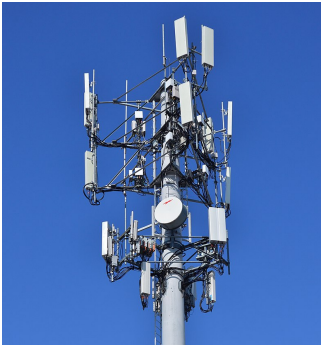
Why E.T. Can’t Phone Home

A Global View on IP-based Geoblocking at VoWiFi

Gabriel K. Gegenhuber, Philipp É. Frenzel, Edgar Weippl

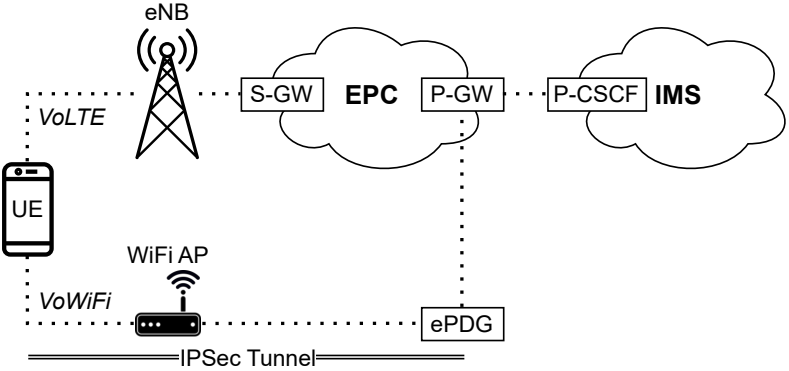
Two Access Technologies at 4G/5G



© Raysonho @ Open Grid Scheduler [CC0]

- VoLTE via **Celltower**
  - also VoNR, Vo5G
- VoWiFi via **WiFi Access Point (AP)**
  - also Wi-Fi Calling

VoWiFi at 4G/5G: Complementing Radio Access with WiFi APs



Motivation and Problem: Anecdotal Evidence of Blocked VoWiFi Service

- **VoWiFi** can be **used for phone calls and messages** (e.g., at places without cellular reception)
  - Nowadays: VoWiFi preferred over radio access when both available (on Android/iOS)
- VoWiFi calls are **billed as normal *local* calls**
  - No roaming revenue for the operator :(
- **Anecdotal evidence** from customers experiencing **issues when abroad**
  - Additional evidence in operator's FAQs

airtel

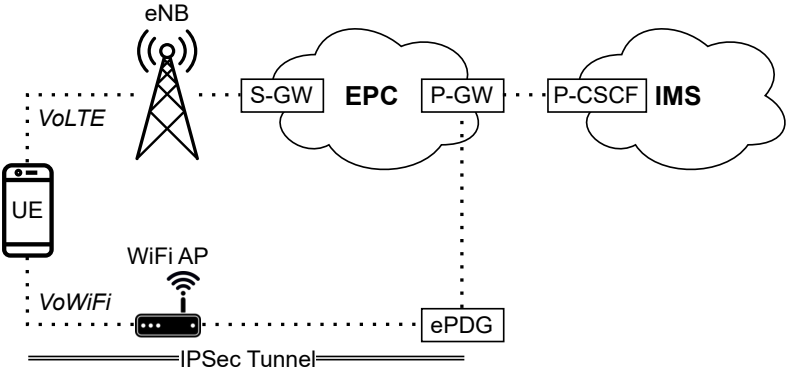
Q22) Can I use WiFi calling in International Roaming?

No, you cannot use WiFi calling in International Roaming.

Hypothesis and Methodology

- Hypothesis
  - Some operators employ **geoblocking practices** at VoWiFi
    - Possibly based on a customers (WiFi) IP address?
- Methodology
  - Simulate clients connecting to the VoWiFi service from different source locations (i.e., IP addresses)
- Coverage
  - Global scale
    - Probe all global operators
    - From worldwide locations (IPv4 + IPv6)

VoWiFi Connection Procedure

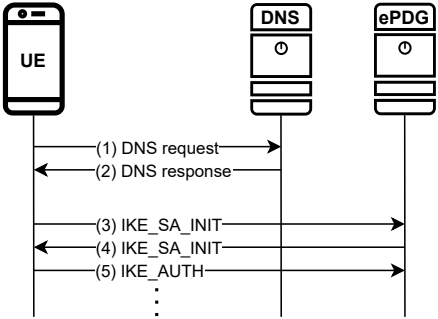


VoWiFi Connection Procedure

- Each operator is identified by MCC + MNC
- ePDG domain: `epdg.epc.mnc⟨id⟩.mcc⟨id⟩.pub.3gppnetwork.org`
- Two steps
  1. **DNS discovery**
  2. **IKE handshake**

VoWiFi Connection Procedure

- Each operator is identified by MCC + MNC
- ePDG domain: `epdg.epc.mnc⟨id⟩.mcc⟨id⟩.pub.3gppnetwork.org`



Measurement Methodology

- Two measurement cases (executed from all available vantage points)
  1. **DNS discovery**
     - Resolve all possible ePDG domains (i.e., 1.1M domain name combinations)
     - Use iterative requests to query authoritative DNS server
       (because offloading to central DNS might introduce noise due to caching, anycast routing, etc.)
  2. **IKE handshake**
     - Send first packet of IKE handshake, wait for response
     - Executed for all discovered IP addresses

Getting Vantage Points from Worldwide Locations

- Problem
  - We need to simulate **customers** connecting to local/foreign VoWiFi services **from all over the world**
  - Getting bare-metal servers as vantage points not feasible
- Solution
  - Using commercial **VPN services**

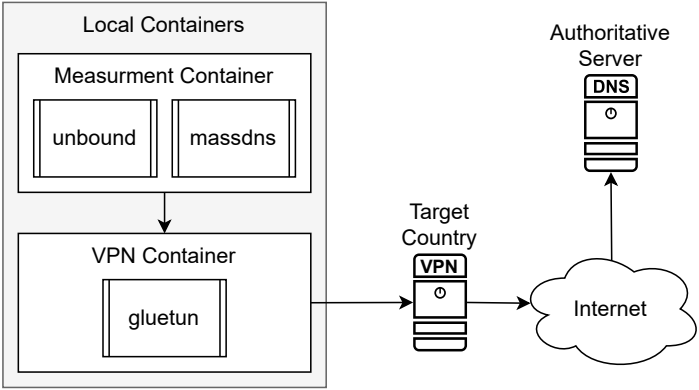
Used VPN Services

- 10 VPN services
- 1 cloud service
  - via WireGuard

Service	Countries[a]	IPv6 Support
Amazon EC2 (Cloud)	23	✓
Cloudflare WARP	120	✓
CyberGhost	91	×
hide.me	50	✓
HideMyAss	210	×
IVPN	36	✓
Mullvad	43	✓
NordVPN	60	×
Private Internet Access	84	×
ProtonVPN	68	×
Surfshark	100	×

[a] As advertised by the VPN/cloud service.

Dockerized Infrastructure (*DNS discovery*)

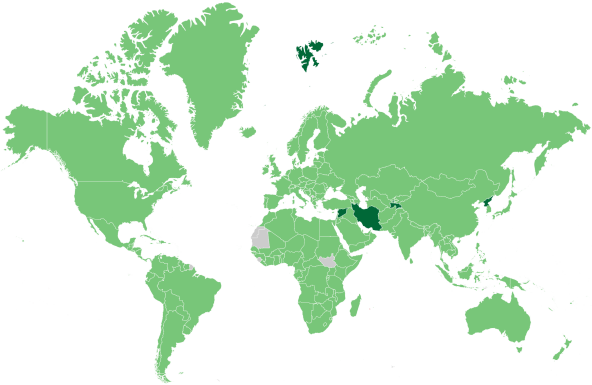


Measurements from 219 Countries (July - August 2024)

	IPv4		IPv6	
Service	Countries	Measurements	Countries	Measurements
Amazon EC2 (Cloud)	21	2,456	22	2,212
Cloudflare Warp	208	8,934	208	7,417
CyberGhost	90	4,025	0	0
hide.me	49	1,994	46	1,641
HideMyAss	207	2,969	0	0
IVPN	36	3,975	34	791
Mullvad	34	1,930	33	1,538
NordVPN	59	2,166	0	0
Private Internet Access	83	5,337	0	0
ProtonVPN	68	3,801	0	0
Surfshark	100	4,562	0	0
Total	219	42,149	208	13,599

Measurment Coverage: 219 Countries

- DNS: found VoWiFi deployments in 109 (IPv6: 16) countries
  - 423 ePDG domains (IPv6: 31)
  - IKE: 101 (IPv6: 10) countries responsive
- Overall 219 (IPv6: 208) countries covered by our VPN-powered vantage points



Dual-stack (1) IPv4 only (2)
No coverage & no VoWiFi (3) Missing coverage (4)

Results: DNS-based Blocking

- **DNS-based geoblocking** discovered at **one operator** (Vodafone Germany)
  - ECS (EDNS Client Subnet) Extension allows easy validation (cf. Appendix)

    Resolving standardized ePDG domain to CNAME reference:

    ```
    $ dig epdg.epc.mnc002.mcc262.pub.3gppnetwork.org
    => returns CNAME epdg.epc.drz1.vodafone-ip.de
    ```

    Actual resolution (Google vs. Vodafone IP range):

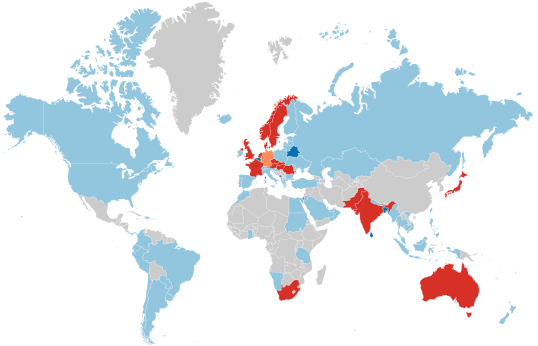
    ```
    # requesting via Google IP (United States)
    $ dig +trace epdg.epc.drz1.vodafone-ip.de +subnet=104.154.0.0/24

    # requesting via Vodafone IP (Germany)
    $ dig +trace epdg.epc.drz1.vodafone-ip.de +subnet=109.192.0.0/24
    ```

- Interesting (non-)findings at other operators
  - Geographical differentiation (separating domestic vs. abroad customers by returning different IP sets)
  - Load-balancing

Results: IKE-based Blocking

- Discovered at providers from Europe, Asia, Oceania, Africa
  - Overall 12.5% (IPv4) and 65.2% (IPv6) of all tested domains are geoblocked
- Usually **all foreign countries are blocked** (i.e., ePDG solely accessible from domestic IPs)
- Blocking discovered for **both IPv4 and IPv6** connections
  - For some operators, IPv6 can be used to circumvent blocking :)

Discovered Geoblocking: Regional Differences



No geoblocking (1) DNS entry only (2)
Blocked[IKE] (3) Blocked[DNS] (4) No VoWiFi (5)

Blocking is Popular within EU Countries

- Discovered geoblocking at **many operators within EU/EAA countries**
  - Austria, Czech Republic, Denmark, France, Germany, Hungary, Luxembourg, the Netherlands, Norway, Romania, Sweden, and the United Kingdom
- Most EU operators also block connections from **neighboring EU countries**
  - Intra-EU roaming via **radio access** is possible **without additional cost**
  - Single exception: one Slovakian operator exempting EU/EAA countries from the blocking

Limitations and Discussion

- Study **limited** to discover **simple blocking** on the IP layer
  - Some operators allow first handshake, block VoWiFi at a **later stage**
  - Result is a **lower bound**, more blocking in practice!
- Operators depend on external broker for geolocation (e.g. MaxMind)
  - Geolocation not always accurate
- Discovered practices (potentially) conflicting
  - Consumer protection, social policy (e.g., net neutrality rules, open Internet guidelines)

Implications of IP-based Blocking

- Complicates the life of telco researchers
  - E.g., limited coverage during security-related probing in my upcoming publication: *Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments*
- Implications to **emergency calling**
  - All discovered geoblocking measures are simple IP-based rules, no context available
  - In practice, **they also block emergency calling connections** ϟ

Dissemination: Discussions with BEREC/EENA/GSMA

- BEREC
  - Email from International Roaming WG
    - “There are currently no legal obligations for WIFI calls”
- EENA
  - Discussion on 2024-04-17
    - “will study the topic and discuss with its community”
- GSMA
  - Fraud and Security Architecture Group
  - Discussion on 2024-06-17

Open Source: *Scanywhere* Measurement Framework

sbaresearch / **scanywhere**

scanywhere Public

main | Go to file t | + | Code

README | GPL-3.0 license

scanywhere

Internet scanning anywhere and everywhere.

Globally deploy and distribute your Internet measurements, scans and experiments leveraging cloud infrastructure and consumer-grade VPN subscriptions.

About

Internet scanning anywhere and everywhere. Globally deploy your Internet measurements, scans and experiments leveraging cloud infrastructure and consumer-grade VPN subscriptions.

vpn | global | large-scale | network-measurement | gluetun

Readme

GPL-3.0 license