

RIPE

# How asymmetric is the internet?

A study to reinforce the use of Traceroute

Wouter de Vries and José Jair Santanna  
Design and Analysis of Communication Systems

**UNIVERSITY OF TWENTE.**

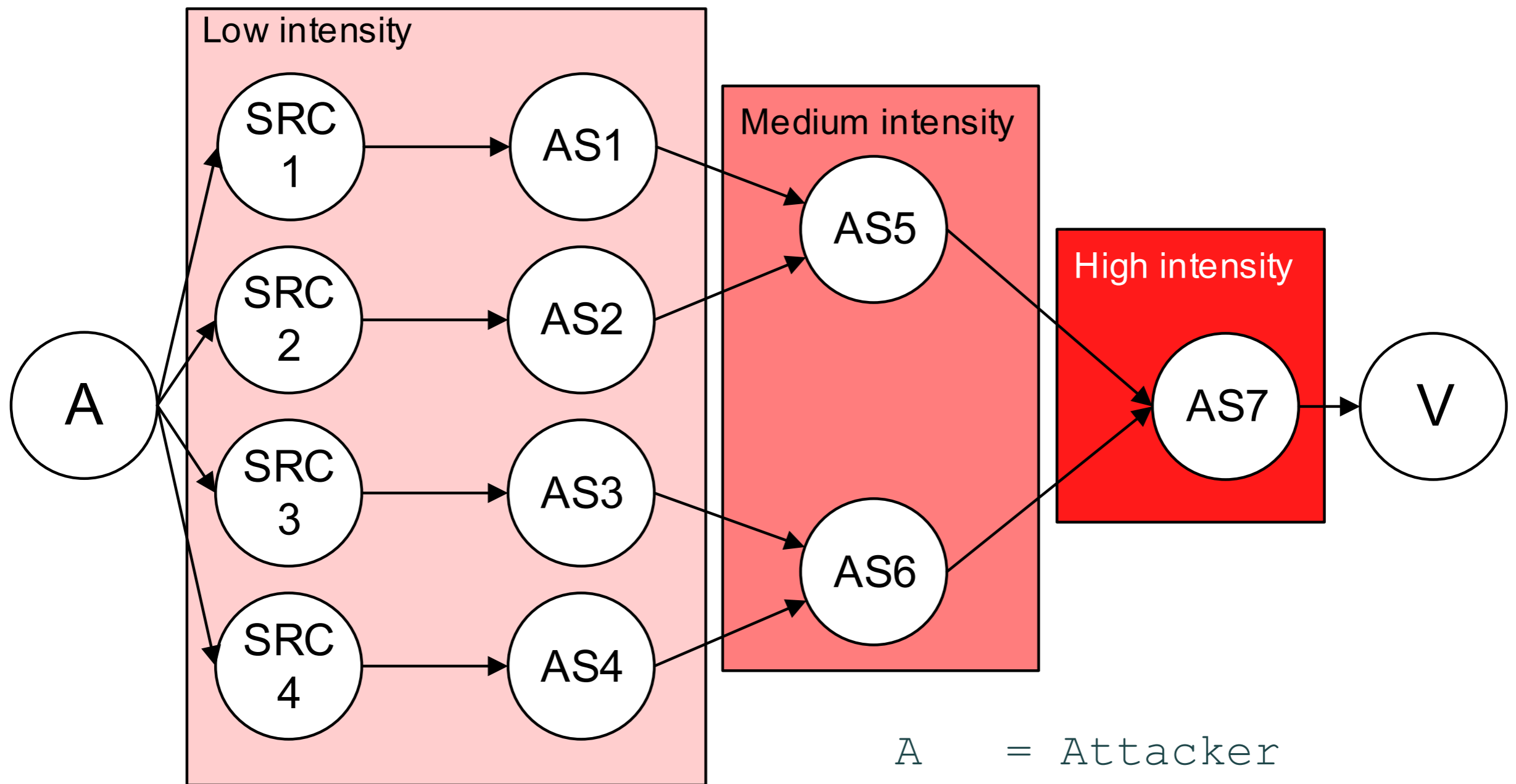


# Introduction – What is the purpose?

---

- Toward the mitigation of DDoS attacks
- Which networks does a DDoS pass through
- Mitigate the attack as close to the source as possible

# Introduction – What is the purpose? (2)



A = Attacker  
SRCn = Source of traffic  
ASn = Autonomous System  
V = Victim



# Why on the AS Level?

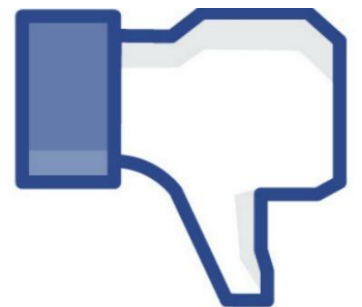
---



## Advantages

VS

## Disadvantages



# Introduction - Problem

---

- Measuring the reverse path of an attacker is less trivial than it seems
- Path can be, and often is, asymmetric[1][2][3]

[1] Y. He, M. Faloutsos, S. Krishnamurthy, and B. Huffaker, "On routing asymmetry in the Internet," in Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE, vol. 2, Nov. 2005

[2] Y. He, M. Faloutsos, and S. V. Krishnamurthy, "Quantifying routing asymmetry in the Internet at the AS level." in GLOBECOM. IEEE, 2004

[3] Y. Schwartz, Y. Shavitt, and U. Weinsberg, "On the Diversity, Stability and Symmetry of End-to-End Internet Routes," in INFOCOM IEEE Conference on Computer Communications Workshops, 2010

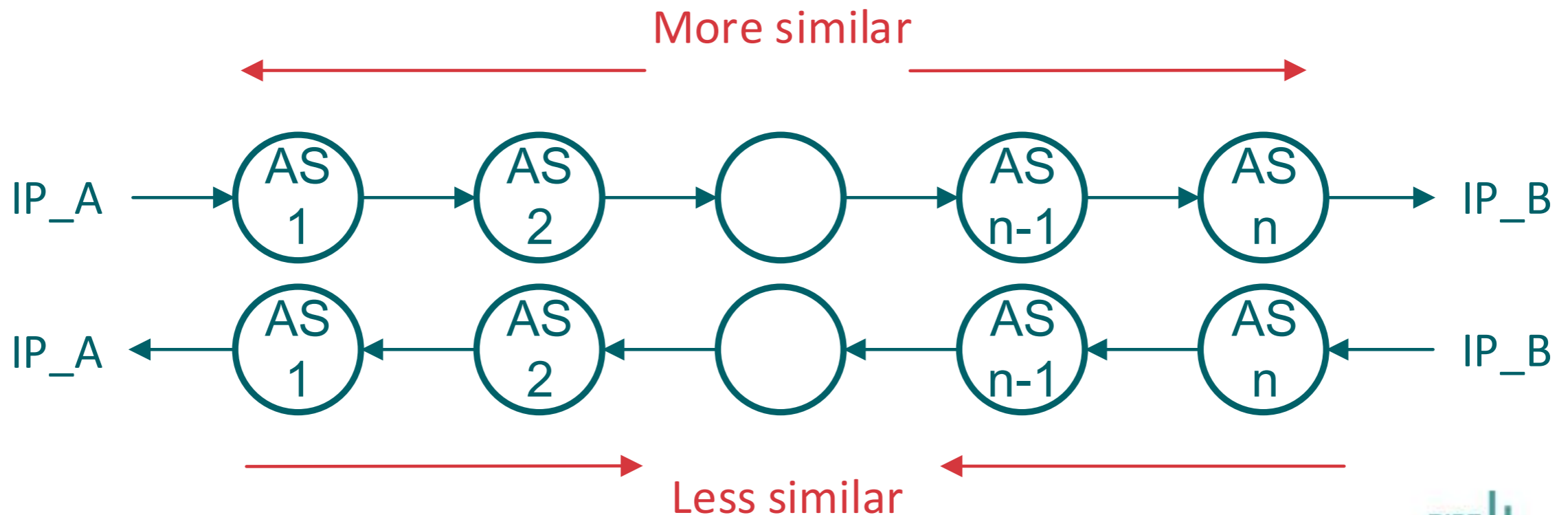


# Introduction – Research question

How asymmetric is the internet?

Expectation:

The internet is more symmetric near the source and target



# Methodology

---

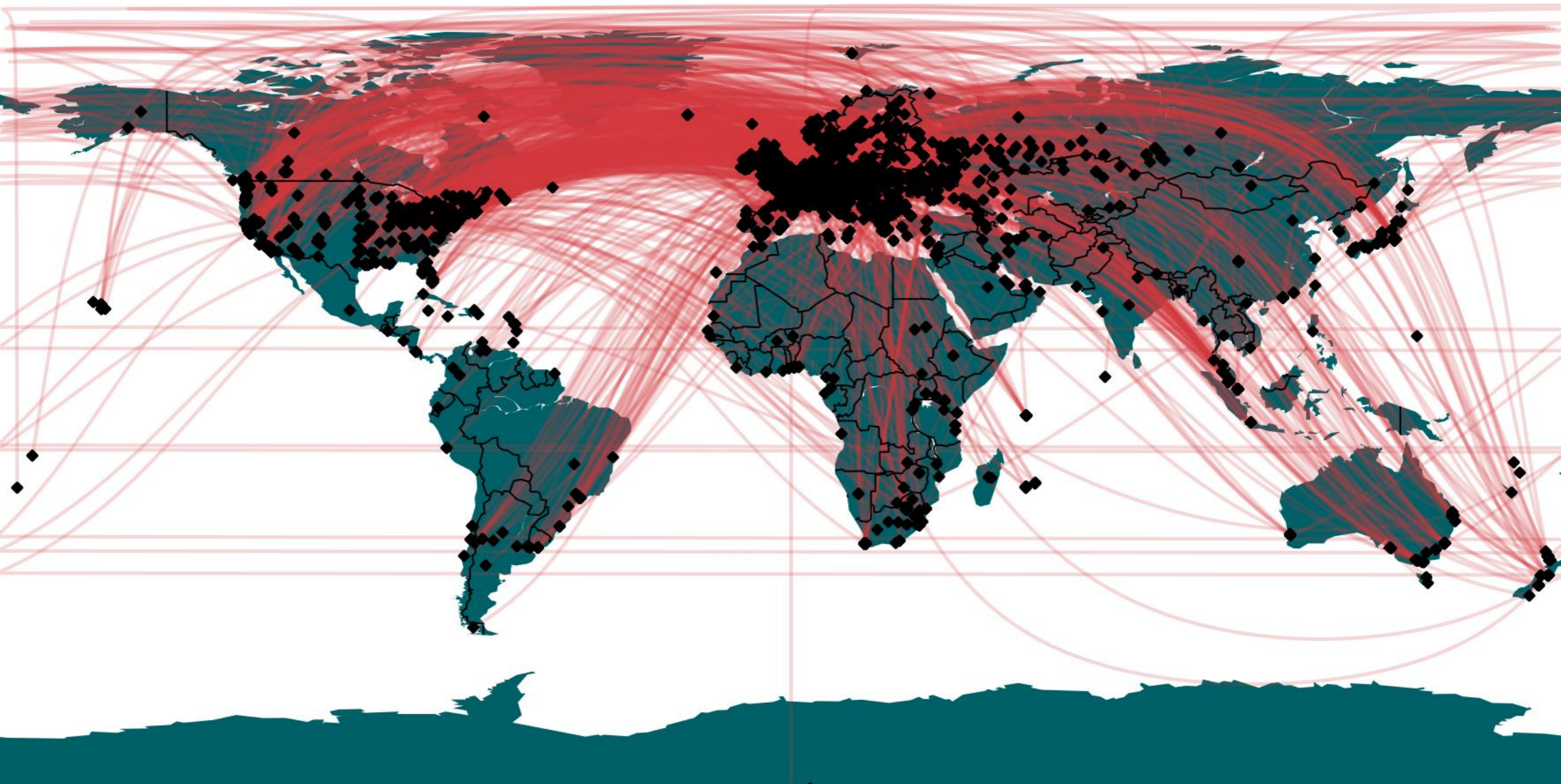
- Large scale measurements, using RIPE Atlas
- **4000** out of 7000\* probes located worldwide
- **2000** pairs of probes to measure paths between
- Thanks to RIPE Atlas our UDM limit was greatly increased

\*Approximately





# Selected probe distribution



Pairs randomly selected





# Methodology – Pairs

---

<b>Continent</b>	<b>Probe count</b>	<b>Fraction</b>
Europe	2.681	67,03%
North America	724	18,10%
Asia	267	6,68%
Africa	157	3,93%
Oceania	109	2,73%
Others	62	1,55%
<b>Total</b>	<b>4.000</b>	<b>100%</b>

# Experiment setup

---

- Traceroute
- Two measurements every three hours per pair
- Ten days
- 80 samples per pair
- 160.000 measurements
- 5.256.138 records
- ~1 gigabyte



# Analysis – Determining ASN

---

- BGP Routing tables (Provided by RIS/RIPE)
- Process to list of IP-range/ASN tuples
- Use binary tree to quickly match IP address to ASN with longest prefix matching

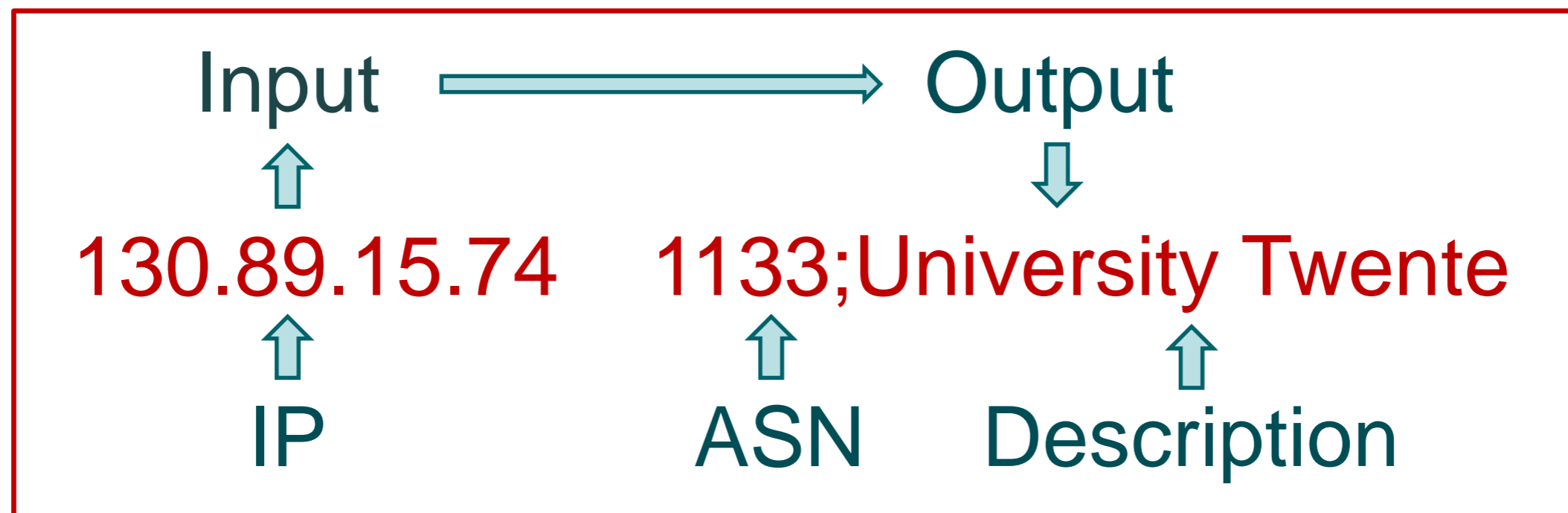


**RIPE**  
**NCC**

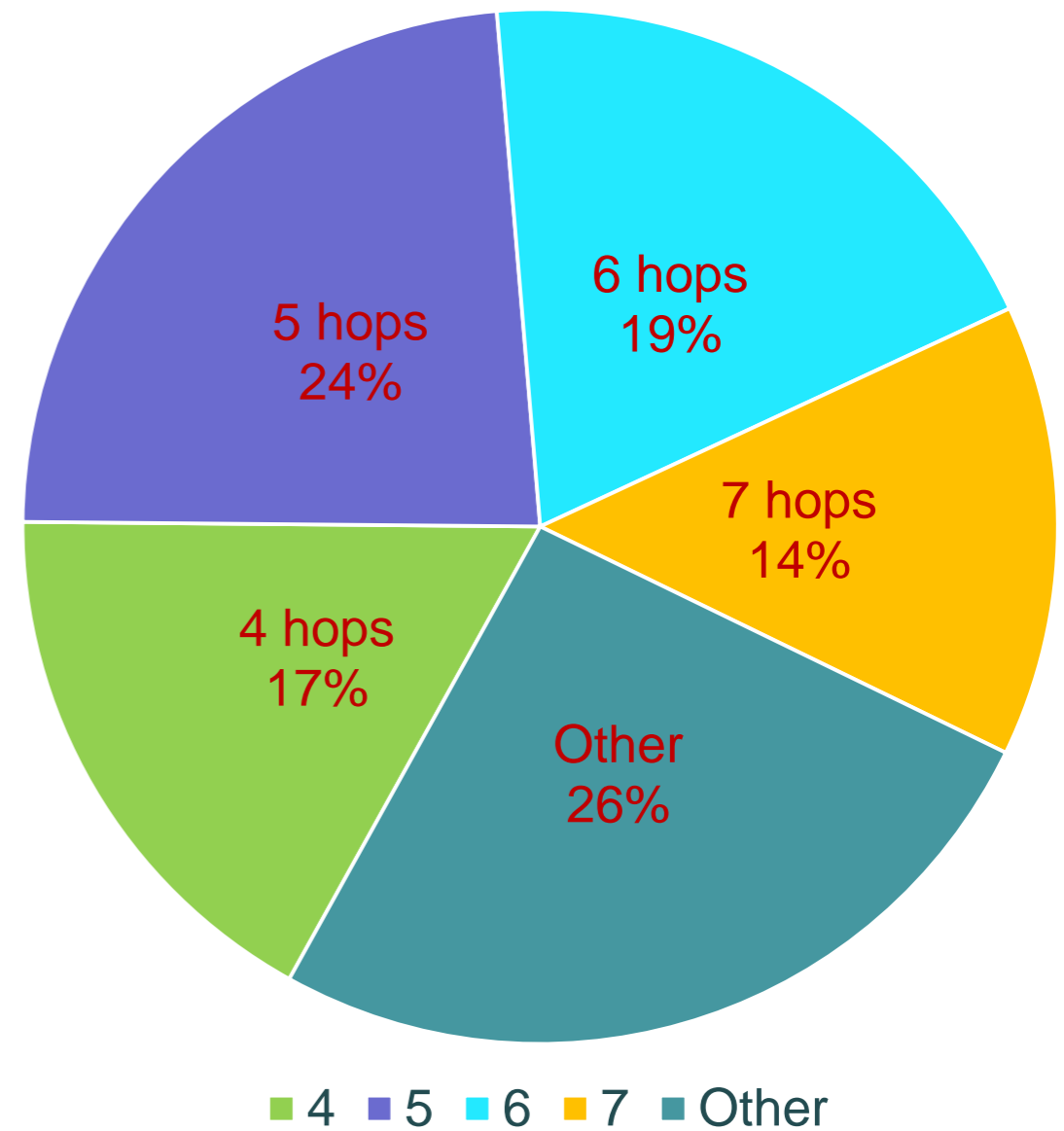
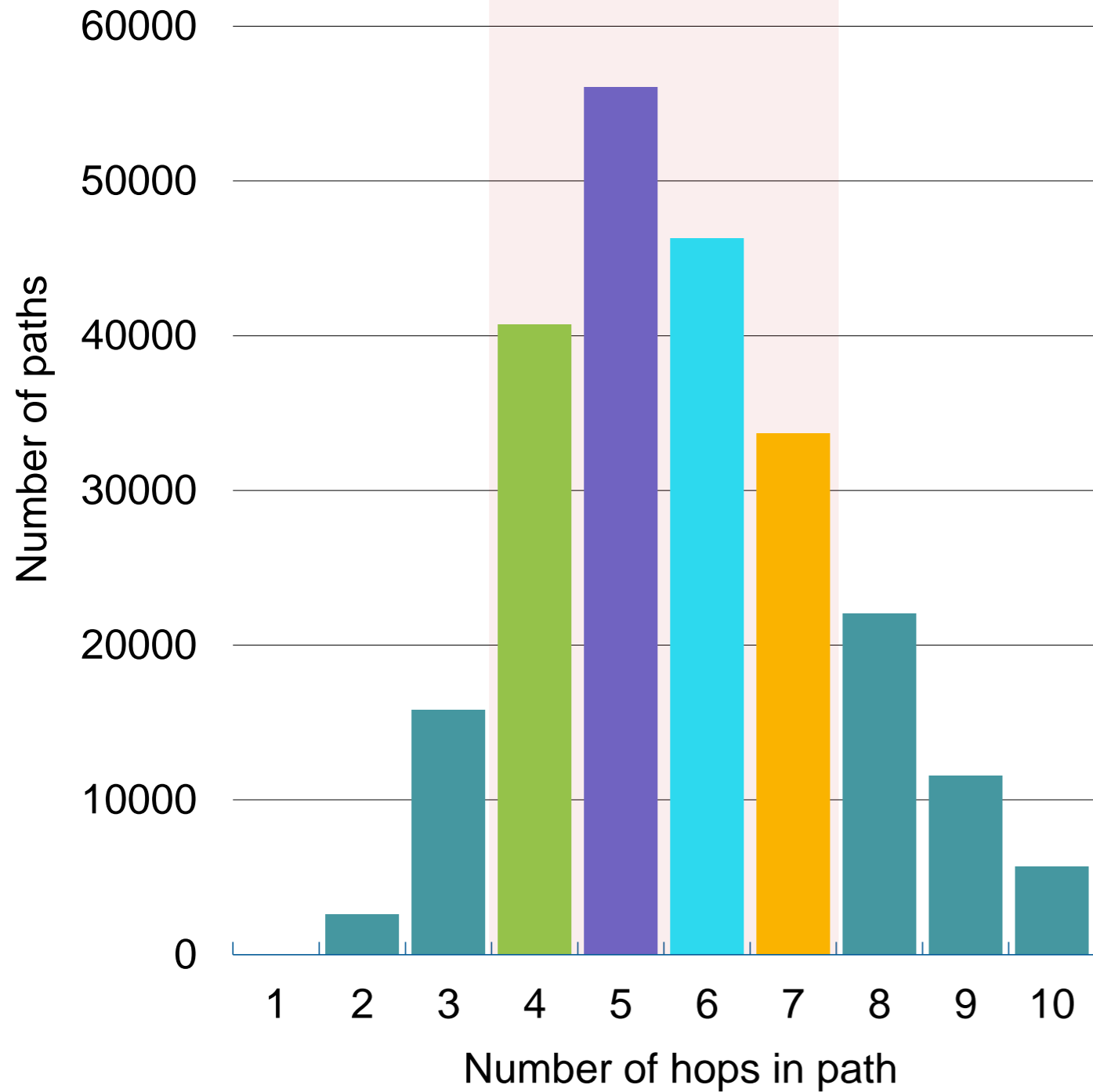


# Analysis – Determining ASN (2)

- Tool to process binary BGP routing table  
<http://bit.ly/XXRstd>
- Tool to build a list of IP-range/ASN tuples  
<http://bit.ly/1tJDoTt>



# Results – Path length on the AS level





# Results – The numbers

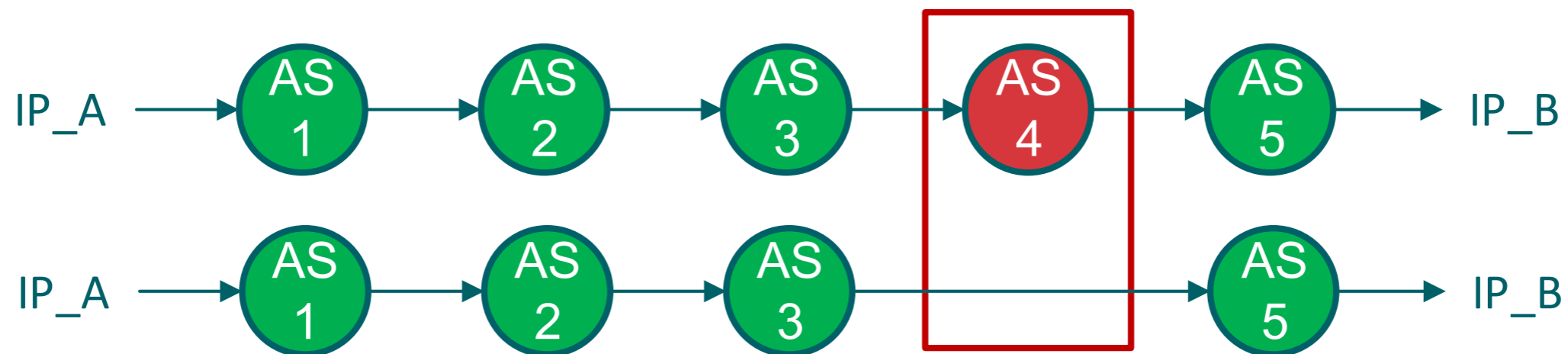
---

- **119.550** measured network paths
- **2.275** unique Autonomous Systems in total
- **1.717** contain probes
  
- **12.6%** (**15.053**) of pairs are symmetric

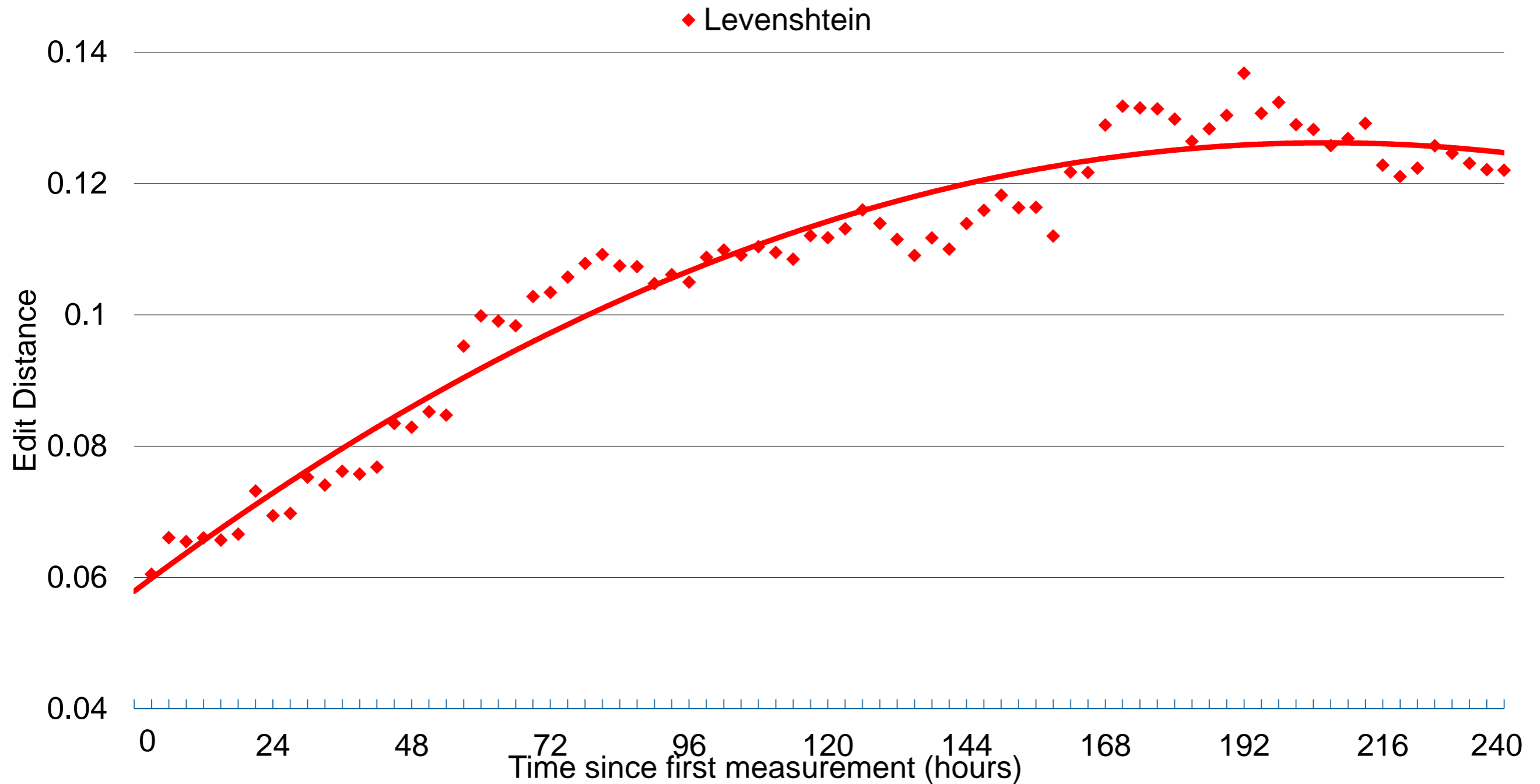
# Results – Change of path over time

- Compare paths from A to B over time
- Determine Levenshtein distance to make two paths equal
- Compare each path to first path

*For example path from A to B with 1 insert/delete/change operation*



# Results – Change of path over time (2)



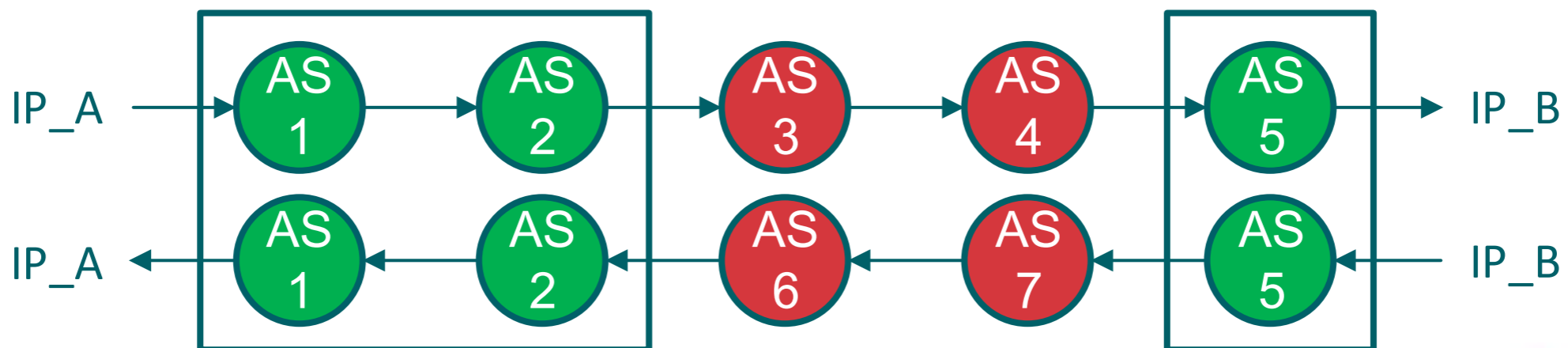
Network paths barely change over time\*



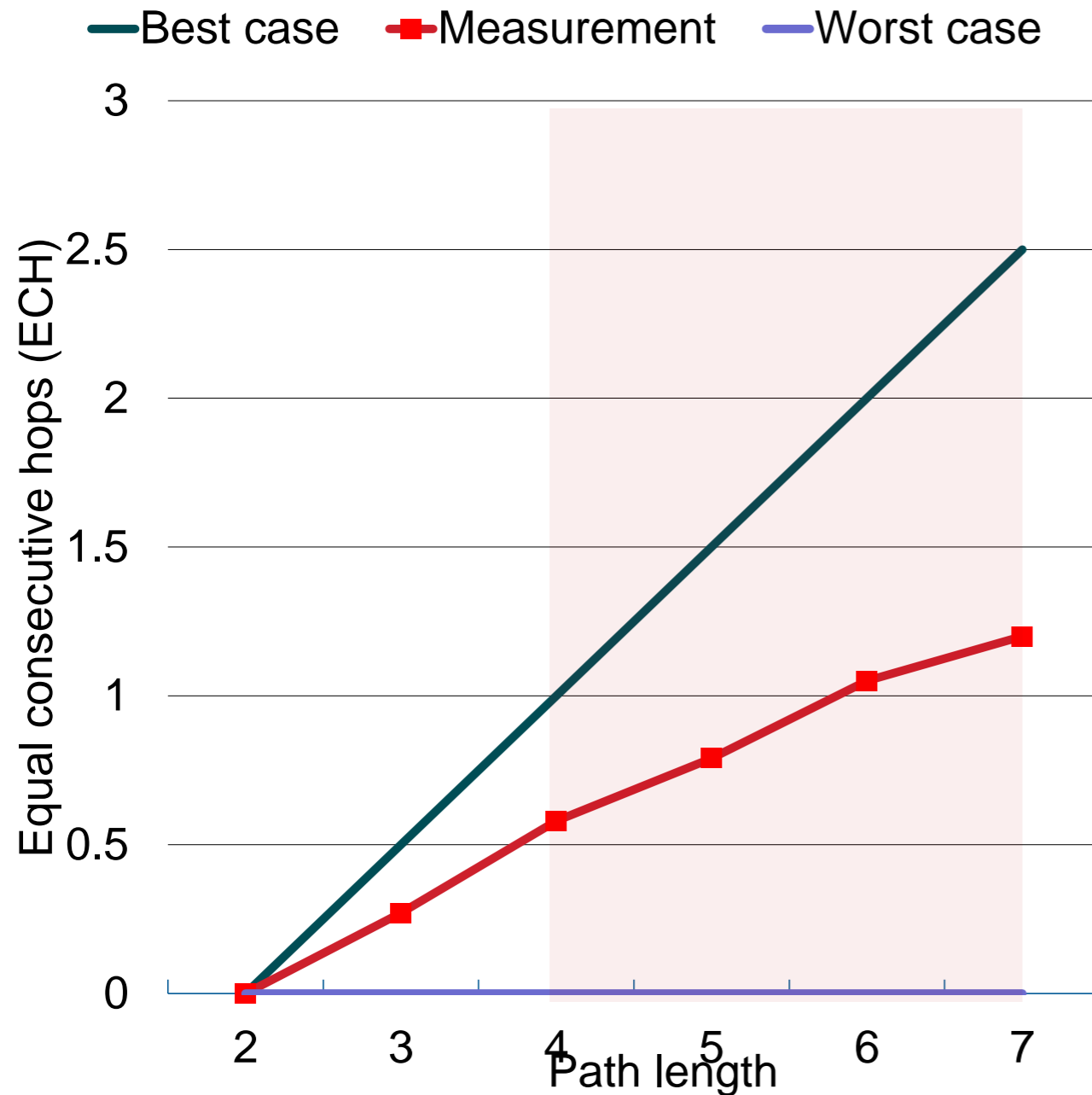
# Results – Equal Consecutive Hops

- Count number of Equal Consecutive Hops (ECH) from left to right and right to left.
- Group by path length
- First and last hop are always equal

*2 + 1 = 3 Consecutive equal hops*



# Results – Equal Consecutive Hops (2)



#	Samples	Std. Dev.	ECH
2	792	0	0
3	8164	0.498	0,27
4	20.038	0,733	0,58
5	27.870	1,013	0,79
6	23.442	1,299	1,05
7	17.223	1,492	1,2

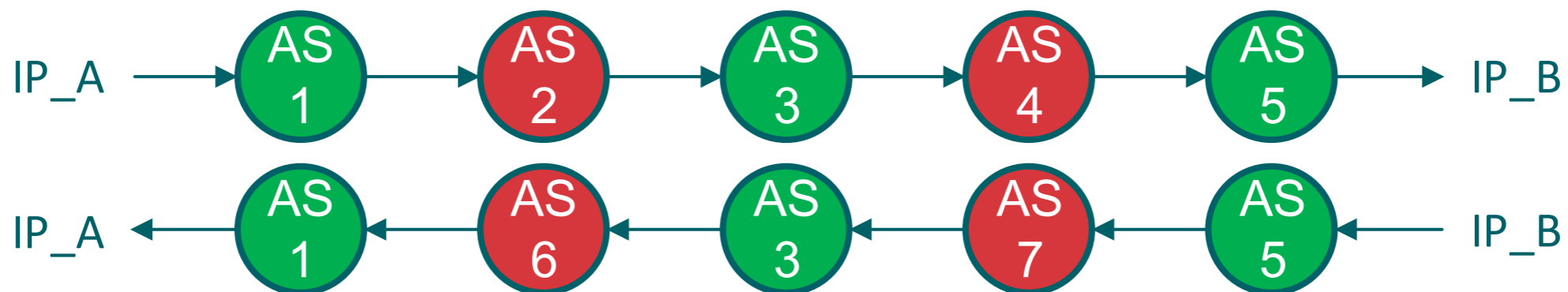
One extra chance to mitigate DDoS attacks



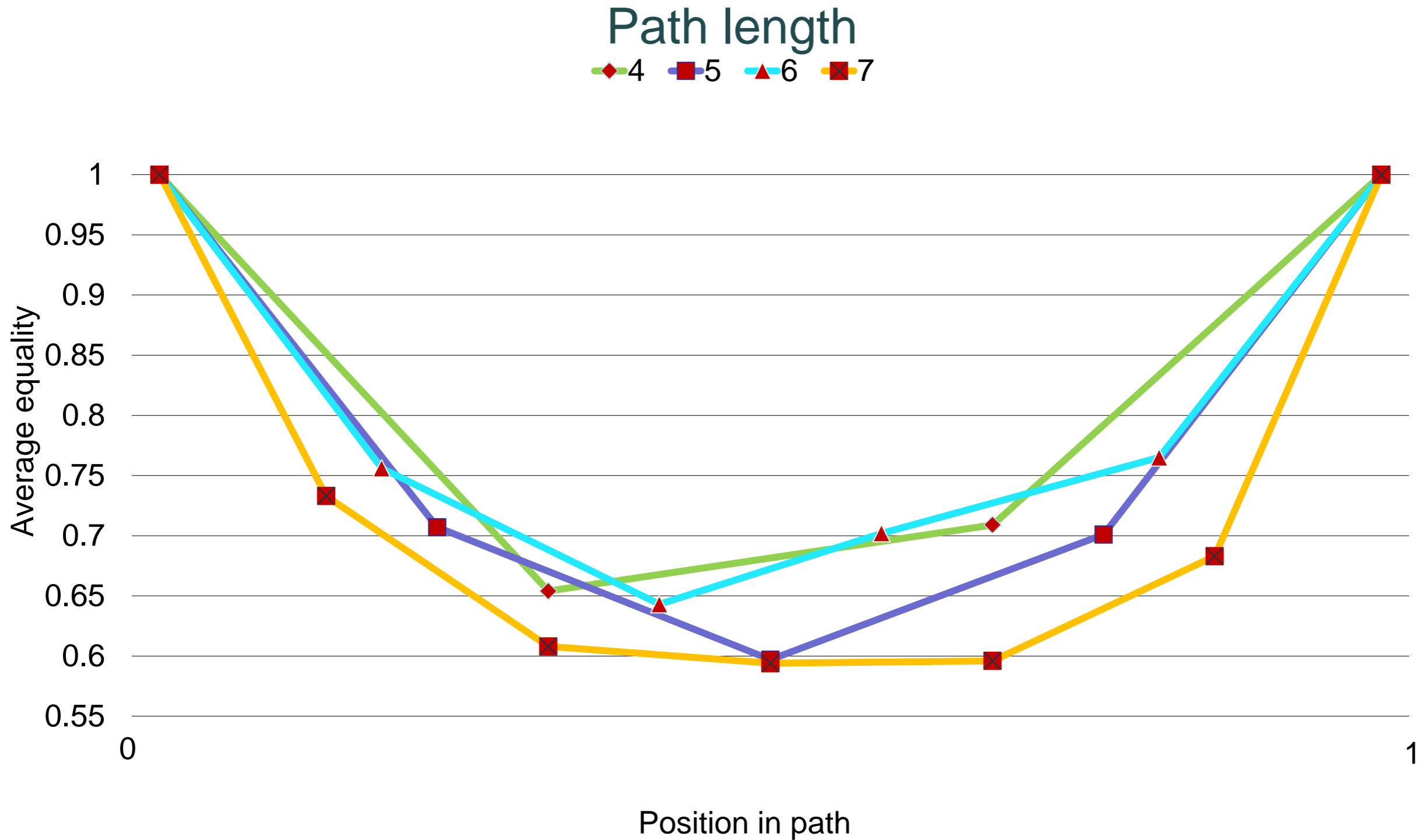


# Results – Equality by position

- Compare hop in forward path to the one in the same position in reverse path
- Either equal (1) or not equal (0)
- Average per position



# Results – Equality by position (2)



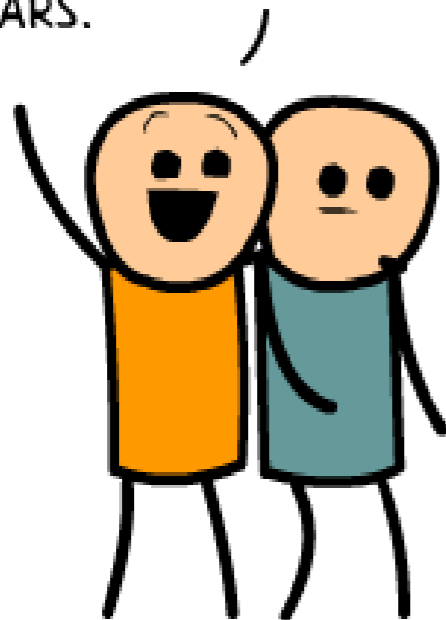
High chance to have equal hops



# Conclusion

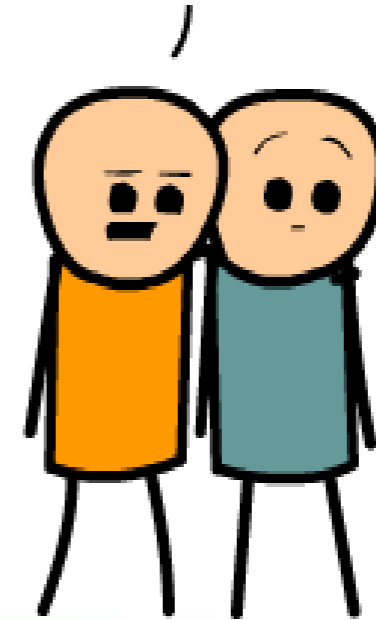
- Internet is mostly asymmetric
- Paths barely change over time
- At least one more chance to mitigate DDoS attacks

SHOOT FOR THE MOON!  
EVEN IF YOU MISS, YOU'LL  
END UP AMONG THE  
STARS.



Replace with  
relevant figure

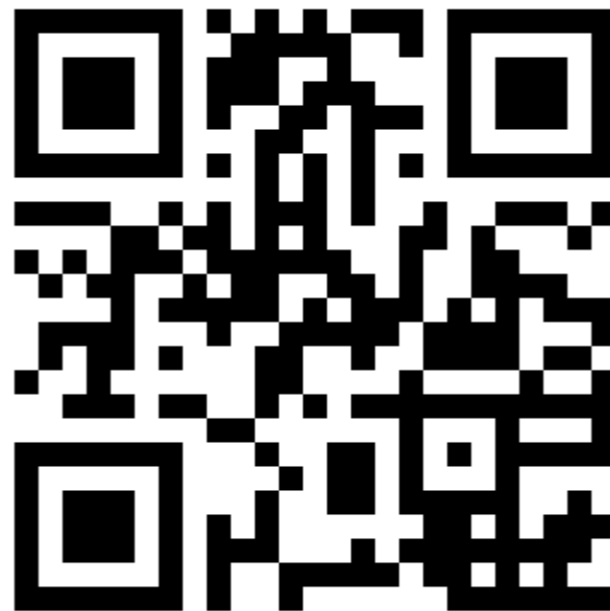
EXTREMELY FAR AWAY AND  
PROBABLY DEAD.



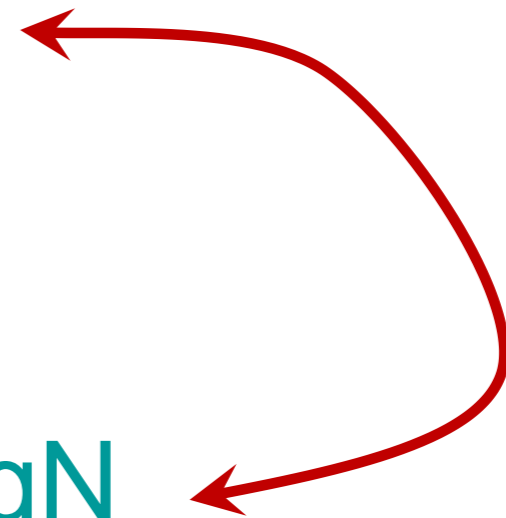
# Data

---

Measurements are available publicly



<http://bit.ly/1qmVfgN>



# Questions?

Comments are also allowed  
(despite the large question mark)



**UNIVERSITY OF TWENTE.**

