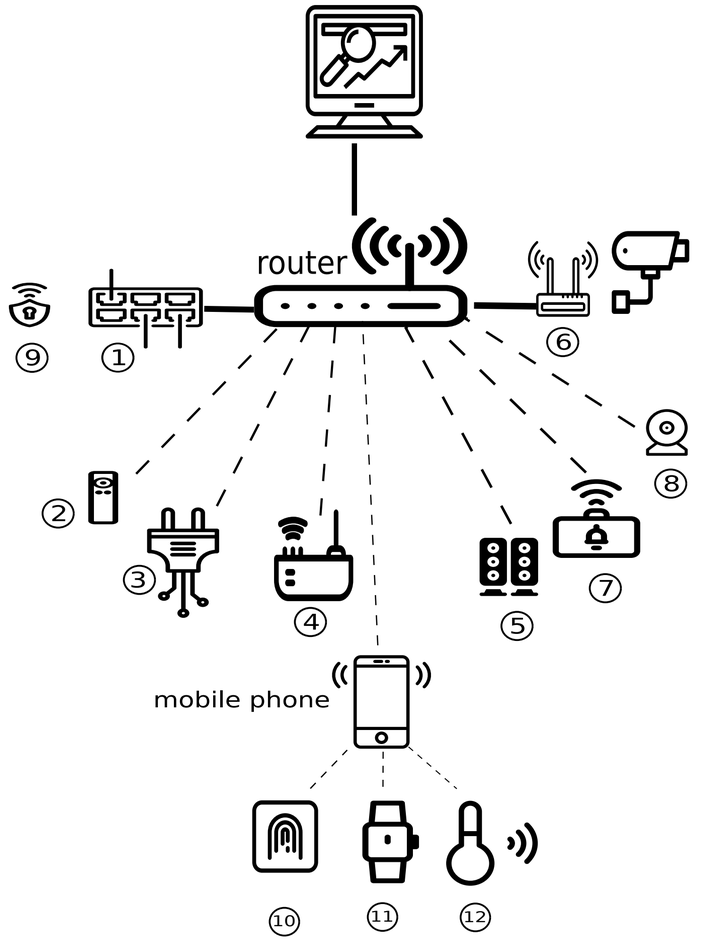
Understanding interactions

We start with our focus on analysing **Network Service Dependencies** in IoT Eco-system which are critical for IoT robustness, resilience and trustworthiness.

In this work we are **NOT** focusing on analysing interactions from security and privacy perspective.

Examining IOT Network Service Dependency

- We decided to examine what network behaviours were exhibited by different COTS IOT devices
- A simple experimental setup:
  - Domestic IoT devices
    - Different application domains
    - Manufacturers
    - Popularity
  - Connect them via a router (Netgear N600) we control
  - Capture and analyse their packets



Devices Under Test

- Hubs *vs* sensors
  - Several controlled via phone app
- Radio comm type
  - Non-WiFi via a hub
- Transport *vs* application protocols

	Device	Hub/ Sensor	Link Type	Protocols	Secure/ Insecure
1	Hive Starter Kit Hub [23]	H	Ethernet	TCP, IGMP, ICMP	S
2	TP-link Smart Plug [46]	H	Wi-Fi	UDP, TCP	S,I
3	Google Home Mini [19]	H	Wi-Fi	UDP, TCP, IGMP, ICMP	S,I
4	Amazon Echo Dot [5]	H	Wi-Fi	UDP, TCP, ICMP	S,I
5	Arlo Security Camera Base Station [10]	H	Ethernet, Wi-Fi	UDP, TCP	S,I
6	Foobot Air Quality Monitor [15]	S	Wi-Fi	TCP	S
7	Nest Smoke Alarm [35]	S	Wi-Fi	UDP, TCP	S,I
8	D-Link Motion Sensor [12]	S	Wi-Fi	UDP, TCP, IGMP	S,I
9	Hive Motion Sensor [24]	S	Zigbee	HA 1.2	S
10	ParrotPot Smart Flower Pot [38]	S	Bluetooth	V4.0 BLE	S
11	MiBand Smart Bracelet [49]	S	Bluetooth	V4.0	S
12	Smart Bluetooth Tracker [45]	S	Bluetooth	V4.0	S

Please note - Our purpose is not to make generalised statements about all IoT devices but to illustrate some of the ways commodity devices behaved and to consider the implications of those behaviours.

Traffic Analysis: In presence of Network Disruption

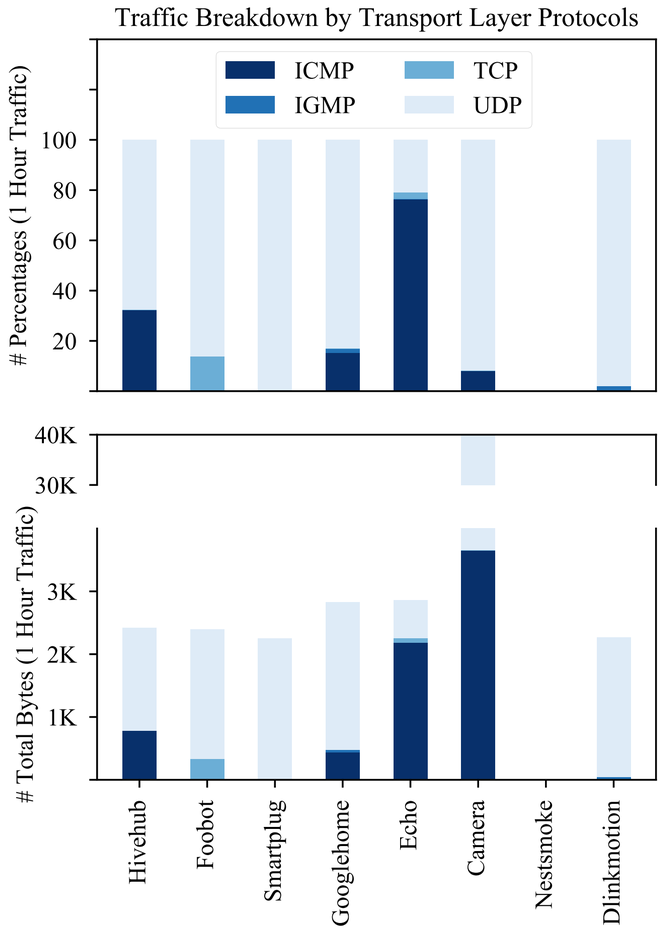
- Breakdown by protocols
  - Application layer protocols
  - Transport layer protocols
- Traffic pattern time-series analysis
- Protocol and service dependency

Yadav et al, “Network service dependencies in commodity internet-of-things devices”, ACM IoTDI, 2019.

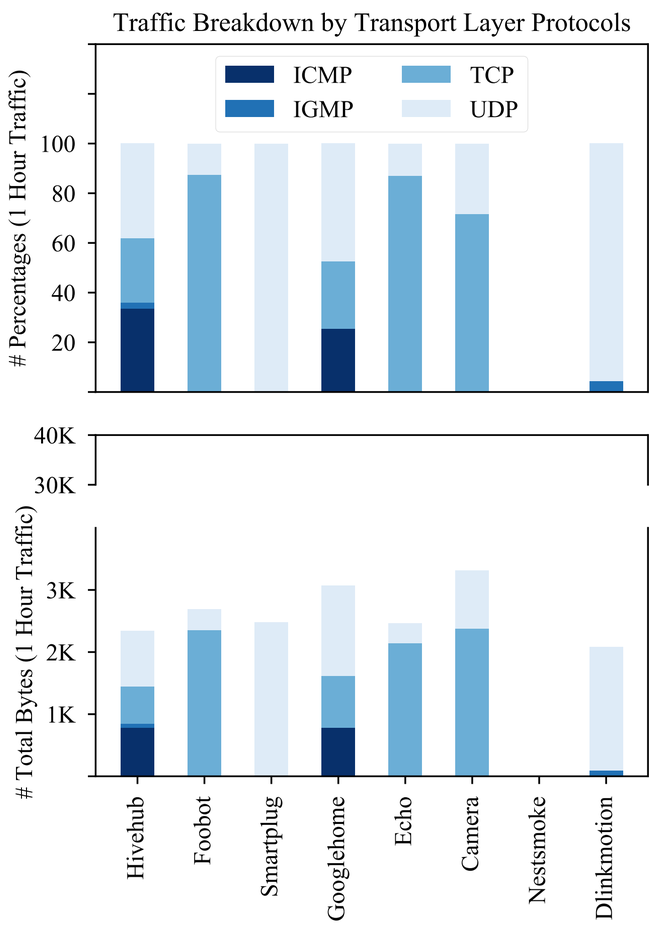
Analyses: Behaviour Under Disruption

	State	Internet	Local router	Devices
#1	Steady state	On	On	On
#2	Internet disconnected	Off	On	On
#3	Internet resumed	On	On	On
#4	Router power-off	Off	Off	On
#5	Router power-on	Off	On	On
#6	Internet resumed	On	On	On
#7	Device restarted	On	On	Off→On

Analyses: Behaviour Under Disruption

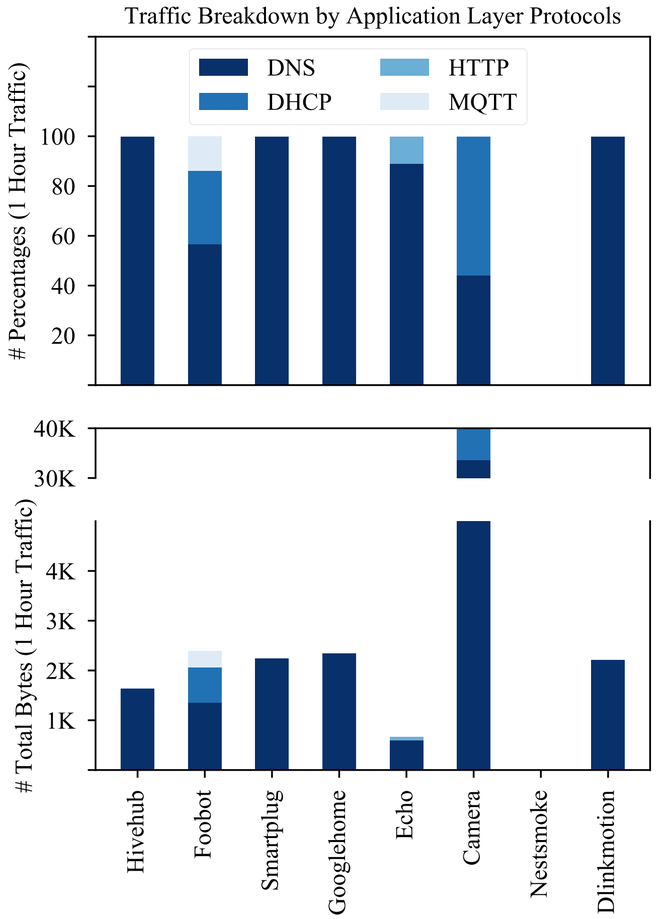


(#1 -> #2)

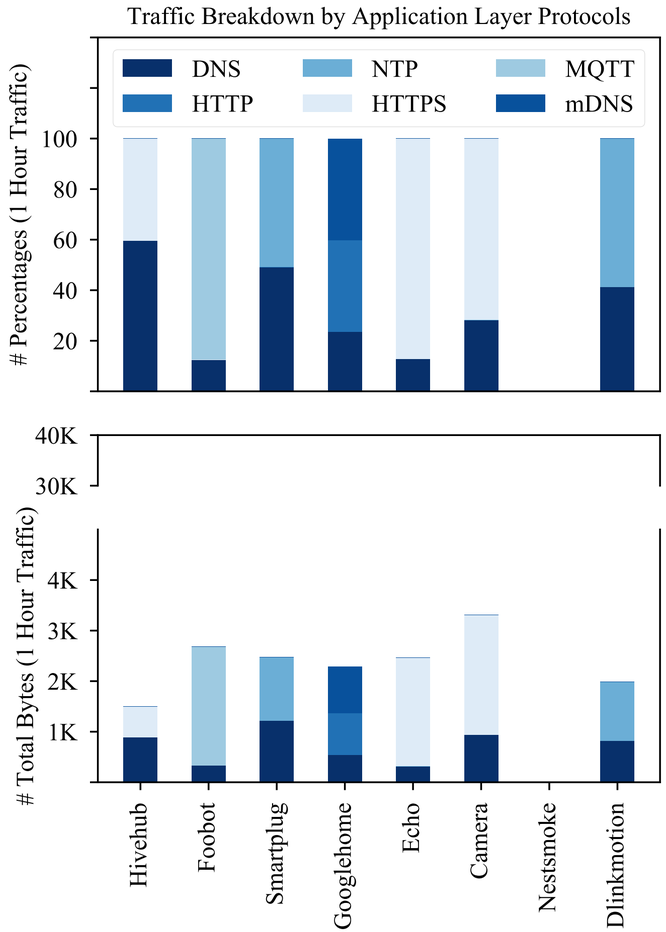


(#2 -> #3)

Analyses: Behaviour Under Disruption



(#1 -> #2)

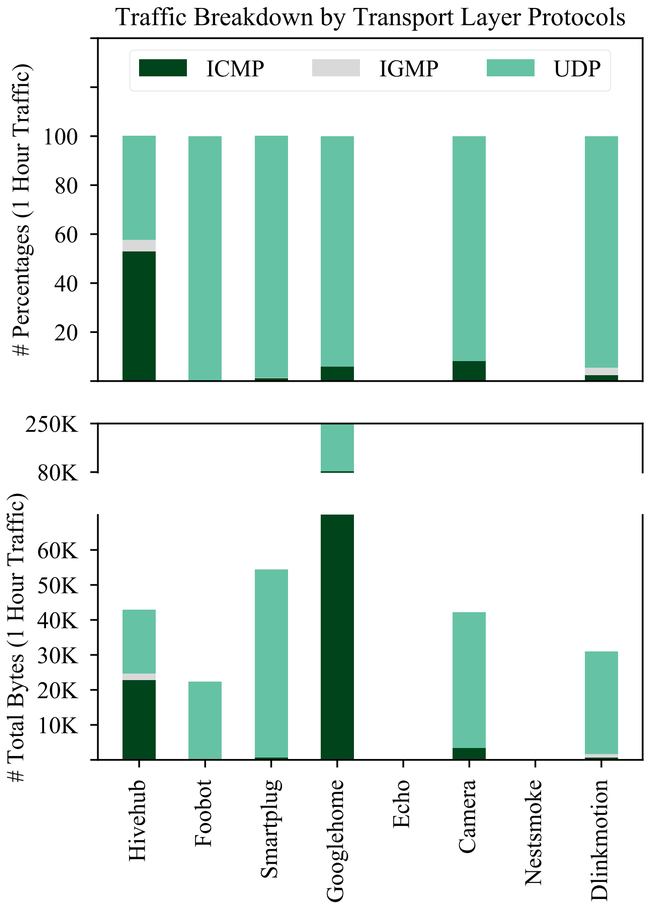


(#2 -> #3)

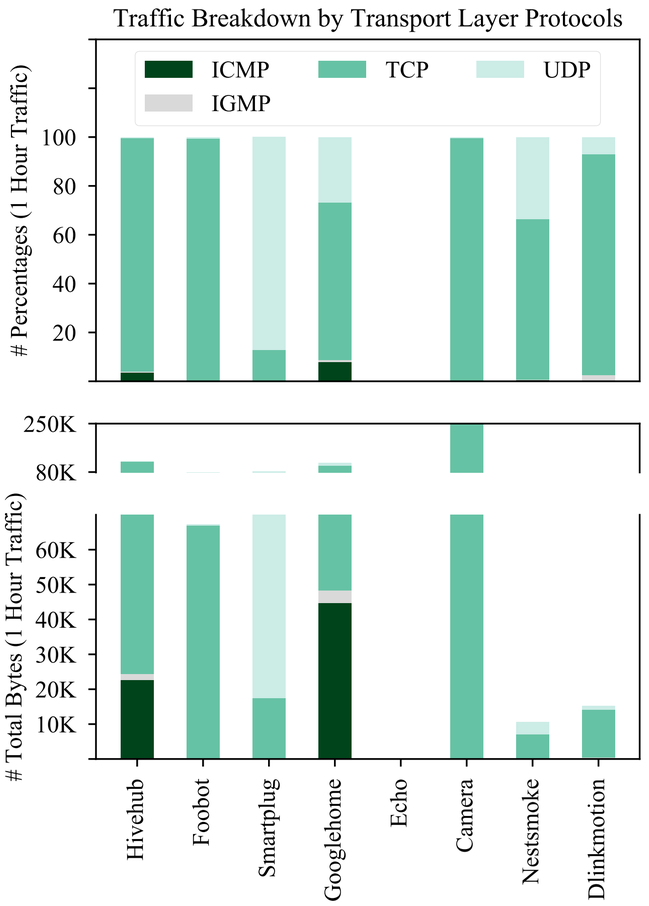
Analyses: Behaviour Under Disruption

	State	Internet	Local router	Devices
#1	Steady state	On	On	On
#2	Internet disconnected	Off	On	On
#3	Internet resumed	On	On	On
#4	Router power-off	Off	Off	On
#5	Router power-on	Off	On	On
#6	Internet resumed	On	On	On
#7	Device restarted	On	On	Off→On

Analyses: Behaviour Under Disruption

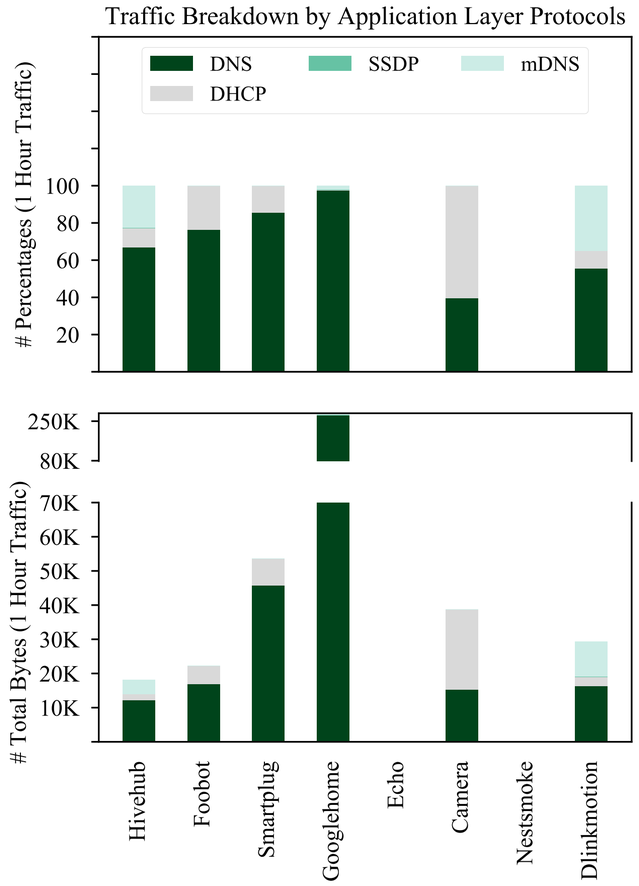


(#4 -> #5)

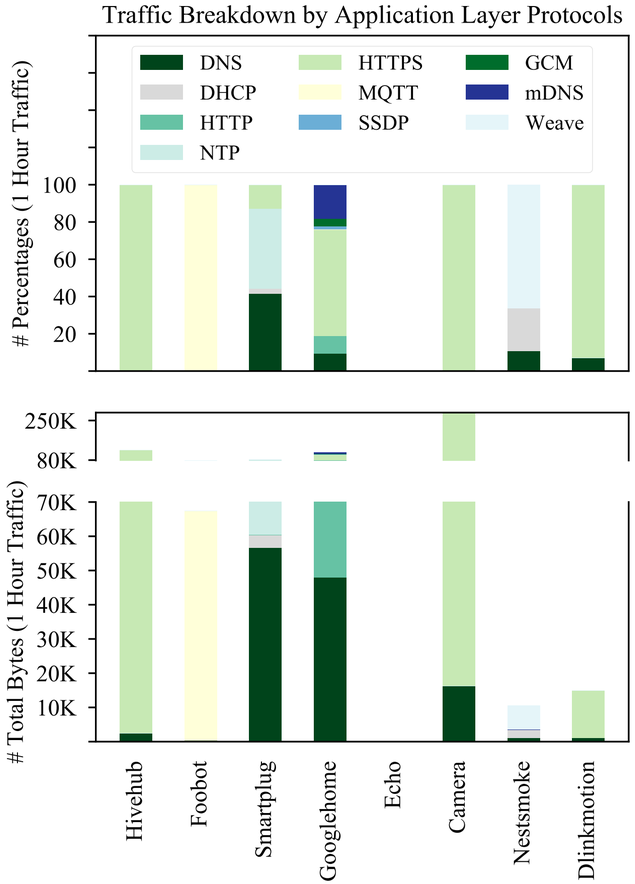


(#5 -> #6)

Analyses: Behaviour Under Disruption



(#4 -> #5)

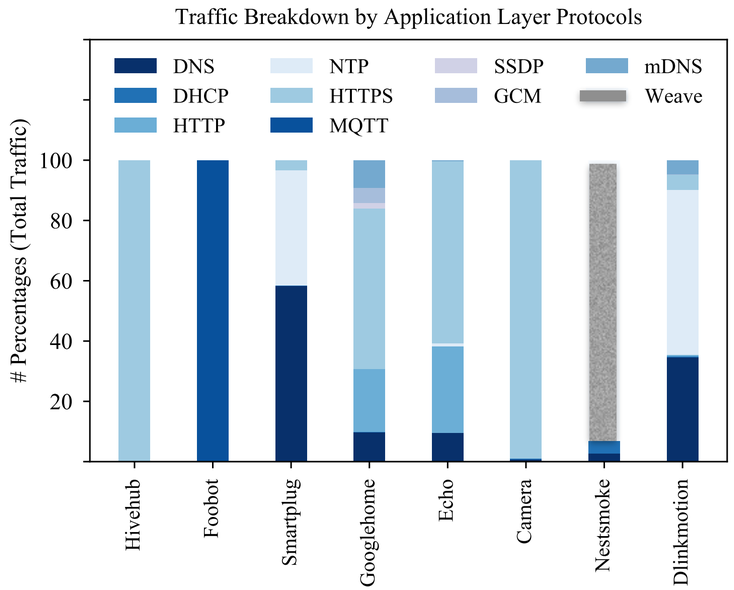


(#5 -> #6)

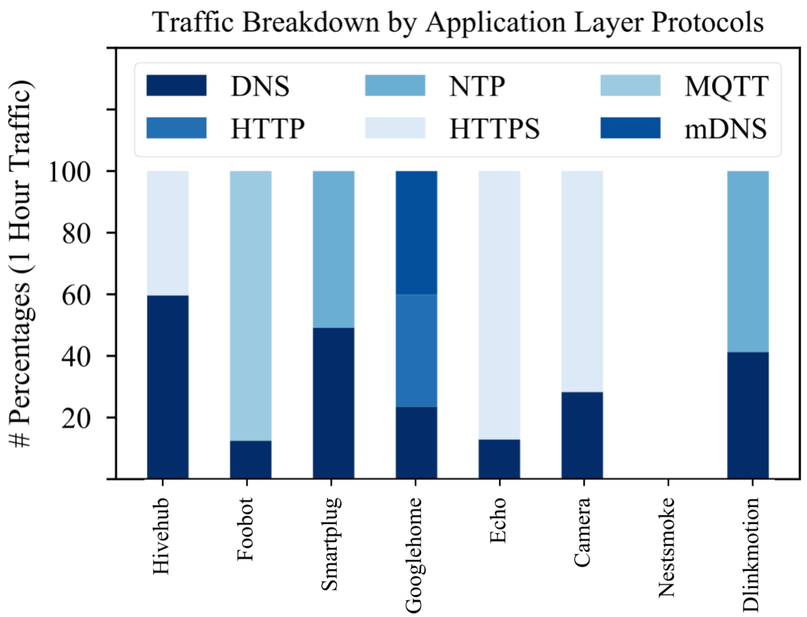
Analyses: Behaviour Under Disruption

	State	Internet	Local router	Devices
#1	Steady state	On	On	On
#2	Internet disconnected	Off	On	On
#3	Internet resumed	On	On	On
#4	Router power-off	Off	Off	On
#5	Router power-on	Off	On	On
#6	Internet resumed	On	On	On
#7	Device restarted	On	On	Off→On

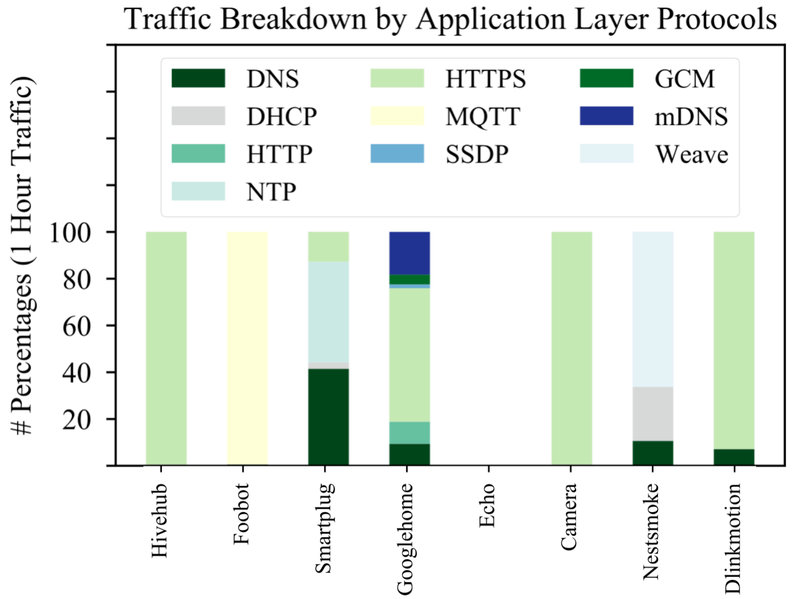
Analyses: Behaviour Under Disruption



(#1)



(#3)

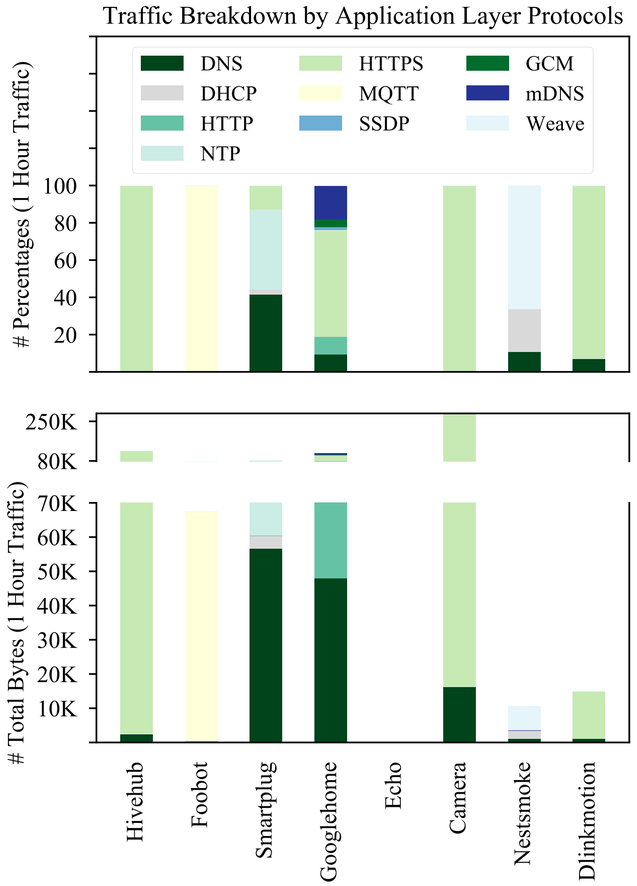


(#6)

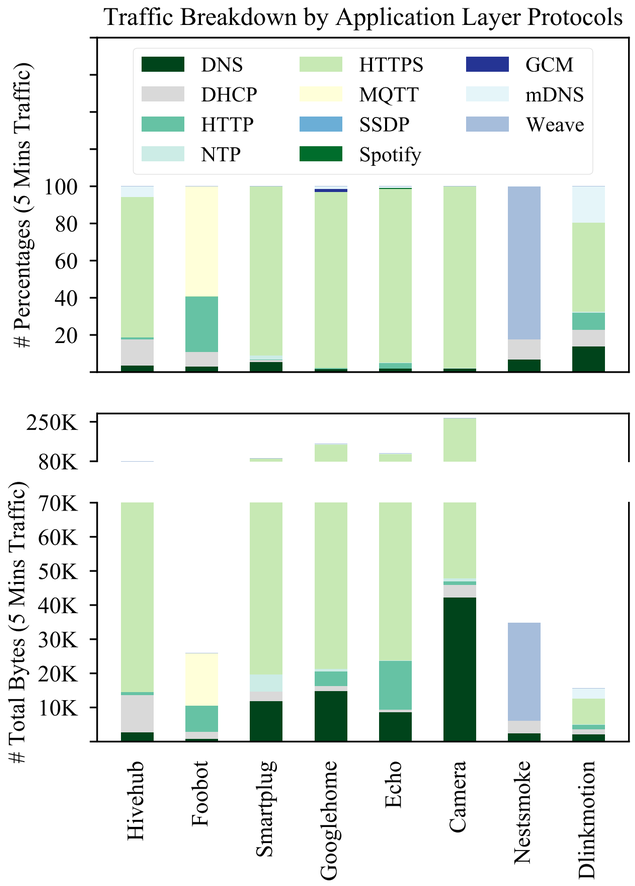
Analyses: Behaviour Under Disruption

	State	Internet	Local router	Devices
#1	Steady state	On	On	On
#2	Internet disconnected	Off	On	On
#3	Internet resumed	On	On	On
#4	Router power-off	Off	Off	On
#5	Router power-on	Off	On	On
#6	Internet resumed	On	On	On
#7	Device restarted	On	On	Off→On

Analyses: Behaviour Under Disruption

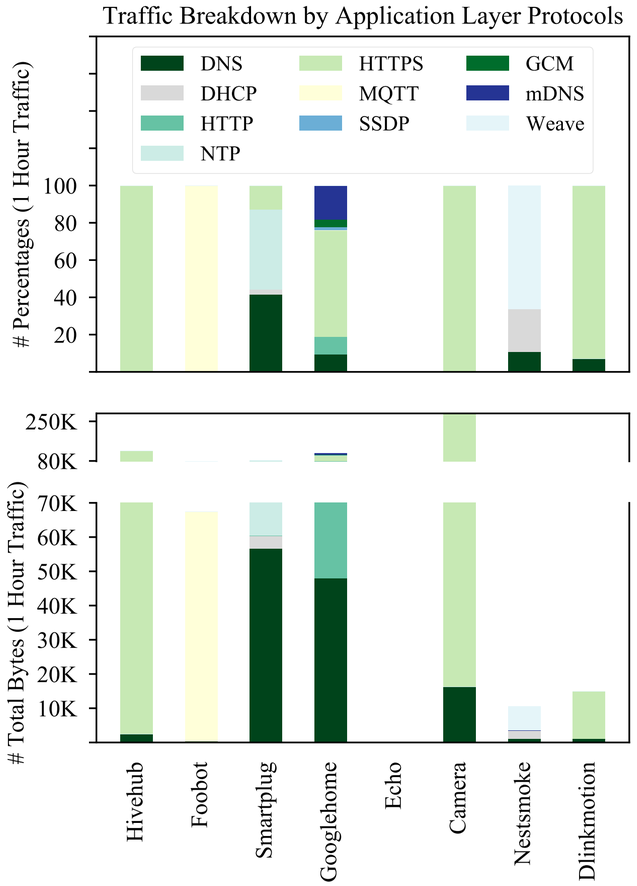


(#6) 1 hour data

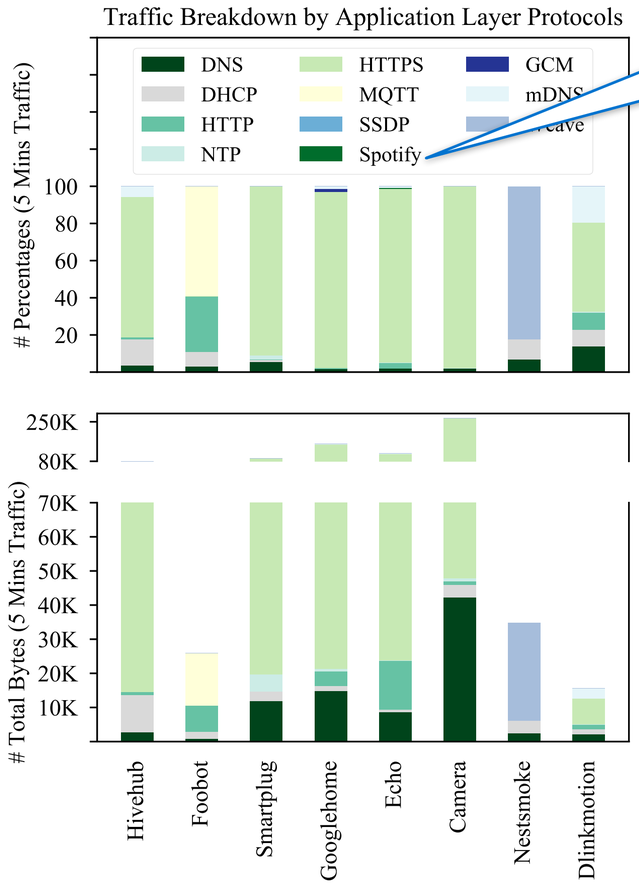


(#7) 5 Mins data

Analyses: Behaviour Under Disruption



(#6) 1 hour data



Echo traces showed new protocol & port

(#7) 5 Mins data

Going forward…

- How can we decouple IoT minimum functionality from Internet services and not only build but also test robustness and resilience?

- Transparency and accountability of the internet service dependency
    - IETF MUD specifications
    - Vulnerability disclosure framework
    - Device lifetime management as a service

poonam.yadav@cl.cam.ac.uk **@pooyadav**

richard.mortier@cl.cam.ac.uk **@mort___**