

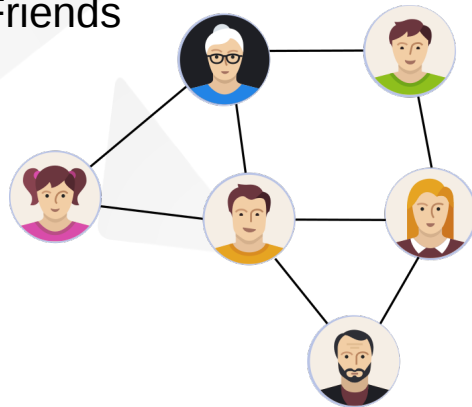
# Friend-to-friend ネットワークにおける 効率的な分散ルーティング

非線形物理学講座  
高橋彰

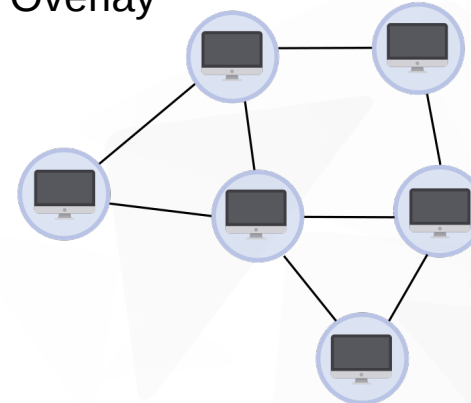
## Friend-to-Friend (F2F) ネットワーク

- ・ネットワーク上の各ノードは信頼のおける特定ノードとのみ通信
- ・匿名性やプライバシー保護を重視
- ・ネットワークトポロジーが現実世界の信頼関係ネットワークに対応
  - 複雑ネットワーク研究の知見を活用
- ・各ノードは隣接ノード以外の情報を知らない
  - 分散ルーティングの必要性

Friends



Overlay



S. Roos (2016)



本研究の目的：F2F ネットワークにおける分散ルーティングの効率性向上

# 先行研究 : Embedding and Routing Algorithms in Freenet

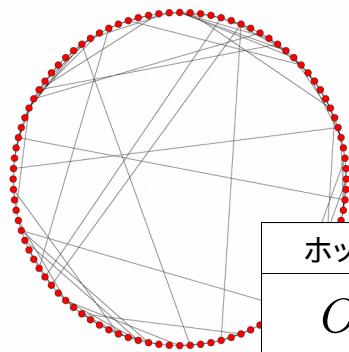
## ① Kleinberg のスモールワールドモデル

ノード間エッジ生成確率

$$p(u, v) \propto d(u, v)^{-r}$$

Greedy ルーティング

ターゲットまでの距離が最も近い  
隣接ノードにメッセージをフォワード

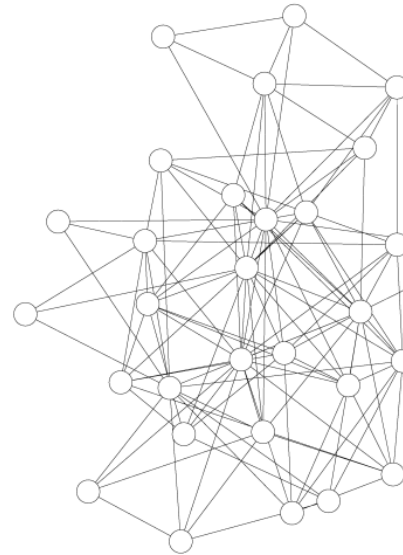


ホップ数期待値

$$O(\log^2 n)$$

J. Kleinberg (2000)

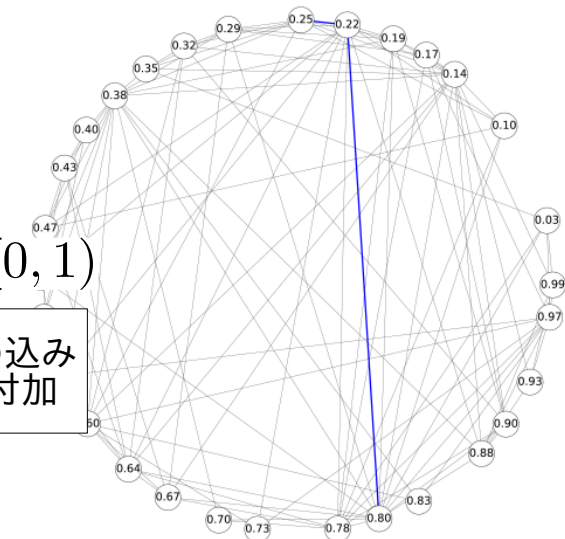
## ② ネットワークの埋め込み (embedding) とルーティング



$$\phi : V \rightarrow [0, 1)$$

円周上に埋め込み  
座標情報を付加

ネットワークデータ  
 $G = (V, E)$



ノード間距離を用いて  
greedy ルーティング

$$\text{距離関数} : d(\phi(u), \phi(v)) = \min[|\phi(u) - \phi(v)|, 1 - |\phi(u) - \phi(v)|]$$

## ③ 埋め込みアルゴリズム : SWAP アルゴリズム

- ・ Kleinberg モデルに基づき座標 (=ID) を割り当て
- ・ メトロポリスヘイスティングス法による

採択確率

$$\beta(\phi_1, \phi_2) = \min \left[ 1, \frac{\prod_{w \in N(v)} d(\phi_1(w), \phi_1(v)) \prod_{w \in N(u)} d(\phi_1(w), \phi_1(u))}{\prod_{w \in N(v)} d(\phi_2(w), \phi_2(v)) \prod_{w \in N(u)} d(\phi_2(w), \phi_2(u))} \right]$$

O. Sandberg (2006)

## ④ 問題点

- ・ SWAP アルゴリズムは Kleinberg モデルの特徴を正確に反映できず  
→ 単純な greedy ルーティングでは非効率に
- ・ 低次数ノードの存在を無視した恣意的なシミュレーション  
→ 現実の F2F ネットワークトポロジーにおけるパフォーマンスは未評価

# 提案手法 : Degree-and-distance-directed DFS

ルーティング効率を向上させるには…

- ① 埋め込みアルゴリズムの改良
- ② ルーティングアルゴリズムの改良

方針 :

- ・ F2F ネットワークのスケールフリー性に着目
- ・ 次ノード選択に度数に応じた重み付け

## 提案アルゴリズム

隣接ノード  $v$  からターゲットノード  $t$  への  
ホップ数期待値

$$E(l(v, t)) = \sum_i ip(l(v, t) = i) \approx 1 - e^{k_v p(v, t)}$$

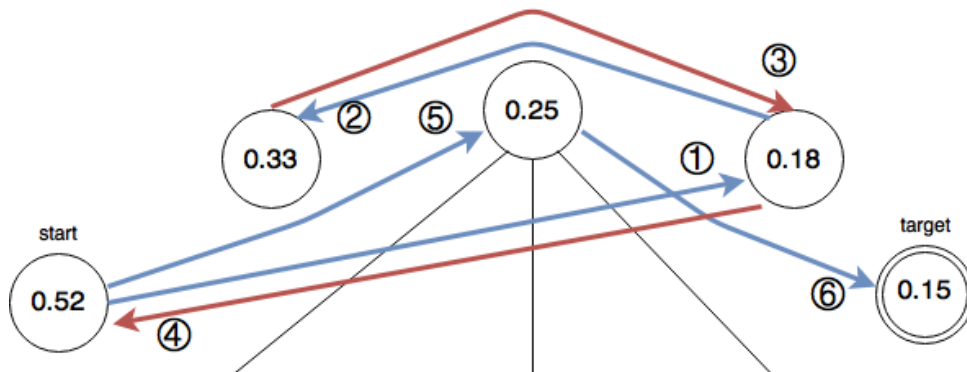
(Simsek & Jensen (2008))

- ・ Kleinberg モデル
- ・ SWAP アルゴリズム

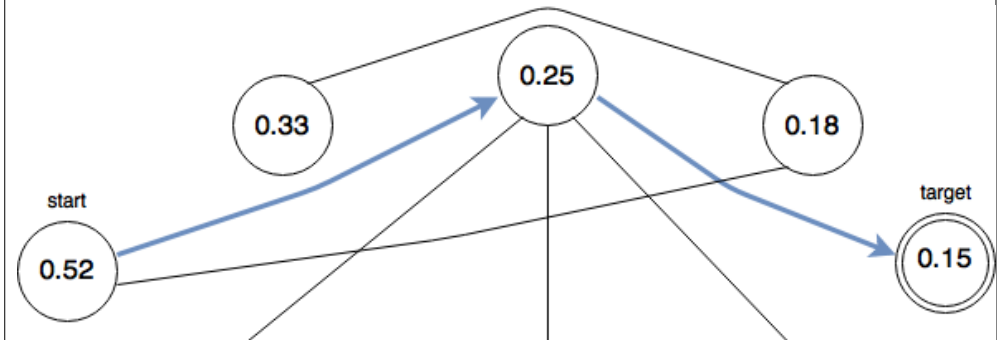
各ノードは以下の  $g(v)$  を最小化する  $v$  に  
メッセージをフォワード ( $k_v$  は  $v$  の度数)

$$g(v) = \frac{d(\phi(v), \phi(t))}{k_v}$$

従来法 (距離情報 + DFS)



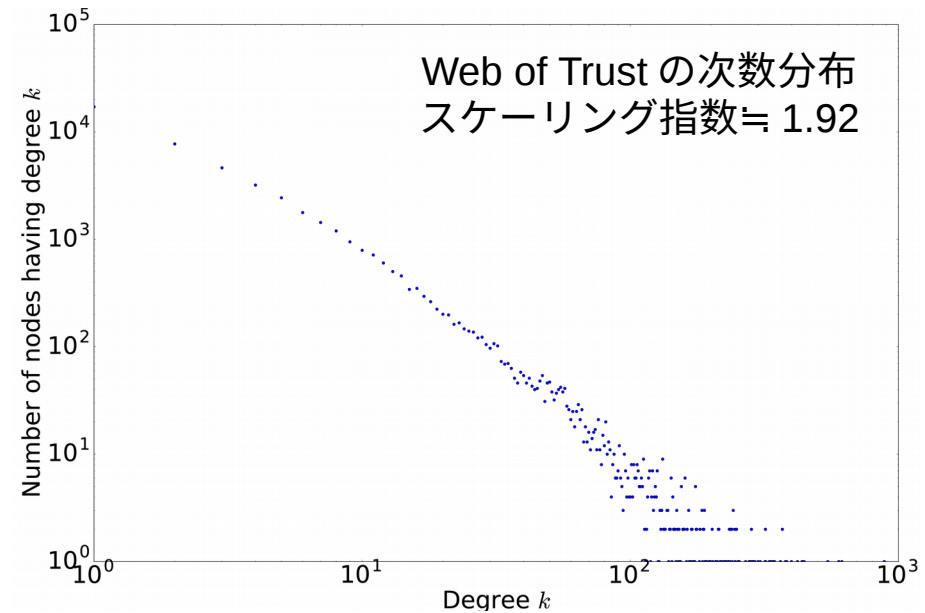
提案手法 (距離情報 + 度数情報 + DFS)



# シミュレーション実験

## 使用データ：Web of Trust (WoT)

- ・PGP 公開鍵の信頼性を保証するための仕組み
- ・現実世界における信頼関係ネットワークに対応
  - ・**ノード**：公開鍵の所有者
  - ・**エッジ**：ノード間の相互的なデジタル署名≡信頼関係
- ・典型的なスケールフリー性とスモールワールド性
  - ・ネットワークサイズ  $|V| = 48983$
  - ・平均最短経路長 = 6.60

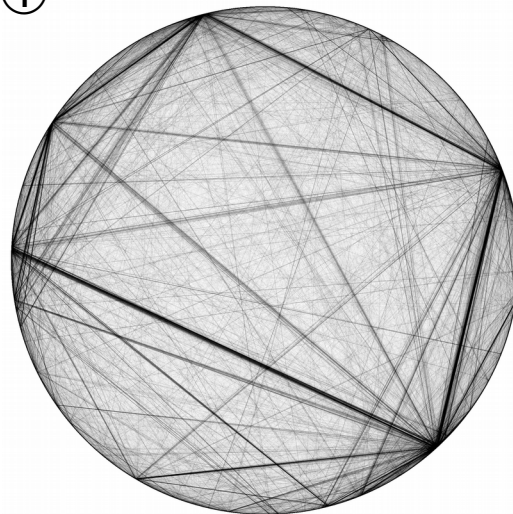


## 未処理の WoT ネットワークに対する実験

### シミュレーション手順

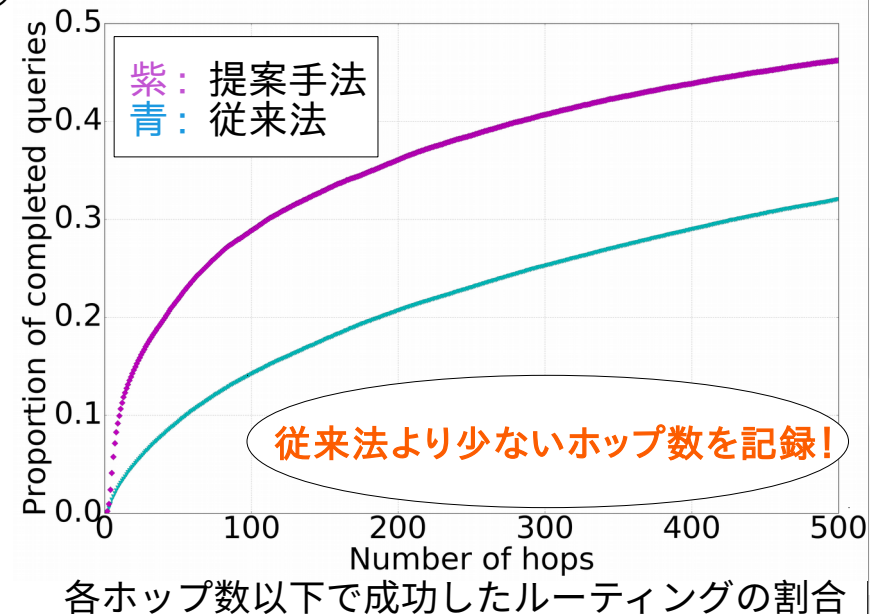
- ① SWAP アルゴリズム  
→ ノードへ座標を割り当て
- ② ランダムに選んだターゲット  
へのルーティングを実行  
→ パフォーマンスを比較

①



SWAP アルゴリズムにより  
円周上に埋め込まれたネットワーク

②



# 結論 & 今後の展望

## 結論

- ・未処理の F2F ネットワーク実データを使用
  - 現実的な状況に近いシミュレーション
- ・SWAP アルゴリズム + 次数情報を取り入れたルーティング
  - 従来の Freenet プロトコルよりも少ないホップ数を達成
- ・ホップ数の最適値には程遠く改善の余地は大いにあり

## 今後の展望

- ・さらに Freenet の実装に近い環境ではどうなるか？
- ・さらに良いヒューリスティックの設定方法はないか？
- ・SWAP アルゴリズム自体を改良できないか？

# References

- I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, “Freenet: A distributed anonymous information storage and retrieval system,” in *Designing Privacy Enhancing Technologies*, pp. 46–66, Springer, 2001.
- I. Clarke, O. Sandberg, M. Toseland, and V. Verendel, “Private communication through a network of trusted connections: The dark freenet,” *Network*, 2010.
- J. Kleinberg, “The small-world phenomenon: An algorithmic perspective,” in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pp. 163–170, ACM, 2000.
- S. Roos and T. Strufe, “Dealing with dead ends: Efficient routing in darknets,” *ACM Transactions on Modeling and Performance Evaluation of Computing Systems*, vol. 1, no. 1, p. 4, 2016.
- D.-M. S. Roos, *Analyzing and Enhancing Routing Protocols for Friend-to-Friend Overlays*. PhD thesis, TU Dresden, Germany, 2016.
- O. Sandberg, “Distributed routing in small-world networks,” in *Proceedings of the Meeting on Algorithm Engineering & Experiments*, pp. 144–155, Society for Industrial and Applied Mathematics, 2006.
- Ö. Şimşek, and D. Jensen, “Navigating networks by using homophily and degree,” *Proceedings of the National Academy of Sciences*, vol. 105, no. 35, pp. 12758–12762, 2008