Providing Security for Wireless Community Networks

Milena Radenkovic, **Heidi Howard**, Jon Crowcroft,
Murray Goulden, Christian Greiffenhagen,
Derek McAuley, Richard Mortier

Workshop on Participatory Networks and Privacy:
New Research Issues - 12th September 2013

Global Digital Divide

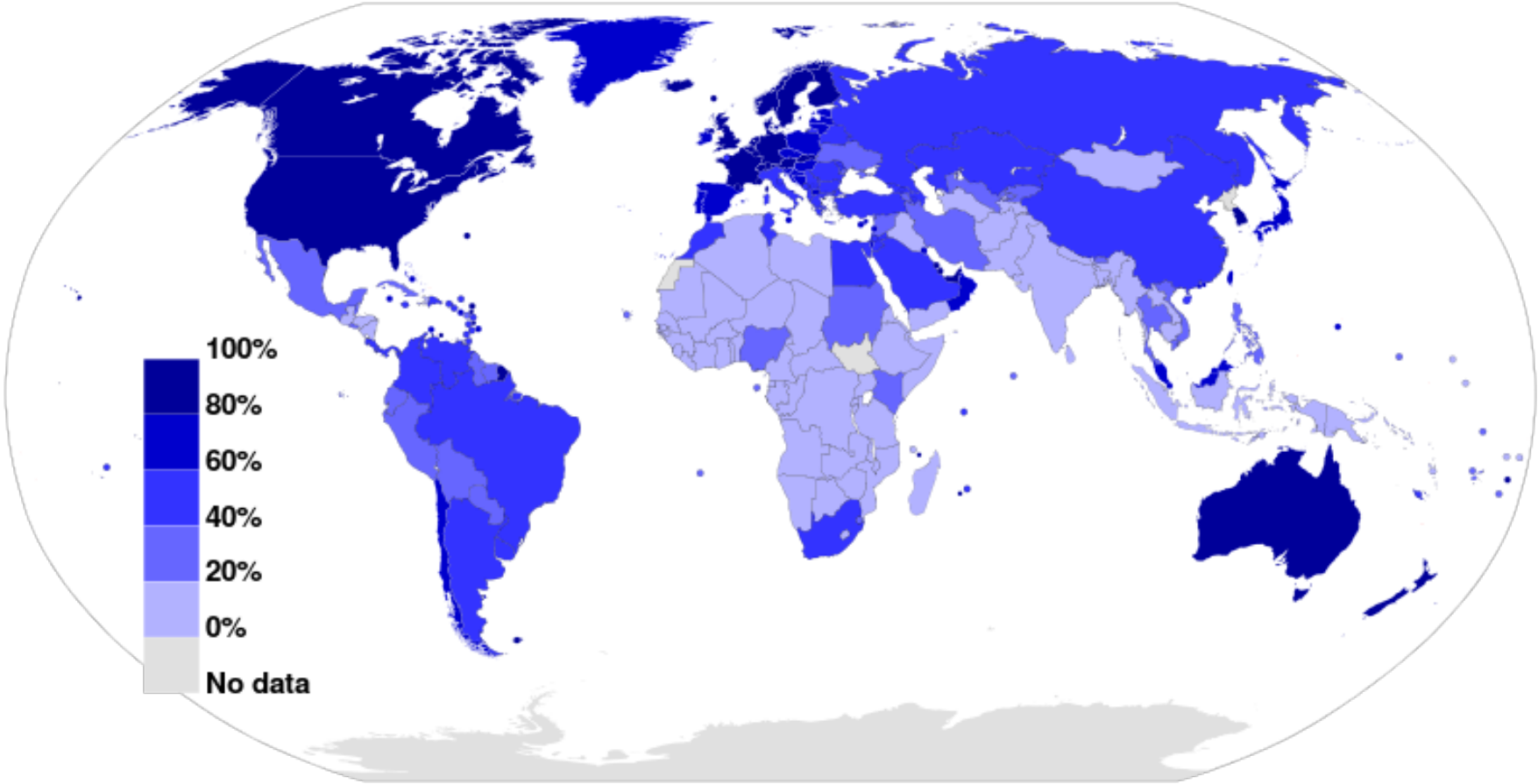


Figure: Internet penetration as a percentage of a country's population (ITU, June 2012)

National Digital Divide

13 % of people in UK do not have internet access, but why?

Reason	Percent
Don't need the internet	54
Lack of Skills	22
Equipment cost too high	15
Other	15
Access costs too high	14
Internet access elsewhere	8
Privacy/Security concerns	4
Disability	3

Figure: Reasons for households not having Internet access (Office for National Statistics, August 2012)

Local Digital Divide

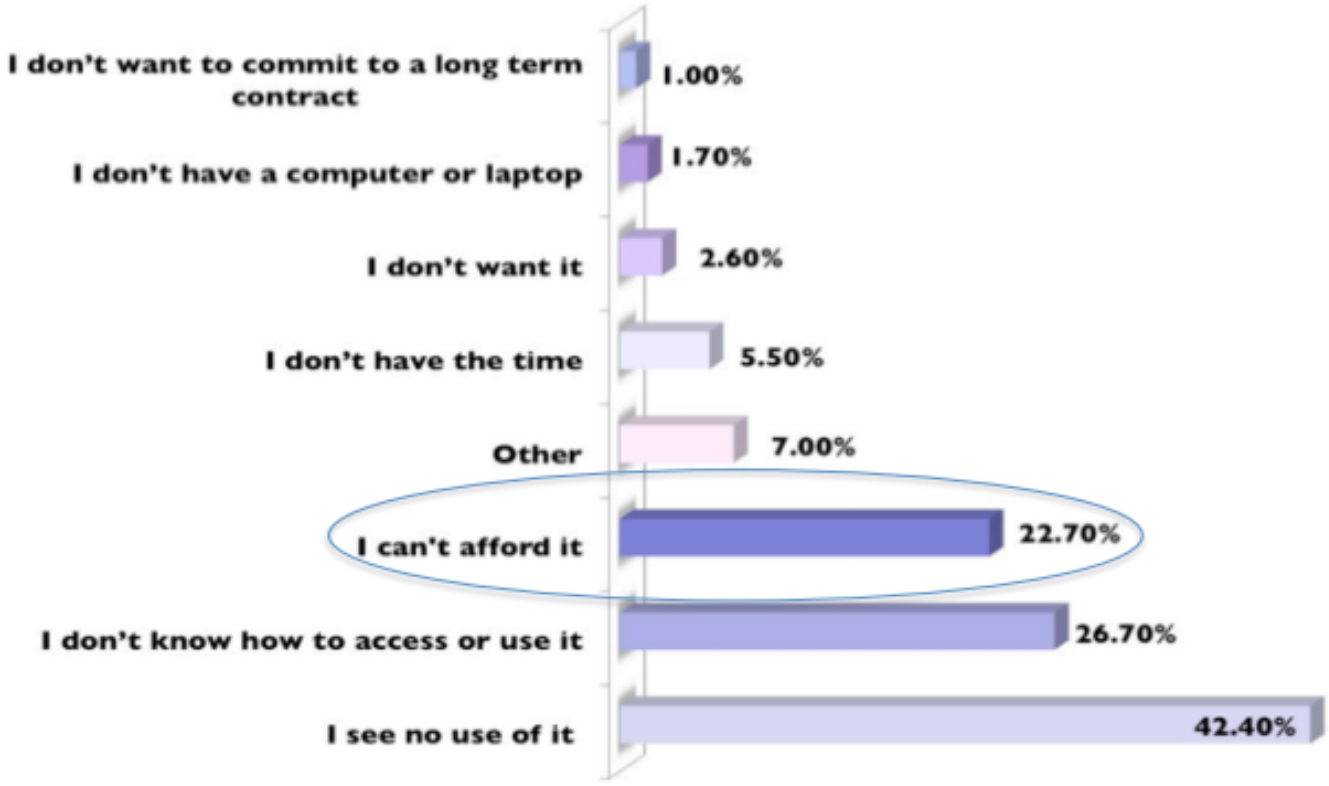


Figure: Internet penetration as a percentage of a country's population (Nottingham Citizens Survey, 2011)

Local Digital Divide

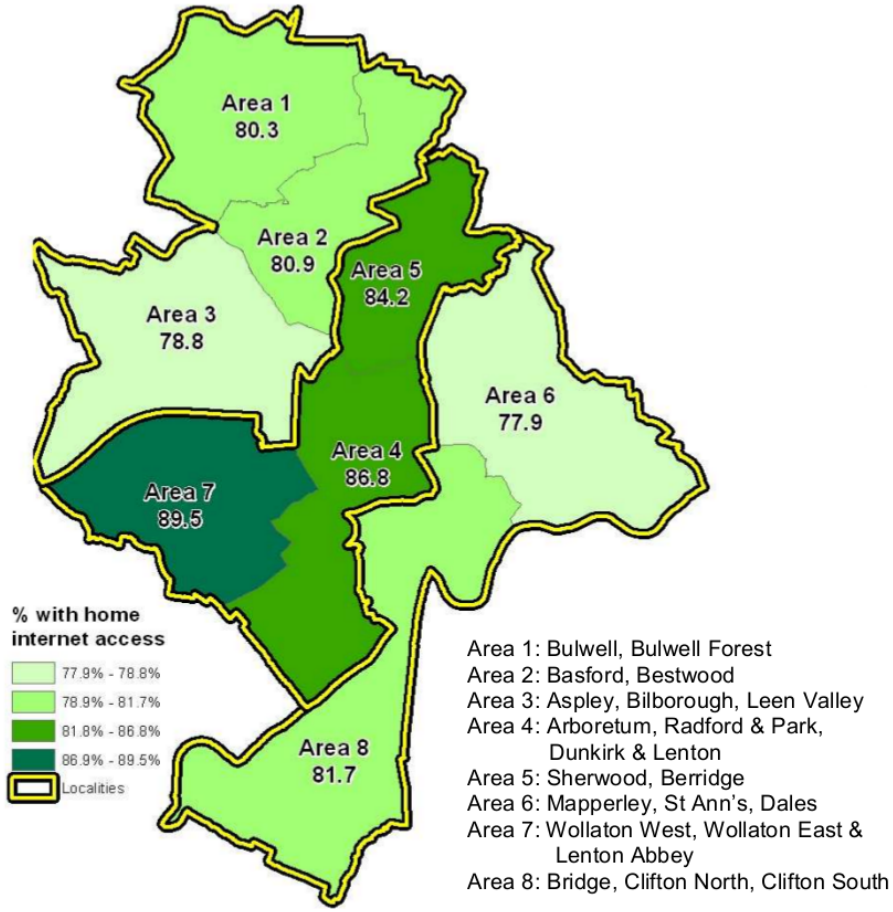


Figure: Proportion of respondents to citizens survey with access to the internet (Nottingham Citizens Survey, 2012)

Local Digital Divide

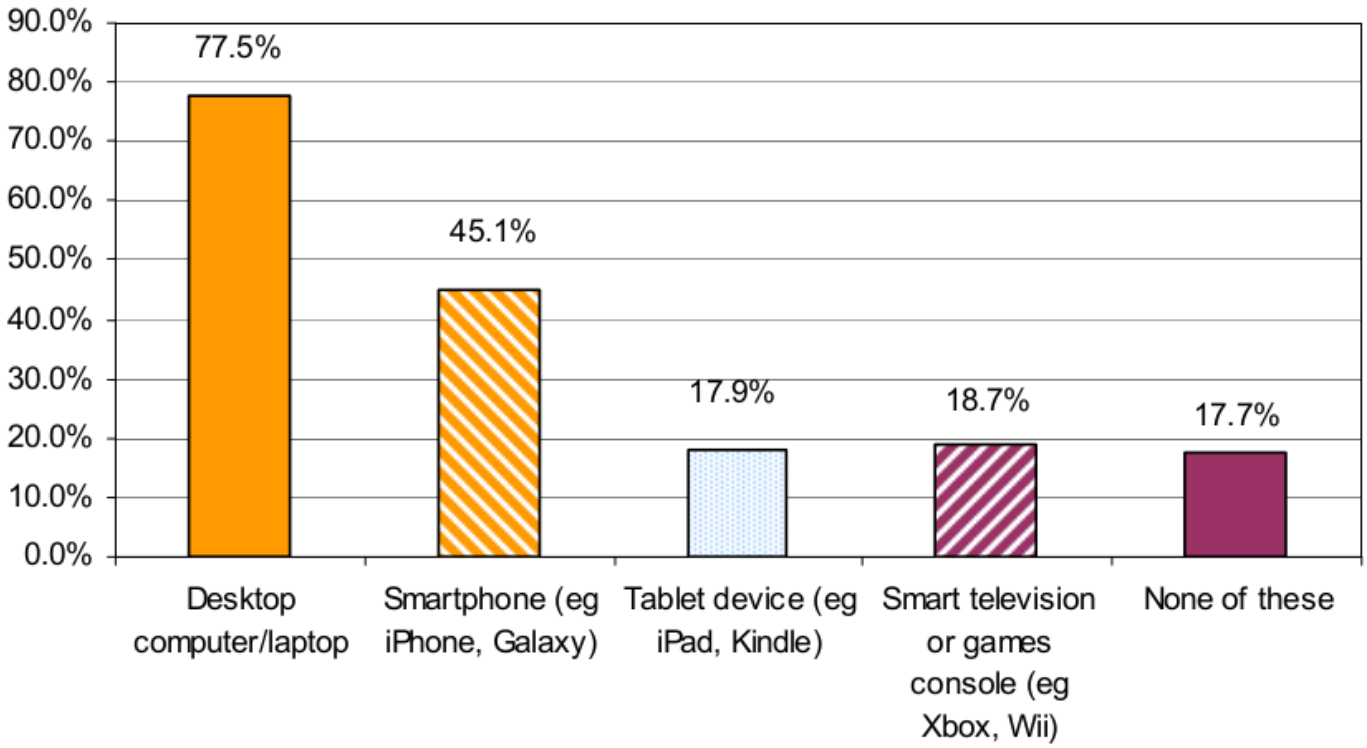


Figure: Methods of accessing the internet (Nottingham Citizens Survey, 2012)

Lowest Cost Denominator Network

Lowest Cost Denominator Networking introduces a new level of basic access, bridging the gap between no access and full access. Offering less than best effort access to all

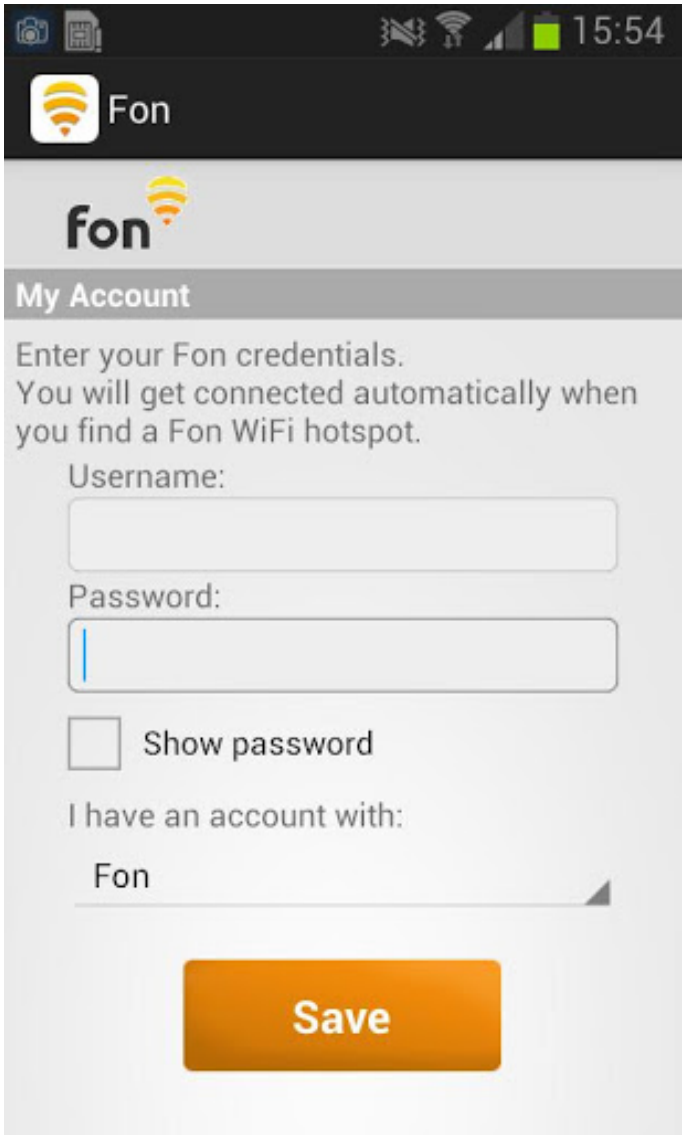
Wireless Community Networks

Co-operates where you share your WiFi and in turn can use other's WiFi. Fon is the most popular WCN, with 11.6 million Fon hotspots worldwide.

Fon members share their broadband via a dedicated Fon router: either purchased from Fon or provided by the ISP

Fon router replaces home router, providing 2 VWANs: an encrypted one for the home user and an open one for Fon members, priority is given to the home users

Wireless Community Networks



Fon members connect to the open "FON" network and enter credentials into a web-based captive gateway or via a mobile app.
Fon demonstrates that people are willing to share their internet connection but this doesn't help with digital exclusion.

Introducing PAWS

Public Access Wifi Service (PAWS) is a WCN, enabling members of the community to share their unused broadband capacity with neighbours over WiFi, this part is simple, the challenge is providing:

- Confidentiality, Integrity & Availability
- Ease of Use
- Priority
- Authentication, Authorization & Accounting
- Scalability

Ease of Use

How can we enable sharers to open up their networks? Challenges:

- Home routers are provided by ISPs, plugged in and left on default settings
- Sharers may have forgotten admin passwords
- Sharers will not want to reconnect all their devices
- Sharers have a range of routers, some act as modems

Approaches:

- Re-configure sharer's home router
- Replace the sharer's router
- Add a dedicated router to the sharer's network
- Software solution such as Whisper or Wi-sh

We use a dedicated Netgear WNDR3800 router running OpenWRT

Priority

We need to give capacity to PAWS users, with minimal disruption to the sharers.
Challenges:

- Our router is not the gateway router
- Fluctuation in network capacity over time
- Wide range of networks with very difference characteristics, e.g. Fiber Vs ADSL
- Data usage caps

Approaches:

- Actively measure network capacity at all times, dynamically throttle at PAWS access point
- Work with ISPs and use Quality of Service

We used Project BISmark developed at Georgia Tech to measure capacity visible to the PAWS access point and statically set throttling at the PAWS access point

Authentication

Users need to be able to authenticate themselves to the PAWS network at any of the PAWS access points

Challenges:

- Supporting a range of user devices
- Many devices OSes (such as Android and iOS) limit the application API
- Aim for support for roaming between PAWS developments
- Ease of use is key
- User may share/lose passwords, choose weak passwords, use same passwords for other applications

Approaches:

- WPA, WPA2, WPA Enterprise
- MAC address filtering
- Captive portal with user credentials

We use user credentials, authenticated by local RADIUS servers for each deployment, this could be linked to the 3rd party authentication servers

Authentication

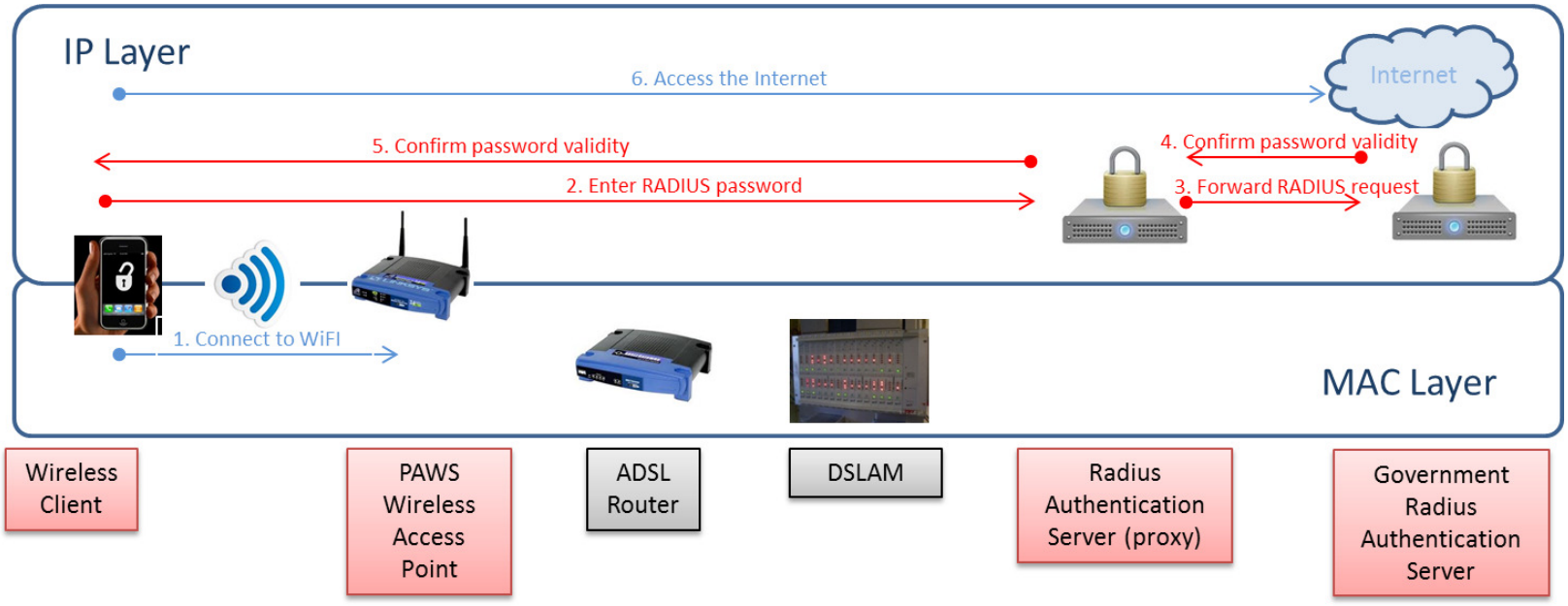


Figure: RADIUS Authentication, within a hotspot deployment

Accountability & Authorization

PAWS user traffic needs to have a separate public IP address from the sharer. Sharers must not be held accountable for users' actions online

Challenges:

- Sharers need to feel secure
- Legal issues

Approaches:

- Work with ISPs to provide sharers with dual IPs
- Keep logs of all traffic sent, MAC associations with the PAWS access point
- VPN traffic somewhere else, to alter source IP

Using a VPN to a secure endpoint so all PAWS network traffic has a source IP distinct from the sharer's.

Confidentiality

Challenges:

- Traffic passes through the sharer's home router
- WiFi Encryption often provides weak security
- End-to-end encryption often not available
- Fake PAWS hotspots

Approaches:

- WiFi Encryption
- VPN
- Limit access only to hosts with end-to-end encryption i.e. HTTPS only
- SSL encryption

We already get this fixed for free with VPN to the user's devices

Scalability

When travelling, authentication is directed to your home authentication server and the nearest VPN server

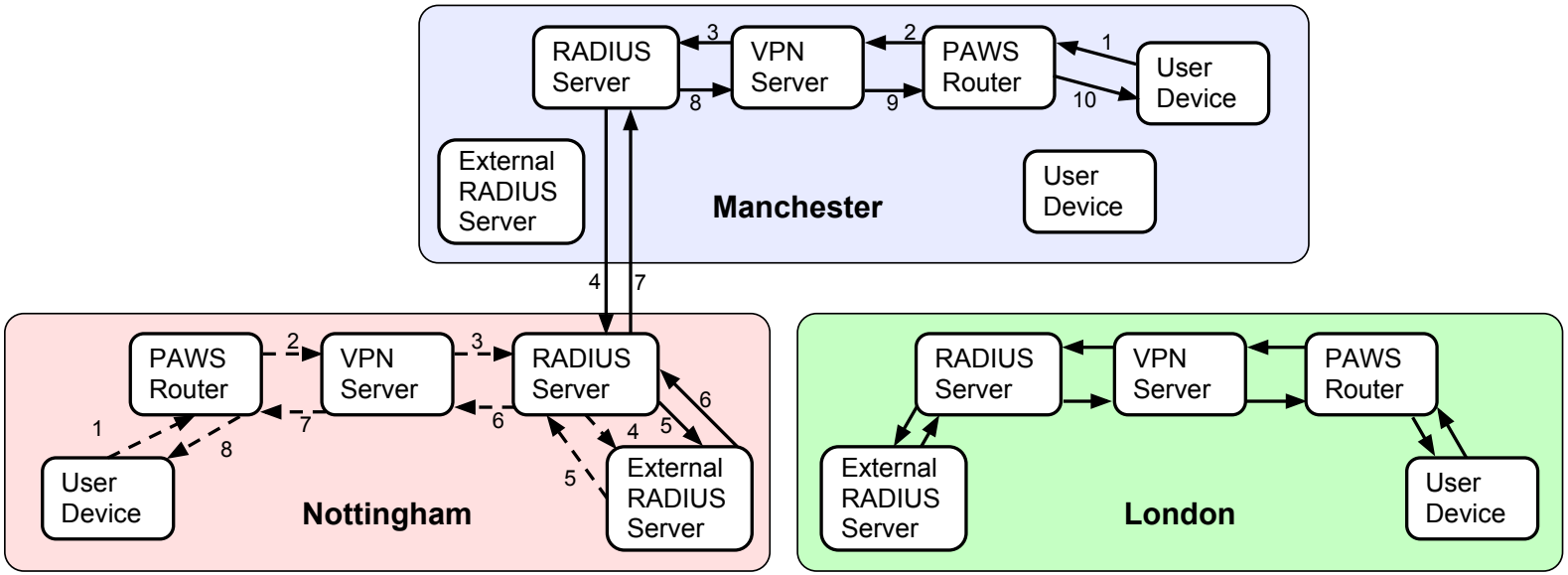


Figure: RADIUS Authentication, across a hotspot deployments

Limitations

- VPN setup on some client devices is difficult
- The most widely supported VPN is PPTP, but it's been proven insecure
- Some home routers block VPN traffic by default
- PAWS Routers currently cost £110 each
- Single point of failure, all traffic routed though VPN server
- Little incentive to share
- Throttling being too conservative
- Legal & ISPs Terms of Service

Research in the wild: Aspley, Nottingham

3 month trial

1/3 without internet access

50 new internet users 50 sharers

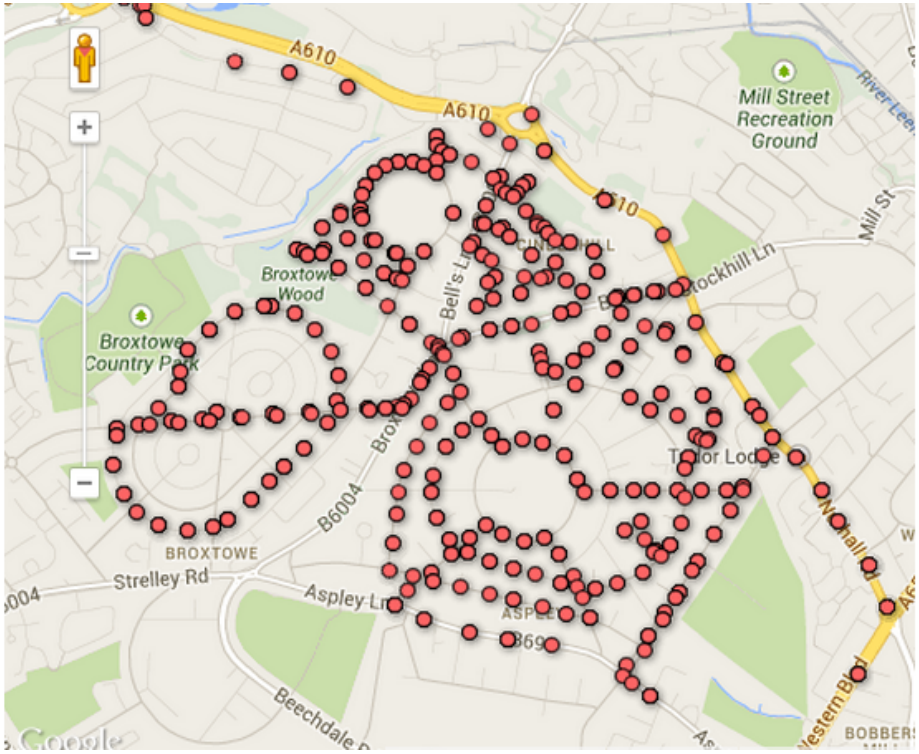


Figure: War drive data from Aspley

Research in the wild: Aspley, Nottingham

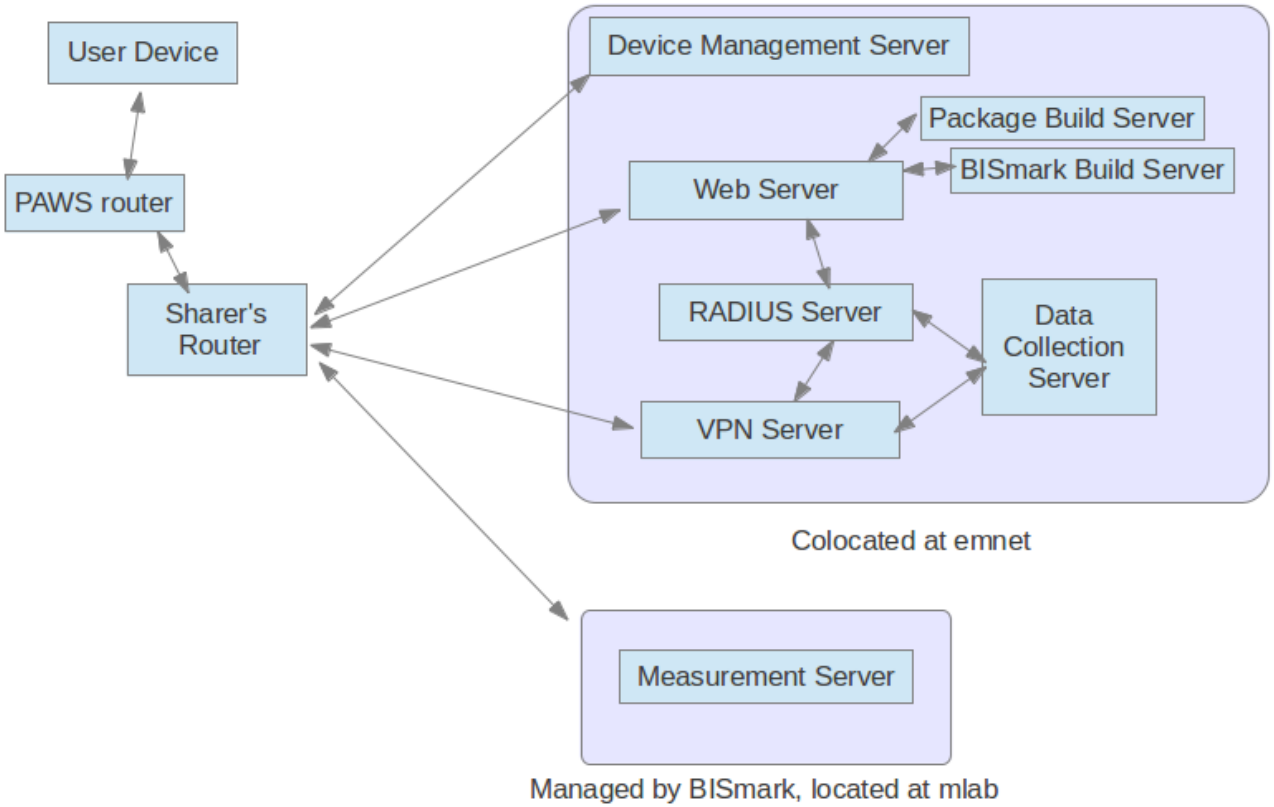


Figure: Architecture of Aspley deployment

Future Work

- Two tier system, where users who are also sharers get more bandwidth
- For users who are also sharers, use their PAWS box as the VPN endpoint instead
- VPN from PAWS AP instead of client devices, combined with WPA Enterprise from the device to PAWS AP
- Client apps to map coverage, automatically connect to VPN
- Implement fallback in PAWS access points
- Dynamic Throttling

Discussion