Fuse 5G, Utrecht
January 19th, 2024

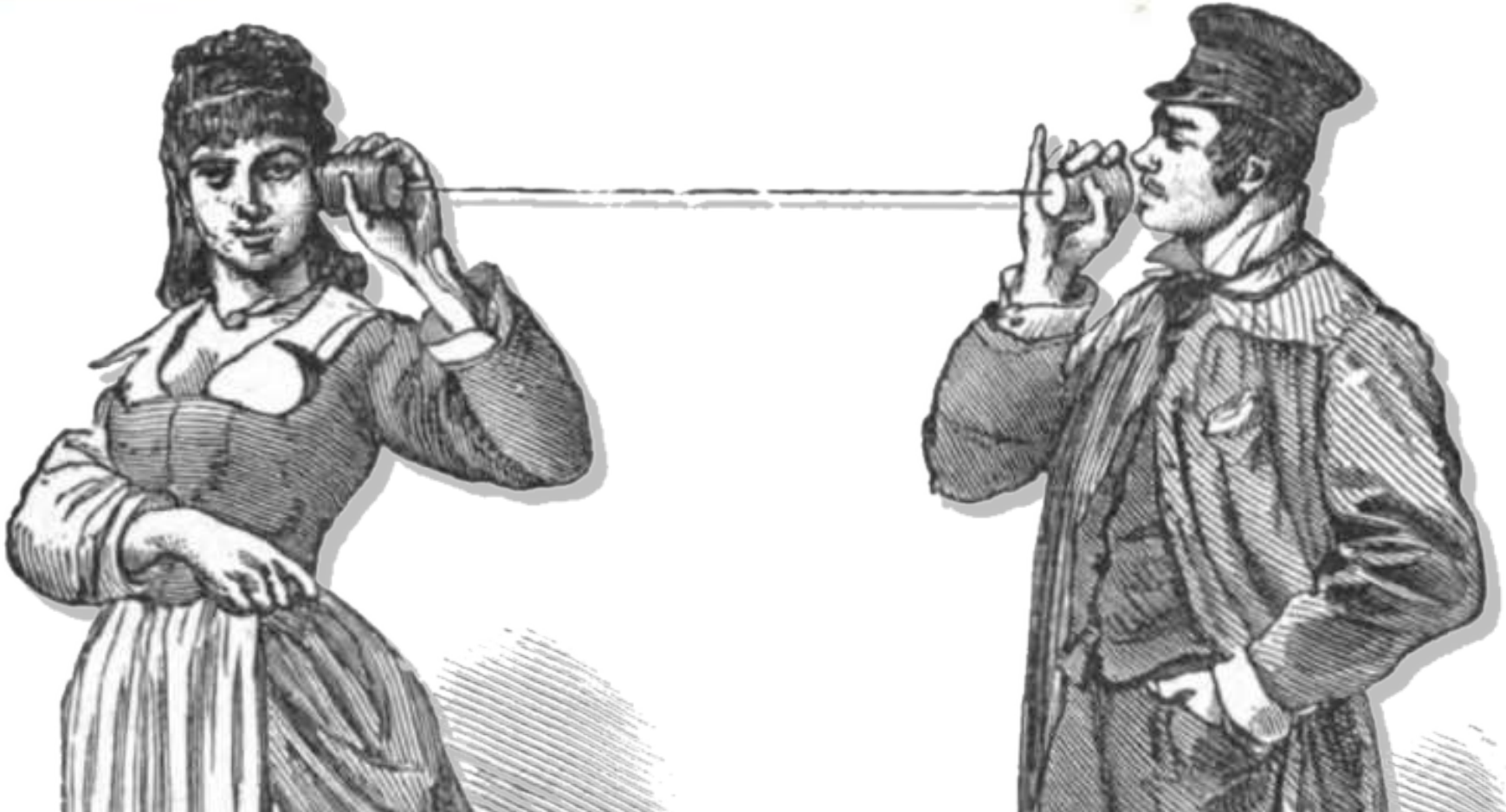
MobileAtlas: Distributed Measurement and Security Testing

Speaker: Adrian Dabrowski

Co-Authors: Gabriel Gegenhuber, Wilfried Mayer, Edgar Weippl

Three City States

From Landline ...



... to Wireless!

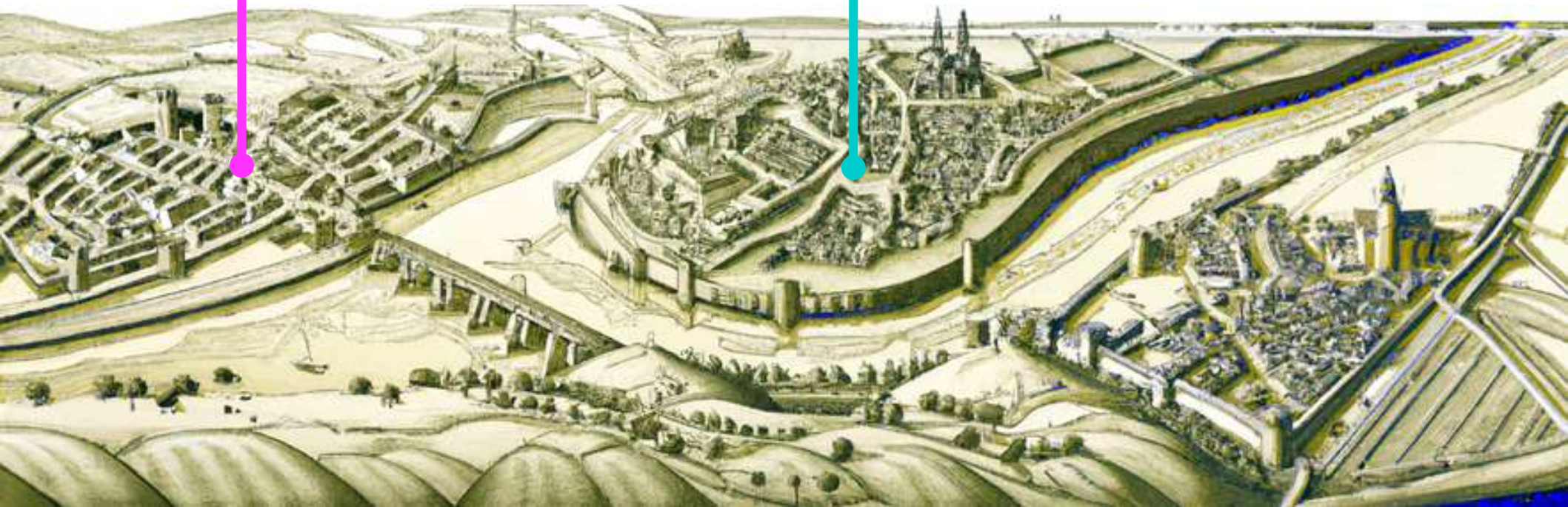
Three Major MNOs

KnighT Mobile

Three Major MNOs

KnighT Mobile

AT&X



Three Major MNOs

Three Major MNOs + more

Red-Yellow
Air

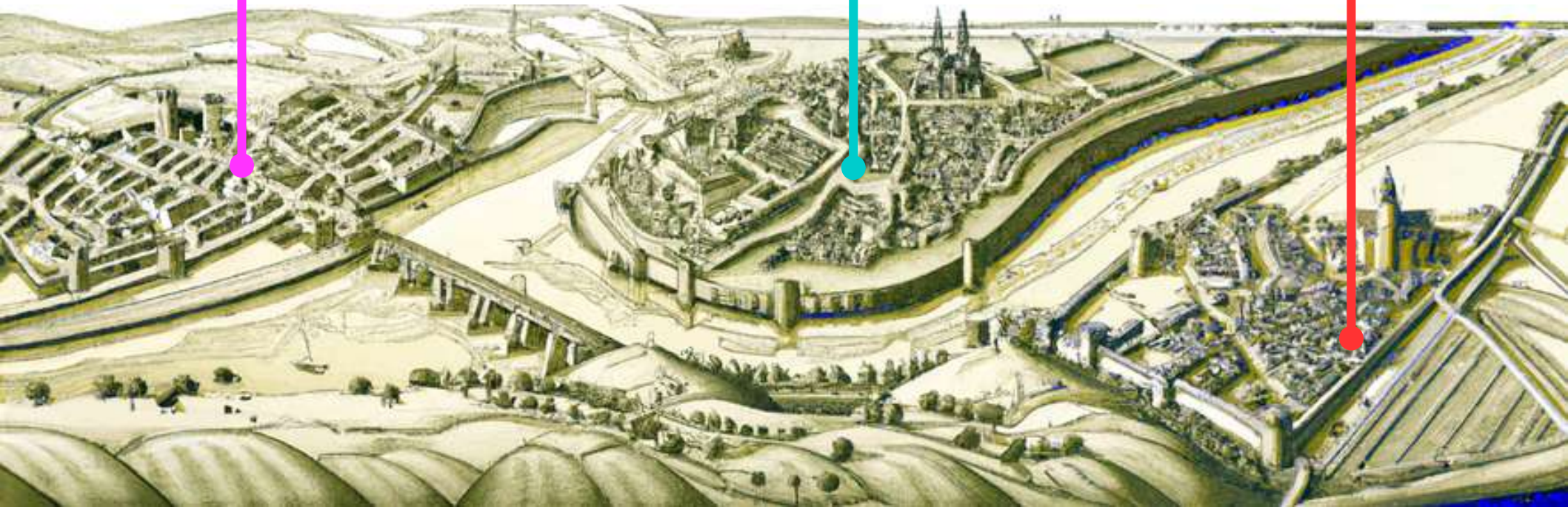
KnighT Mobile

Marathon
HelvetiaCom

AT&X

Trinity
Gentlebank

dragonfone



Social Network Explosion

RoyalTweet

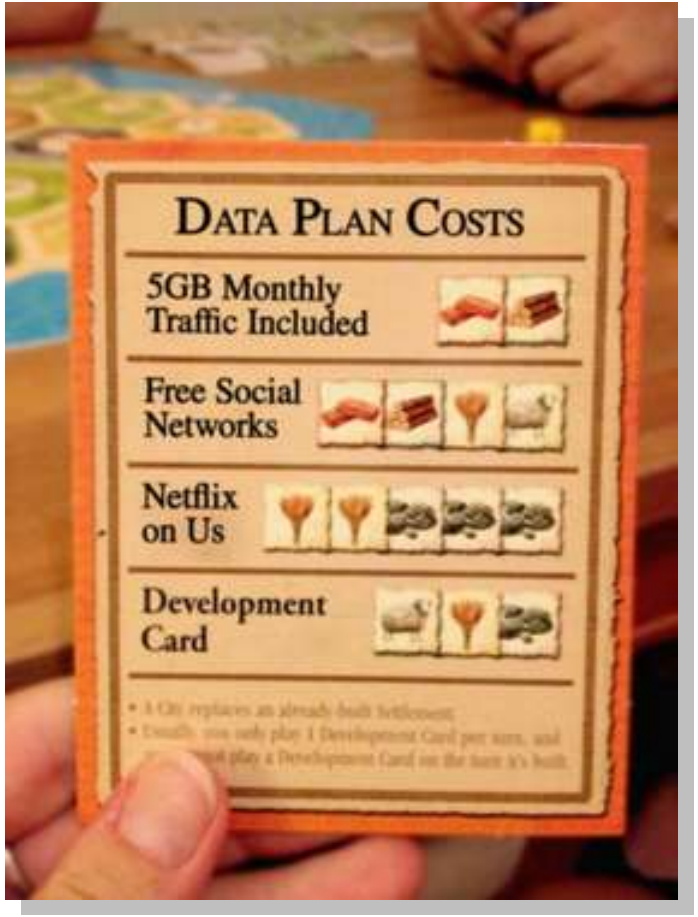
Pidgingram

JesterGram

BardBoard

PesantPost

Combos with “Free” Traffic



- Popular with certain demographics
- Monthly data allowance
  - PLUS FREE:
    - Video Streaming
    - Audio Streaming
    - Social Networks
    - ...

Real (Addictive) Transformation

This is Archibald

- Has found a traffic accounting vuln.
- Likes to visit his friends “abroad”
- Repeatedly experiences roaming oddities

Cellular (Security) Research

- “Prisoner” of geography
- Frequencies and MNOs geographically bound
- Limited number of MNOs per territory
- Many stationary cell towers

Distributed Measurements

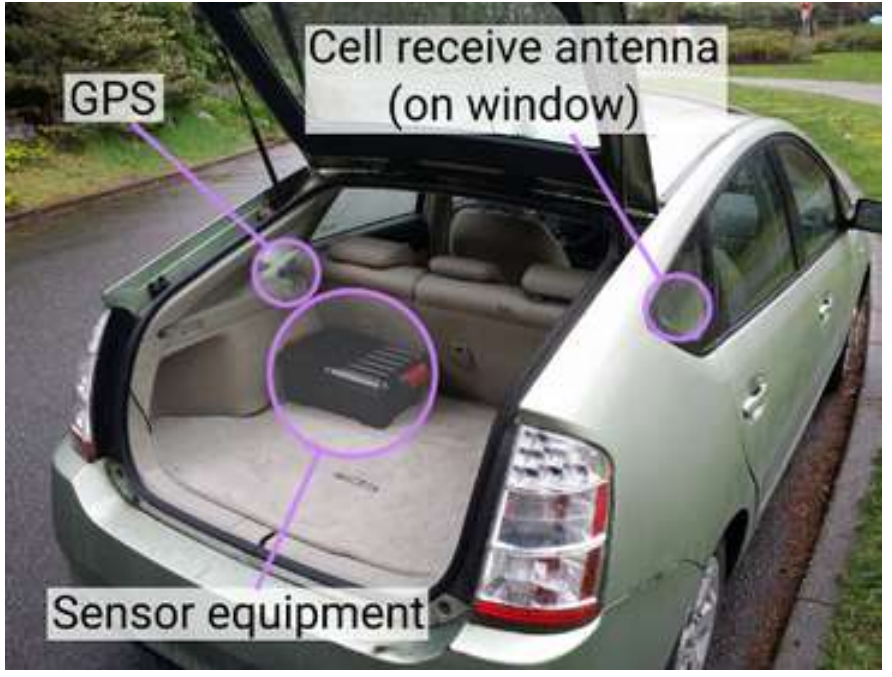
- IMSI Catcher Catcher (2014)
- SeaGlass (2017)
- Monroe (2015-2018)

IMSI Catch me if you can

- Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, Edgar Weippl
  - TU Wien, SBA Research
- Continuity ++

SeaGlass (2017)

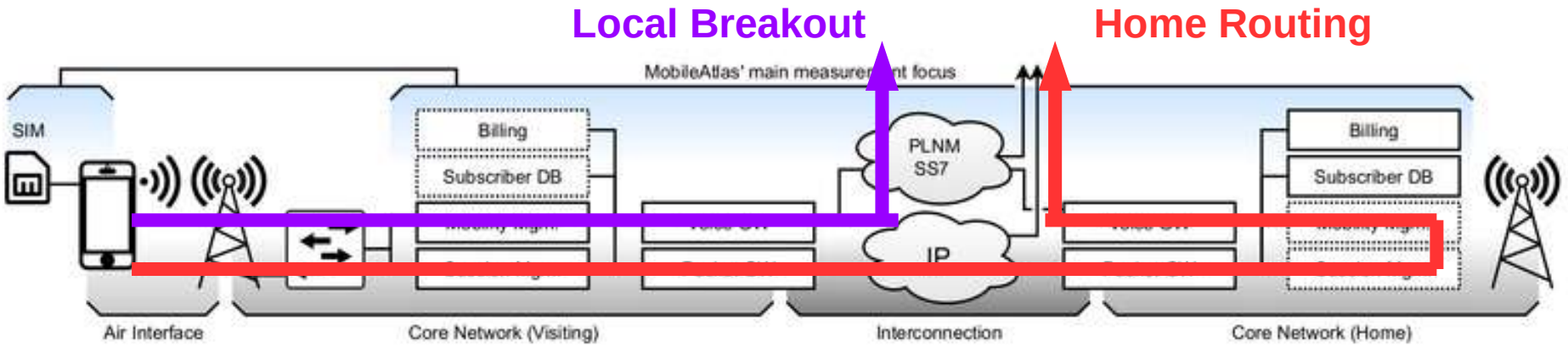
- Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno
  - University of Washington
- Mobile, In Cars
- Coverage ++



Monroe

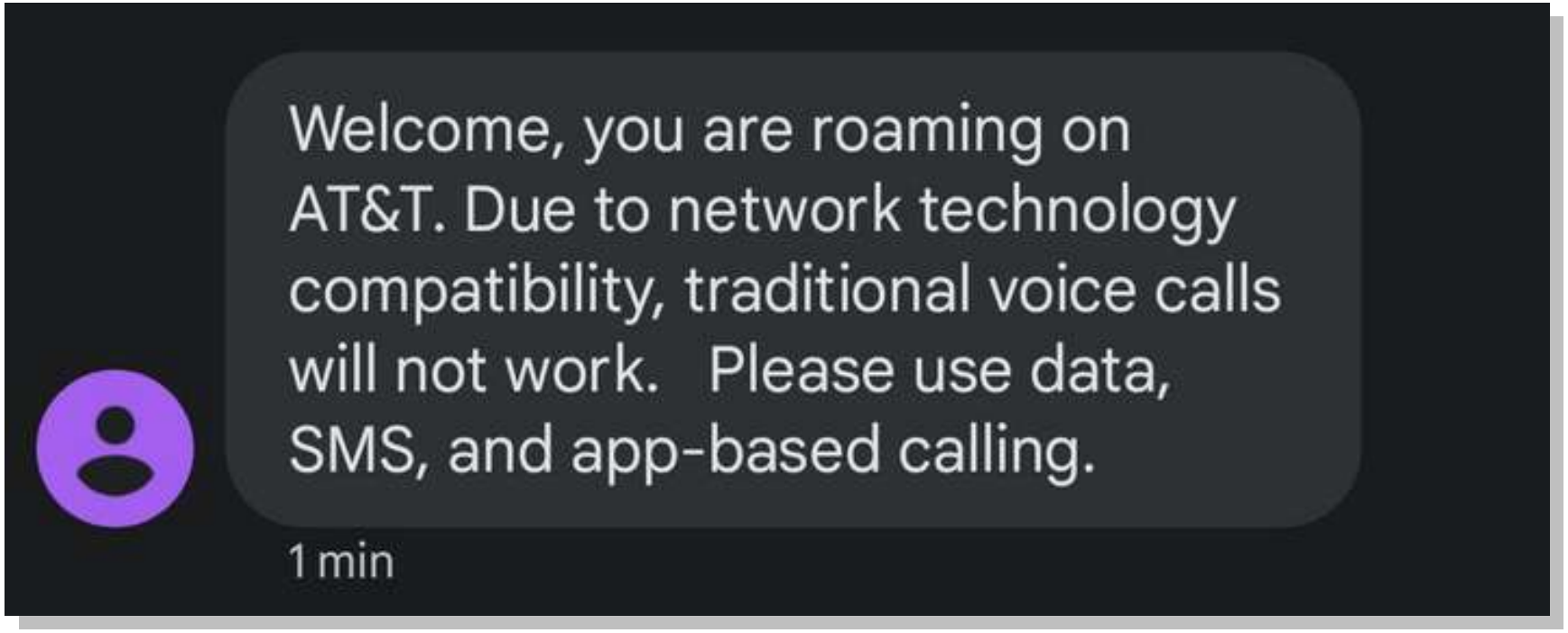
- Horizon 2020 Project
  - Simula (Norway), Imdea Networks (Spain), Karlstad University (Sweden), Politecnico Di Torino (Italy), Nextworks (Italy), Celerway Communications (Norway), Telenor (Norway)
- First Roaming Measurements

Why Roaming ~~is Complex~~ *interesting*?



- Visiting and Home network need to work together
- Some traffic passes both, other just the visiting MNO
  - Data typically uses home routing (except Travel SIMs and Google Fi)
  - Voice typically uses local breakout for latency, but with a custom CallerID

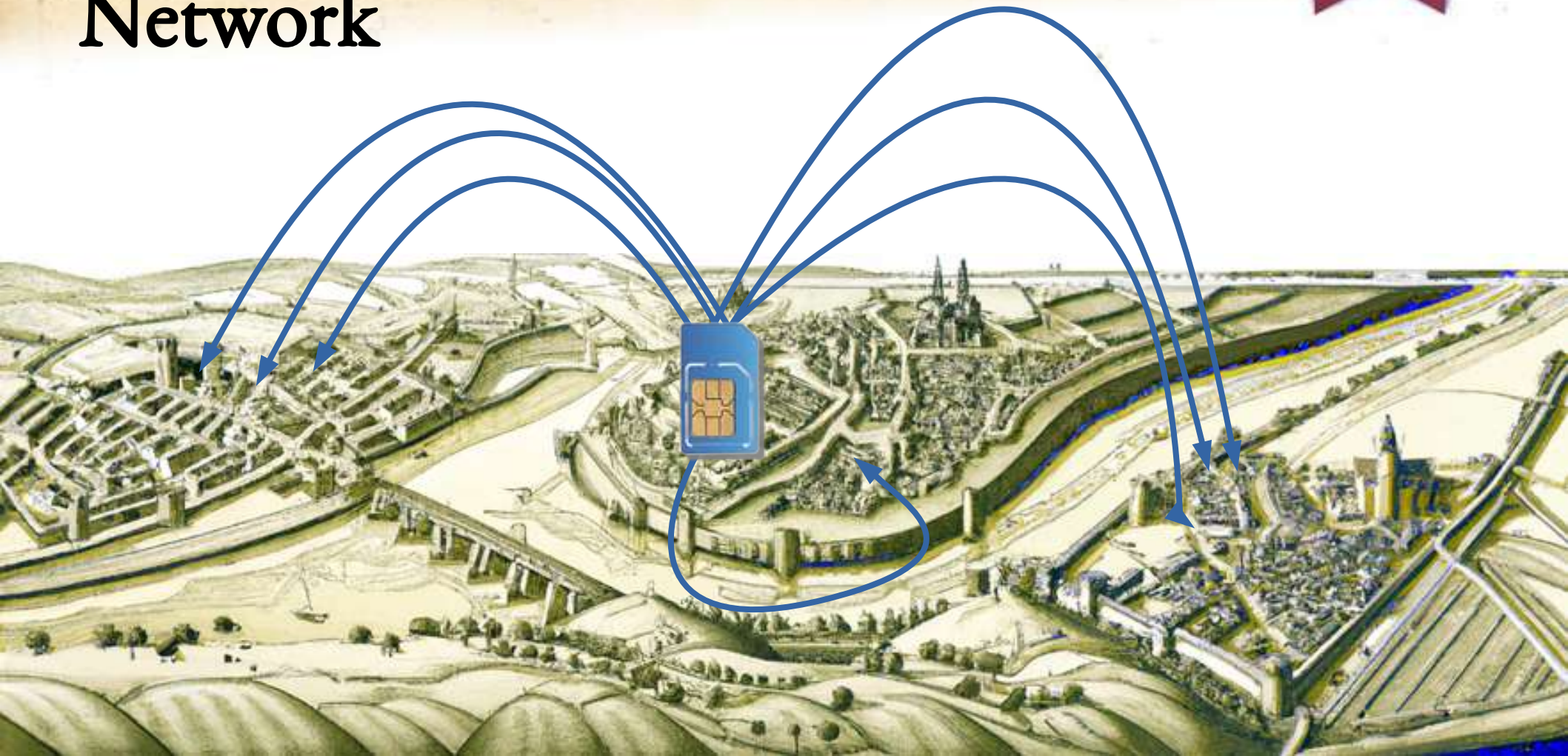
And Then, There is VoLTE's (Non-)Roaming...



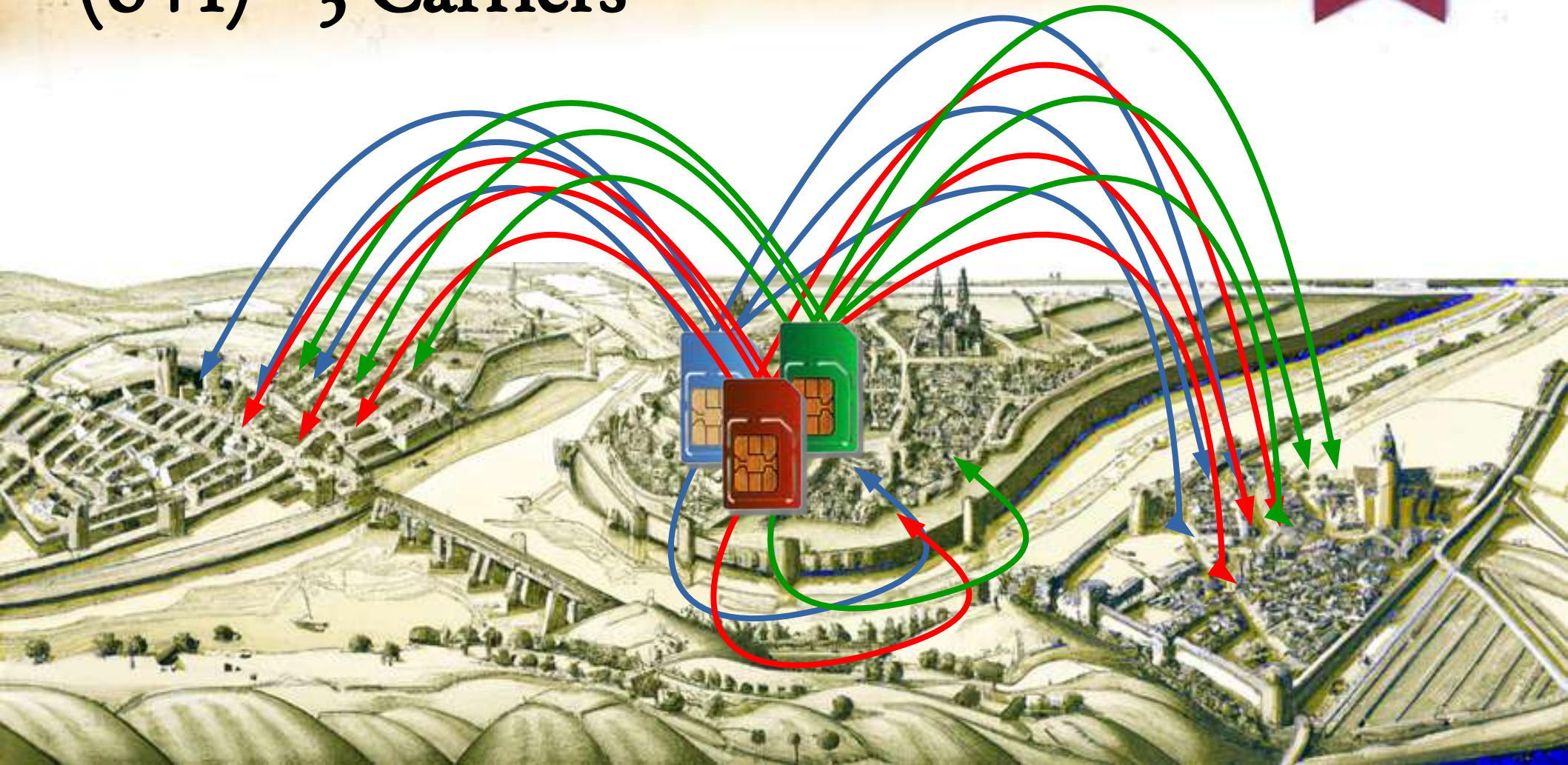
Archibald likes to travel

#wanderlust

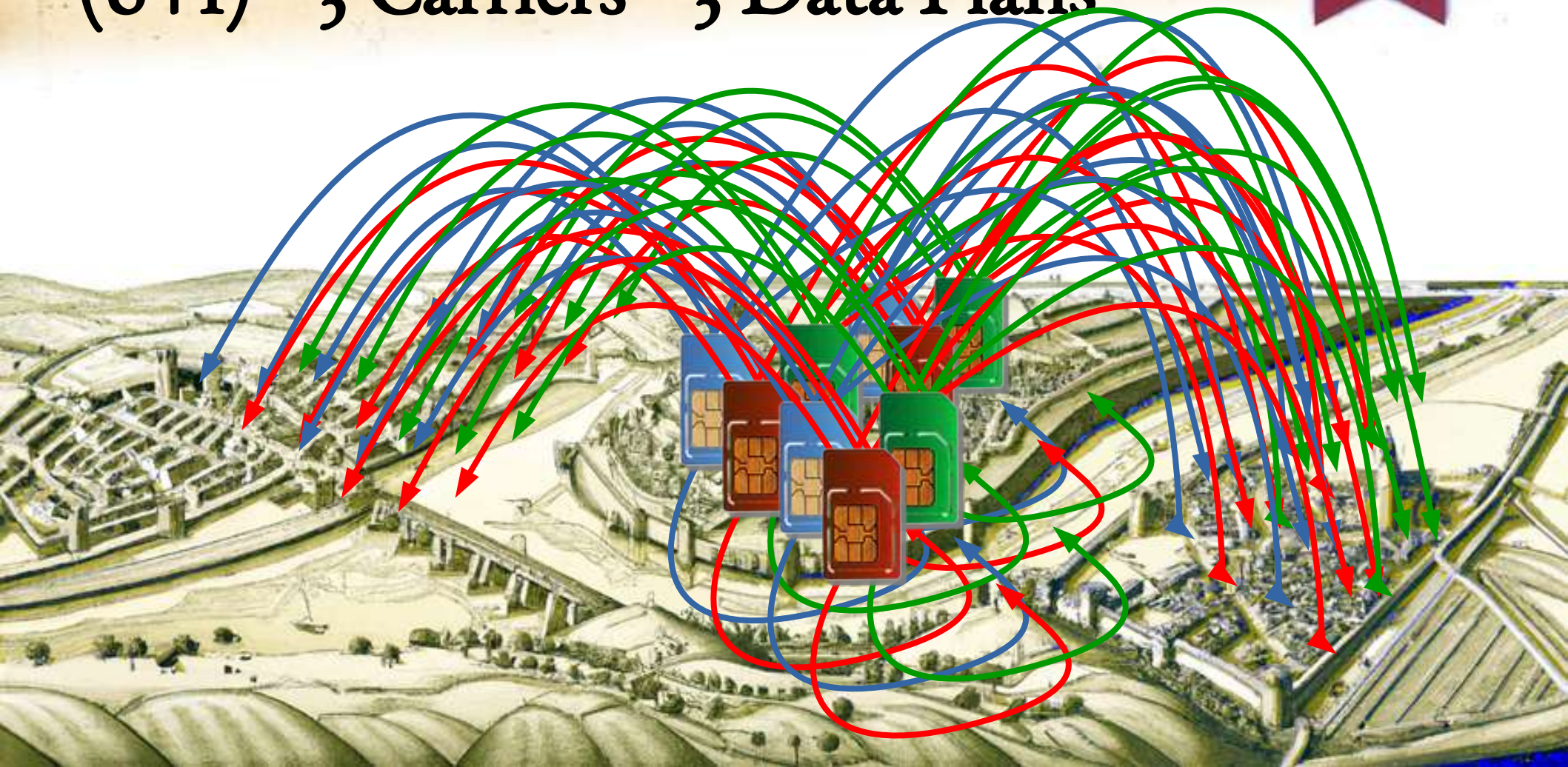
One SIM has 6 Roaming + 1 Home Network



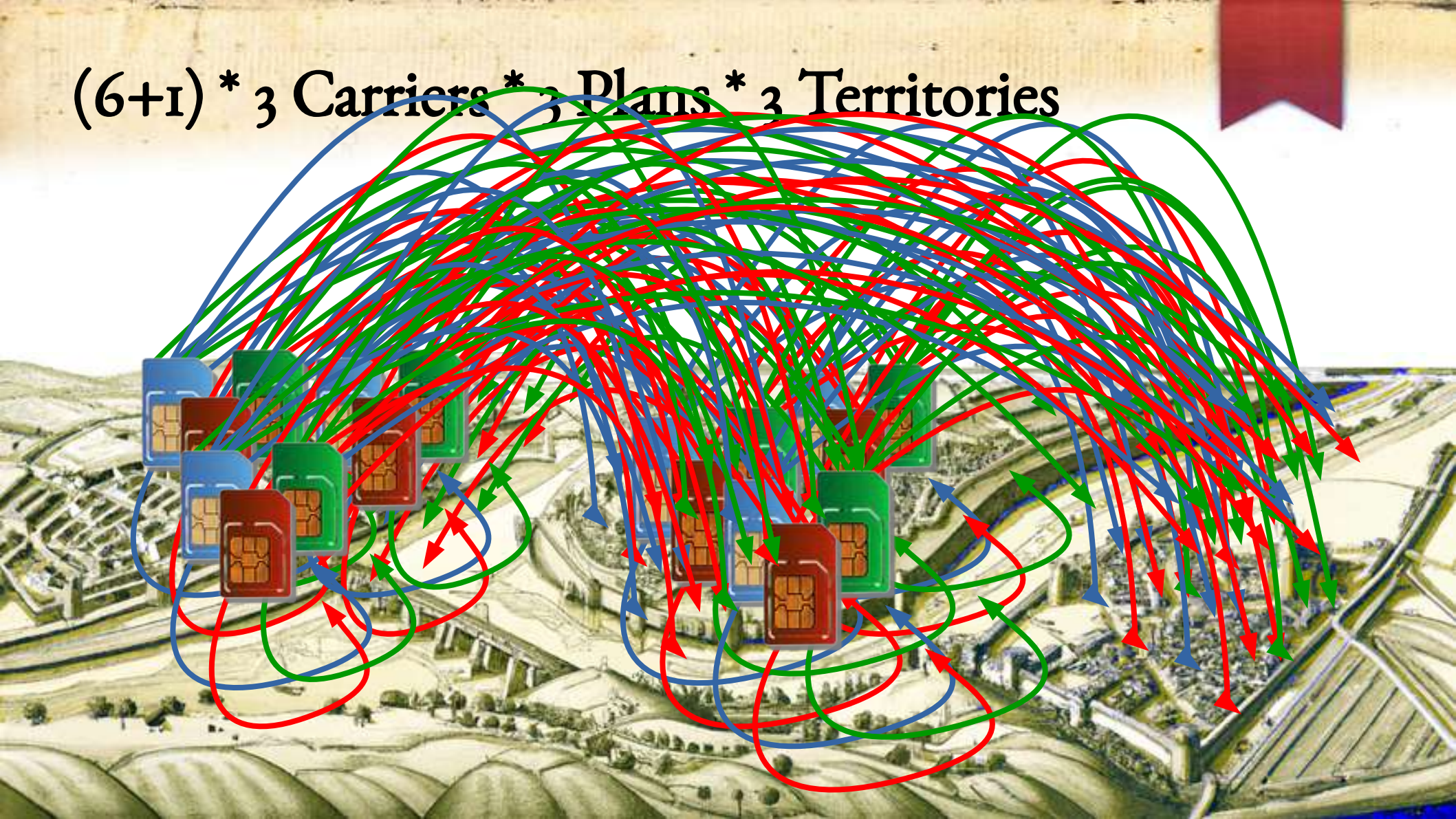
(6+1) * 3 Carriers



(6+1) * 3 Carriers * 3 Data Plans



(6+1) * 3 Carriers * 3 Plans * 3 Territories



(6+1) * 3 Carriers * 3 Plans * 3 Territories = 189

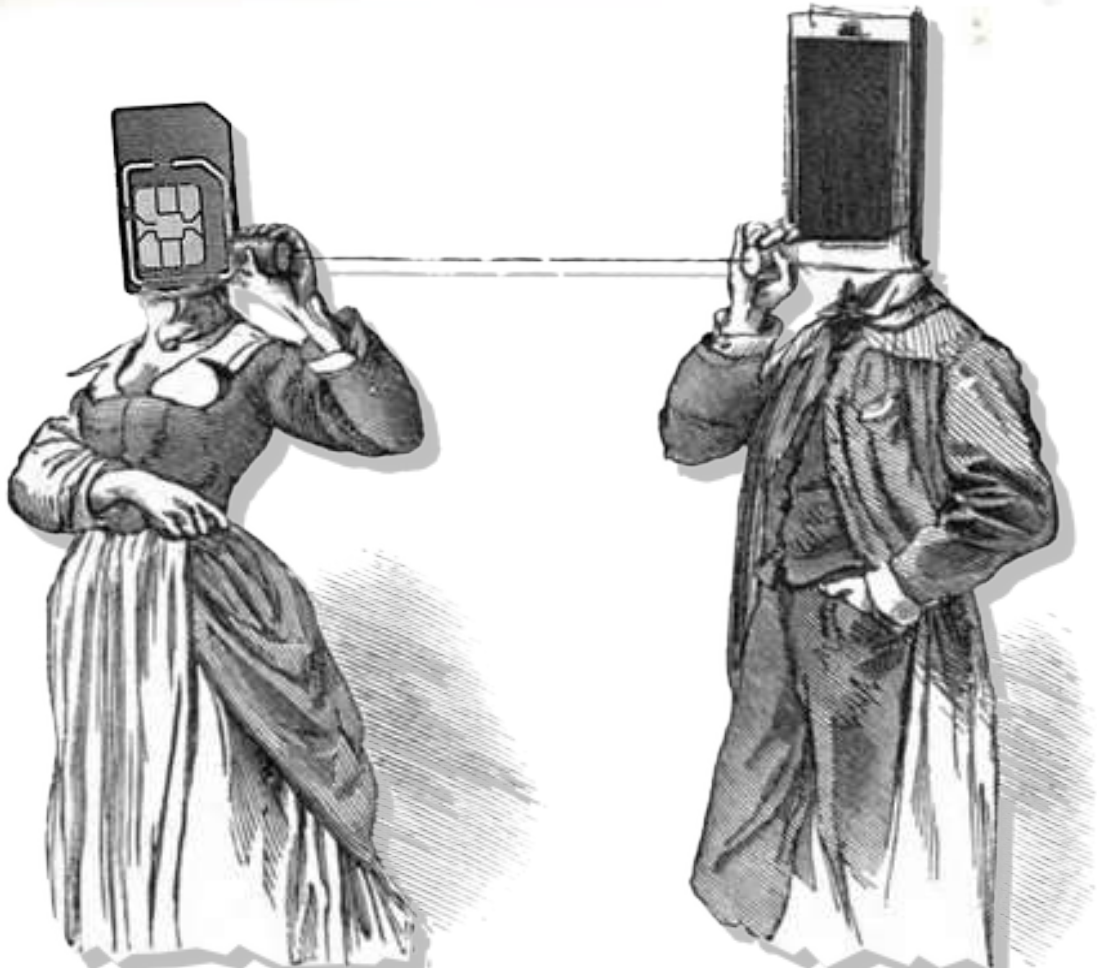
How to Scale, Automate?

- Buy a lot of SIMs and a lot of modems
  - Hardware costs
  - Monthly costs
  - Thus, bankruptcy!

How to Scale, Automate?

- One modem at each territory, and ship SIMs around
  - Low hardware overhead
  - Long shipping times
  - Manual labor

Decouple SIM and Phone/Modem



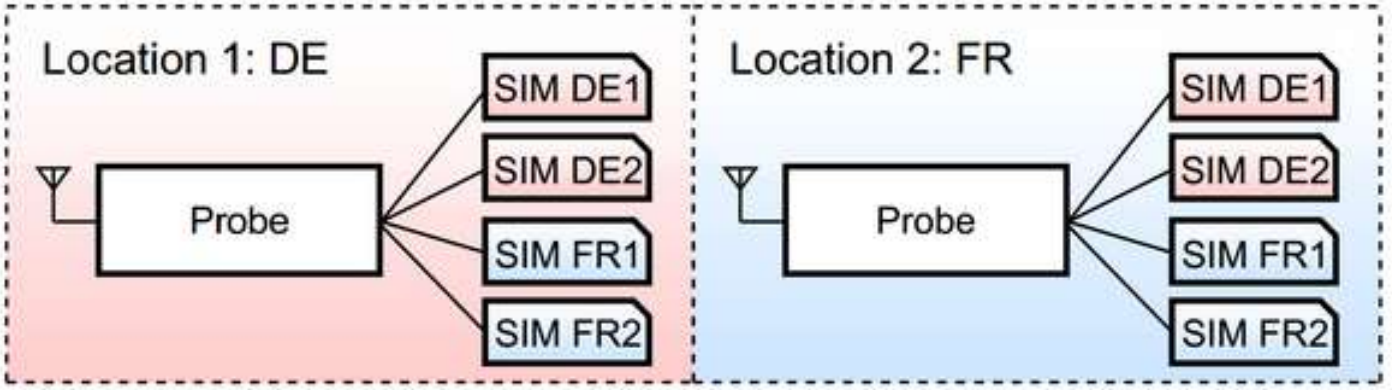
MobileAtlas

Geographically Decoupled Cellular Measurements & Exploitation

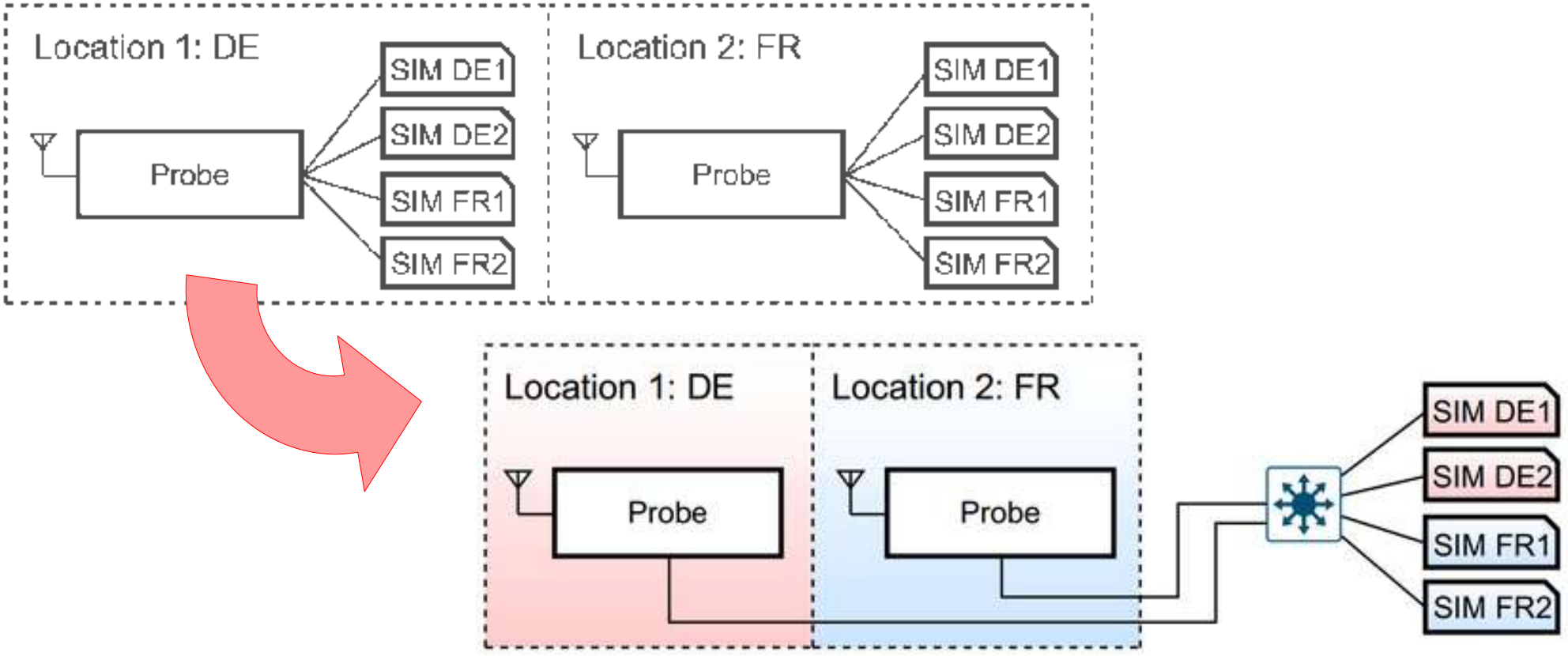
Our Goals

- Scalability
- Automatability
- Control background noise
- Low-cost, open design
- SIM communication
- Full feature spectrum

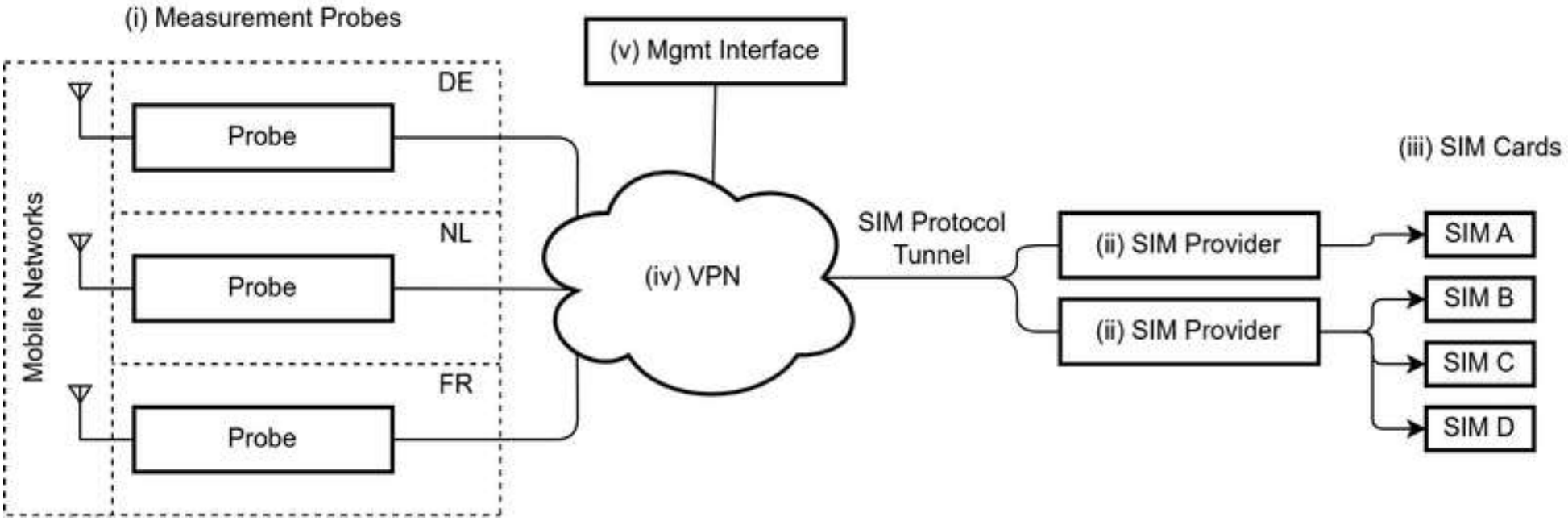
Combating the Combinatorial Explosion



Combating the Combinatorial Explosion

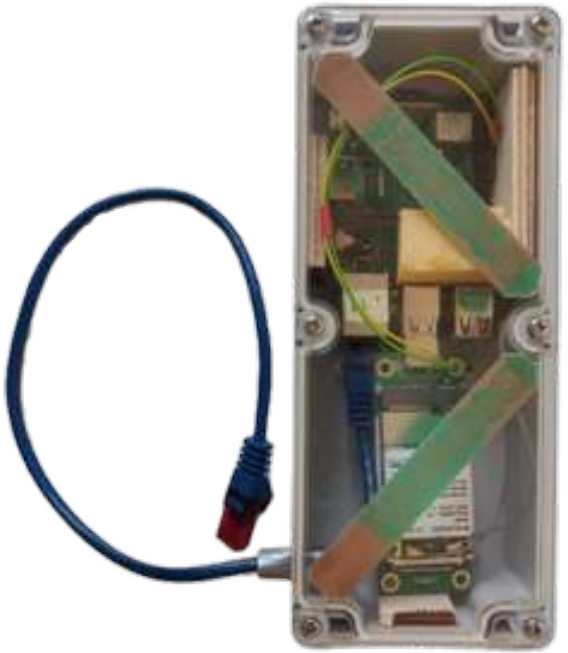


MobileAtlas Platform Architecture



Hardware: Probes

Version 1 (2019)



Version 2 (2022)

Hardware: SIM Provider

- SIM Provider software executed on system (e.g., laptop)
- SIM card attached to system
  - PC/SC Reader
  - “Cheap” SIM Reader
  - Modem (AT+CSIM)
  - Android Phone (via Bluetooth rSAP)

Challenges (Selection)

- SIM protocol
- Traffic Metering
  - Background traffic
  - Delay

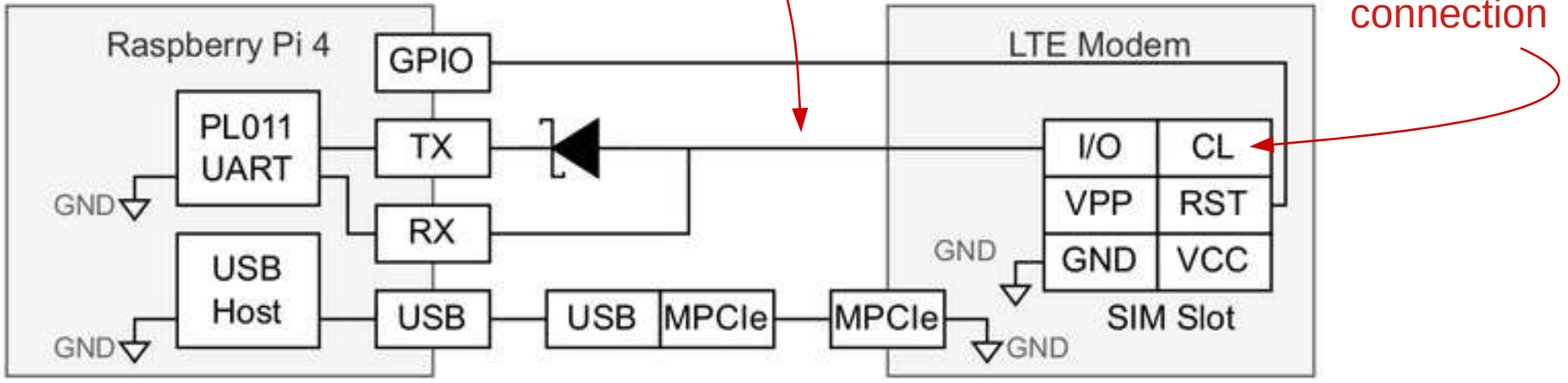
SIM Interface

- SIM protocol
  - In-device, low latency
    - But network has latency
  - Synchronous I/O
  - 1-5 Mhz clock speed
  - Multiple voltages
  - APDU relay request/response

SIM Interface

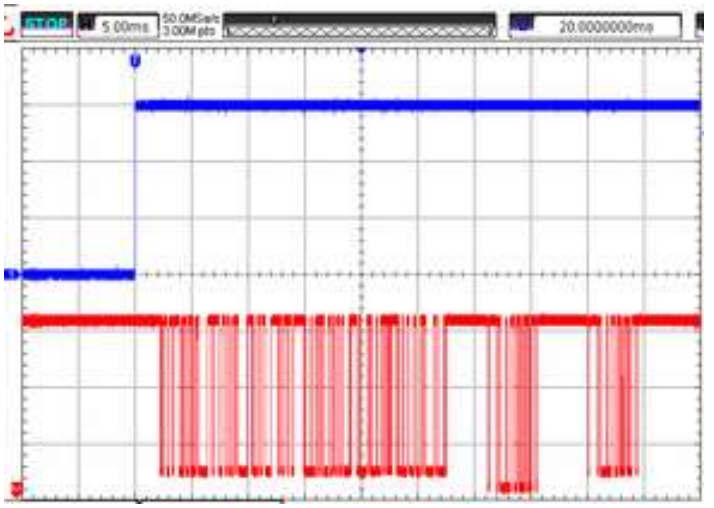
"Open Collector Bus"
modem provides pull-up

No clock
connection



SIM Interface

- We can negotiate speed & electric parameters independently (SIM Provider, Modem)
  - 1.8V, 3V, 5V
  - ATR and PPS
- Waiting Time eXtensions (WTX)
  - We tested 1000 ms latency
- Future work: cache/emulate some files locally.

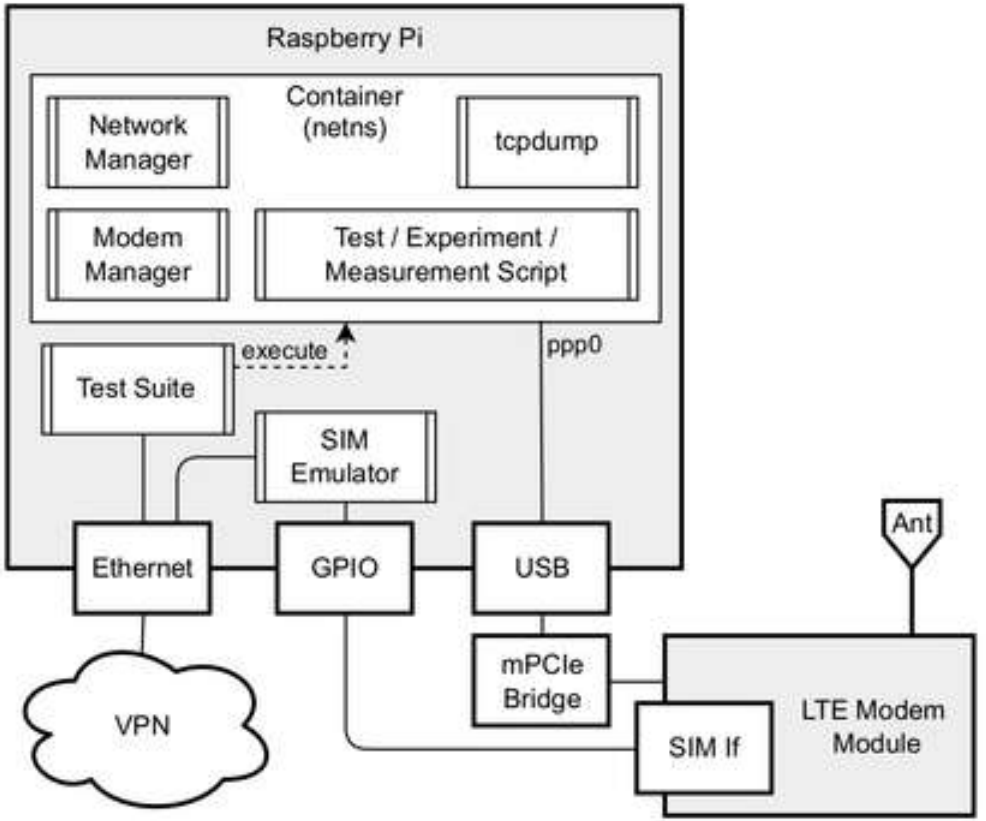


Traffic Metering

- Control our background traffic
- CDR often not realtime
  - ~x Hours, domestic
  - ~x Days, roaming
- No Standard
  - Web, SMS, App, USSD
- Granularity

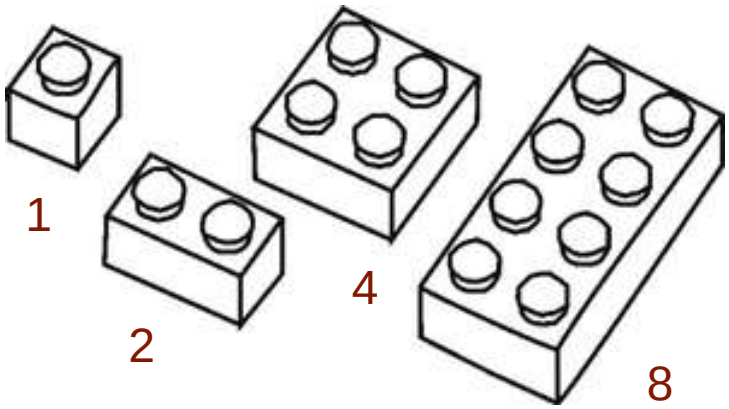
Eliminate Background Traffic

- Only one container is connected to the modem's data connection
- Linux network namesapces (similar to Docker)



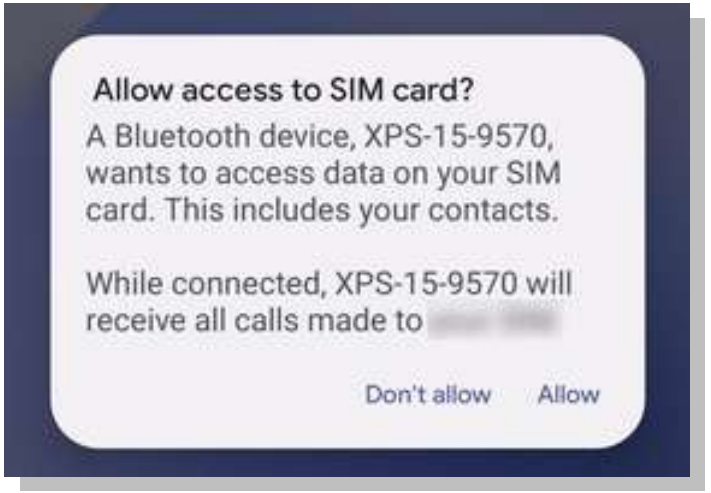
Delayed Traffic Accounting

- Charge Data Records (CDR) are often delayed by hours
- Use **binary encoding** for size of testing data: size = 2^{testnr} MB
- Hours later, we can unambiguously distinguish which traffic was accounted and which was free.



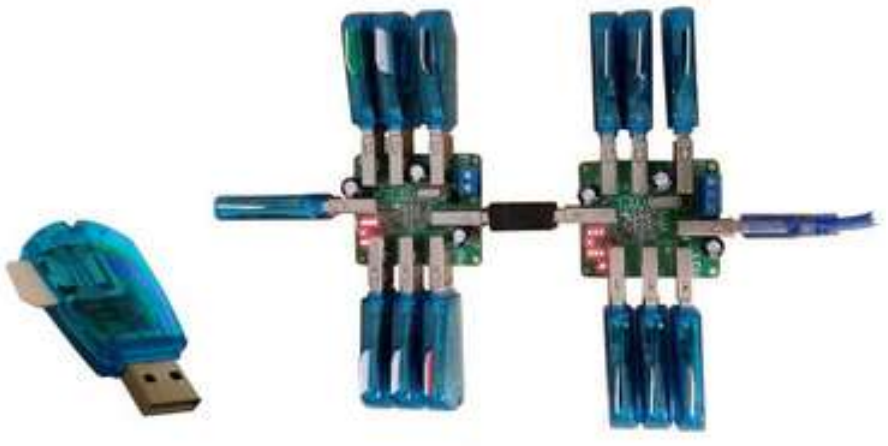
What about eSIMs ?

- Not universally available
- Not universally transferable
- We include them in MobileAtlas via BT rSAP Prototcol
  - Android Phone connects to SIM Provider system (e.g., Laptop) and shares its SIM card
  - No root required

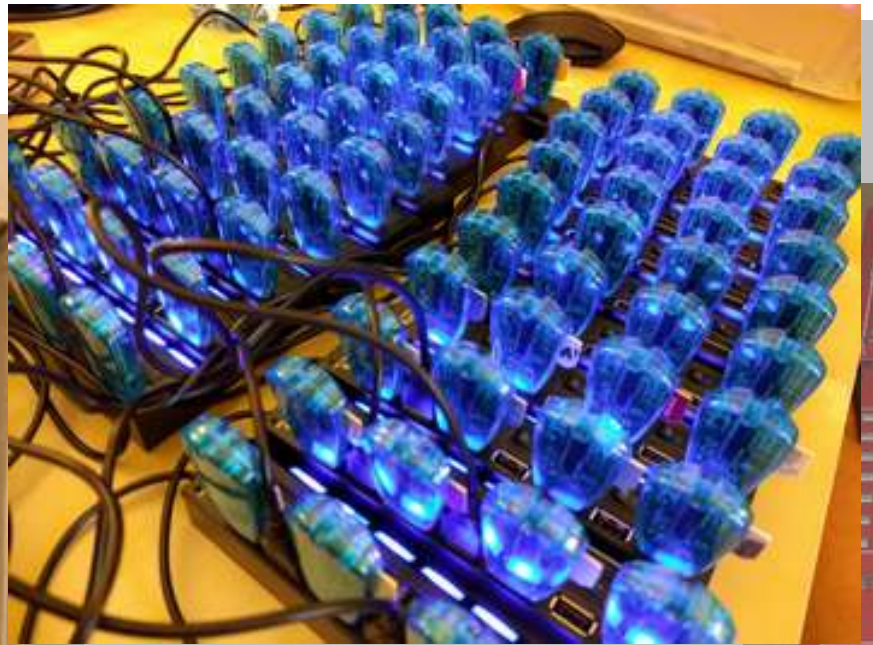


Things We Have Learned...

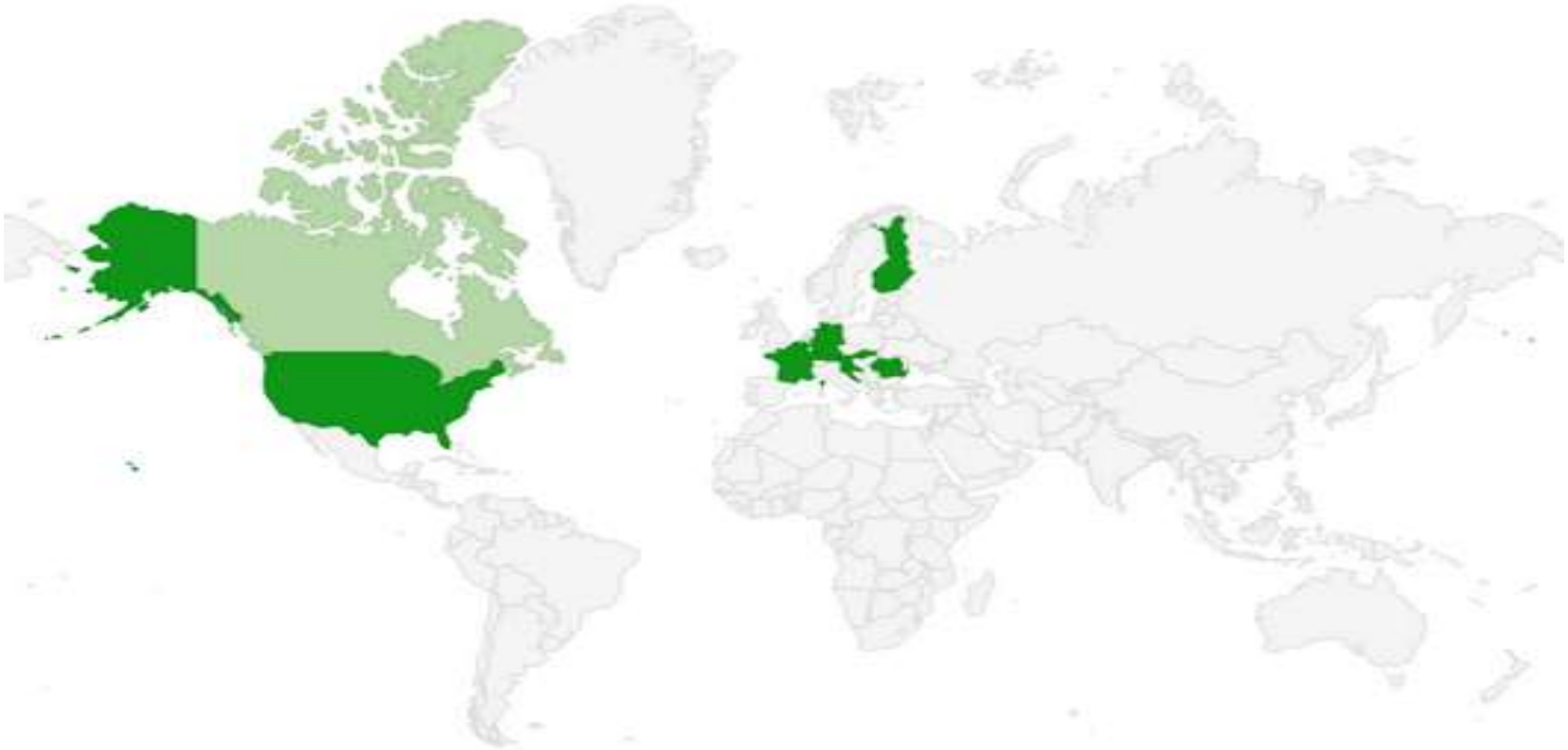
- IMSI is not a good primary key for a SIM card
  - SIMs change IMSI to select roaming partner network
  - Travel SIMs (also Google FI) are cloud-controlled SIMs
- Hard to reach USB's 127 device limit
  - Lousy hardware, weak drivers, power consumption



Adventures in USB Land



Where Do We Stand Today?



Ethical Considerations

- Radio regulation
  - Modems unaltered
  - Globally certified
  - No SDR
- No enrichment
  - We let expire same or bigger amount of unaccounted traffic from our data allowance.
- Network influence
  - No DoS, no abnormal traffic amounts
- Local LAN
  - All traffic via VPN
- SIM registration
- Guest LAN access

Measurement & Exploits (Selection)

Showcase A: Zero Rating and Free Riding

Zero-Rating


+ Smart Net
MESSAGING
€4,99/mês
€6,99/mês
1 mês grátis
Aderir
SOCIAL
€4,99/mês
€6,99/mês
1 mês grátis
Aderir
VIDEO
€4,99/mês
€6,99/mês
1 mês grátis
Aderir
MUSIC
€4,99/mês
€6,99/mês
EMAIL&CLOUD;
€4,99/mês
€6,99/mês
MEO
Tráfego grátis para apps MEO já incluído no seu tarifário

Zero-Rating: Carrier Perspective

- Data traffic needs to be separated
  - Billed traffic
  - Zero-rated traffic
- Classification of traffic that belongs to zero-rated applications
  - Based on various metrics

Traffic Classification: Popular Metrics

- TCP/UDP Port
  - Vague
- **IP Address**
  - Accurate, if static
  - Dynamic in cloud hosting
- **DPI**
  - Protocol dependent
- TTL
  - Used to detect tethering
- Machine Learning
  - Detect various patterns/metrics within packet flow

Hostname-based Classification

HTTP (plaintext)

- Classified via Host Field

```
GET / HTTP/1.1
Host: mobileatlas.eu
User-Agent: Mozilla/5.0
Accept-Language: en-US
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

HTTPS, HTTP3 (TLS)

- Classified via SNI Field

Zero-Rating Study

- Measured 7 operators (of 3 European countries)
- WhatsApp, Snapchat, Facebook/Messenger
  - Communication via WebAPI
    - HTTP, HTTPS, HTTP3
    - IPv4, IPv6
- Measured all operators and applications in 8 countries
  - In September 2021 + May 2022

Zero-Rating Study: Results

USED CLASSIFICATION METRICS AT THE TESTED OPERATORS AND APPLICATIONS

Operator	Roaming	WhatsApp	Snapchat	Messenger/Facebook
AT-1	Yes	IP	IP, Host	$
AT-2	Yes	IP	IP[a]	IP
AT-3	Yes	IP	×	$
HR-1	No	IP	Host	IP
HR-2	Yes	IP	IP, Host[b]	IP
RO-1	No	IP, Host[b]	×	IP, Host[b]
RO-2	×	IP[c]	×	×

$ traffic fully billed. × not part of zero-rating tariff.
[a] IPv4 only. [b] HTTPS only. [c] TCP only.

Zero-Rating Study: Results

USED CLASSIFICATION METRICS AT THE TESTED OPERATORS AND APPLICATIONS

IPv6 billed :-(

Operator	Roaming	WhatsApp	Snapchat	Messenger/Facebook
AT-1	Yes	IP	IP, Host	$
AT-2	Yes	IP	IP[a]	IP
AT-3	Yes	IP	×	$
HR-1	No	IP	Host	IP
HR-2	Yes	IP	IP, Host[b]	IP
RO-1	No	IP, Host[b]	×	IP, Host[b]
RO-2	×	IP[c]	×	×

$ traffic fully billed. × not part of zero-rating tariff.
[a] IPv4 only. [b] HTTPS only. [c] TCP only.

Zero-Rating Study: Results

USED CLASSIFICATION METRICS AT THE TESTED OPERATORS AND APPLICATIONS

HTTP3 (QUIC) billed :-(

Operator	Roaming	WhatsApp	Snapchat	Messenger/Facebook
AT-1	Yes	IP	IP, Host	$
AT-2	Yes	IP	IP[a]	IP
AT-3	Yes	IP	×	$
HR-1	No	IP	Host	IP
HR-2	Yes	IP	IP, Host[b]	IP
RO-1	No	IP, Host[b]	×	IP, Host[b]
RO-2	×	IP[c]	×	×

$ traffic fully billed. × not part of zero-rating tariff.
[a] IPv4 only. [b] HTTPS only. [c] TCP only.

Phreaking Revised: Spoof Hostname

- Hostname-based classification
  - HTTP (HTTPS?)
    - Write custom relaying script
    - Sometimes only simple regex within first bytes of packet
  - HTTPS/HTTP3
    - Use TLS-based VPN (e.g., OpenVPN) and spoof SNI Header
    - Similar to domain-fronting

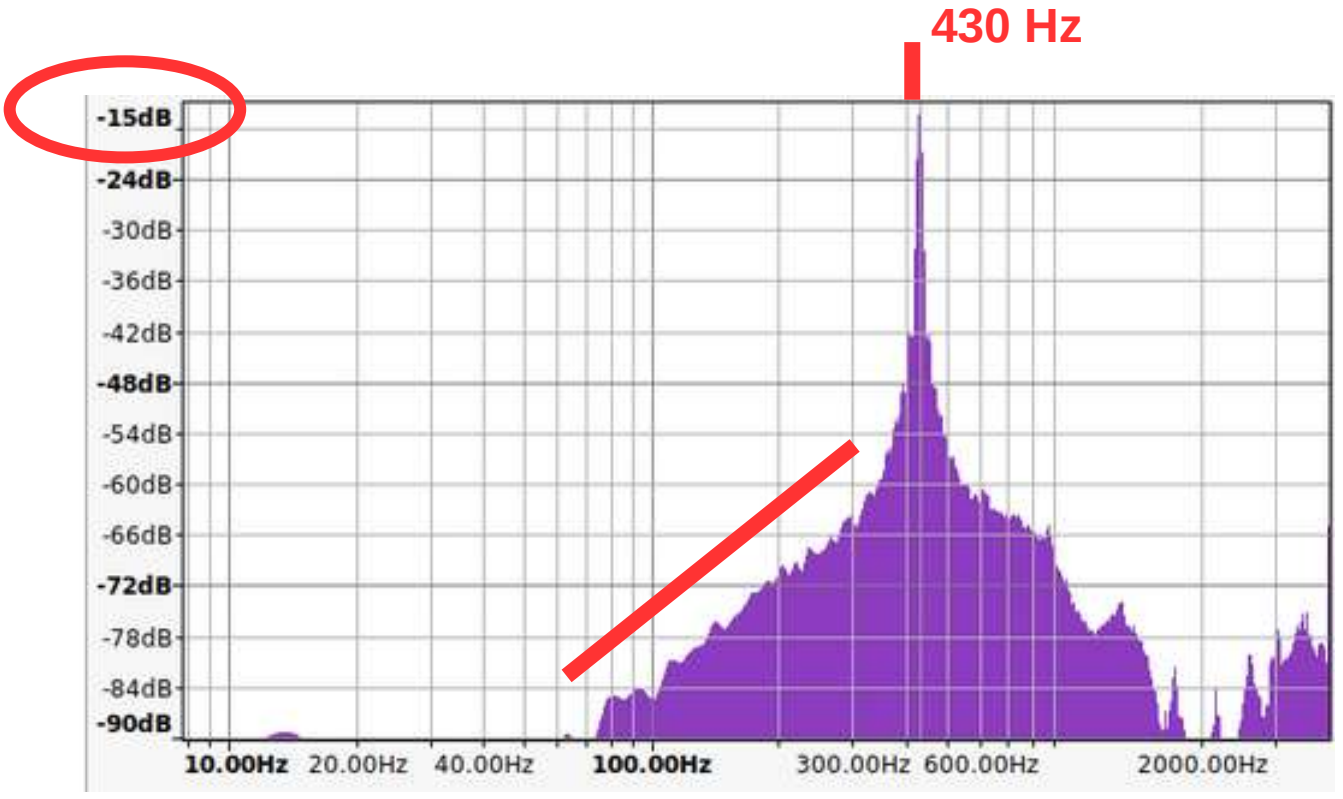
Measurement & Exploits (Selection)

Showcase B: Location Tracking with Ringback Tone Fingerprinting

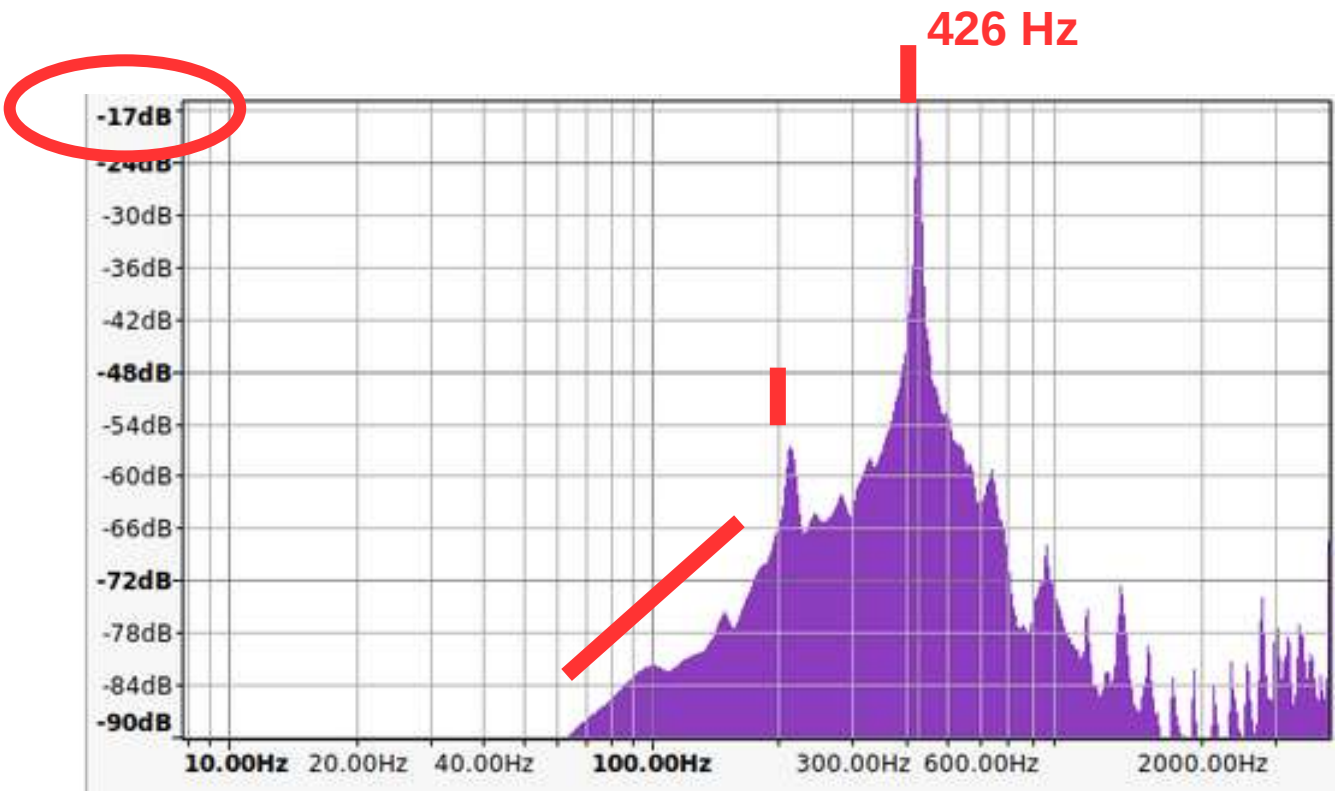
Ringback Tone Fingerprinting

- Ringback tone is issued by the call-terminating operator (“early media”)
  - i.e., the roaming partner
- Different ringback tones in different regions
  - US: 440 + 480 Hz
  - Europe: ~425 Hz

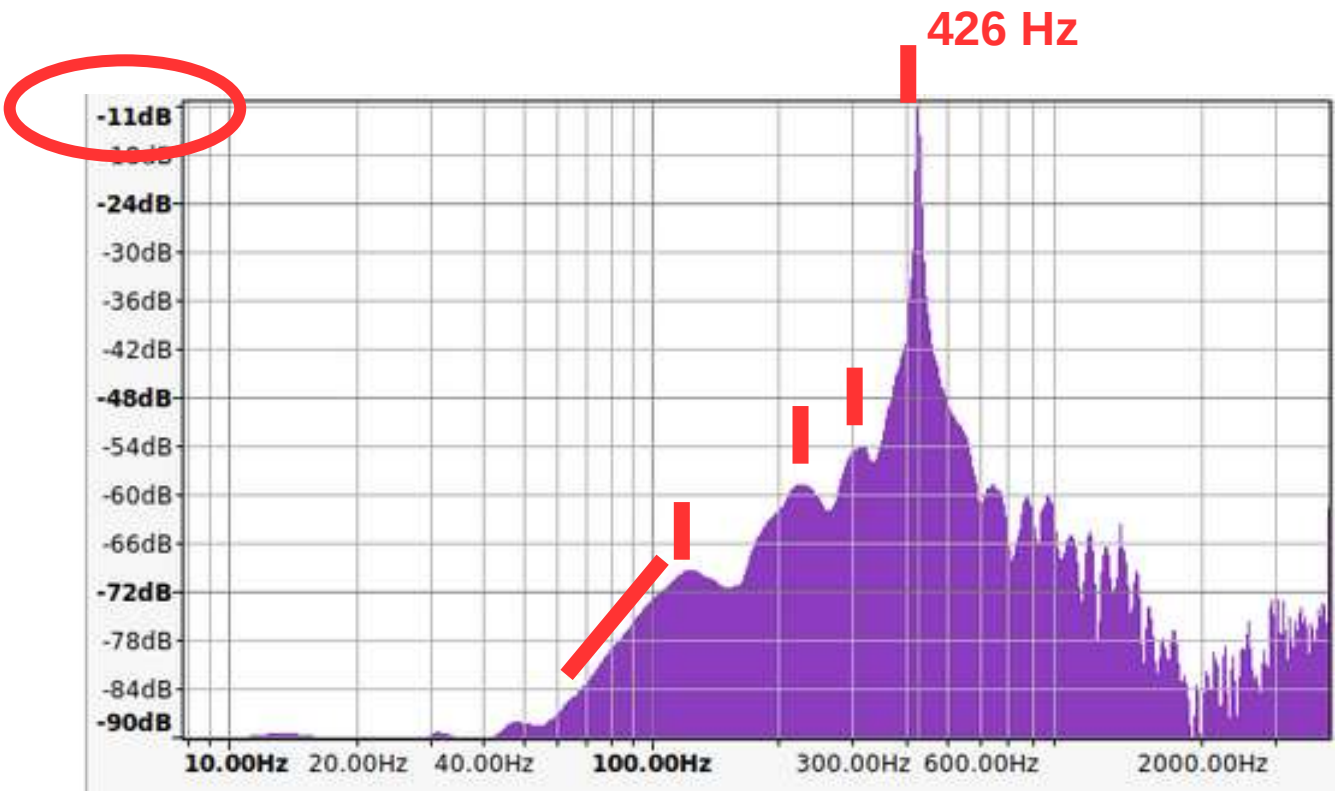
Ringbacktone I: Vodaphone RO



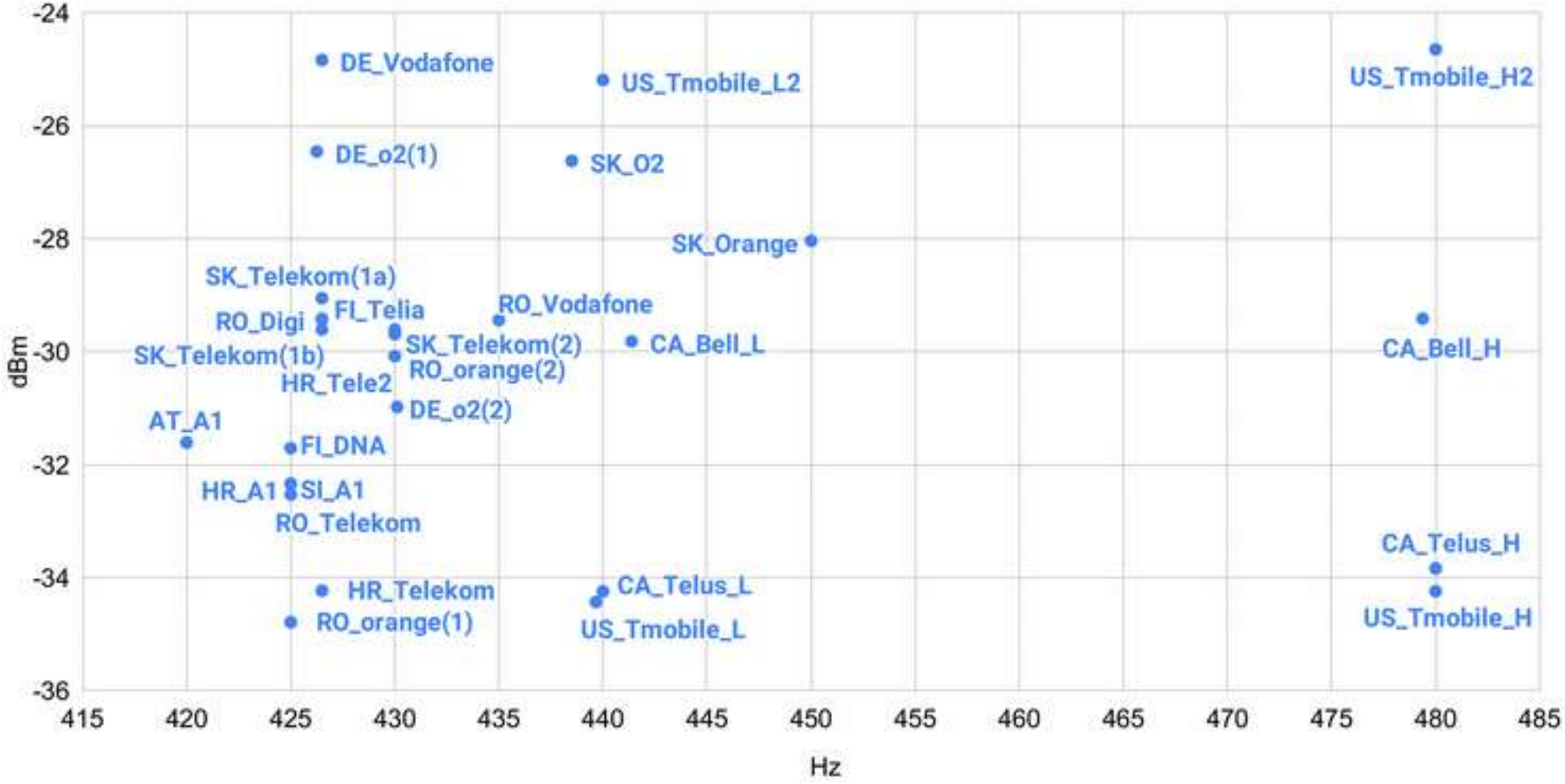
Ringbacktone II: Telekom DE



Ringbacktone III: O2 DE



Amplitude vs. Frequency



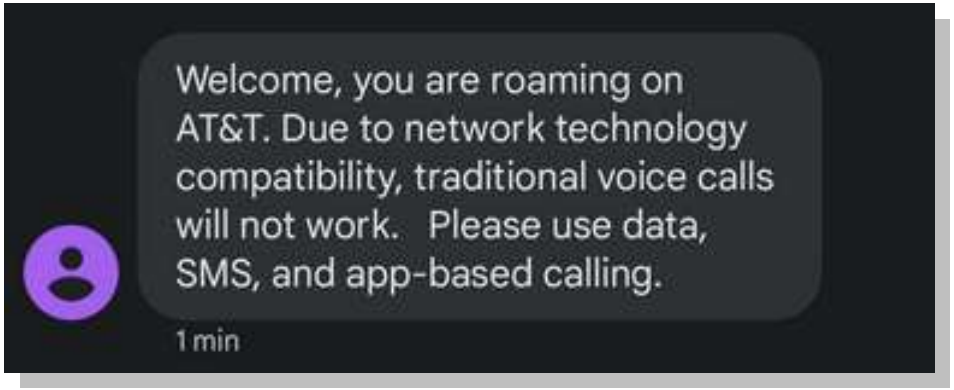
Ringback Tone: a Privacy Leak

- Can differentiate only by Amplitude + Frequency
  - One call, and you know the current (roaming) country/operator of the target
  - Other metrics: overtones, duty cycle
  - Other call progress tones
- Potential abuse for SIM swapping attacks
  - to find responsible (home) operator

Measurement & Exploits (Selection)

Showcase D: Billing without Service

No Service – Double Billing



- Roaming in the USA
- Call from Europe
  - €: passive roaming
- AT&T does not support VoLTE roaming
- Redirected to voice box
  - €€€: active roaming

More?

GLOBECOM 2022

Zero-Rating, One Big Mess: Analyzing Differential Pricing Practices of European MNOs

Gabriel K. Gegenhuber*†, Wilfried Mayer‡§ and Edgar Weippl¶

University of Vienna†, SBA Research§

Email: *gabriel.karl.gegenhuber@univie.ac.at, ‡wmayer@sba-research.org, ¶edgar.weippl@univie.ac.at

Abstract—Zero-rating, the practice of not billing data traffic that belongs to certain applications, has become popular within the mobile ecosystem around the globe. There is an ongoing debate whether mobile operators should be allowed to differentiate traffic or whether net neutrality regulations should prevent this. Despite the importance of this issue, we know little about the technical aspects of zero-rating offers since the implementation is kept secret by mobile operators and therefore is opaque to end-users and regulatory agencies.

This work aims to independently audit classification practices used for zero-rating of four popular applications at seven different mobile operators in the EU. We execute and evaluate more than 300 controlled experiments within domestic and internationally roamed environments and identify potentially problematic behavior at almost all investigated operators. With this study, we hope to increase transparency around the current practices and inform future decisions and policies.

Index Terms—zero-rating, net neutrality, mobile broadband, roaming, traffic differentiation, network management

I. Introduction

Cellular networks have become a major access technology to the public Internet that can also be used across national borders. In June 2017, the European Union abolished data roaming charges within the intra-EU/EEA area under the "roam like at home" regulation. While roaming is foreign

insights into the classification metrics that are currently used within the industry.

Our main contributions are:

- We propose a methodological approach to probe endpoints for zero-rating.
- We use this approach to evaluate zero-rating of four popular applications at seven operators from three countries.
- We test the effect that intra-EU roaming has on zero-rating by executing our experiments during domestic and roaming usage scenarios in eight different configurations.
- We evaluate our results and give an overview of the used classification metrics and encountered differences.

The remainder of this paper is organized as follows. Section II gives an overview of related studies that are relevant to this work. In Section III, we describe our methodological approach and quickly introduce the tested applications. We execute our experiments. Section IV [illegible] that were collected throughout this study. Section V discusses our results in Section V and concludes this paper.

II. Related [illegible]

Aside from hot debates about [illegible] seem, net neutrality has also been [illegible] from a technical perspective, [illegible] usually aim to detect traffic [illegible]

USENIX Security 2023

MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research

Gabriel K. Gegenhuber, *University of Vienna**

Wilfried Mayer, *SBA Research*

Edgar Weippl, *University of Vienna*

Adrian Dabrowski, *CISPA Helmholtz Center for Information Security†*

Abstract

Cellular networks are not merely data access networks to the Internet. Their distinct services and ability to form large, complex compounds for roaming purposes make them an attractive research target in their own right. Their promise of providing a consistent service with comparable privacy and security across roaming partners falls apart at close inspection.

Thus, there is a need for controlled testbeds and measurement tools for cellular access networks doing justice to the technology's unique structure and global scope. Particularly, such measurements suffer from a combinatorial explosion of operators, mobile plans, and services. To cope with these challenges, we built a framework that geographically decouples the SIM from the cellular modem by selectively connecting both remotely. This allows testing any subscriber with any operator at any modem location within minutes without moving parts. The resulting GSM/UMTS/LTE measurement and testbed platform offers a controlled experimentation environment, which is scalable and cost-effective. The platform is extensible and fully open-sourced, allowing other researchers to contribute locations, SIM cards, and measurement scripts.

Using the above framework, our [illegible] in commercial networks

once or longitudinal from different vantage points, (ii) they allow to quickly measure the scale of a found or known problem, i.e., gauge the real-world impact, and (iii) they function as a testbed to rapidly develop and test potential security vulnerabilities on a large scale. Additionally, tools such as ZMAP [17] provide the ability to routinely make Internet-wide scans, which became a staple for papers on measurement and security alike.

These platforms and tools share that –in accordance with the layered network model– they are access technology agnostic. However, mobile networks, unlike any other access network, combine multiple access technologies and generations on top of each other. Furthermore, since Mobile Network Operators (MNOs) are only given a small geographical area (usually a country) to operate in, they form vast roaming alliances to allow devices (and their traffic) to traverse through multiple networks. This creates complex compound systems where entities of different operators handle different parts of the user traffic.

To explore [illegible]

Conclusion

Conclusion

- Cellular research feels like being a geographic prisoner
- SIM tunneling enables new research opportunities
  - Rapid testing of many MNOs
  - Roaming
  - Early detect of problems
  - Long term measurements
- Showcases
  - Zero-Rating, Call Progress Tones, Proactive SIM, Billing inconsistencies

Measure & Exploit MNOs Globally

- Archibald can now measure, test, and develop exploits globally
- Escaping the geographic prison
- SIM tunneling enables new research opportunities
  - Rapid testing of many MNOs
  - Roaming, compliance, routing fraud, ...
  - Quality control (early detect of problems, Long term measurements, net neutrality)
- Showcases
  - Zero-Rating, Call Progress Tones, Billing inconsistencies

https://mobileatlas.eu

@GGegenhuber
gabriel.gegenhuber -at- univie.ac.at

@atrox_at
adrian.dabrowski -at- cispa.de