LATVIJAS UNIVERSITĀTE

Pakalpojumatteices atstaroto amplificēto apjomīgo uzbrukumu kapacitātes mērīšana

Artūrs Lavrenovs

24-11-2023

NACIONĀLAIS ATTĪSTĪBAS PLĀNS 2020

EIROPAS SAVIENĪBA
Eiropas Sociālais fonds

IEGULDĪJUMS TAVĀ NĀKOTNĒ

SAM 8.2.2. 3. kārtas projekta “LU doktorantūras kapacitātes stiprināšana jaunā doktorantūras modeļa ietvarā” (Līguma Nr. 8.2.2.0/20/I/006)

Promocijas darba struktūra

- **Publikācijas** – visdetalizētākais avots, disertācija bieži atsaucas
- **Promocijas darbs – Disertācija** – **pētījuma kopsavilkums** – svarīgākais no publikācijām + sasaiste starp tām + pamatojumi + novērojumi + diskusijas + u.t.t.
- **Promocijas darba angļu kopsavilkums** – izrāvumi no disertācijas (kopsavilkuma kopsavilkums) – vislabāk sekot līdzi prezentācijai
- **Promocijas darba latviešu kopsavilkums** – tiešs tulkojums ar oficiālo terminu (termini.gov.lv) piemeklēšanu un pielāgošanu

LATVIJAS UNIVERSITĀTE

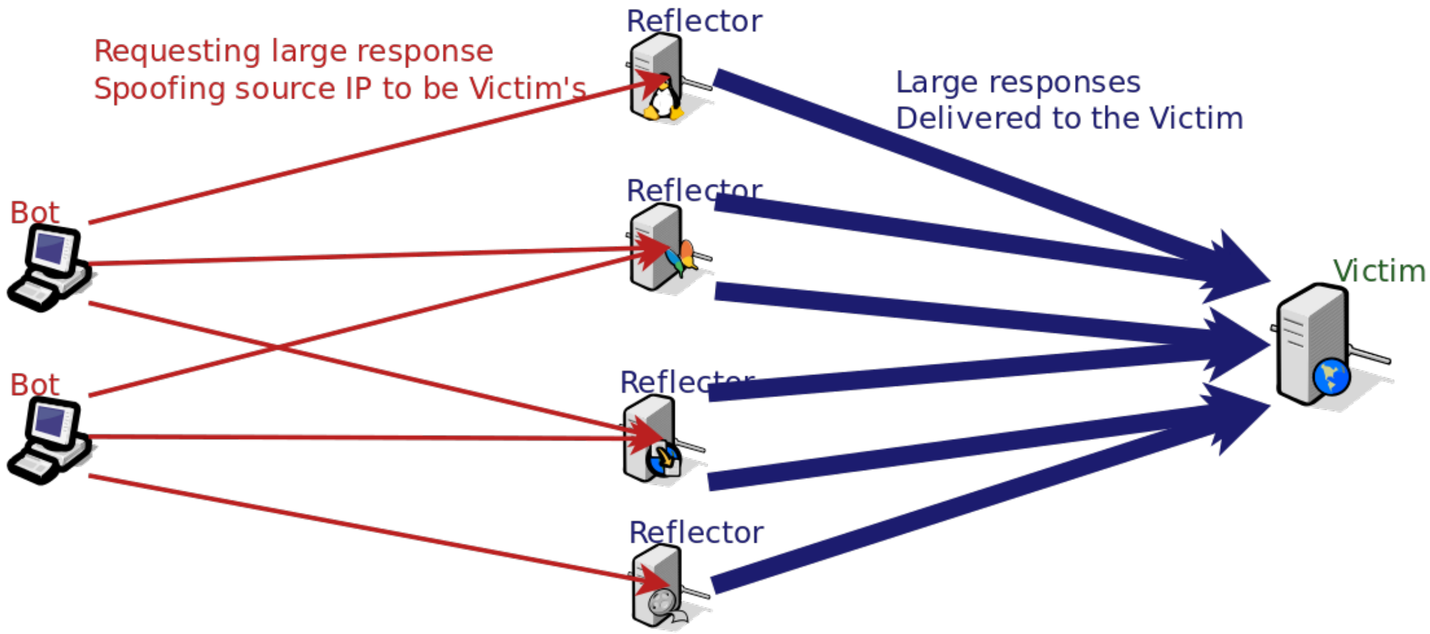
Pētījuma konteksts

- Izkliedētā **Pakalpojumatteice** *(DDoS)* – uzbrukumi, kas iztērē upura tīkla vai skaitļošanas resursus, liedzot apkalpot leģitīmos lietotājus
- **Atstarošana** *(reflection)* – atbilžu sūtīšana citam adresātam, nevis tam, kas to ir pieprasījis
- **Amplifikācija** *(amplification)* jeb pastiprināšana – (ievērojami) lielāku atbilžu ģenerēšana
- **Apjomīgie** *(volumetric)* – upura tīkla resursu (datplūsma, skaitļošanas, pakešu) pārtēriņš
- **Uzbrukuma kapacitāte** – maksimālā uzbrukuma datplūsma konkrētam upurim
- Šajā pētījumā: **Pakalpojumatteices atstaroto amplificēto apjomīgo uzbrukumu kapacitātes mērīšana**

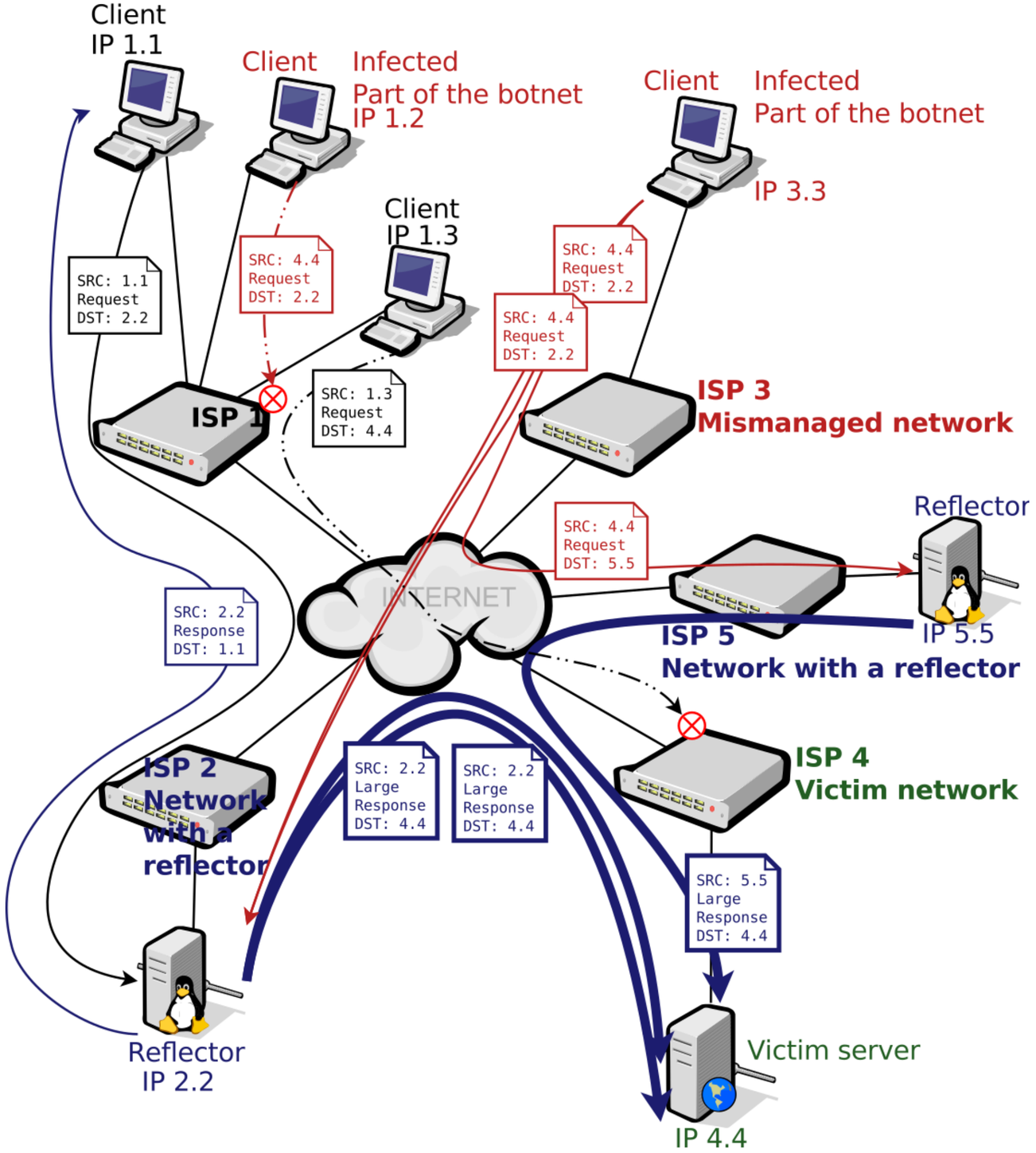
LATVIJAS UNIVERSITĀTE

Pētījuma ierobežojumi *(scope)*

- **Internetā sasniedzami** *(publicly reachable)* **servisi** (iekārtas)
- **UDP** bāzēti protokoli
- **IPv4**
- **Problemātiskākais DDoS** paveids – **<u>atstarotais amplificētais apjomīgais</u>**
  - <u>Visās publikācijās un industrijā vizualizēts:</u>



LATVIJAS UNIVERSITĀTE



Labāka vizualizācija izpratnei

- 22 gadus aktuāla problēma
- Zināmi **perfekti** risinājumi
  - BCP 38
  - Tīklu attīrīšana no atstarotājiem

LATVIJAS UNIVERSITĀTE

Vēsture

- 1999 – pirmais DDoS (tiešais tīkla) uzbrukums
- 2001 – sākas pirmie **atstarotie amplificētie apjomīgie** DDoS uzbrukumi (DNS), turpinās šobrīd un vēl turpināsies gadiem
- ...-2011 – pirms CDN (Cloudflare u.c.) industrijas realitāte
- ...-2013 – maģistra pētījums – tīkla skenēšana, urķuslazdi, u.c.
- 2014 – NTP DDoS un pirmās publikācijas mēģinājums
- 2017 – Leverett prezentācija Rīgā "Cyberchess 2017" par “potenciāla” novērtēšanas metodoloģiju → tiek definēta mērīšanas metodoloģija pretstatam tai
- 2018 – pirmie rezultāti, izmaiņas metodoloģijā un tehniskajos risinājumos
- 2020-2023 – šī brīža metodoloģija un dati

LATVIJAS UNIVERSITĀTE

Problēma

- Kāda ir globālā DDoS uzbrukumu kapacitāte?
  - Teorētisks novērtējums (Leverett and Kaplan) – praktiski neviens neizmanto
  - Ne-ekstrapolējams privileģēts skats (ISP, IXP) – derīgs relatīvam novērtējumam
  - Industrijas ziņojumi (*technical report, threat advisory, white paper*) par notikušiem uzbrukumiem*:

Organization	Service abused (port)	Capacity	Date reported
Arbor – DDoS mitigator	Memcached (UDP 11211)	1.7 Tbps	05 Mar 2018
Akamai – CDN provider	Memcached (UDP 11211)	1.3 Tbps	01 Mar 2018
Cloudflare – CDN provider	Memcached (UDP 11211)	260 Gbps	27 Feb 2018
Cloudflare – CDN provider	SSDP (UDP 1900)	100 Gbps	28 Jun 2017
Akamai – CDN provider	CLDAP (UDP 389)	24 Gbps	04 Mar 2017
Cloudflare – CDN provider	NTP (UDP 123)	400 Gbps	13 Feb 2014
Cloudflare – CDN provider	DNS (UDP 53)	75 Gbps	20 Mar 2013
Cloudflare – CDN provider	SNMP (UDP 161)	21 Gbps	03 Aug 2012

* Lielākie industrijas ziņotie uzbrukumi 2.X Tbps, bet tie ir multi-protokolu

Problēma ar industrijas avotiem

- **Visi** izmanto šo industrijas publicēto kapacitāti
  - Lēmumu pieņēmēji – no tīkla administratora līdz likumdevējiem un starptautiskām organizācijām
  - Industrijā
  - Zinātnē un pētniecībā
- Industrijas publicētā kapacitāte
  - 1 uzbrukuma novērotā kapacitāte 1 upurim konkrētā dienā
  - Kapacitāte nekad nav 100% izmantota
  - Industrija publicē detaļas par rekordiem, ko ir izdevies apstrādāt
  - Konkrētā protokola individuālu uzbrukumu (ne-globāla) kapacitāte nav publiska, ja rekordi netiek lauzti

LATVIJAS UNIVERSITĀTE

Motivācija, pamatojums un tēze

- 20+ gadus pastāvoša problēma, situācijas uzlabojumi ir nepietiekami pret tīkla pieslēgumu ātruma pieaugumu
- **Publiski** nav zināma globālā uzbrukumu kapacitāte
  - Šajā konkrētajā mirklī
  - Vēsturiski, izmaiņas, tendences
  - Vai mūsu aktivitātes samazina to? Cik liela ir mūsu ietekme?
- Autora apgalvojums un motivācija
  - Uzbrukuma kapacitātes nezināšana ir viens no iemesliem, kādēļ šī DDoS problēma vēl joprojām ir globāli aktuāla
- **Tēze**: Ir iespējams novērtēt globālo uzbrukumu kapacitāti, mērot individuālo atstarotāju īpašības

LATVIJAS UNIVERSITĀTE

Pētījumā paveiktais

- Definēta un realizēta jauna pakalpojumatteices globālās kapacitātes mērīšanas metodoloģija
- Realizētā metodoloģija pielietota 6 protokoliem
- Analizēti mērījumu rezultāti, izpētīti pieejamie datu skati un vizualizācijas
- Identificēta un analizēta nepieciešamība pēc iekārtu klasifikācijas
- Esošā alternatīvā metodoloģija aktualizēta, metodoloģija un rezultāti salīdzināti
- Apskatītas uzbrukumu kapacitātes tendences un rezultātu potenciālais pielietojums

LATVIJAS UNIVERSITĀTE

Publikācijas

- Disertācija ir pētījuma kopsavilkums
  - katra nodaļa atbilst vienai vai vairākām publikācijām, kur apzināti **autors ir pirmais vai vienīgais autors**
    - **tiešie** rezultāti publicēti **8** starptautiski recenzētās publikācijās (visas indeksētas *Scopus* un *Web of Science)*
    - referēts 8 starptautiskās konferencēs (7 – autors, 1 – līdzautors)
  - publikācijas ir plašākas, satur arī līdzautoru darbu
- Kopā **14** publikācijas indeksētas *Scopus (12)* un *Web of Science (9)* kopš iestāšanās doktorantūrā (2013.) + 1 apsolīta, bet neindeksēta

LATVIJAS UNIVERSITĀTE

Piedāvātā metodoloģija

- Identificē protokolus un ievainojamības mērījumiem
- Identificē Internetā publiski sasniedzamas iekārtas, kas apkalpo protokola servisus – **skenēšana** ←parasti pētniecība beidzas šeit
- Katrai iekārtai sūta vairākus pieprasījumus un analizē atbildes – **mērīšana**
  - Amplifikācija
  - Tīkla datplūsmas ātrums, apjoms, aiztures
  - Ierobežojumu atklāšana
- No individuāliem mērījumiem, definējot ierobežojums – **kapacitātes aprēķins**

LATVIJAS UNIVERSITĀTE

Realizētā metodoloģija

- Pēc iekārtas identificēšanas pārbauda, vai amplificējamā funkcionalitāte darbojas
- Ja darbojas, nosūta 50 (100) pieprasījumus secīgi maksimāli ātri
- Izfiltrē no datu kopas ne-amplificētas iekārtas
- Nosaka slieksni tam, kuras iekārtas rada kapacitāti – 80% atbilžu
- Analizē individuālo protokola un iekārtu īpašības
- Aprēķina kopējo protokola kapacitāti

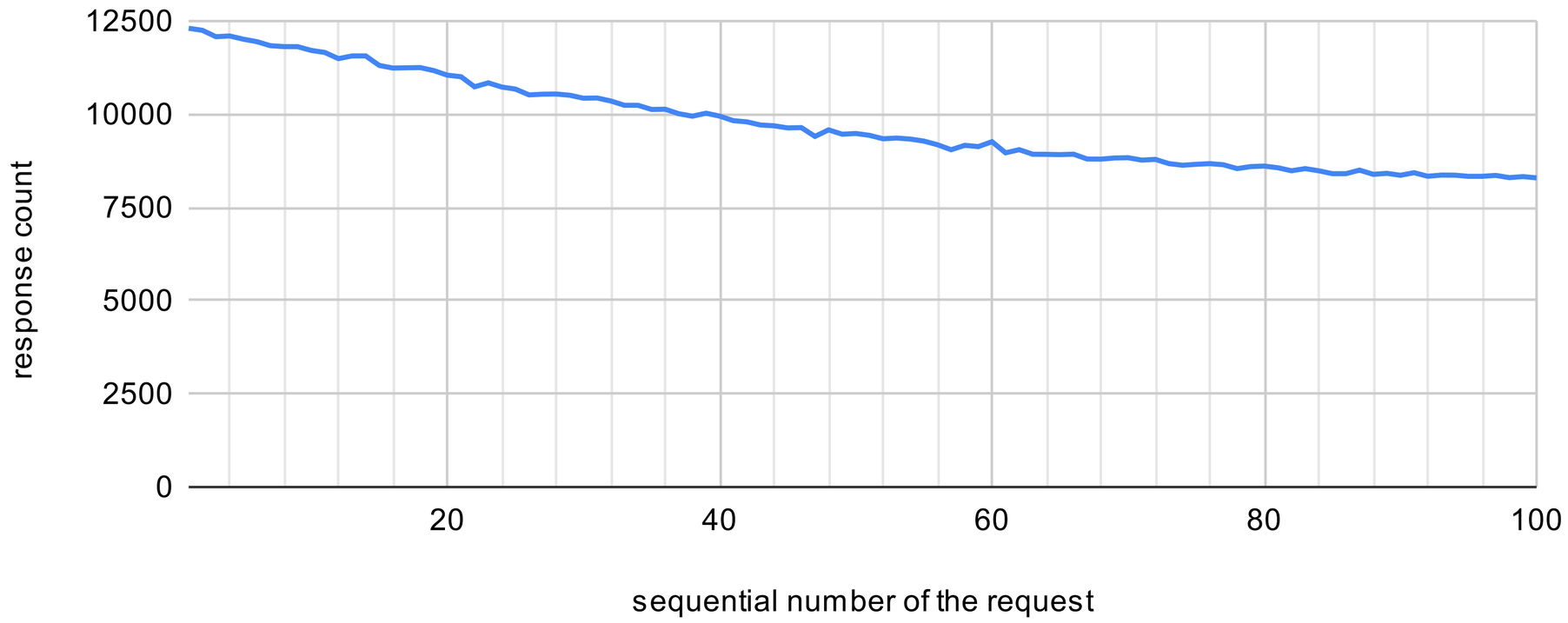
LATVIJAS UNIVERSITĀTE

Mērījuma piemērs: NTP

- Amplificējams pieprasījums `monlist`
- Skenēšanas solī: 656,923 iekārtas ← praktiski visi skenēšanas pētījumi apstājas šeit
- Mērījumi veikti: 168,650 iekārtām ← reti tiek veikti ierobežoti (amplifikācijas) mērījumi visa veida avotos
- Mērījumu kopa pēc izfiltrēšanas (BAF>=5): 22,222 iekārtas ← reti/unikāls
- Kapacitātes aprēķins (RR 80%): 5028 iekārtām ← unikāls skats, nevienā publiskā avotā nav veikts
- Katram protokolam savas īpatnības, rezultāti un secinājumi

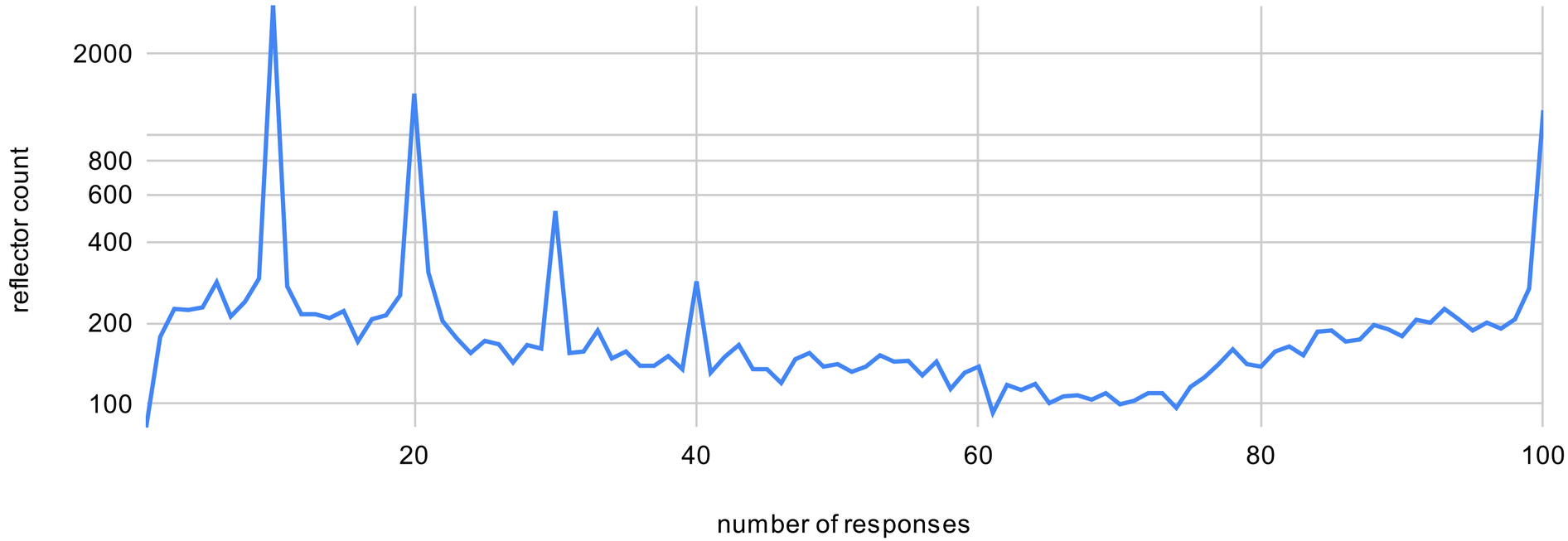
LATVIJAS UNIVERSITĀTE

NTP: Pirmie dati izraisa vilšanos



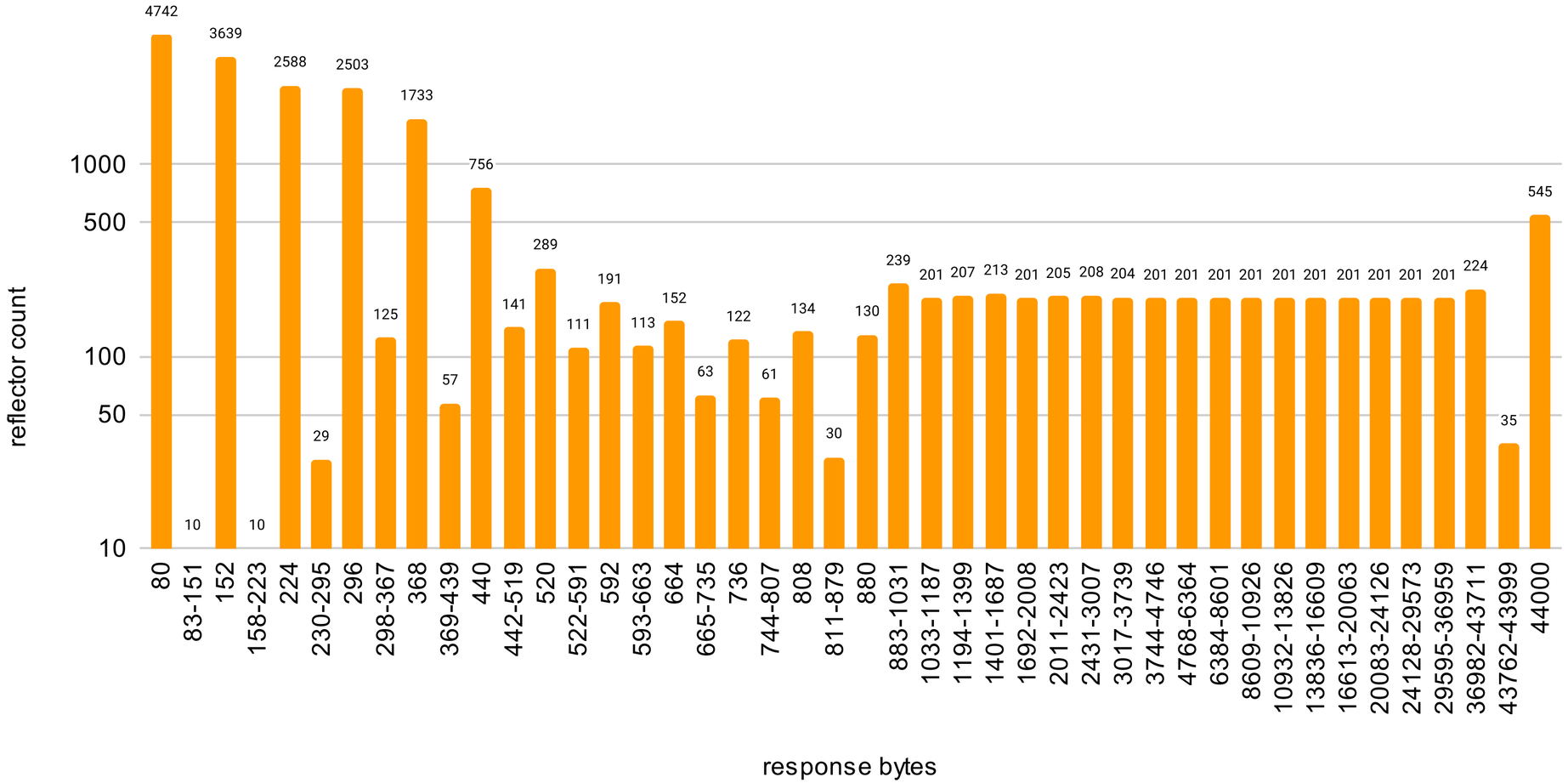
LATVIJAS UNIVERSITĀTE

NTP: RRL – unikāls skats



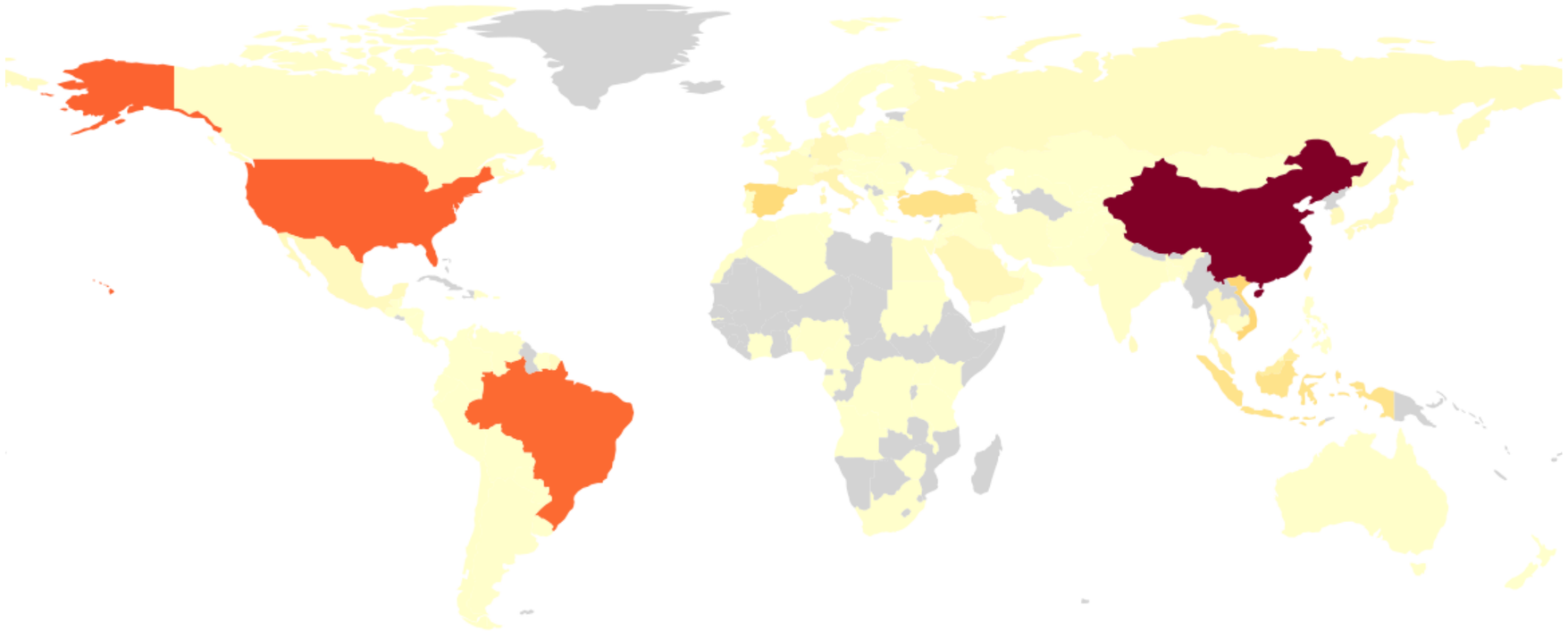
LATVIJAS UNIVERSITĀTE

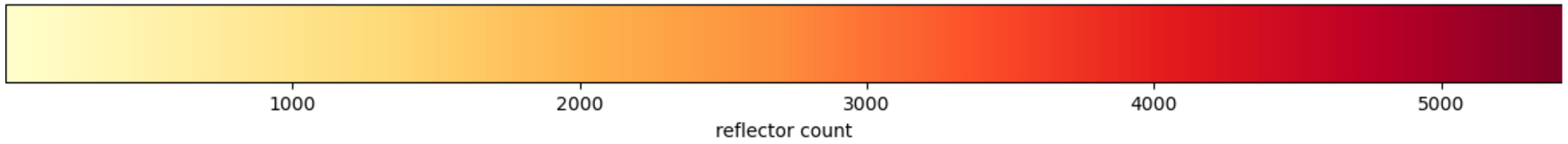
NTP: Atbilžu izmēru sadalījums (BAF) – rets/unikāls skats



LATVIJAS UNIVERSITĀTE

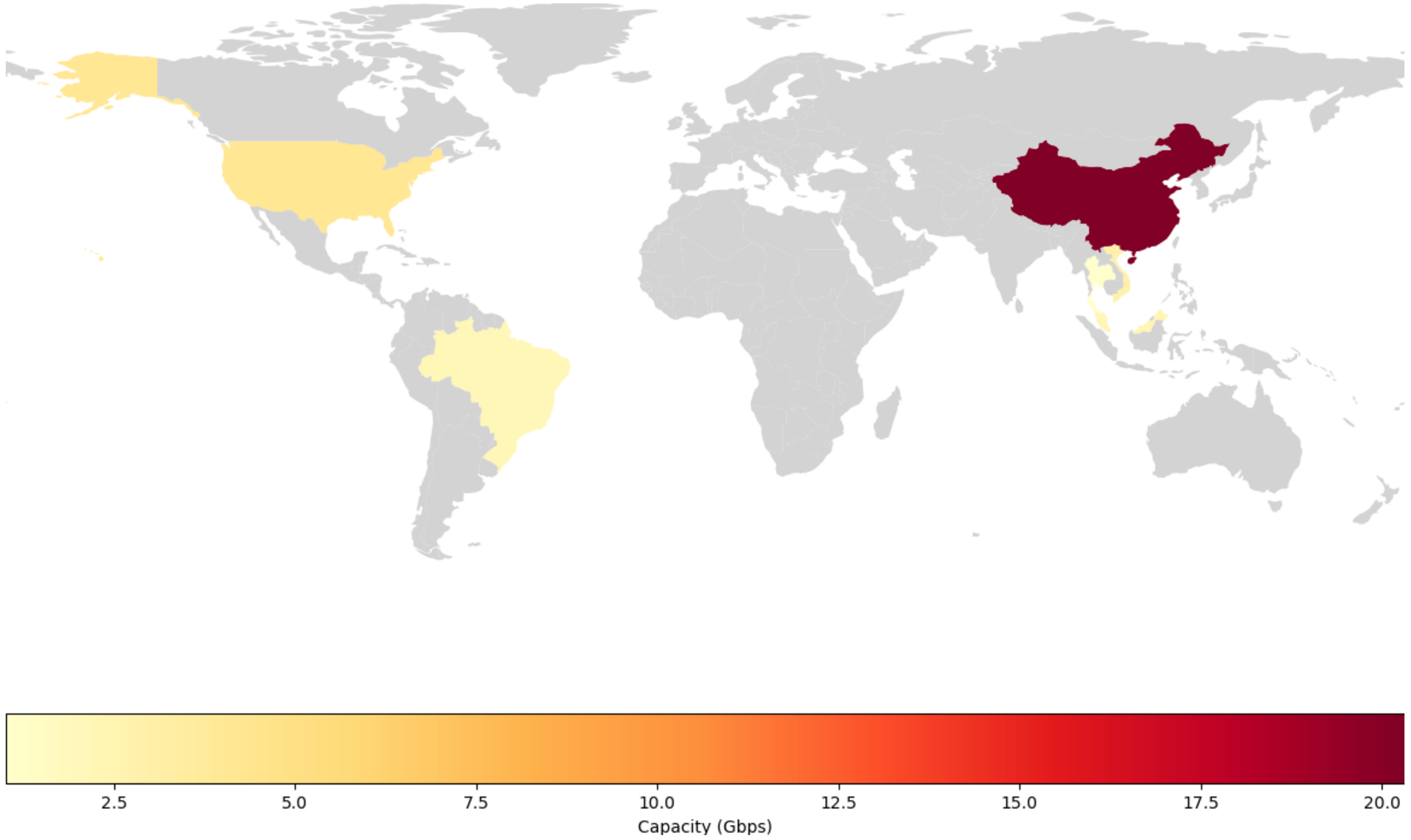
NTP: Ģeogrāfisks sadalījums – Klasika pētniecībā





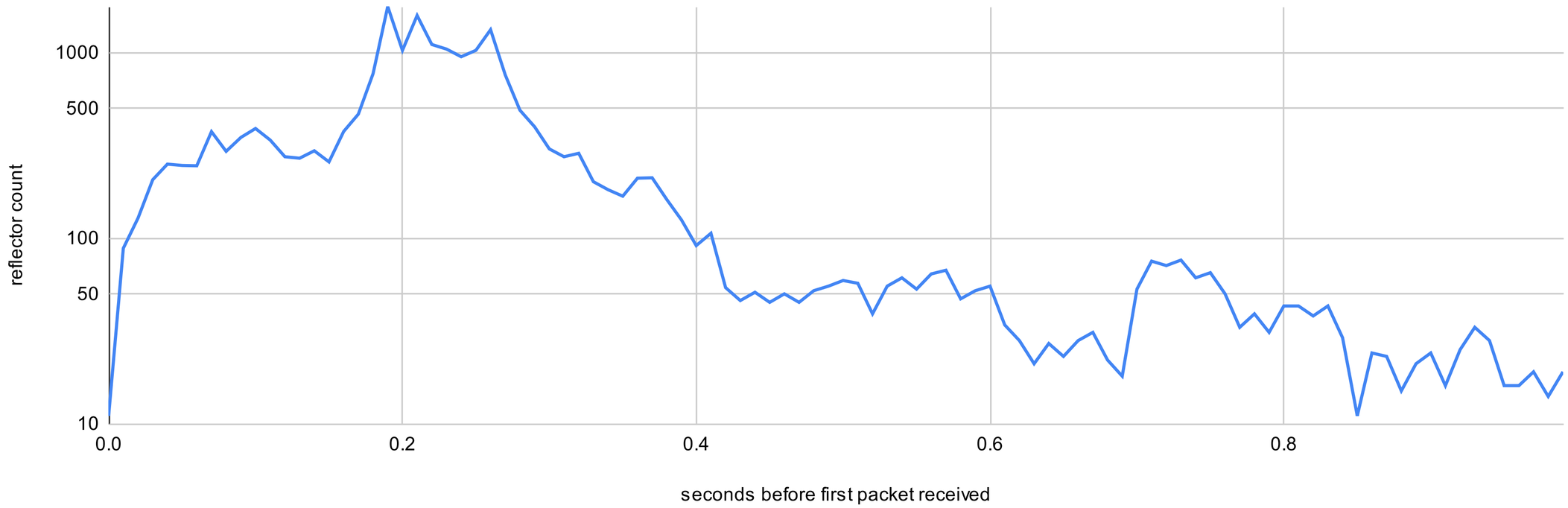
LATVIJAS UNIVERSITĀTE

NTP: Ģeogrāfisks kapacitātes sadalījums (RR80%, min. 1Gbps) – unikāls skats



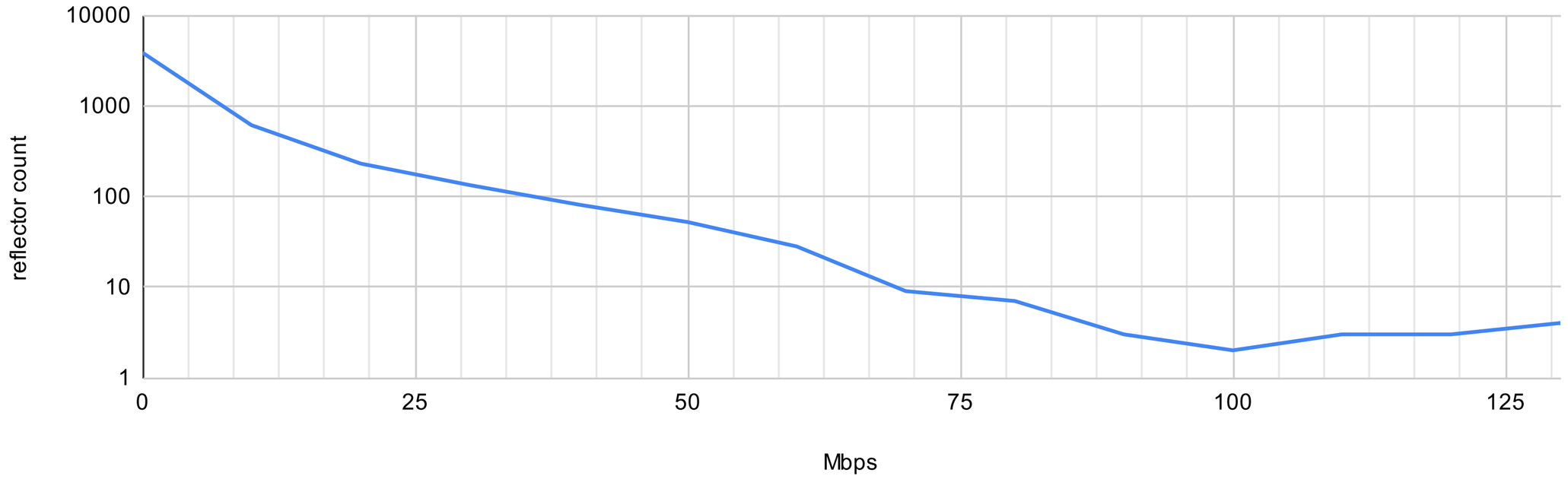
LATVIJAS UNIVERSITĀTE

NTP: Aiztures summa (RTT) – rets/unikāls skats



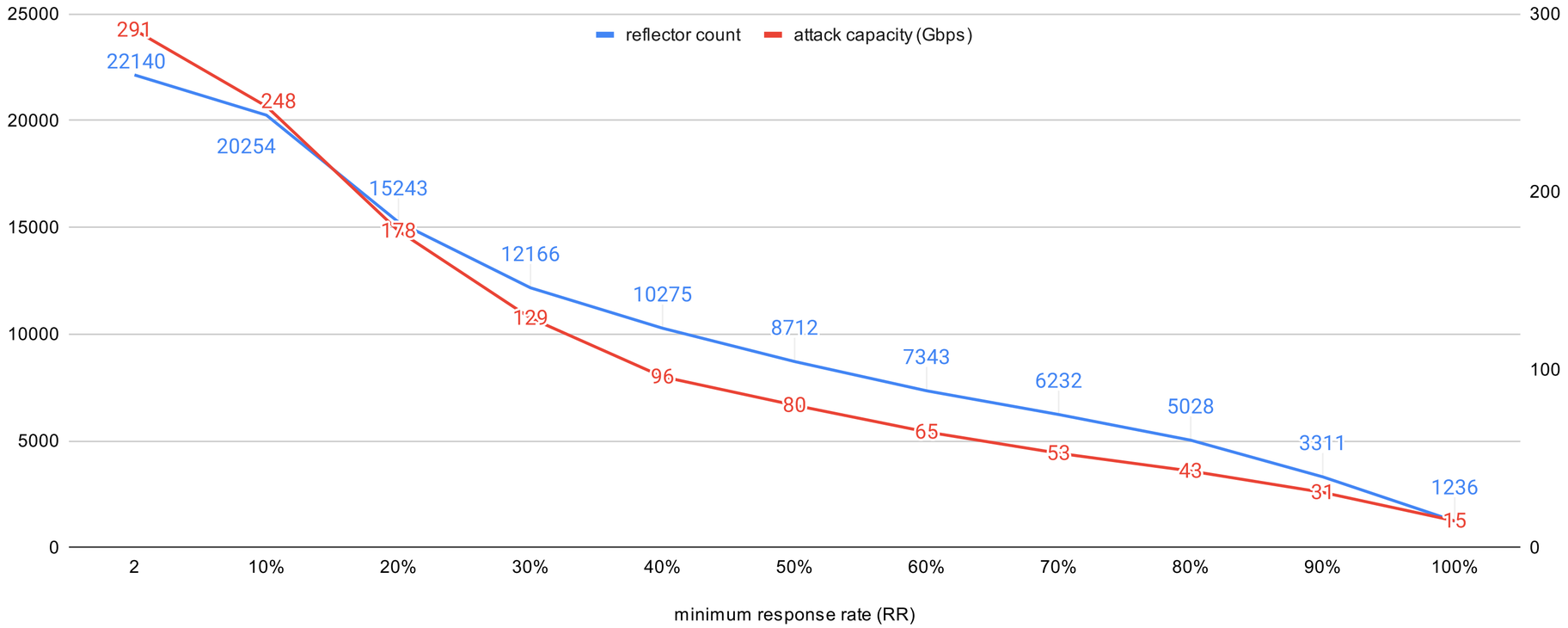
LATVIJAS UNIVERSITĀTE

NTP: Atstarotāju ātrums – unikāls skats



LATVIJAS UNIVERSITĀTE

NTP: Kapacitāte atkarībā no ierobežojumiem (RR) – UNIKĀLS skats



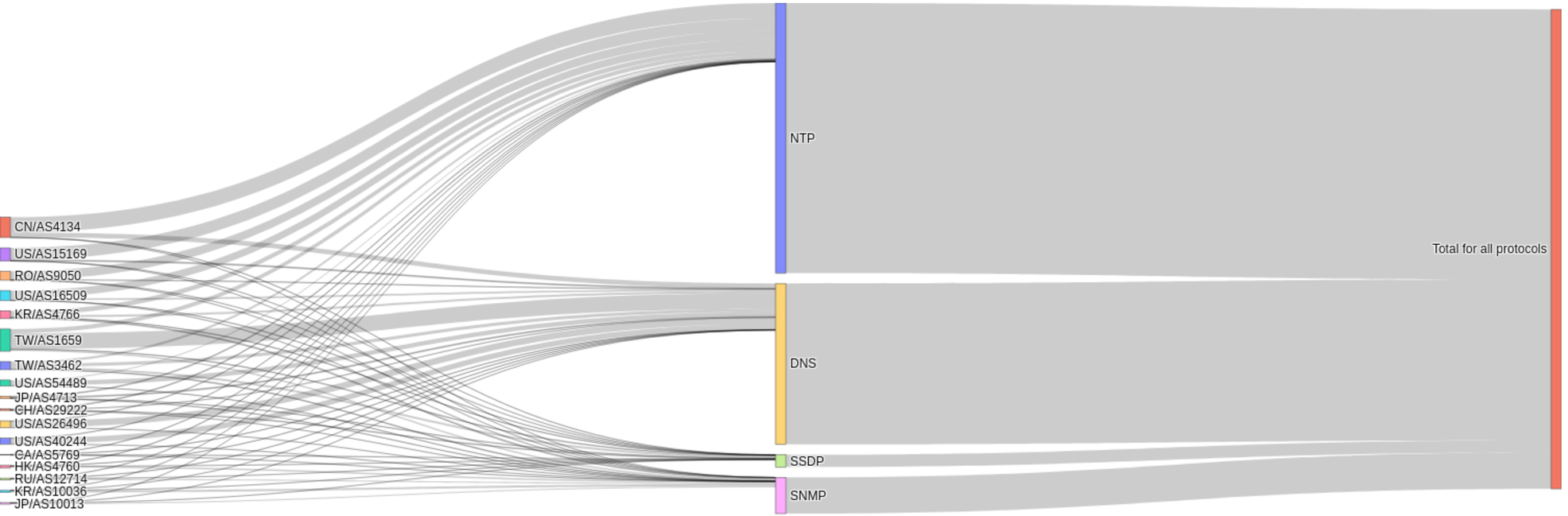
LATVIJAS UNIVERSITĀTE

Rezultāti

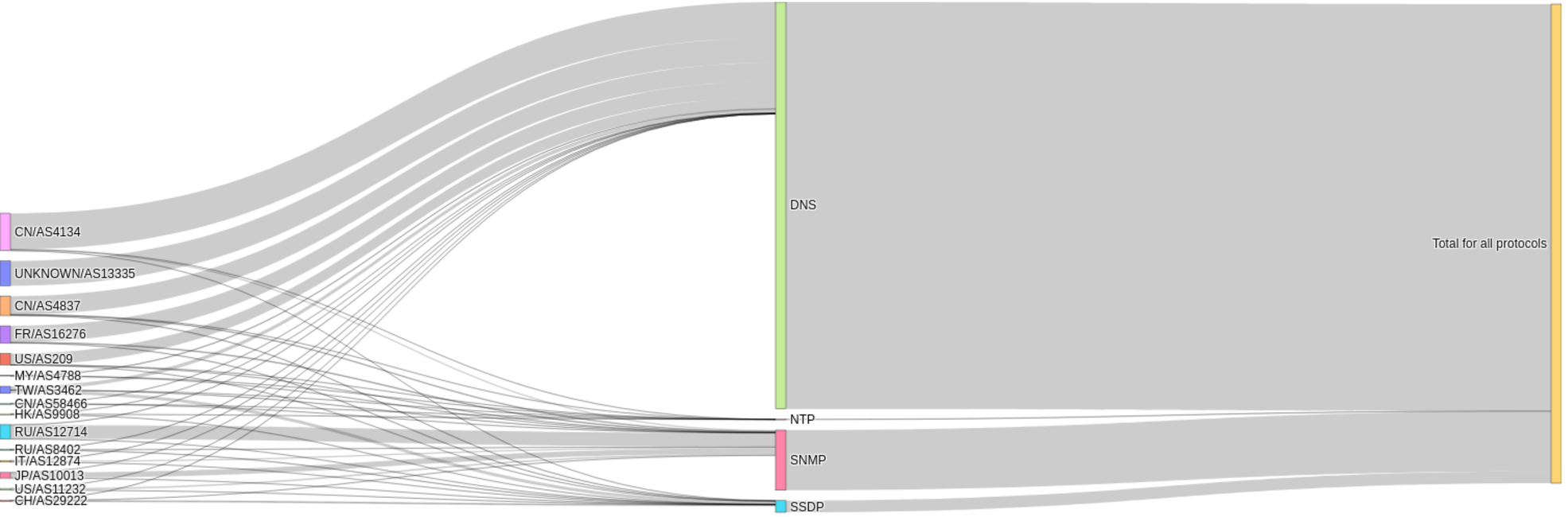
- Aprēķinātā uzbrukumu kapacitāte mērāmajiem protokoliem (Maijs 2020)
  - NTP – **43 Gbps**
  - DNS – **27.5 Tbps**
  - SSDP – **808 Gbps**
  - SNMP – **2.47 Tbps**
  - CLDAP – **870 Gbps**
  - Memcached – nav nomērāms
- 5 protokolu globālā uzbrukumu kapacitāte: **31.33 Tbps**

LATVIJAS UNIVERSITĀTE

Metodoloģiju rezultātu salīdzinājums



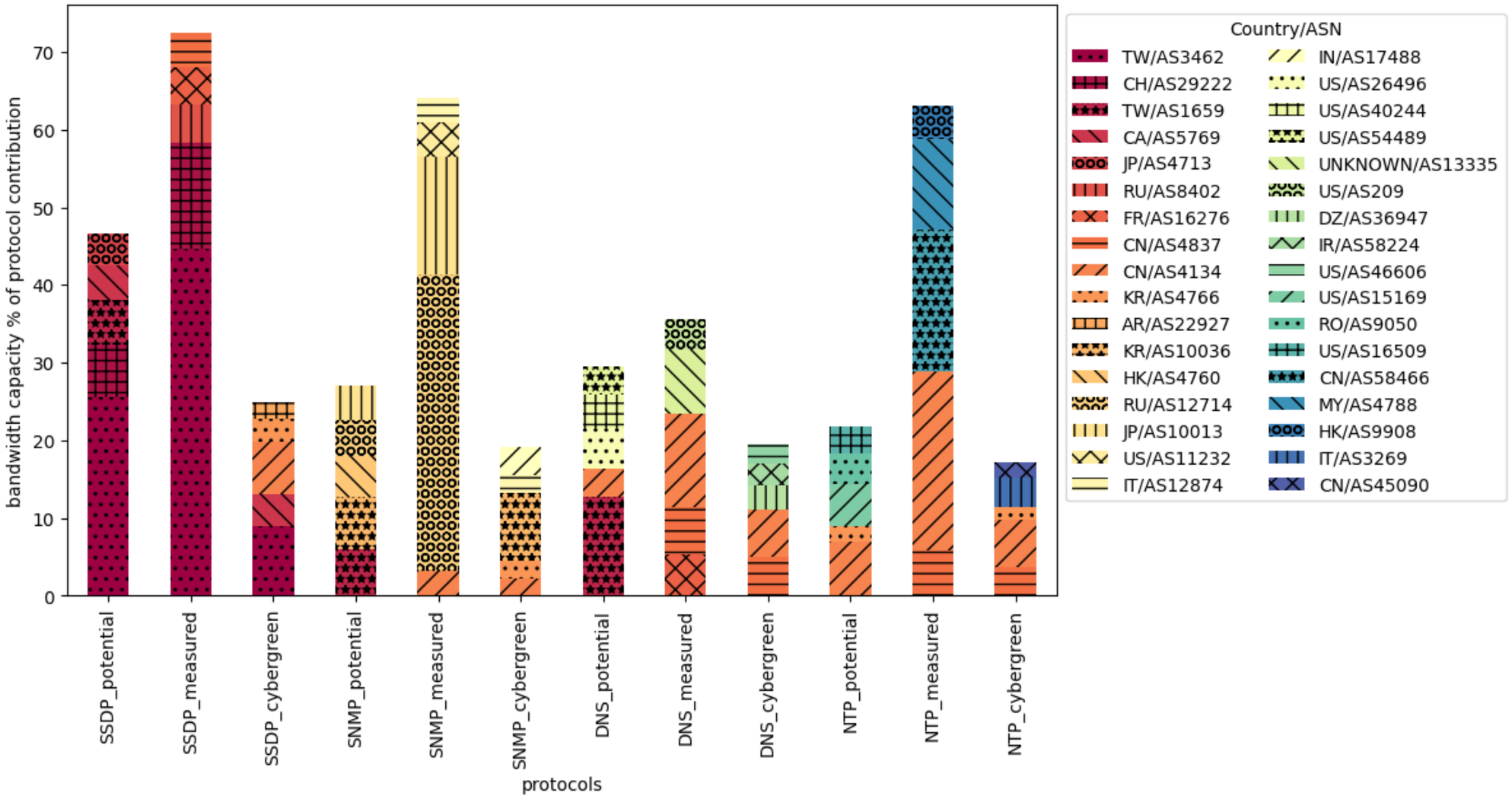
Teorētiskais novērtējums



Mērījumi

LATVIJAS UNIVERSITĀTE

AS uzbrukumu kapacitāte – teorētiskais, mērījums, skaits



LATVIJAS UNIVERSITĀTE

Mērījumi vs. Teorētiskie novērtējumi

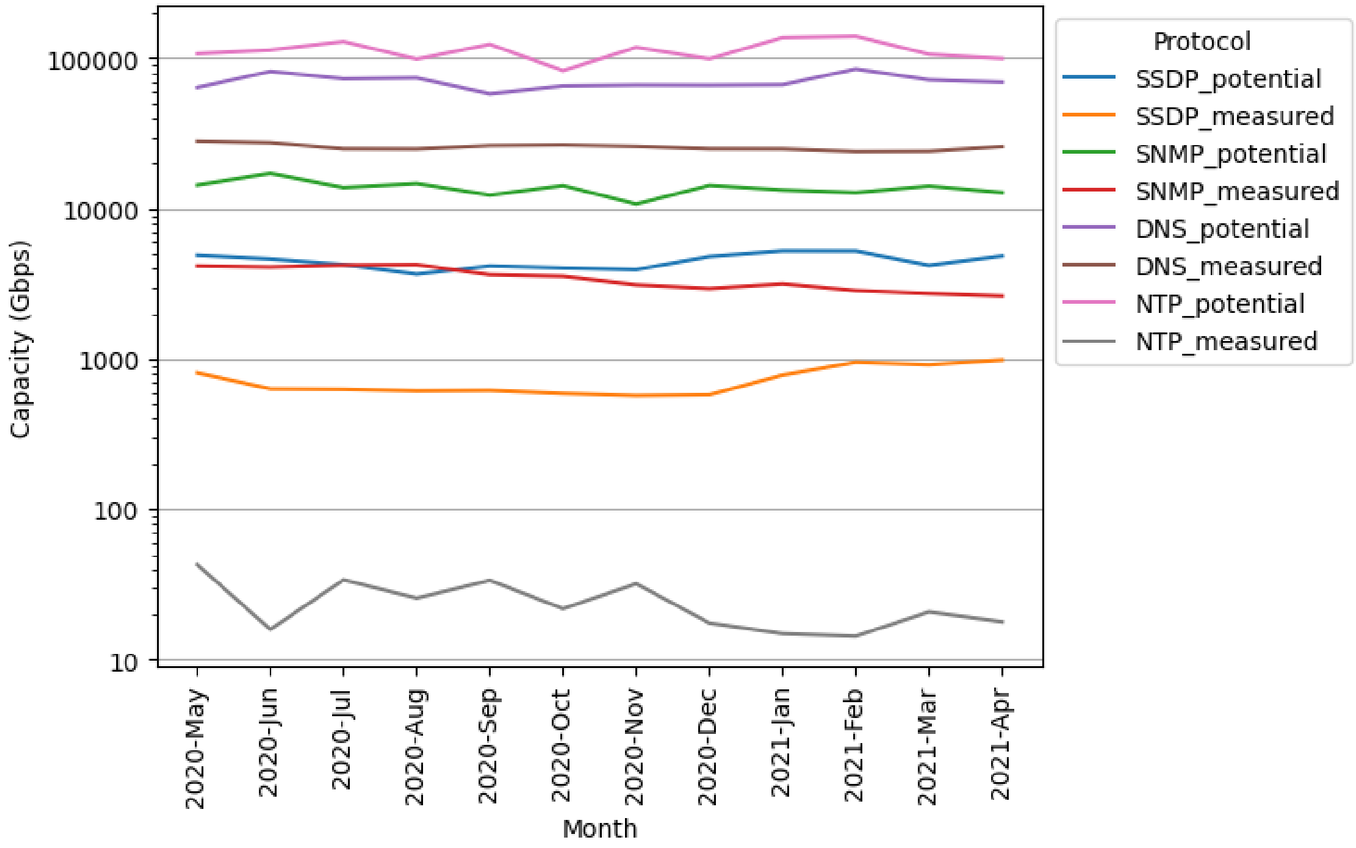
Mērījumi

- Plusi
  - Precizitāte un uzticamība
  - Var noteikt individuālo iekārtu ierobežojumus (RRL, ātrumu, amplifikāciju)
  - Var noteikt situācijas uzlabojumus (pēc periodisku mērījumu uzsākšanas)
- Mīnusi
  - Nav iespējams atskatīties vēsturē
  - Ja ir izmaiņas mērīšanā, tad dati var kļūt nesalīdzināmi

Teorētiskie novērtējumi

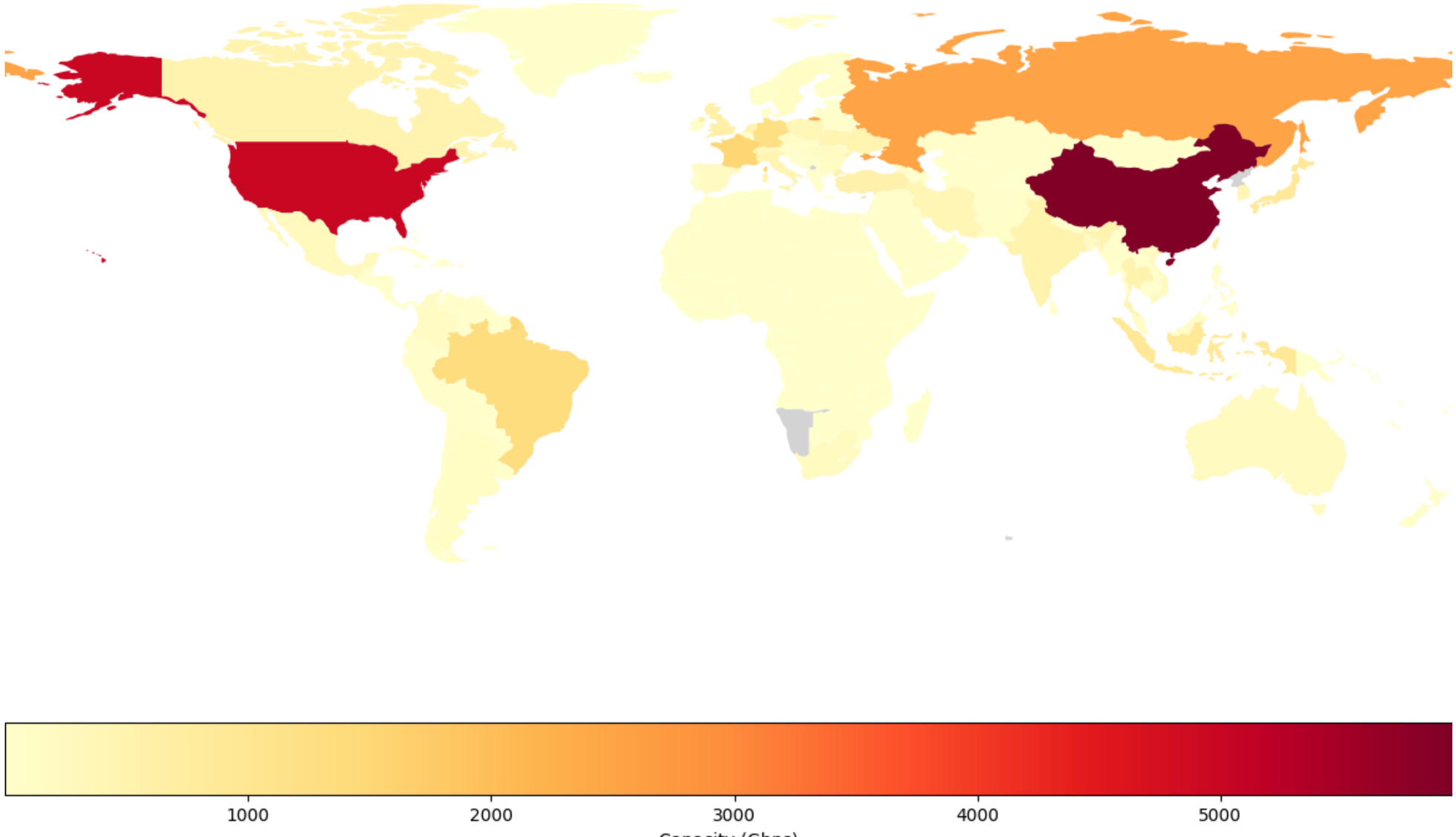
- Plusi
  - Maz resursu, lai ātri veiktu novērtējumu
  - Var mainīt datu avotus
  - Var aprēķināt novērtējumu jebkuram laika posmam, ja ir dati
- Mīnusi
  - Nevar noteikt sasniedzamai iekārtai realizētos ierobežojumus (RRL)
  - Nevar novērtēt iejaukšanos un uzlabojumus

Izmaiņas gada griezumā



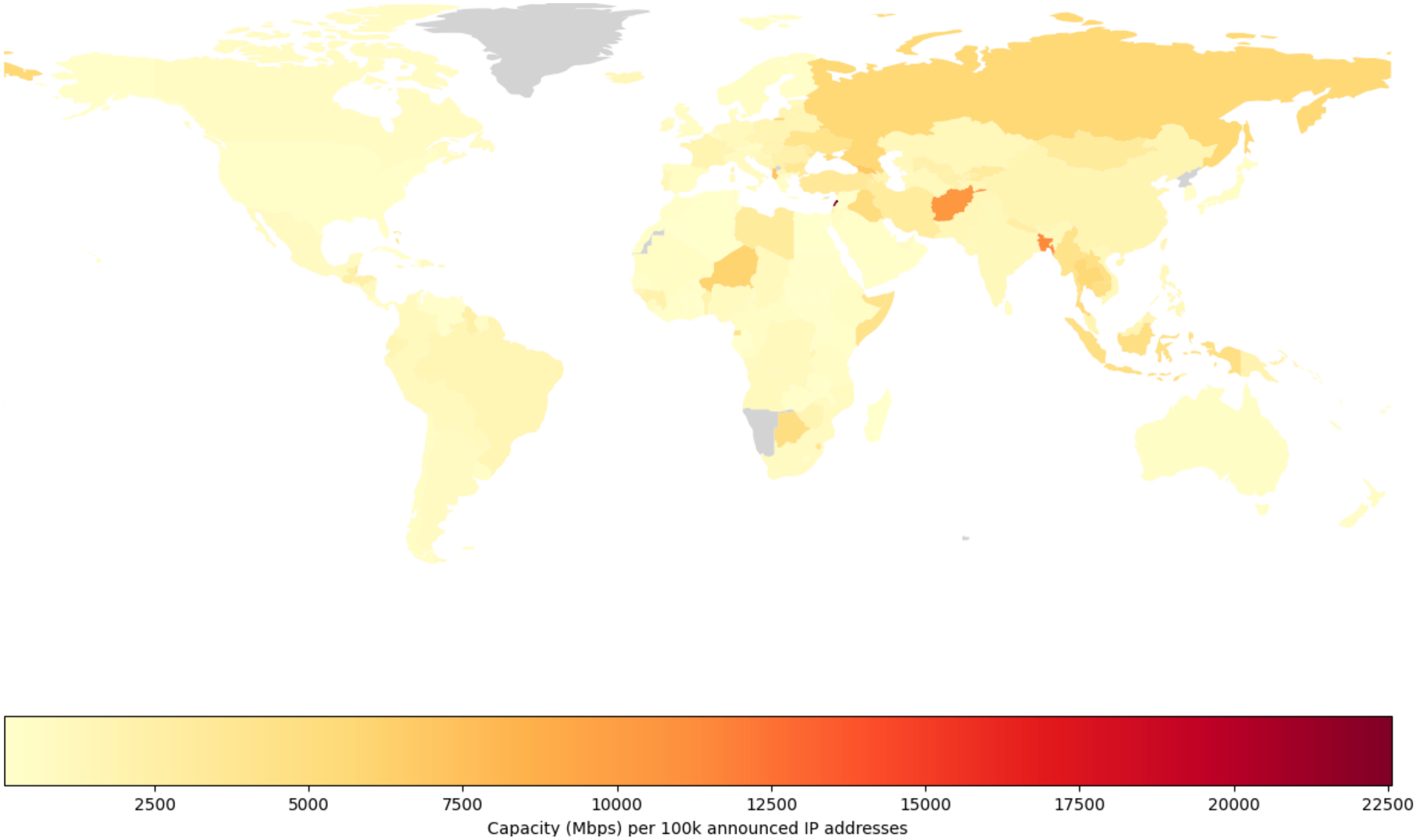
LATVIJAS UNIVERSITĀTE

4 protokolu kapacitāte (Maijs 2020)



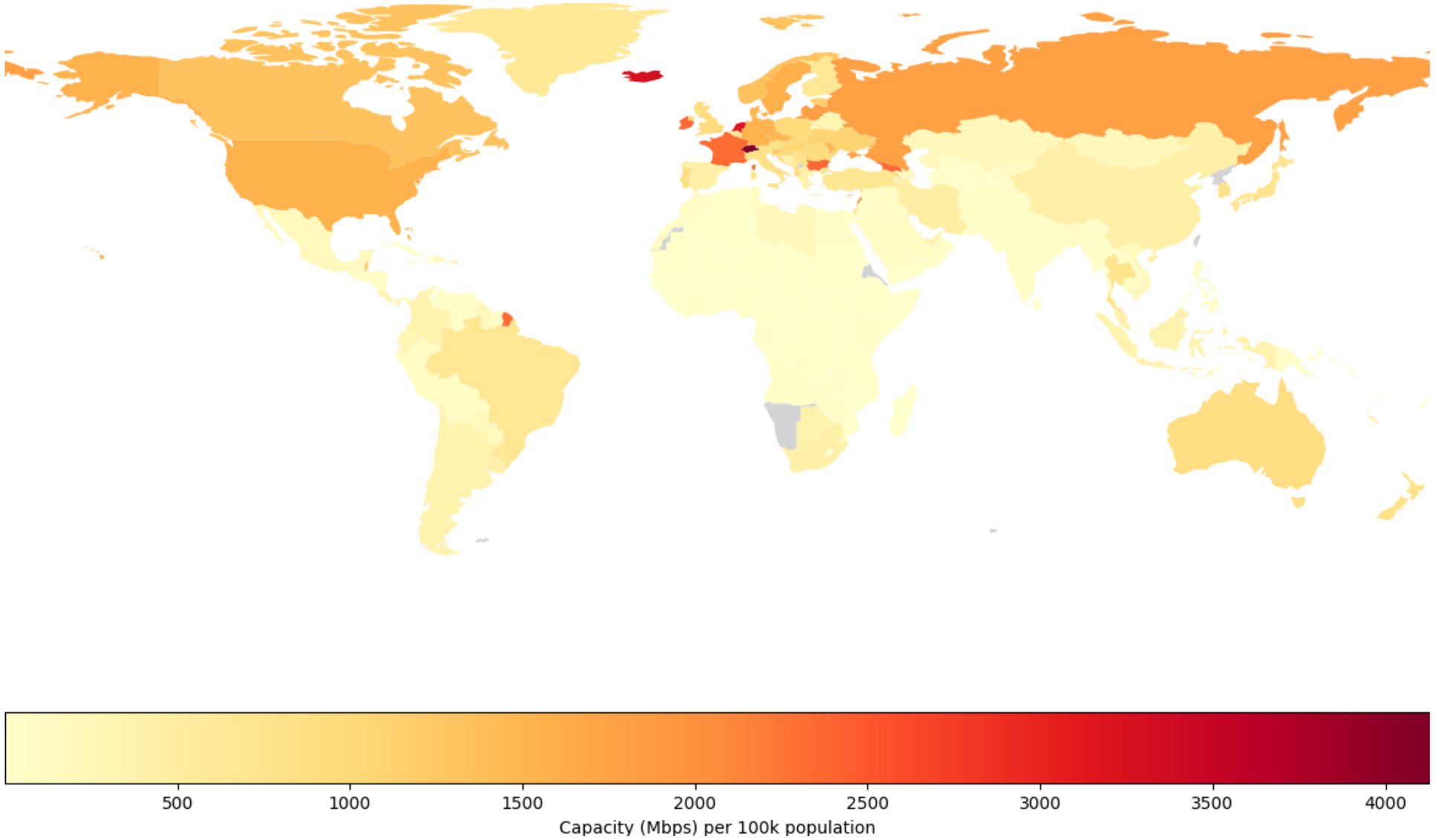
LATVIJAS UNIVERSITĀTE

4 protokolu kapacitāte (Maijs 2020) – relatīvi pret IP adrešu skaitu



LATVIJAS UNIVERSITĀTE

4 protokolu kapacitāte (Maijs 2020) – relatīvi pret iedzīvotāju skaitu



LATVIJAS UNIVERSITĀTE

Secinājumi

- Metodoloģija darbojas, bet ar daudz atrunām un ierobežojumiem
- Pirms pētījuma uzsākšanas bija autora pieņēmums, ka teorētiskais novērtējums ir nekvalitatīvs/nederīgs, bet realitātē labi saskan ar mērīšanu un abām metodoloģijām ir sava loma
- AS ietekme un atbildība ir daudz lielāka par valstīm un reģioniem, koncentrēšanās uz valstīm nav korekta (“politkorekta”), bet tagad tas ir pierādīts
- Relatīvas metrikas ir objektīvākas
- Nepieciešama iekārtu klasifikācija – datu skats un atbildība pāriet no AS un valstīm uz konkrētiem ražotājiem

LATVIJAS UNIVERSITĀTE

Paldies par klausīšanos!

LATVIJAS UNIVERSITĀTE