IFIP SEC 2020, 21-23 September 2020

Security and Performance Implications of BGP Rerouting-resistant Guard Selection Algorithms for Tor

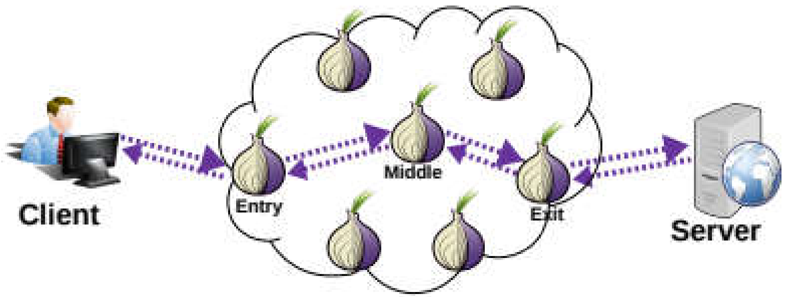
Asya Mitseva*, **Marharyta Aleksandrova**[+], Thomas Engel[+], Andriy Panchenko*

* Brandenburg University of Technology, Cottbus, Germany
{firstname.lastname}@b-tu.de

[+] University of Luxembourg, Esch-sur-Alzette, Luxembourg
{firstname.lastname}@uni.lu

Motivation (1/2)

- **Privacy has become a concern**
- **Access to the Internet is censored in many countries**



- **The Tor network** - *most popular anonymization network*
  - Sender anonymity: hides the IP addresses of users
- **Problem:** Tor does not protect against global network adversary
  - Known to be vulnerable to *traffic correlation* attacks
  - Autonomous systems (ASs) apply *active routing attacks* to put themselves at both path ends
  - Alarming observations registered (WPES '04, CCS '09, CCS '13, Usenix Sec '15)

Motivation: Counter-RAPTOR & DPSelect

- Analysis for top-93 TOR client ASs
- Performance comparable to Vanilla TOR (shadow experiments)

- Counter-RAPTOR (S&P ‘17): $\alpha = 0.5$

$$W_i = \alpha R_i + (1 - \alpha)\bar{B}_i$$

  - Client resilience is improved
  - No much of information leakage (mean)

- DPSelect (PETS’19):

$$W_i = e^{\epsilon\left(\alpha (R_i)^{x_1} + (1-\alpha)(\bar{B}_i)^{x_2}\right)}$$

  - Vulnerabilities of Counter-RAPTOR
    - Information leakage over multiple observations
    - Worst case analysis
  - Differential privacy
  - Comparable resilience

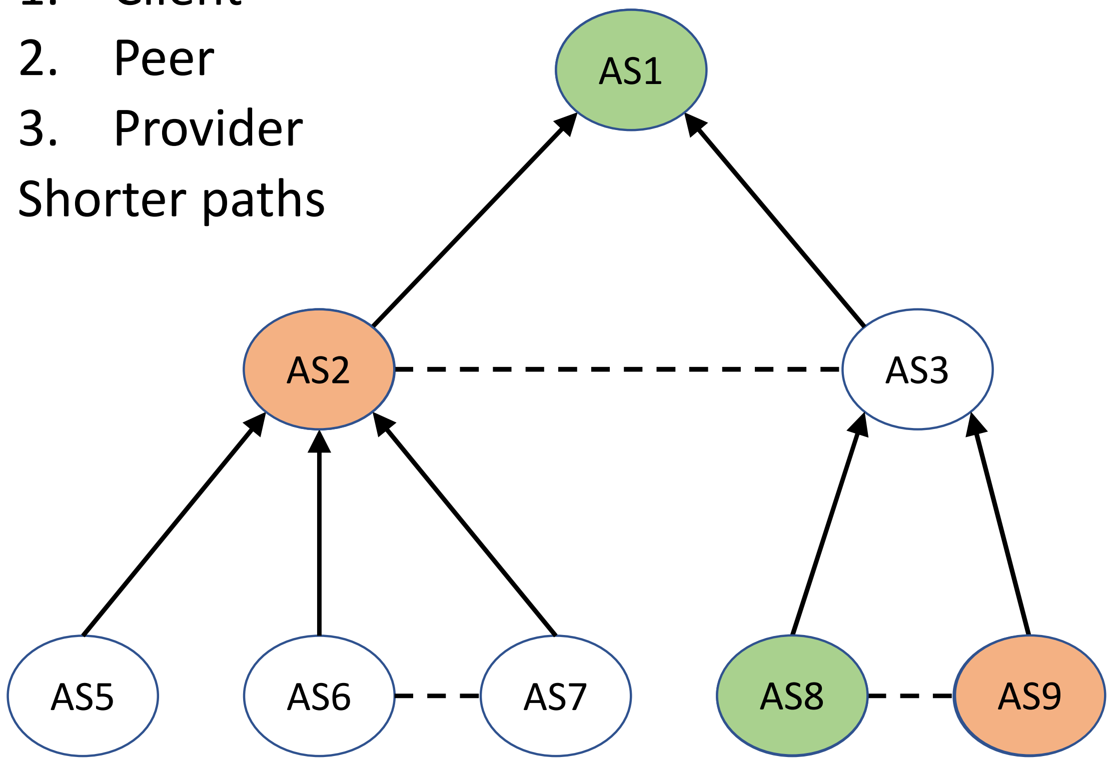
R=1

R=0.5

Rooting:

1. Client
2. Peer
3. Provider

Shorter paths



Location dependent

Our Evaluation Scenario

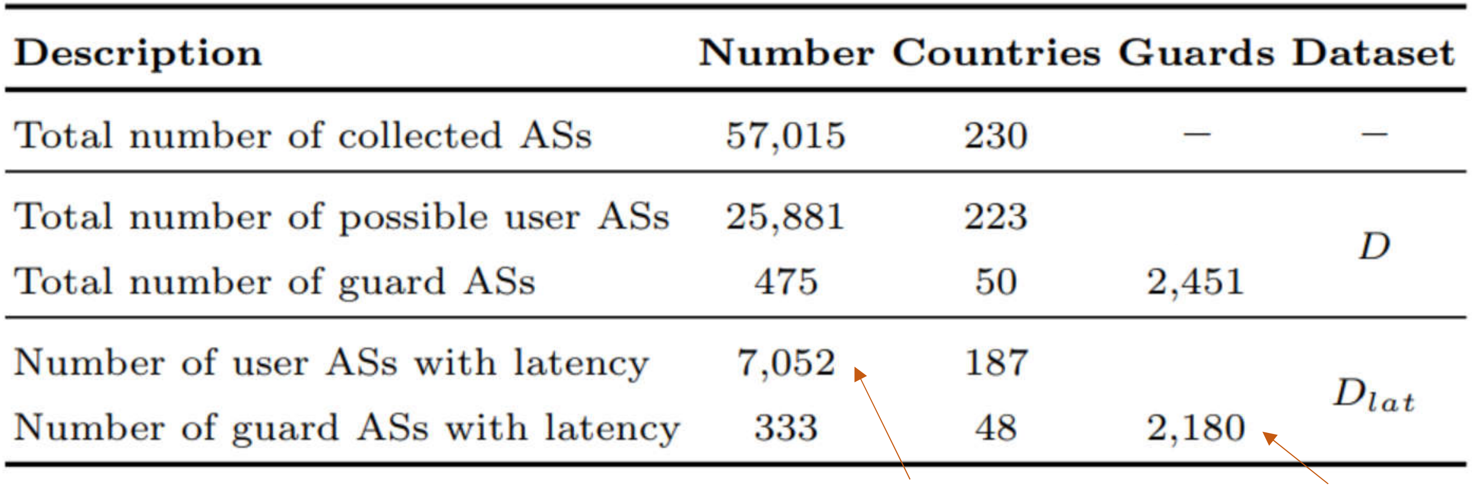
- ***Our doubt:*** AS resilience is client-specific and easy predictable
- Potential attacker: *malicious Tor middle node*

Do Counter-RAPTOR and DPSelect increase the vulnerability of a Tor client to a malicious middle node?

Our datasets

Info about:

1. Guards ASs
2. User ASs
3. AS relationships



Description	Number	Countries	Guards	Dataset
Total number of collected ASs	57,015	230	–	–
Total number of possible user ASs	25,881	223		D
Total number of guard ASs	475	50	2,451	
Number of user ASs with latency	7,052	187		D_{lat}
Number of guard ASs with latency	333	48	2,180	

91% of IPs

89% of guard ASs

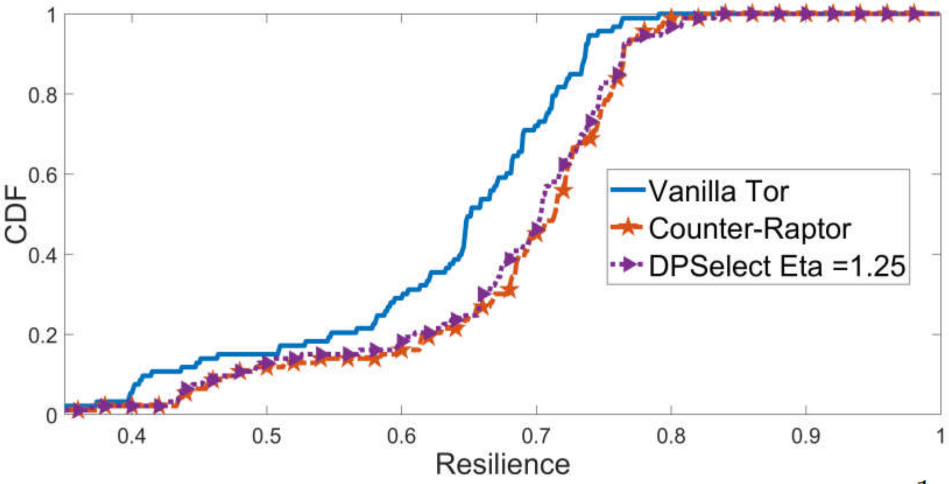
Sources:

- CAIDA March 2017 – *ASs and relationships*
- CollecTor March 1, 2017 – *guards*
- Wacek, C., et al.: An Empirical Evaluation of Relay Selection in Tor. In: NDSS (2013) – *reduced map of the Internet including latency measurements between hosts*

Large scale (previous works: top-93 TOR client ASs)

Our Findings (1/6)

Top-93 user ASs



$$W_i = \alpha R_i + (1-\alpha)\bar{B}_i$$

$$R_i \in [0,1]$$

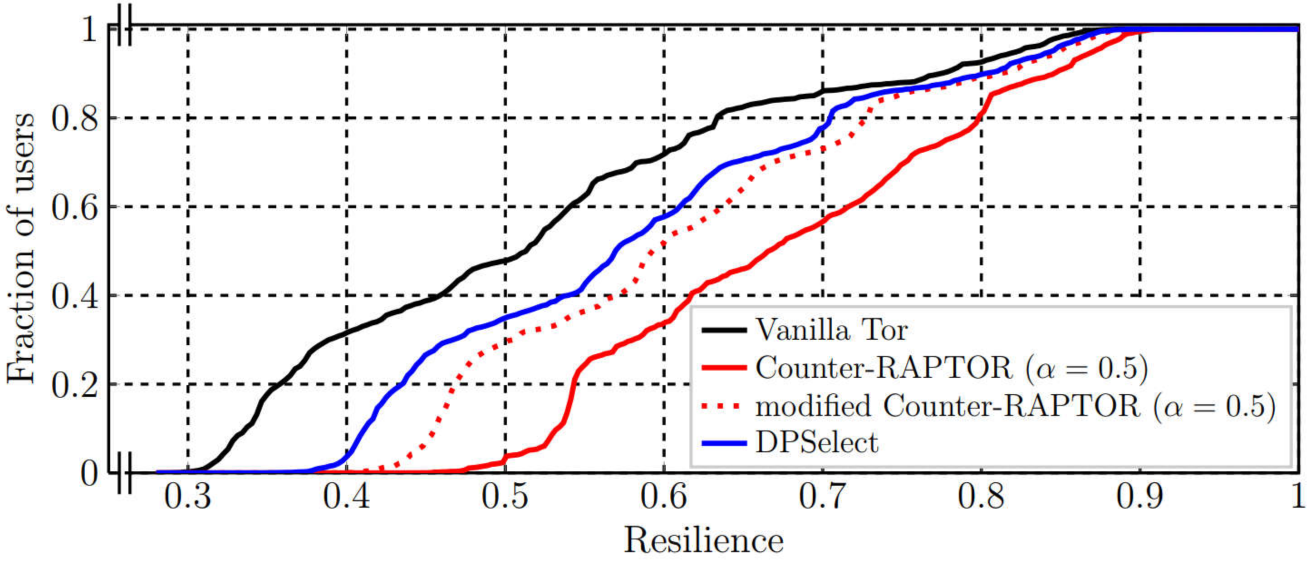
$$\bar{B}_i = \frac{B_i}{\max_i B_i}$$

$$R_i^* = \frac{R_i}{\sum_i R_i}$$

$$B_i^* = \frac{B_i}{\sum_i B_i}$$

Hanley, Hans, et al. "DPSelect: A differential privacy based guard relay selection algorithm for tor." *Proceedings on Privacy Enhancing Technologies* 2019.2 (2019): 166-186.

25881 user ASs



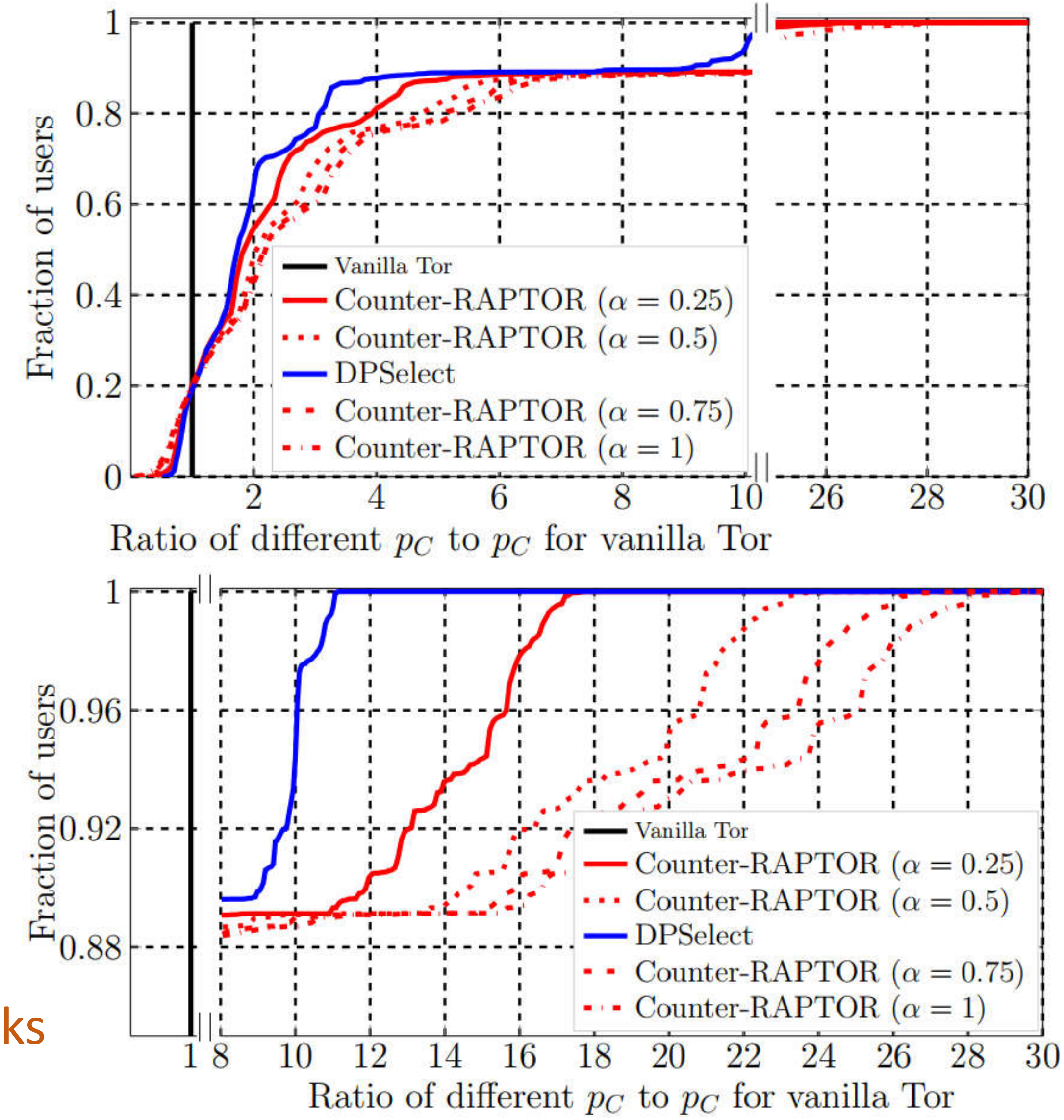
DPSelect is not as good as the original Counter-RAPTOR

Our Findings (2/6)

- **Geo-information leakages**
  - *Hypothesis: Counter-RAPTOR & DPSelect leak information about client location*
  - What about geographical position?
  - Is a client more probable to choose an entry from the same country?
  - ***Our metric:*** probability to select a guard from the same country as client

$$\frac{p_c}{p_c(vanillaTor)}$$

Can be used to improve guard placement attacks

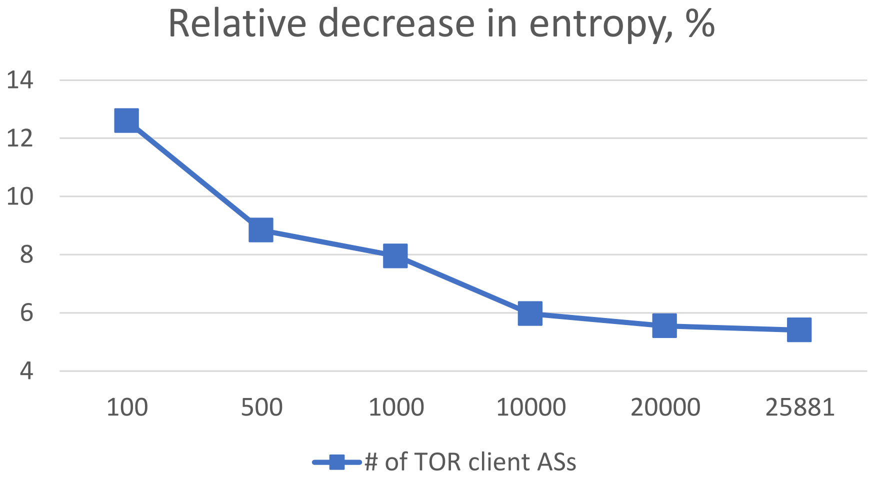


Measuring information leakage

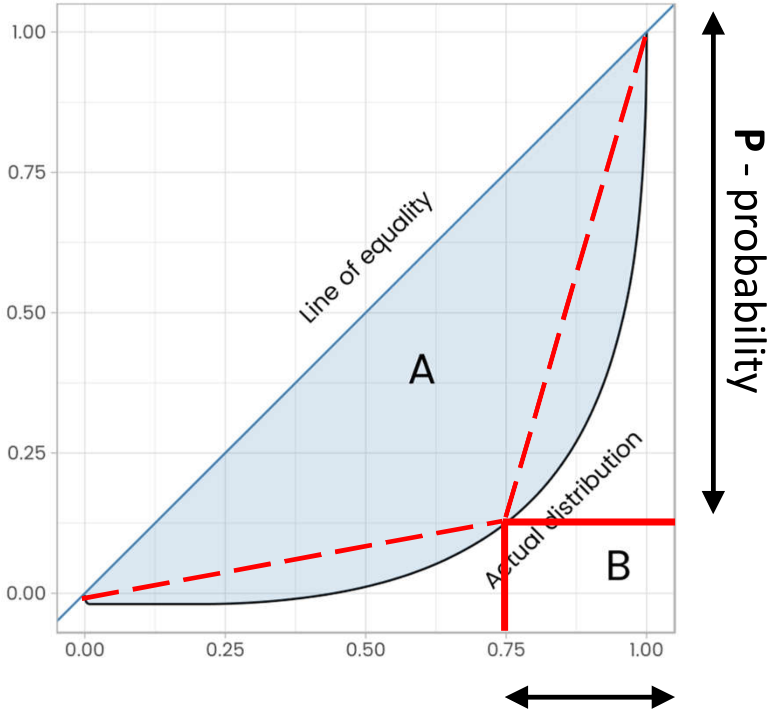
Counter-RAPTOR – relative decrease in entropy

Depends on the number of client ASs

25% of probability evenly distributed between **75%** of users
75% of probability evenly distributed between *25%* of users



How to measure inequality → Gini index



F - fraction of users (# of IP addresses)

$$conf\_increase = \frac{P}{F}$$

We use simplified version (corresponds to 2 levels of income in economics)

Our Findings (3/6)

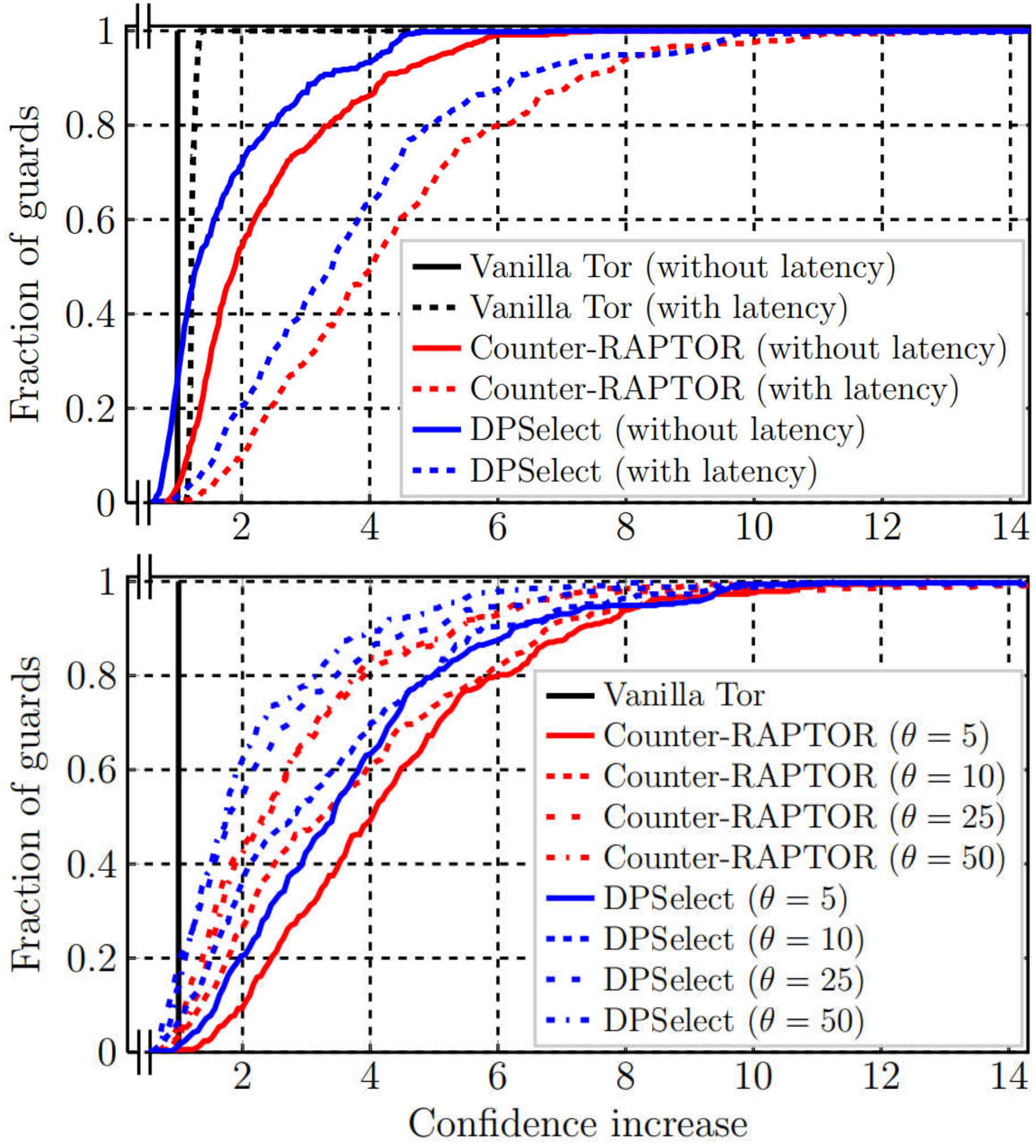
- **Information gain from the position of malicious Tor middle node**
- **Our metric:**

$$conf_{increase} = \frac{probability}{fractionofIPs\ 25\%}$$

Adding latency – simulating latency-based attacks

Hopper, N., et al.: How Much Anonymity Does Network Latency Leak? In: ACM CCS (2007)

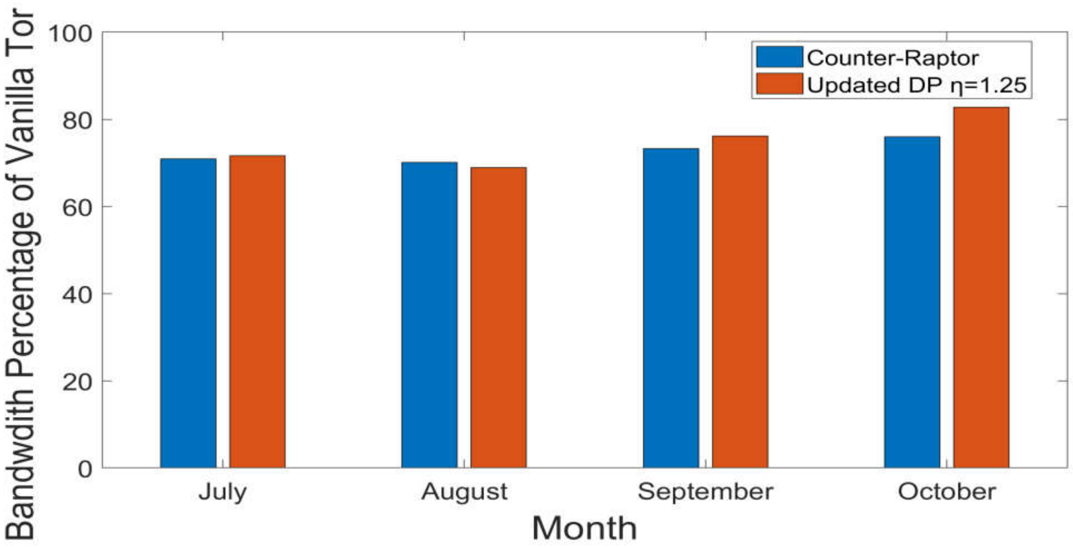
latency measurement precision $\theta = 5$



Our Findings (4/6)

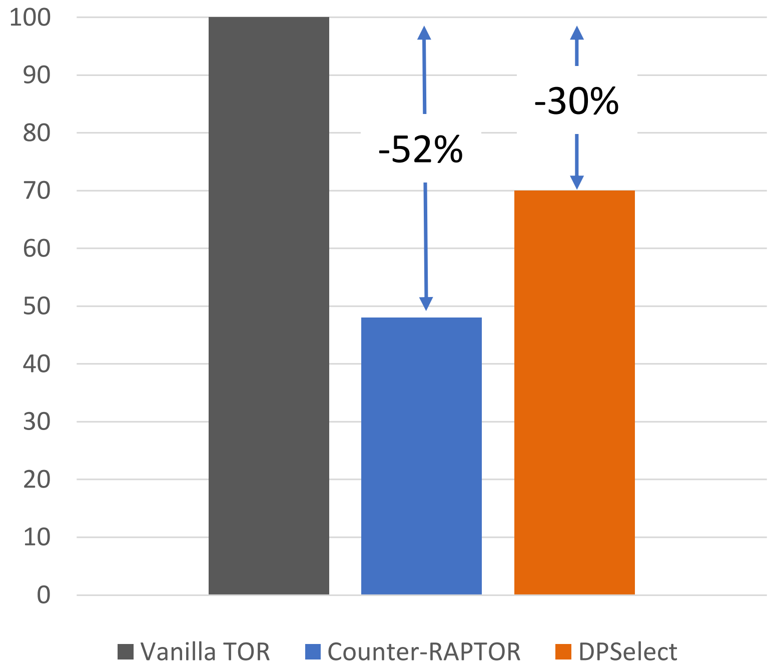
- Performance analysis
  - Average bandwidth of DPSelect in the selection of Tor entry nodes

Top-93 user ASs



Hanley, Hans, et al. "DPSelect: A differential privacy based guard relay selection algorithm for tor." *Proceedings on Privacy Enhancing Technologies* 2019.2 (2019): 166-186.

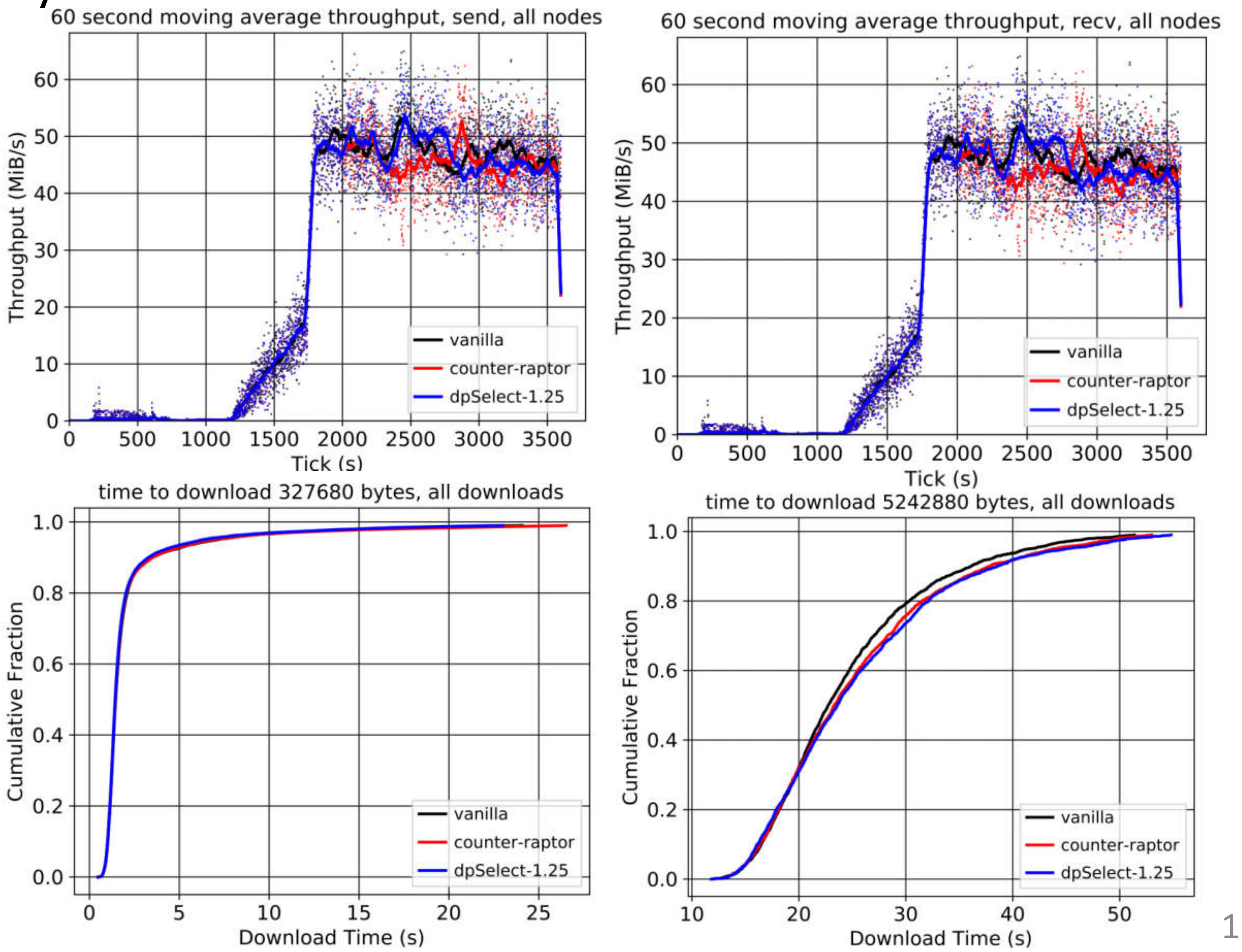
25881 user ASs



Performance analysis: Counter-RAPTOR & DPSelect

Performance is similar to Vanilla TOR.

How can this be explained?



Hanley, Hans, et al. "DPSelect: A differential privacy based guard relay selection algorithm for tor." *Proceedings on Privacy Enhancing Technologies* 2019.2 (2019): 166-186.

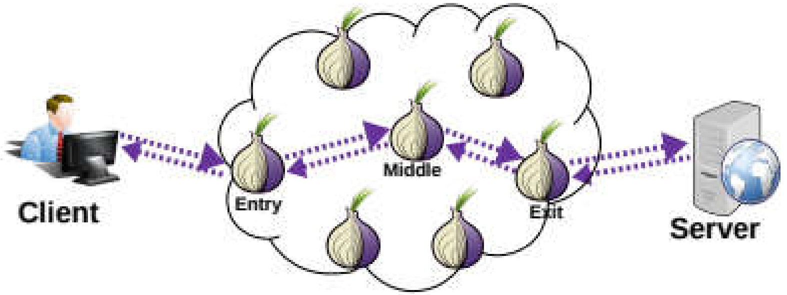
Performance analysis: Intuition

Consensus for March 1, 2017

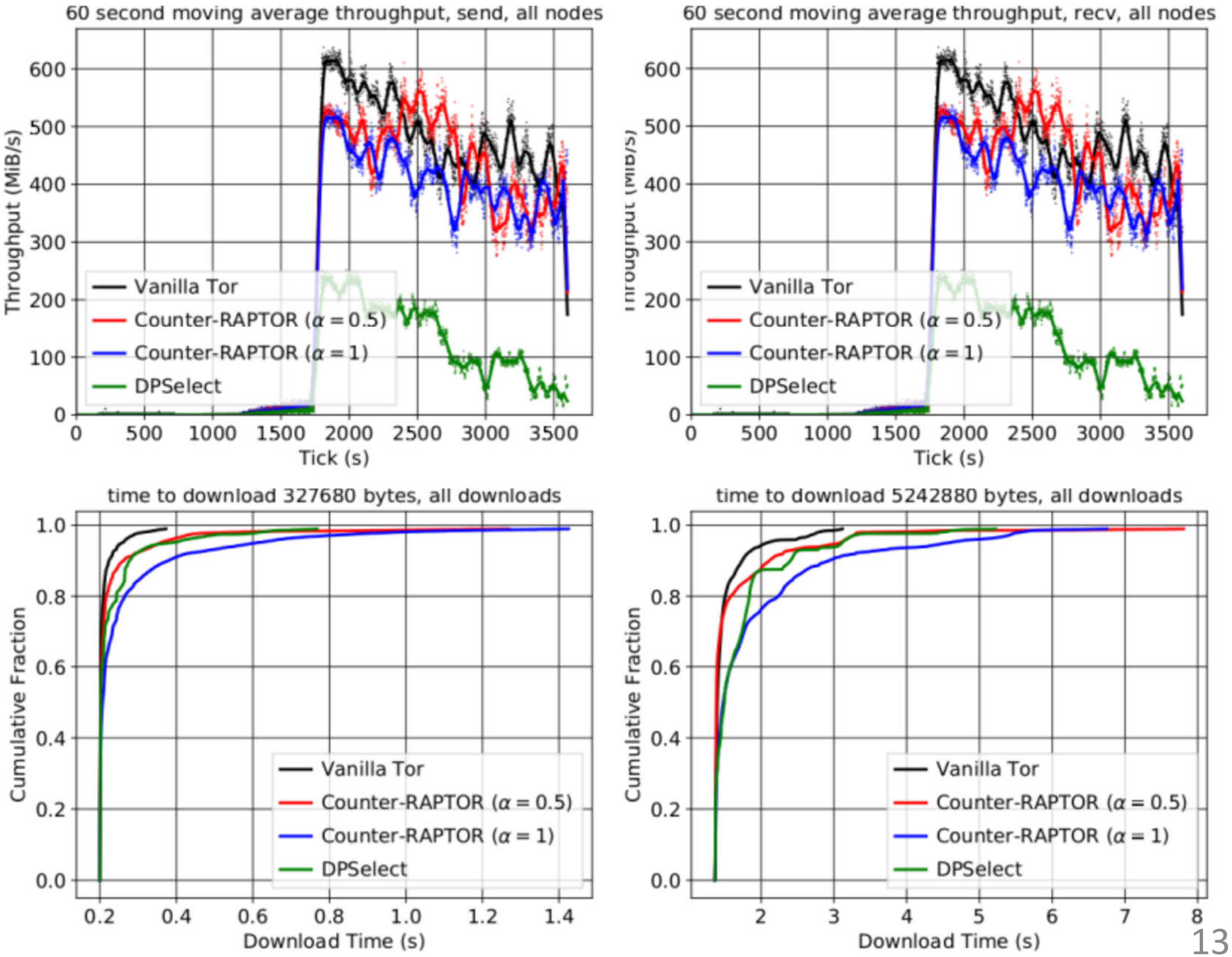
	$B(guard)$	$B(middle)$
min	$1840\ Kib/s$	$577\ Kib/s$
median		$97\ Kib/s$

Only 6% of middles have greater bandwidth

Middle relays are the bottleneck



Our Findings (5/6)



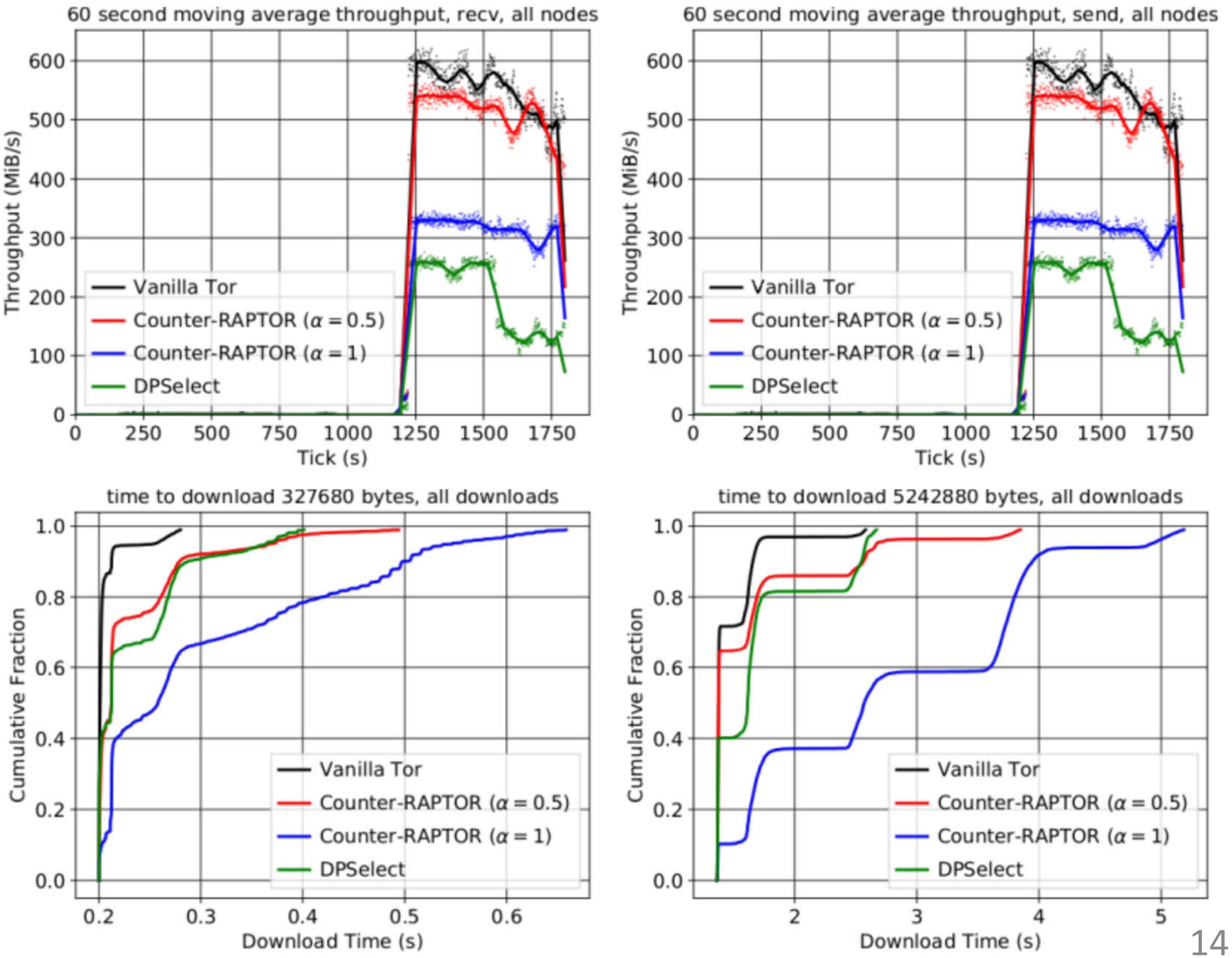
Experiment 1:

1. *B*(middle) >> *B*(guard)
2. *B*(exit) >> *B*(guard)
3. Same latency between nodes

Our Findings (6/6)

Experiment 2:

1. *B*(middle) >> *B*(guard)
2. *B*(exit) >> *B*(guard)
3. Same latency between nodes
4. All users from the same AS
5. 2 types of guars
    1. **High** performance + *low* resilience
    2. *Low* performance + **high** resilience



Conclusions

Analysis of Counter-RAPTOR & DPSelect

- DPSelect achieves only 1/3 of the claimed resilience ➔ does not protect from rooting attacks
- Both methods leak geographical information
- Analysis with regard to malicious middle OR:
  - We proposed new metric
  - Both methods empower a malicious node to fingerprint user location better
- Performance analysis
  - Degradation of average bandwidth for large scale
  - Scenarios when performance is seriously affected