Insights on Impact of DLTs in Provider Networks

David Guzman, Dirk Trossen, Mike McBride, Xinxin Fan

November 2022

IETF 115

Related Material

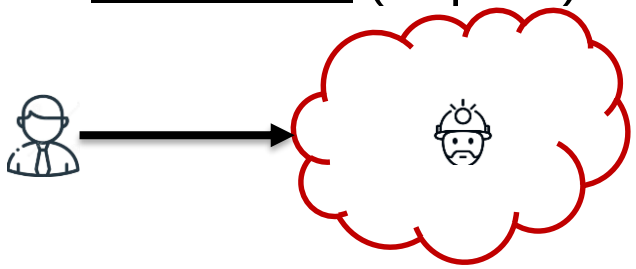
- IIC White Paper
  - https://www.iiconsortium.org/pdf/2022-01-10-Impact-of-Distributed-Ledgers-on-Provider-Networks.pdf
- draft-trossen-rtgwg-impact-of-dlts
  - https://datatracker.ietf.org/doc/draft-trossen-rtgwg-impact-of-dlts/
- Insights on Impact of Distributed Ledgers on Provider Networks. ICBC 2022 (accepted)

Background: Permissionless Distributed Concensus Systems

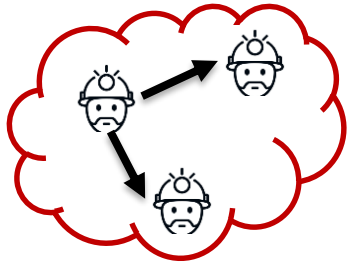
- DHTs -> host and receive content (files)
  - Goal: Decentralize and distribute a file system, a network file system, in a **permissionless** fashion over a **faulty** network.
- DCSs -> agree on the status of a state machine
  - Goal: Decentralize and distribute a state machine in a **permissionless** fashion over a **faulty** network.
- DLTs -> consensus oriented on distributed content
  - Goal: Decentralize the distributed state machine that is stored on a network file system.
    - Decentralized “voting” system
    - Often the state machine is replicated (ledger)
    - Networks are internet-scale
    - P2P networks

DLT Service Interactions

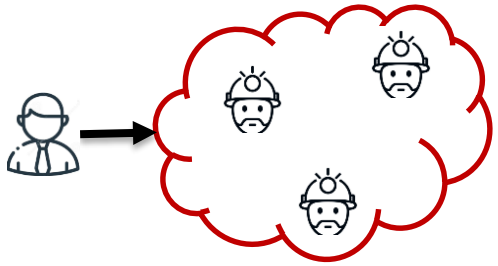
A client **commits** a transaction (request) to the DCS



A miner (peer) **commits** a found block to the DCS, using previouly **discovered** clients



Any client or miner can **read** the blockchain in the DCS



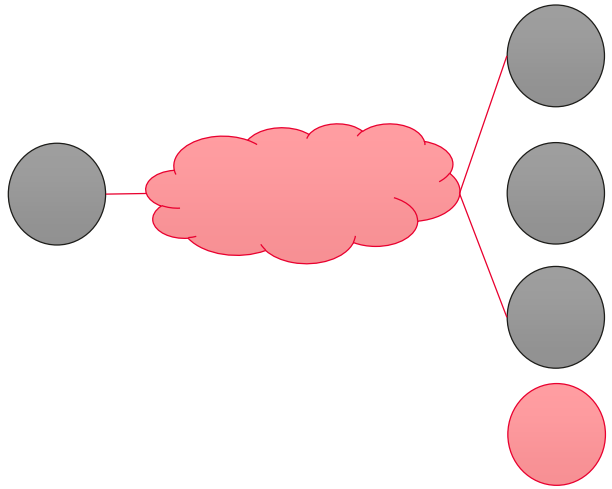
Key Mechanism: Randomized Atomic Broadcast

Randomized atomic broadcast sends single message to ***randomized set*** of receivers to

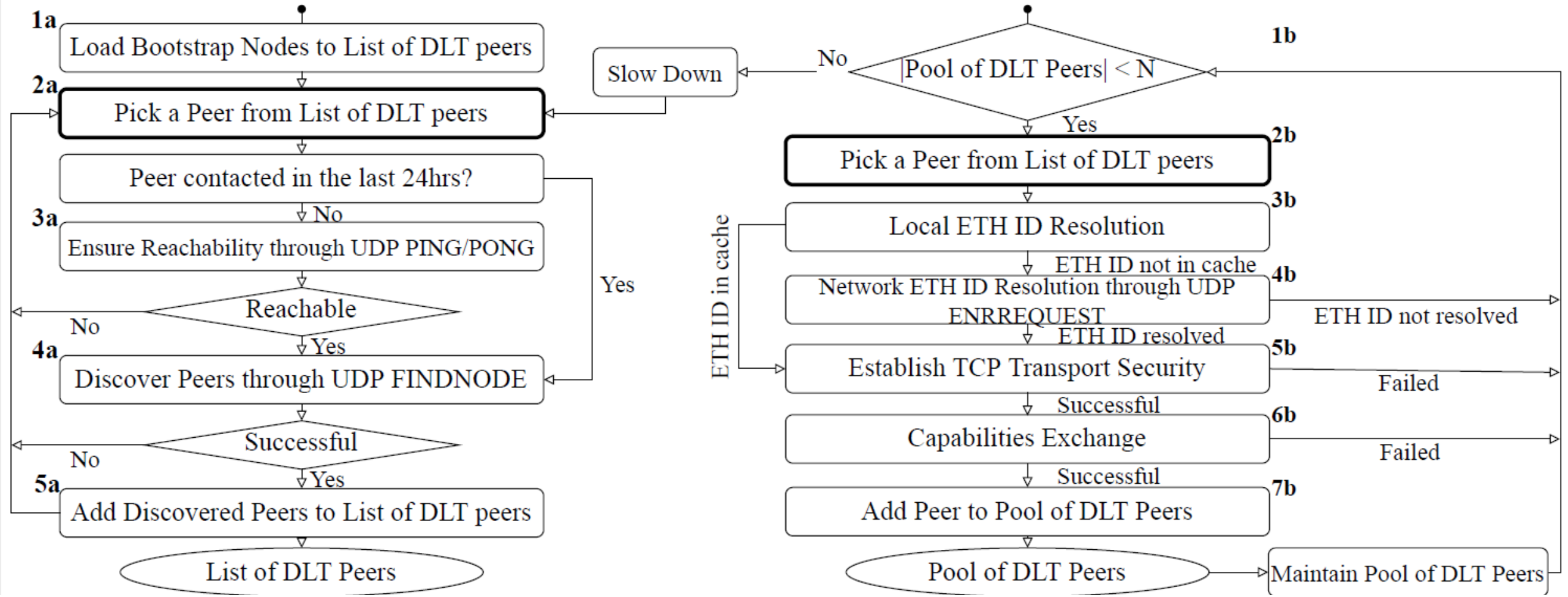
- avoid possible collusion of (parts) of a stable receiver set
- ensure distribution of ledger information across ALL peers over time

-> copes with the permissionless but also large scale nature of the DCS

-> built as ***P2P system*** on top of IP networks, using UDP, TCP, and QUIC



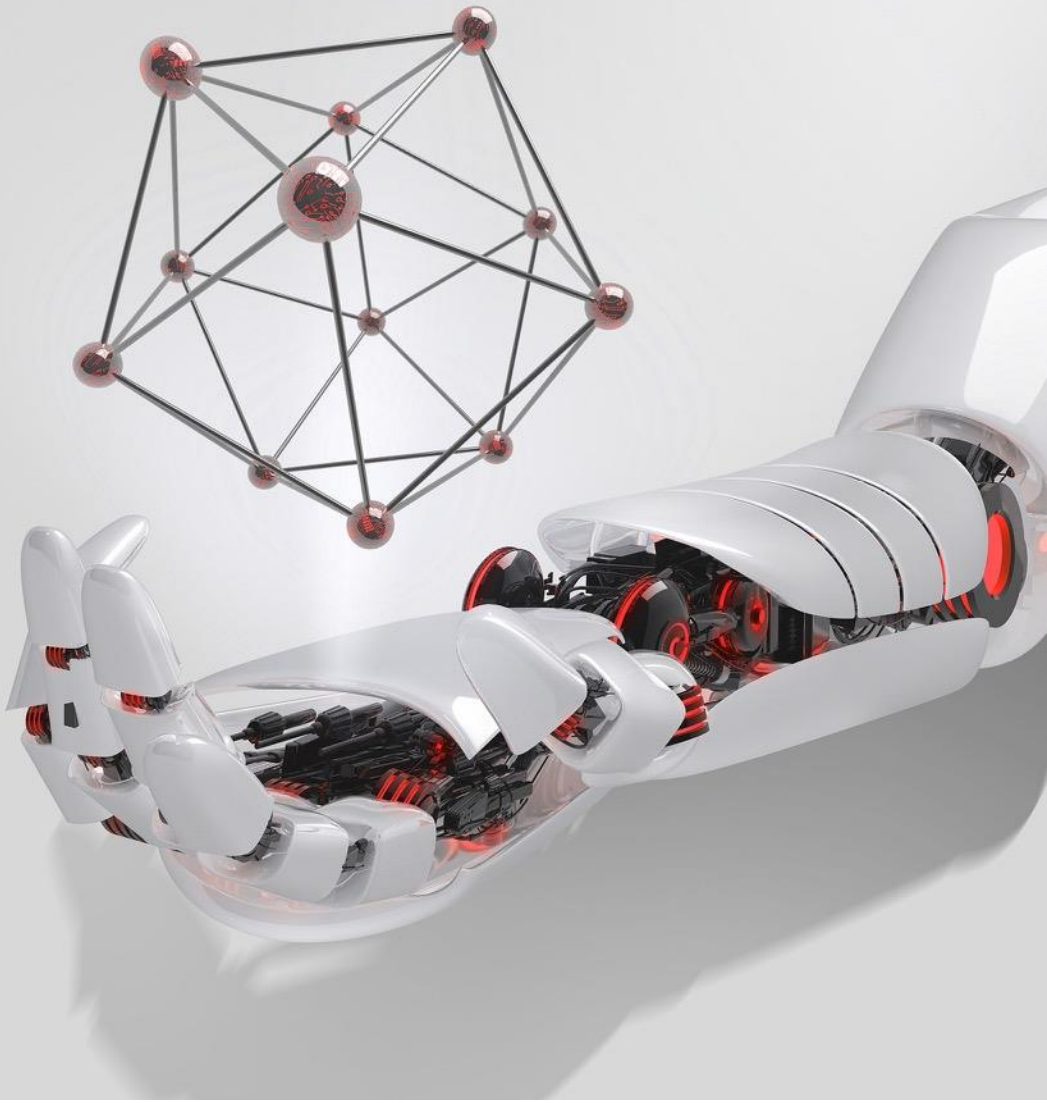
Communication Patterns of (DCS) P2P System



Challenges for Users and Provider Networks

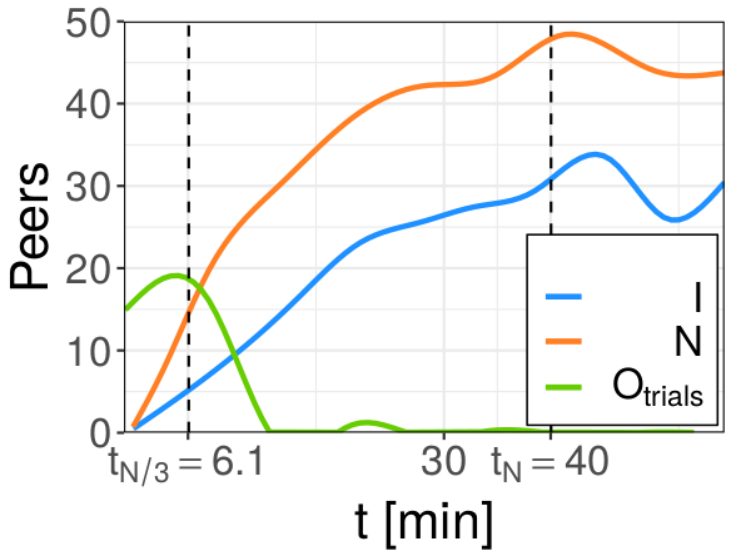
- Costs for **pool maintenance**
  - Peers need to continuously establish and maintain reachability information
  - Each peer maintaining a constantly changing pool (TCP/QUIC)
- Costs for **resilience and reliability**
  - Failing nodes causing latency on pool establishment (hence DC, content retrieval)
  - Timeouts inducing removal of peers, replenishing the pool
- Need to **match capabilities**
  - Upper layer capabilities are required for transacting (a bit different from DHT).
- Unicast Replication
  - Intention to achieve diffusion/propagation among many DLT peers instead of efficient network-level multicast.
- IP address privacy
  - Peers need to expose their IP address

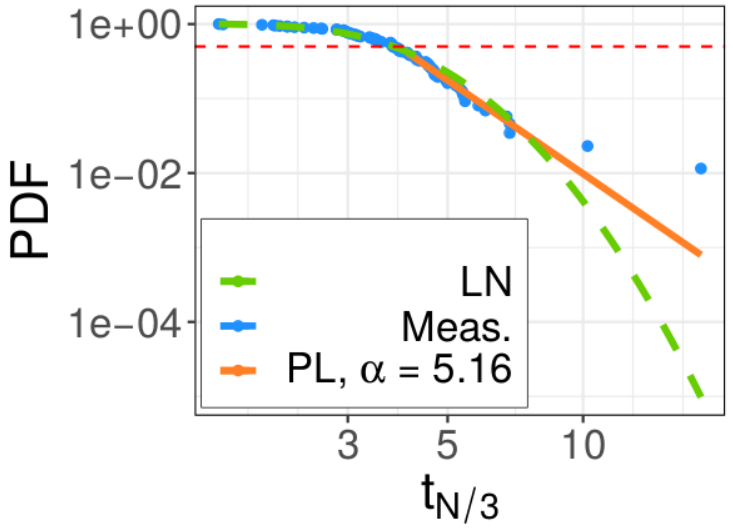
Experimental Insights

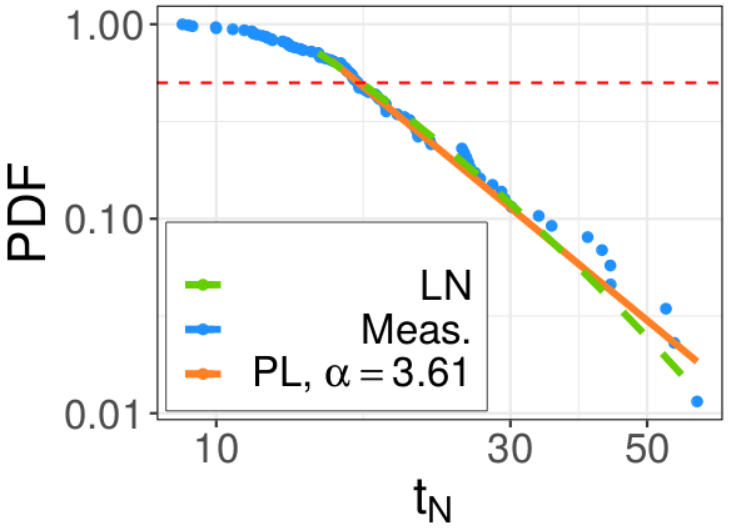


Pool Establishment Time

- $t_{N/3}$, is reached at 4min with 50%probability
- time to complete a pool of DLT peers is reached at ~20min

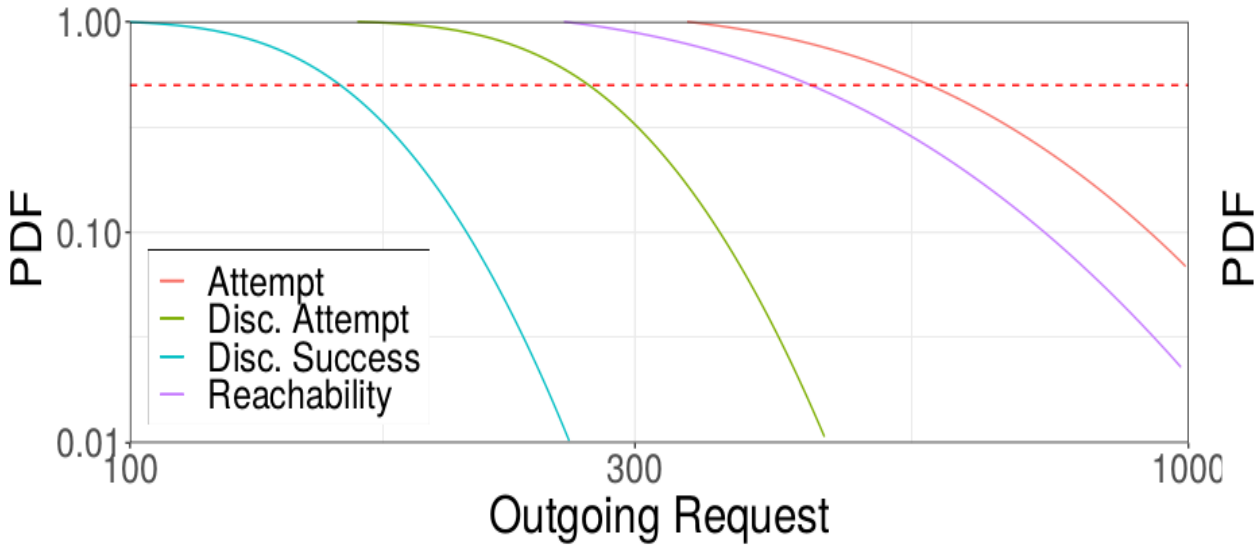


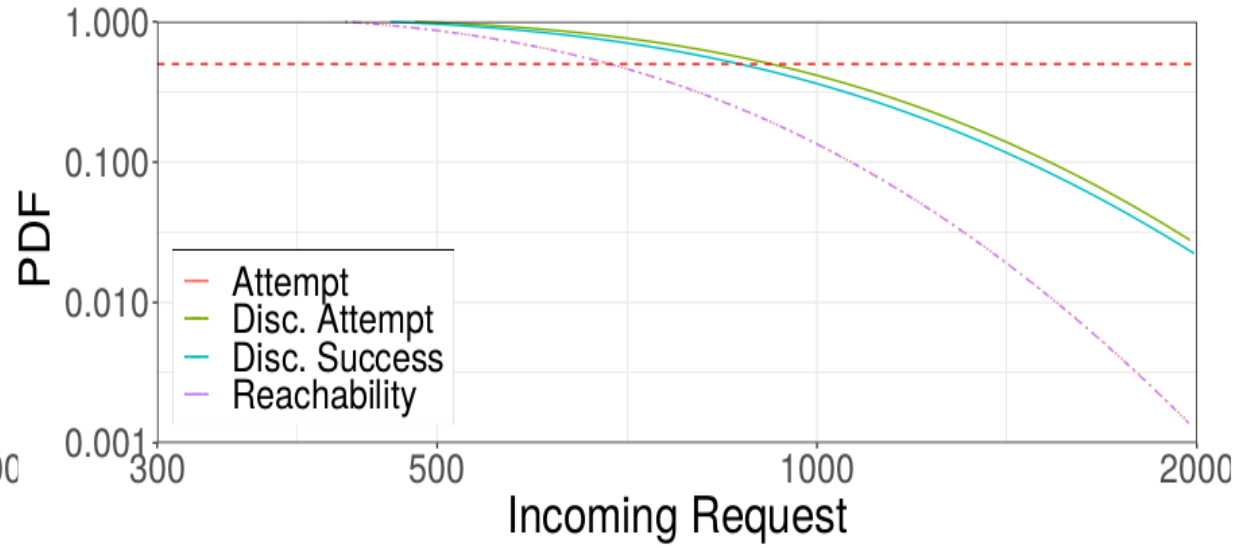




Randomized Discovery Protocol

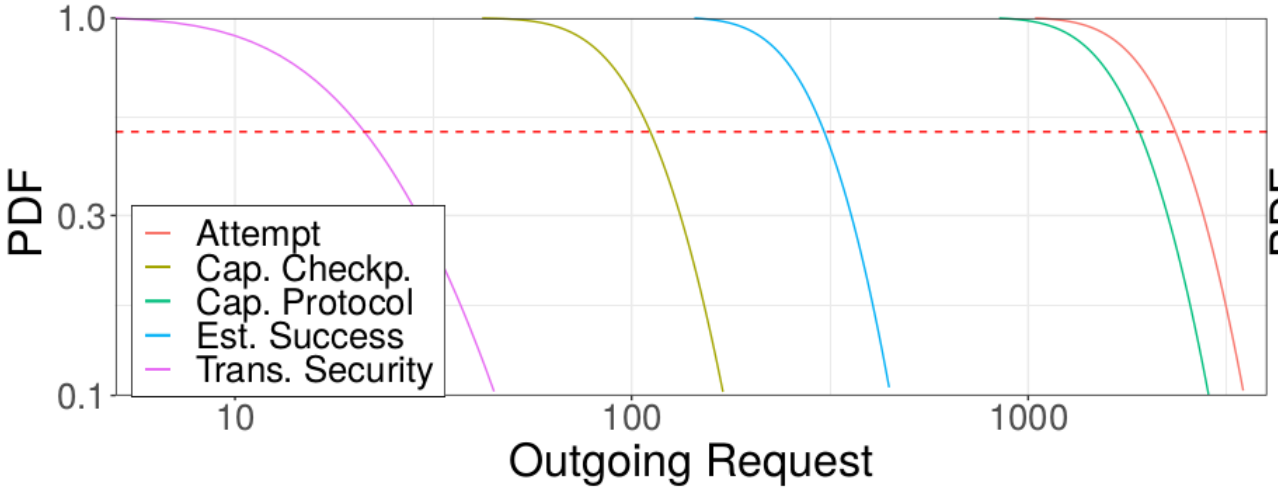
- Reachability: ≈77% of the contacted peers are reachable,
- out of these peers ≈63% are used to further topology discovery.
- ≈57% successfully executed a complete discovery protocol.

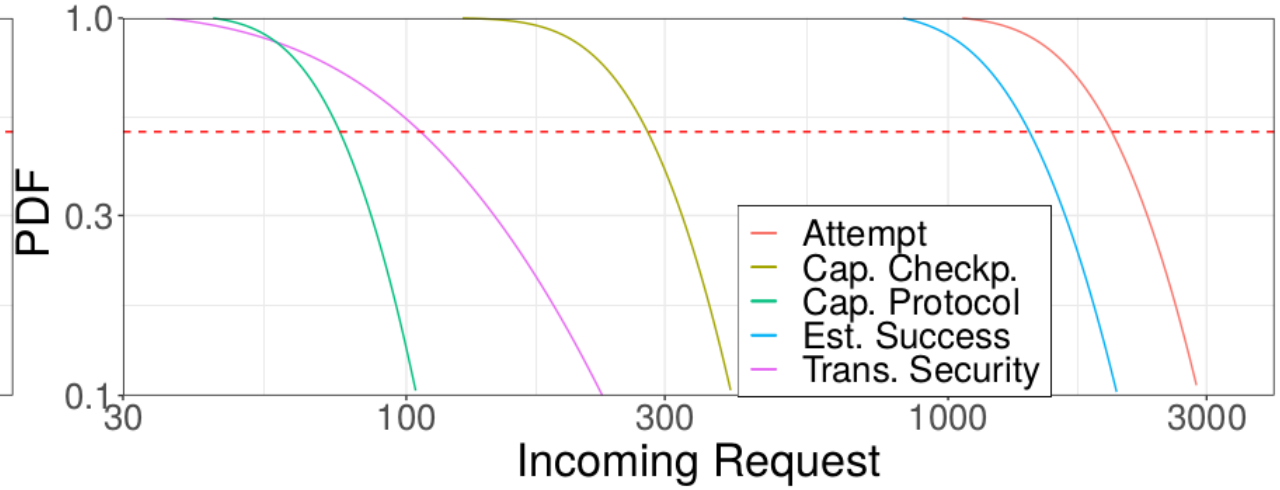




Pool Establishment Protocol

- 82% of errors occur while trying to decrypt the remote secret and find the proper blockchain checkpoint,
- 18% I/O errors (invalid ciphertext length, unexpected end of file)





HUAWEI

Can the network help?

Observations

1. Miners provide a **service capability** to other miners and clients in the DLT
2. **Constraints** (as investigated in ETH) for ***right*** miners include reachability, TLS capabilities, certain HW, checkpoint, …
3. A group of peers is **instantaneously randomized** to ensure protection against collusion
    1. Pool creation and maintenance (done at EVERY peer) is core mechanism to enable instantaneously randomized operations as unicast operations
    2. Fixed group size is defined through heuristics (theoretical bounds) on the probability for converging to consensus among those group members

Can the network help?

From observations/insights to a proposed design

1. Use **service-centric abstraction** (miners are service instances to DLT service). Routing on Service Addresses https://datatracker.ietf.org/doc/draft-trossen-rtgwg-rosa/
2. Use **routes to (pool of) service instances** to enable instantaneously randomized operations
3. Reachability to ***right peers*** by is ensured by encoding constraints as part of naming structure
4. Replacing randomized unicast with a **forward multicast capability** to a fixed size subset of peers
5. Ensure that EVERY request leads to **randomized set of peers** (which excludes using IP multicast)

-> Baseline here will be our insights in ETH over IP

We believe that programmable in-network compute capabilities can help with realizing aspects of such design

Thank you.

Bring digital to every person, home and organization for a fully connected, intelligent world.

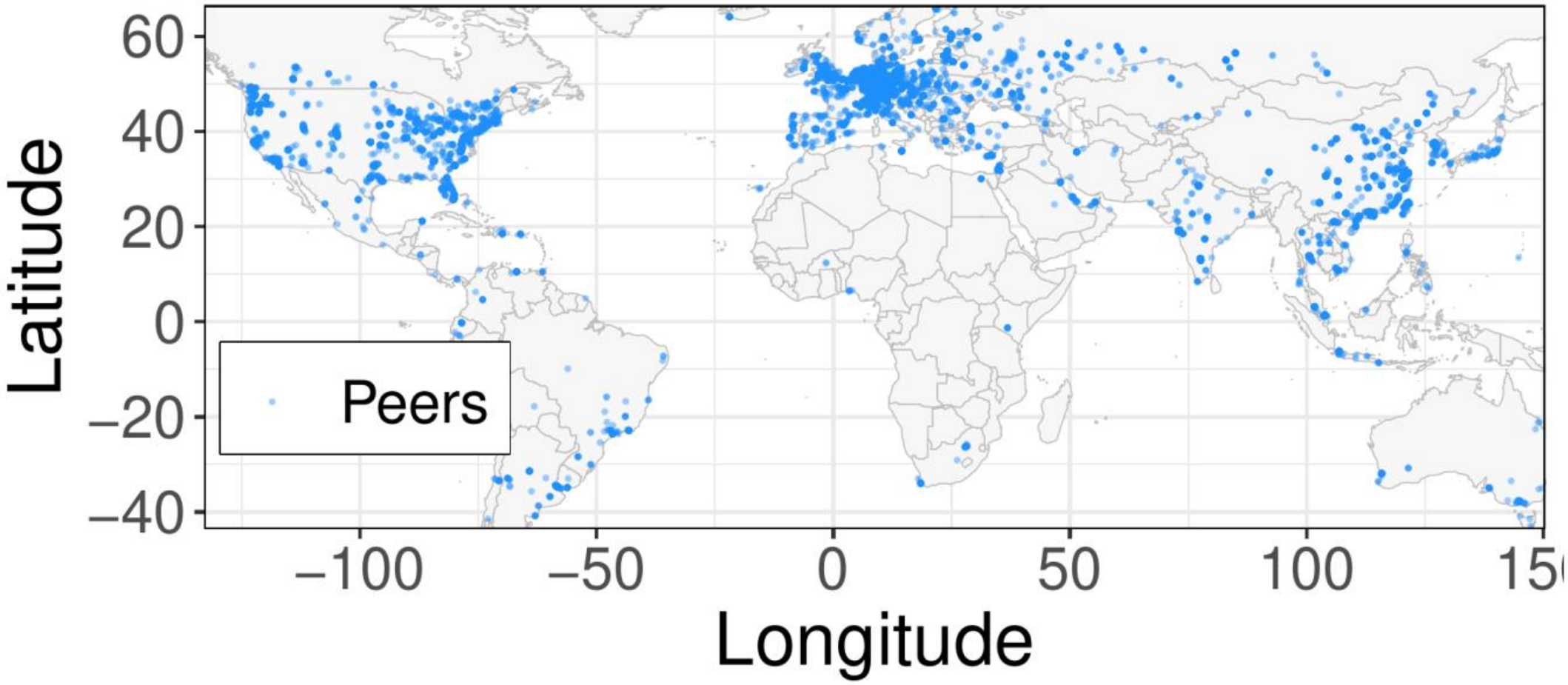
Copyright©2018 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

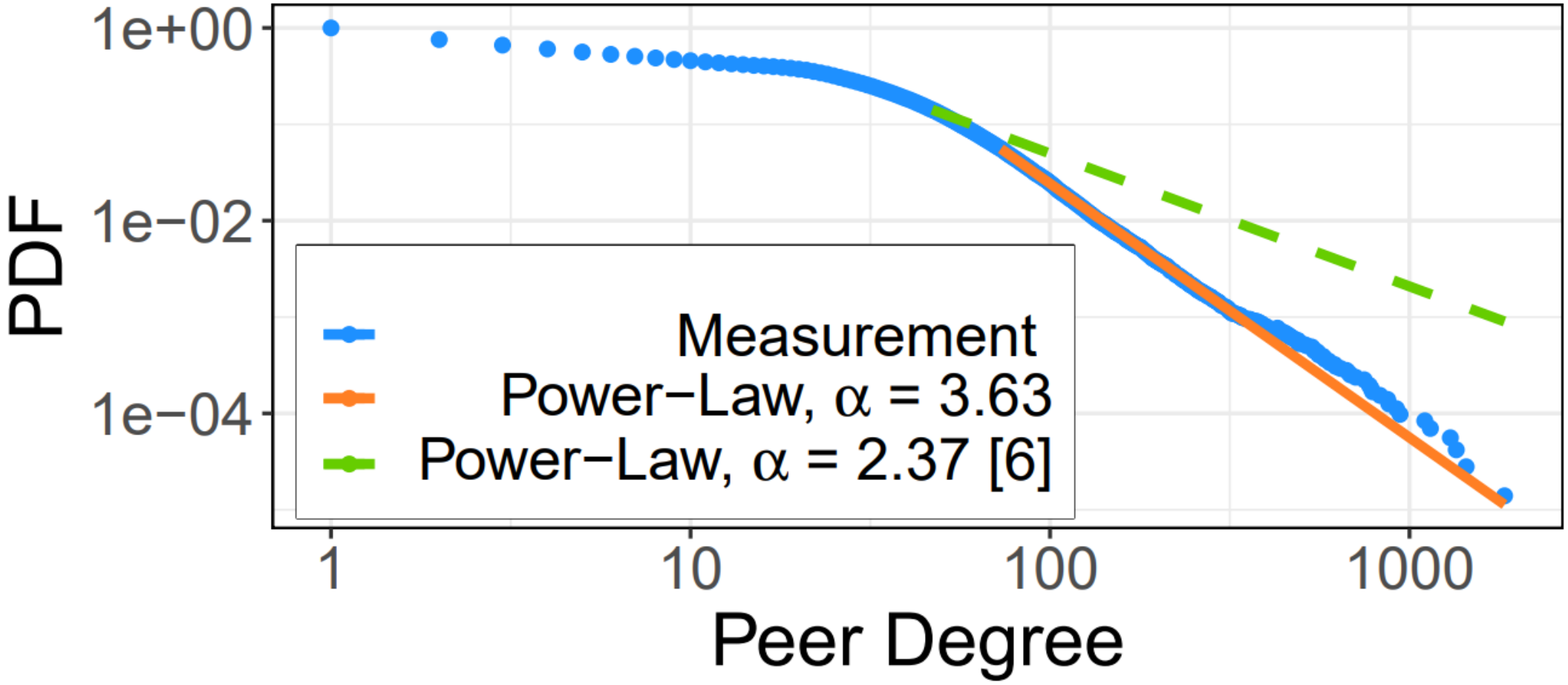
Experimental Insights

- Go-ethereum client syncronizing to the ethereum mainnet
- Geth/v1.10.2-stable
- Local peer on **: 217.110.131.84**
- UDP/TCP ports : 30303,30313
- Samples taken between : Jan-2022 – Jun-2022
- 8 bootstrap endpoints with v4UDP discover protocol
- Discovered active peers: 72k in comparison to [Gao 2018] 74k
- 100 iterations:
    - SYNC [5hrs] STOP[2mins] SYNC[5hrs] ……
    - Discovery / Pool Establishment [40min] ……..SYNC[4hrs20min]
- Downloaded data : ~280GB

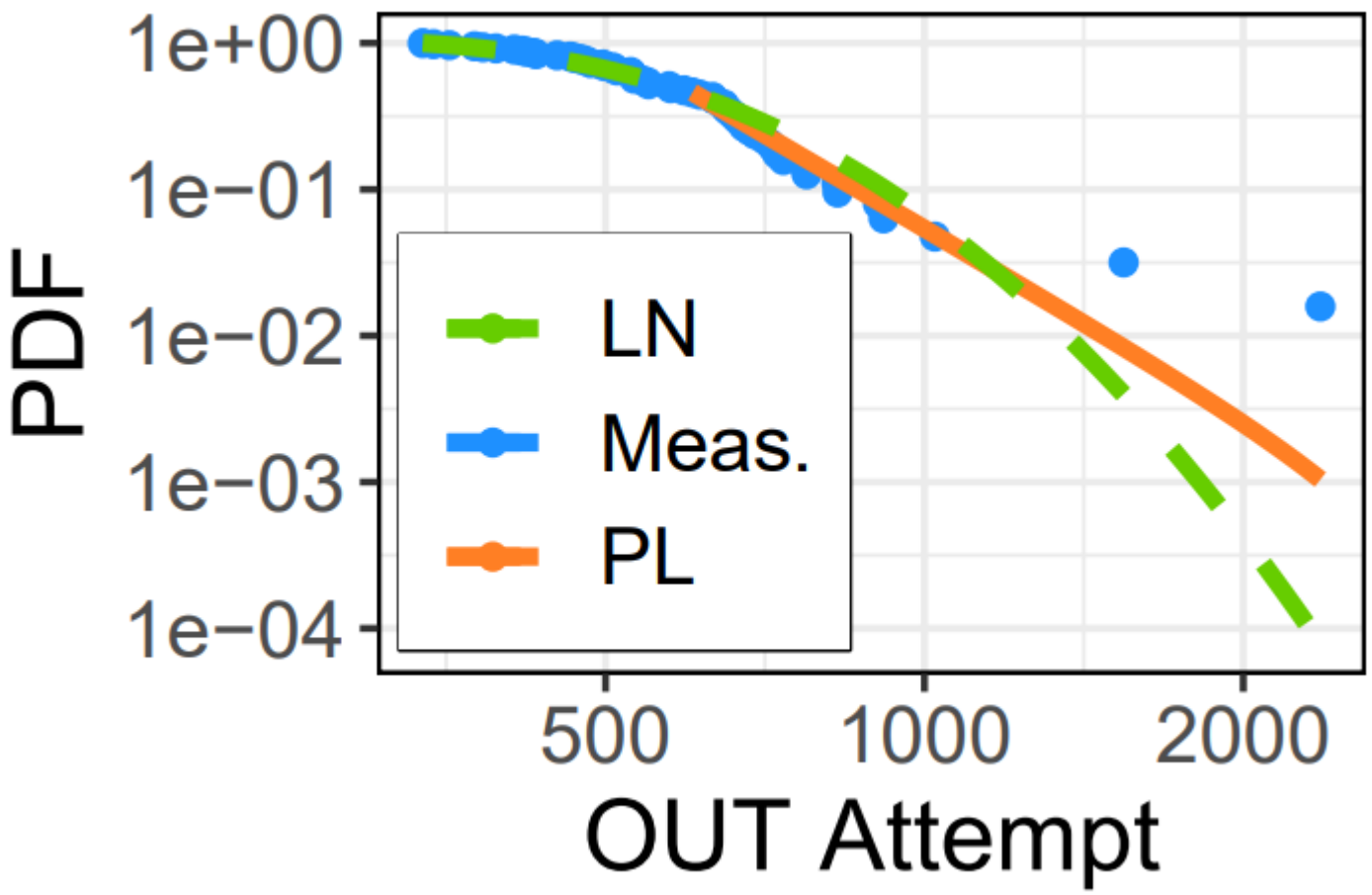
Location Distribution



Peer Degree Distribution



Attempts Distribution



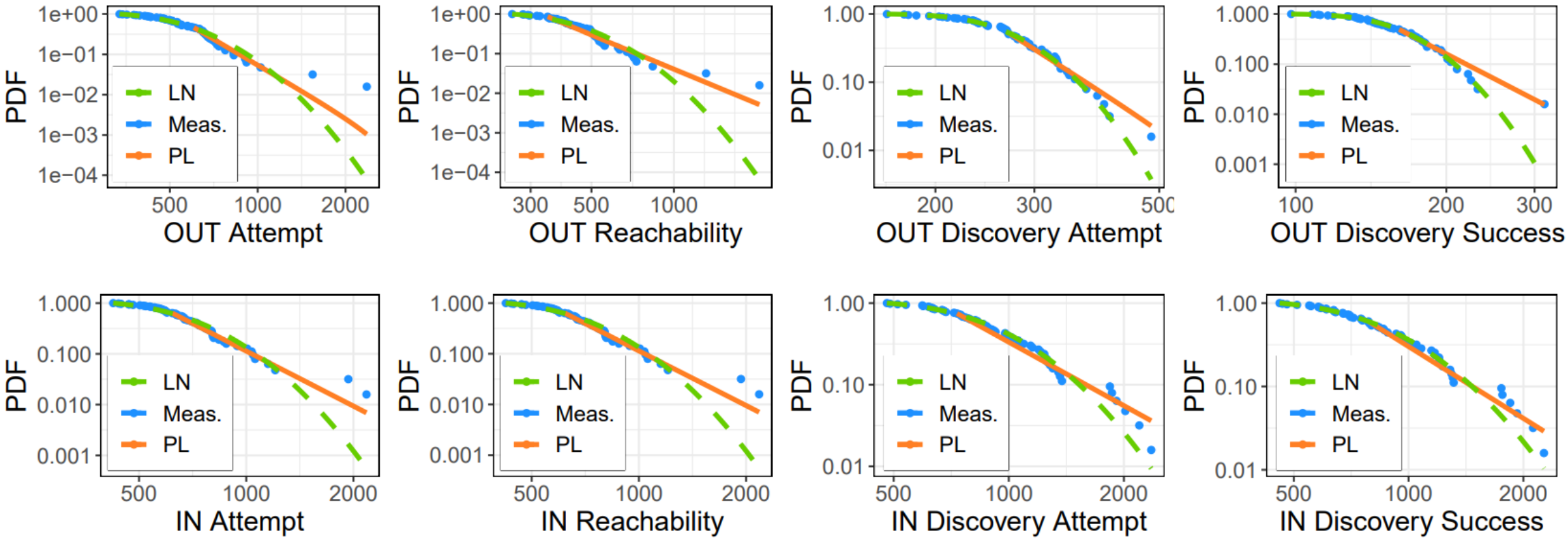


Fig. 5. (a-d) Outgoing, and (e-h) Incoming Discovery KPI Distributions

Parameters

Table 2. Discovery Cost Summary

	Outgoing						Incoming					
	Power-Law			Log-Normal			Power-Law			Log-Normal		
RV	α	x_{min}	p	μ	σ^2	x_{min}	α	x_{min}	p	μ	σ^2	x_{min}
Attempts	5.24	604	0.2	6.31	0.38	336	4.6	620	0.58	6.47	0.37	423
Reachability	3.87	346	**0.03**	6.04	0.41	257	4.58	619	0.59	6.47	0.37	423
Disc. Attempt	6.22	269	0.79	5.61	0.21	164	3.59	732	0.16	6.79	0.41	480
Disc. Success	6.16	161	**0.04**	5.07	0.21	98	3.86	785	0.11	6.72	0.43	459

Parameters

Table 3. Pool Establishment Cost Summary

	Outgoing						Incoming					
	Power-Law			Log-Normal			Power-Law			Log-Normal		
RV	α	x_{min}	p	μ	σ^2	x_{min}	α	x_{min}	p	μ	σ^2	x_{min}
Attempts	4.52	2250	0.33	7.78	0.29	1041	4.81	1973	0.43	7.6	0.29	1063
Transport Security	3.6	23	0.69	3.09	0.56	5	3.03	93	0.62	4.63	0.62	36
Capability Protocol	4.37	1777	0.25	7.57	0.3	845	6.71	83	0.86	4.32	0.26	44
Capability Checkpoint	5.31	114	0.25	4.73	0.31	42	5.52	286	0.46	5.63	0.28	127
Establishment Success	6.21	350	0.26	5.74	0.28	144	5.04	1383	0.75	7.24	0.3	825

HUAWEI