BDCAT: Balanced Dynamic Content-Addressing in Trees

Stefanie Roos, Martin Byrenheid, Clemens Deusser, and *Thorsten Strufe*

INFOCOM ‘17

TECHNISCHE UNIVERSITÄT DRESDEN

BDCAT in a nutshell

What do we want to do?

- *Build a secure, low-delay darknet*

Why is that difficult?

- Publish/access without fear of retribution/censorship
- -> Routing/content addr. in restricted environments

What‘s this paper about?

log

polylog

- Content addressing on a
- tree-shaped (efficient routing!) overlay
- with fair load balancing

log

Content Addressing 101

- Derive identifier from resources that map to a (zone within the) network address

- Register and retrieve information at respective node

A bit more formal, in a network G=(V,E) with resources O:	
id: V -> ID	map: O -> ID
store: O -> V	retrieve: ID -> O

  - *First-term CS students: Hash tables*
  - *Cloud/datacenter people: memcached*
  - *P2P people: DHT*
  - *Everybody else: DNS*

Routing 101

Find a path of links to a destination (store, retrieve)

1. Assign node addresses and connectivity
2. Disseminate connectivity information
3. Calculate distances via neighbors *(DV/LS)*
4. Minimize distance to destination (greedy)

2 degrees of freedom: addresses / connections

- IP: centralized addressing, strategic connections
- DNS: centralized addressing, connect to tree
- DHT: random addresses, connect to routable structure

Information is restricted, connections are fixed! [1]

[1] Vasserman et al. 2009

Meet Embeddings

Single degree of freedom

1. *Adapt addresses*
2. Estimate distances
3. Minimize distance

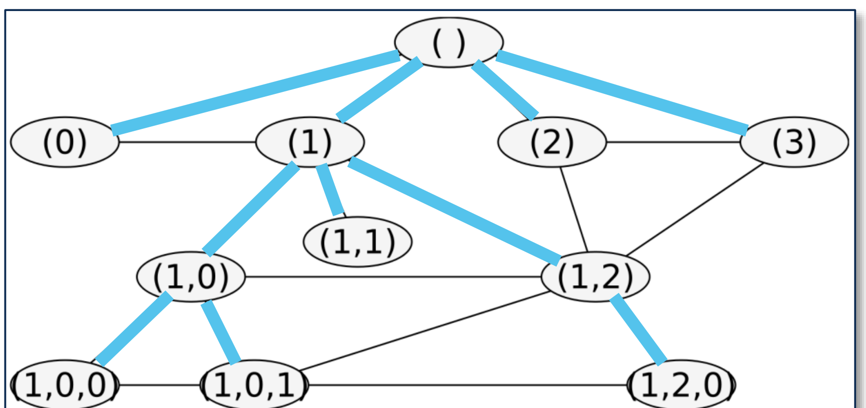
A bit more formal, let *ID(v)* be address of v ∈ V.
A *network embedding* on graph G is a function

$$ID : V \rightarrow M$$

to metric space *M* equipped with a distance

$$d : M \times M \rightarrow \mathbb{R}+ .$$

(1): Approx. routable structure *(greedy?)*, eg a **tree**



PIE embedding[1,2]

$$d(s, t) := |s|+|t| - 2(\mathrm{cpl}\ (s,t))$$

[1] Herzen et al. 2011
[2] Hoefer et al. 2013

Map resources to nodes, *map : O -> M*

Assume max depth of tree to be *L:*

Define metric space to be vectors (of *L* components):

$$map(o) = \left(h_1(o), h_2(o), h_3(o),\ldots,h_L(o)\right)$$

distance measured as above.

Maps uniform into components -> overall namespace

Balanced Dynamic Content Addressing

Trees determined by social graph, unbalanced, ***static.***

Task is to guarantee (f,δ)-balance:

for all v ϵ V less than $f \frac{1}{|V|} + \delta$ assigned.

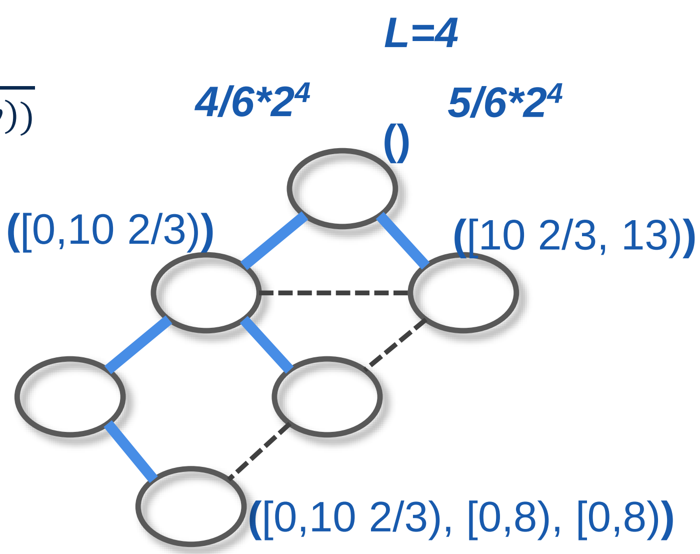
Intervals (zones) assigned to each component:

1. Estimate #nodes in branch *succ(v)*
2. Allocate zones *z(v)* accordingly:

   assign, width: $|z(v)| = 2^L \frac{succ(v)}{succ(parent(v))}$

Distance metric considering zones:

- d(x,y)=|x|+|y|-2con(x,y)
- with: con(x,y)=max{i:x_j ϵ y_j ∀ j≤i}



Balanced ***Dynamic*** Content Addressing

Churn: nodes are unreliable, *trees are delicate*

monitoring ***embedding*** ***content reassignment***

Guarantee polylog stabilization complexity *(+ balance)*

- Tree: Stabilize underlying branches locally
  - Join (or: depart/reconnect)
  - a: local reassignment possible
  - b: escalate to parent

Paper: slightly different algorithm, disseminating estimate of |V|

Results:

- logarithmic *f*: O($\log^3$ n E(S))
- polylog f: O($\log^6$ n)

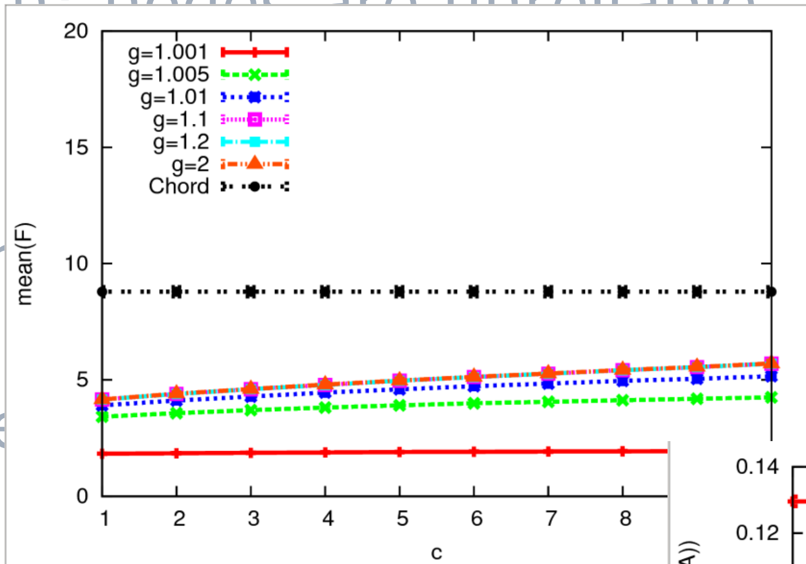
Churn: nodes are unreliable, *trees are delicate*

content reassignment

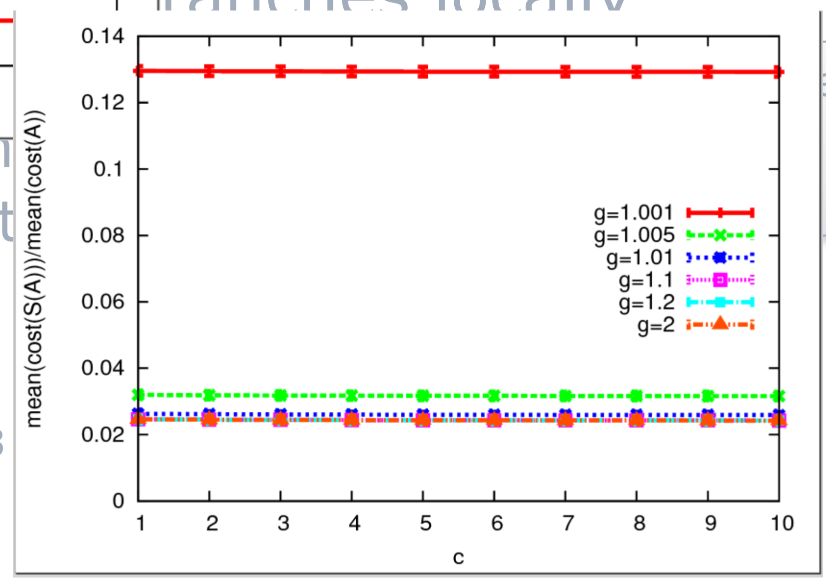
Guar… n complexity *(+ balance)*

- Tre… ranches locally

…erent
…nating



- a: local reassignmen…
- b: escalate to parent…



Results:

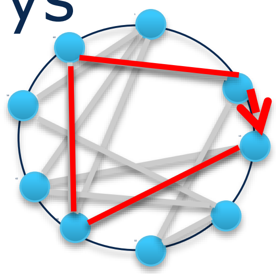
- logarithmic *f*: O($\log^3$…
- polylog f: O($\log^6 n$)

[1] Paul et al. 2012

TECHNISCHE UNIVERSITÄT DRESDEN

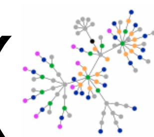
Standing on the Shoulders of Giants

Virtual Overlays



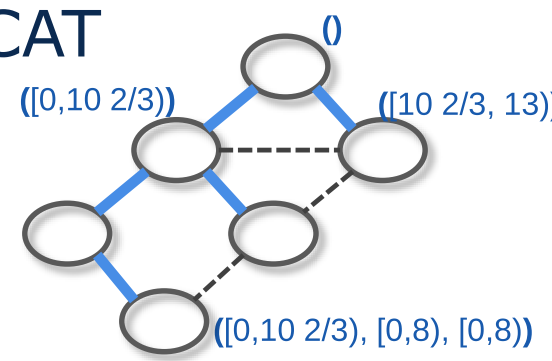
- Long routes
  - Voute: polylog [1]
  - Others: > polylog [2]

Topology-aware hashes [5]

h( , )

- Churn:Reassign everything

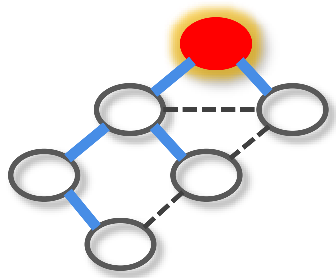
BDCAT



- log / log / polylog

Kleinberg, Prefix Emb. [3,4]

- Unfair load:



[1] Roos et al., INFOCOM 16
[2] Mittal et al., NDSS 12
[3] R. Kleinberg, INFOCOM 07
[4] Hoefer et al., NetSys 2013
[5] Roos et al., MobiArch 2014

References

I. Clarke et al. Private Communication Through a Network of Trusted Connections: The Dark Freenet. Network, 2010.

Eugene Vasserman, Rob Jansen, James Tyra, Nicholas Hopper, and Yongdae Kim. Membership-concealing Overlay Networks. In CCS, 2009.

J. Herzen, C. Westphal, and P. Thiran. Scalable Routing Easy as Pie: a Practical Isometric Embedding Protocol. In ICNP, 2011.

A. Hofer, S. Roos, and T. Strufe. Greedy Embedding, Routing and Content Addressing for Darknets. In NetSys, 2013.

T. Paul et al. C4PS-helping Facebookers manage their privacy settings. In International Conference of Social Informatics

S. Roos and M. Beck. Anonymous Addresses for Efficient and Resilient Routing in F2F Overlays. In INFOCOM, 2016.

R. Kleinberg. Geographic Routing using Hyperbolic Space. In INFOCOM, 2007.

P. Mittal et al. X-vine: Secure and pseudonymous routing in dhts using social networks. In NDSS, 2012.

S. Roos, L. Wang, T. Strufe, and J. Kangasharju. Enhancing Compact Routing in CCN with Prefix Embedding and Topology-Aware Hashing. In MobiArch, 2014.

S. Roos, M. Byrenheid, C. Deusser, T. Strufe. Balanced Dynamic Content Addressing in Trees. https://arxiv.org/abs/1701.03522