Serverless DNS Analytics using ENTRADA 2.0

Maarten Wullink | DNS-OARC31
Austin TX 1 Nov 2019

SIDN LABS

Challenges

- Previous versions of ENTRADA require Hadoop and you would need:
  - Invest more effort to install and maintain
  - Hadoop knowledge
  - Hardware or virtual Hadoop cluster

ENTRADA 2.0

New features:

- Serverless DNS analytics
- Support for multiple SQL query engines
- Quality of service monitoring, round-trip time (RTT) analysis
- Easy deployment using Docker

Serverless DNS analytics

- No need to deploy any servers
- No hardware/network maintenance cost
- Only pay for amount of data analyzed

ENTRADA will:

- Create database schema
- Convert, upload and optimize data

SIDN LABS

• Serverless DNS analytics

Support for Amazon Web Services (AWS)

- S3 storage
- Athena SQL-query engine
- Pricing; $5 per TB of scanned data

SIDN LABS

Quality of service monitoring

Uses passive DNS-data from real world DNS-clients (not probes) to determine Round Trip Time (RTT) between a resolver and the authoritative name server.

High RTT can be caused by:

- Inefficient routing
- Congestion
- Router/switch issues

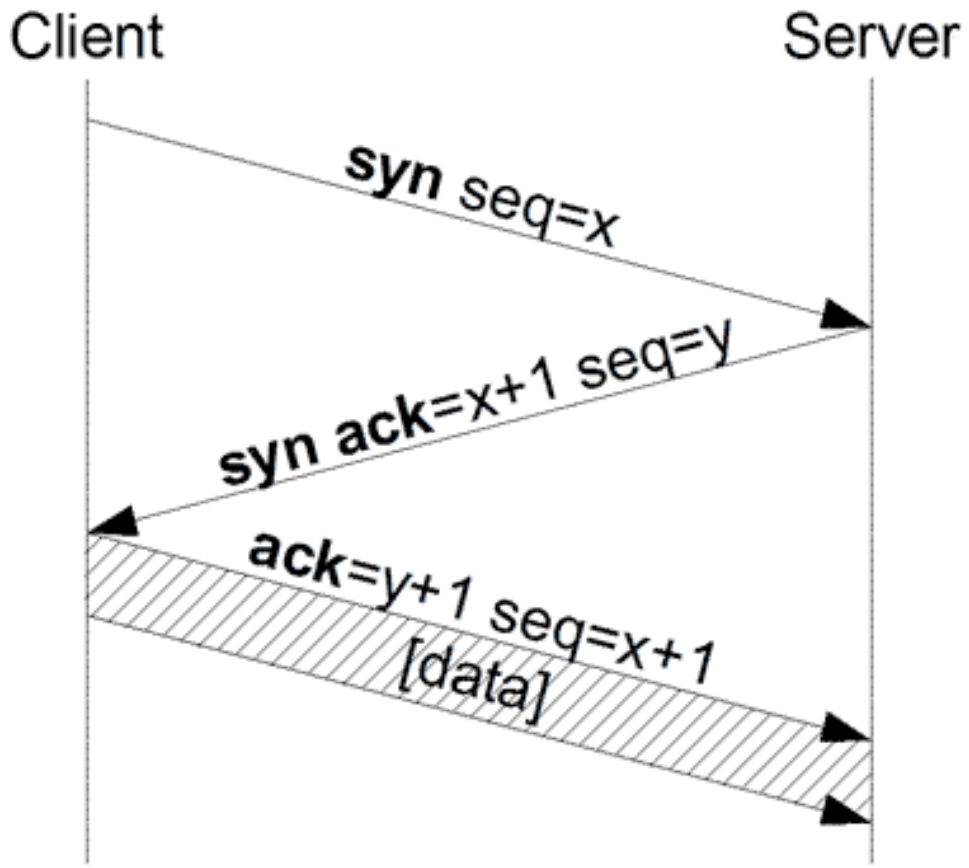
Quality of service monitoring

Analyze the TCP-handshake

For an average day, TCP use:

- 4-5% of queries
- 22-26% of resolvers

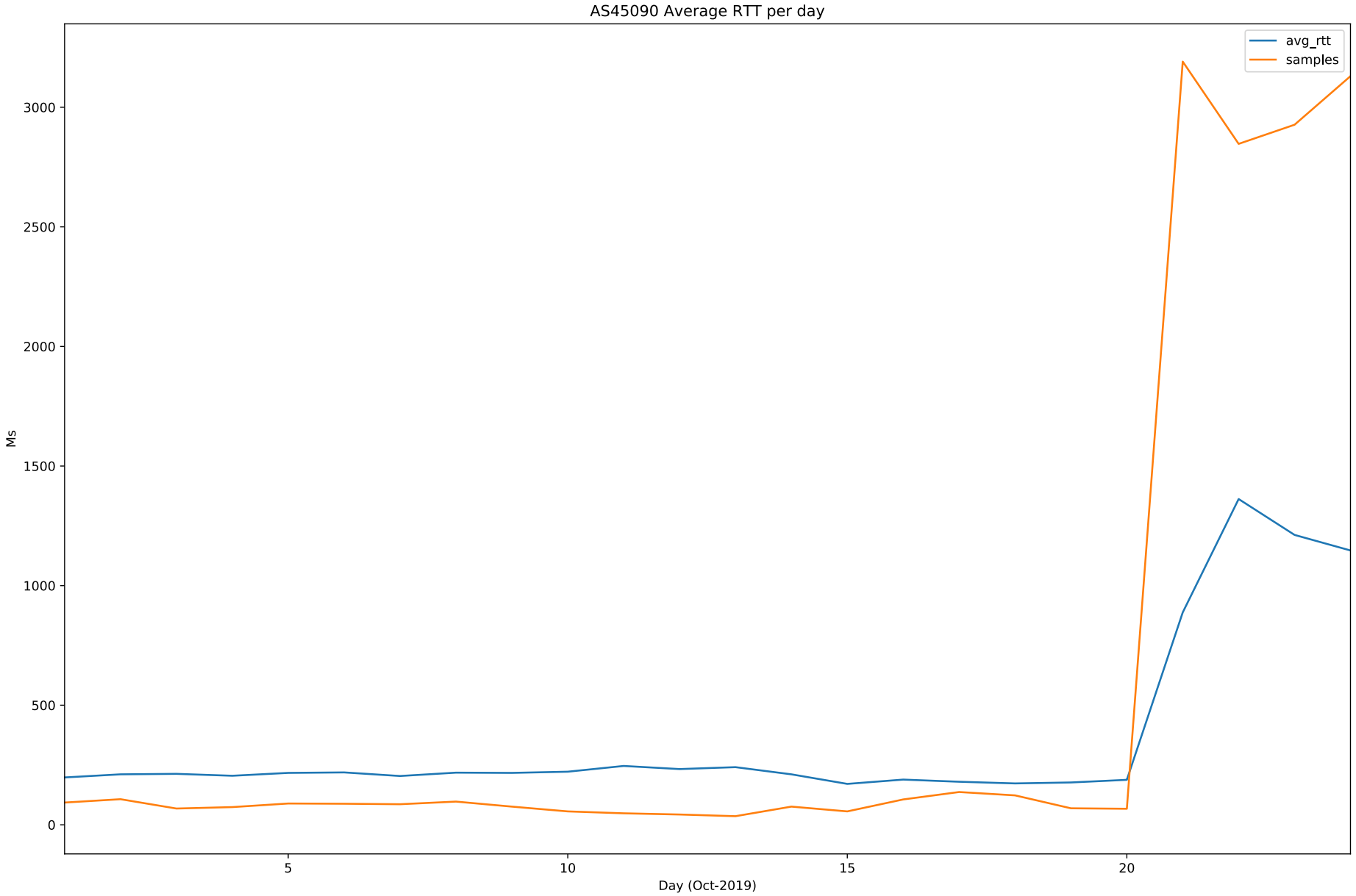
dif(SYN ACK – ACK) = RTT



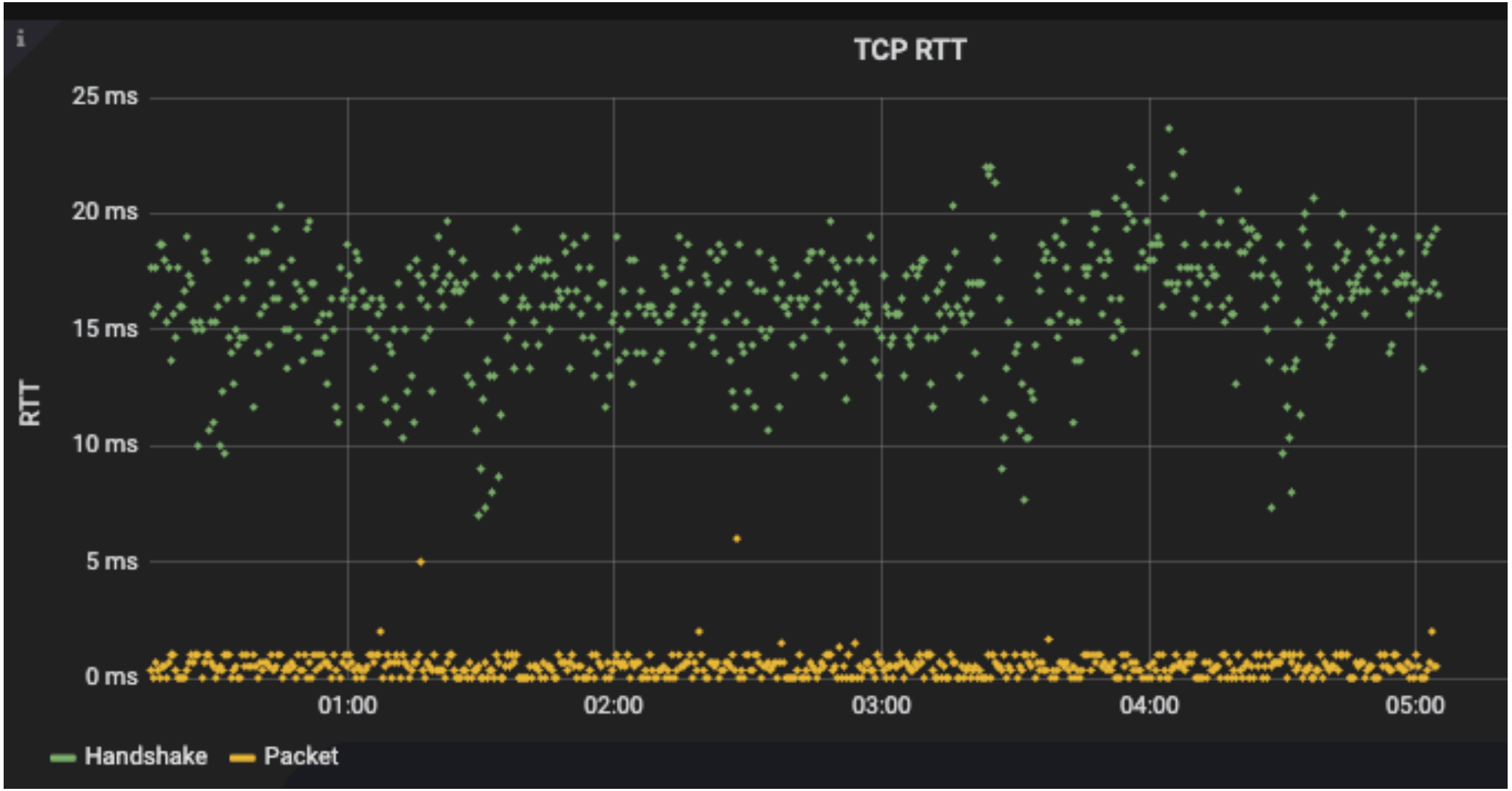
High latency ASNs

asn	Avg RTT	Samples	Operator	Country
45090	1147	3130	Shenzhen Tencent Computer Systems Company Limited	CN
34205	436	716	PJSC Rostelecom	RU
24361	357	2326	CERNET2 IX at Southeast University	CN
4538	298	6256	China Education and Research Network Center	CN
56044	298	4721	China Mobile communications corporation	CN
132525	287	1733	HeiLongJiang Mobile Communication Company Limited	CN
1221	282	4478	Telstra Corporation Limited	AU
56042	280	738	China Mobile communications corporation	CN
24444	274	6361	Shandong Mobile Communication Company Limited	CN

AS45090


AS45090 Average RTT per day
avg_rtt
samples
Ms
0
500
1000
1500
2000
2500
3000
5
10
15
20
Day (Oct-2019)

Quality of service monitor




SIDN.nl


@SIDN


SIDN

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl