特別研究報告書

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

指導教員　　宮崎修次　講師

京都大学工学部情報学科
数理工学コース
平成 24 年 4 月入学

高橋　彰

平成 29 年 1 月 XX 日提出

摘要

本研究では, ネットワークトポロジーのスモール・ワールド性を利用し, 効率的かつ非中央集権的なルーティングを実現するための手法を提起する.

目次

1 序論

近年インターネットを介したコミュニケーションまたは出版は, 我々の生活において大きな位置を占めるようになってきた. それに伴いユーザーのプライバシー保護を重視したコミュニケーションツールの実装に対する需要が非常に高まっている. その要因として, 例えば近年ではエドワード・スノーデンによって公に明らかにされたアメリカ国家安全保障局 (NSA) による大規模な大衆監視が挙げられる.

特定の企業や団体が中央集権的に管理する情報共有方式はこのような監視・漏洩のリスクが高いため, 非中央集権的な情報共有を実現するためのアプローチとして P2P 方式が頻繁に採用される. P2P は中心的な管理者を持たない分散的なオーバーレイネットワークであり, 一般的なクライアント-サーバー方式と比較して負荷分散, スケーラビリティ, 匿名性, 耐障害性等の点で優れている [1]. そして P2P 方式の中でも特にピアの匿名性・プライバシー保護を重視したものは friend-to-friend(F2F)[2], または Darknet[3] と呼ばれる. F2F 方式において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するため, Chord[4] などの分散ハッシュテーブル (DHT) 方式とは異なり, ソフトウェアによって動的にネットワーク構造を最適化することはできず, ネットワーク構造は常に現実の信頼関係ネットワークの部分グラフに対応する. そしてネットワーク上で隣接していないノード同士がデータの送受信を行うためにはいずれかのノードが「知り合いの知り合い」を辿って他方のノードに到達するための経路を探索する必要性が生じる [5].

F2F オーバーレイネットワークの最も代表的な実装例は, Freenet[6] の Darknet モード [3] であり, 基本的なプロトコルは Sandberg[7] が 2006 年に提案した手法に基づいている. Freenet では, 信頼関係のネットワークがスモールワールド性を持つと仮定し, 単純な greedy ルーティング (各ノードは隣接ノード中, 最もターゲットに近いノードを次ノードとして選択) により, $O(\log^2 n)$ のホップ数でルーティングを可能にする Kleinberg のスモールワールドネットワークモデル [8] に基づいている.

ただし Freenet には未だ様々な問題点が残っている. 第一に Sandberg が提案した手法では, Kleinberg モデルが依拠している「格子上で最も近距離にいるノード同士は必ずエッジを持つ」という仮定を決定論的に満たすことができないため, Freenet の実装においては greedy ルーティングの代わりに distance-directed depth-first search (D^2-DFS) が採用されている. しかしこの D^2-DFS アルゴリズムが特定の条件下において $O(\log^2 n)$ のホップ数を達成することができないことは Roos, Strufe らにより解析的に証明された [9] [5][10]. また Freenet では, ノード集合 V から座標空間 $C = [0, 1)$ への「埋め込み」(embedding) $\phi : V \to C$ を生成する Metropolis-Hastings アルゴリズムの一環としてノード同士が座標

(Freenet の実装では ID) を交換する操作を反復するが, この際悪意のあるノードが虚偽の ID 報告を繰り返すことにより, ノードが格子上に偏在し, 結果的にルーティングの効率性が低下するという Pitch black attack[11] などの深刻な脆弱性が指摘されている. よって Freenet の Darkenet モードは効率性や頑健性の面で問題点が残り, 現在もそれらを解決するための研究が続けられている.

本研究では, 以上に挙げられた Freenet の問題点のうちルーティングの効率性に着目する. 今回我々は Simsek, Jensen らによって提案されたルーティングアルゴリズム, expected-value navigation (EVN)[12] を Freenet プロトコルに適用可能な形に修正することにより, スケールフリー性を持った F2F ネットワークにおいて既存ルーティングアルゴリズムよりも高いパフォーマンスを発揮する D^3-DFS を提案する. また, 先行研究のシミュレーション実験においてはルーティングの成功率が向上するように実データの恣意的な改変が施されていたが, 本研究では改変を施さない実データに対するシミュレーション実験を行うことにより, 現実の F2F トポロジーにより近いネットワークにおけるルーティングアルゴリズムのパフォーマンス評価を行った.

2 先行研究

2.1 P2P ネットワーク

2.2 複雑ネットワーク

2.3 Kleinberg モデル

2.4 Greedy embedding

2.5 Freenet プロトコル: 埋め込みとルーティング

2.6 EVN: Expected-value navigation

$$
\begin{aligned}
E(l(v,t)) &= \sum_i ip(l(v,t)=i) \\
&\approx p(l(v,t)=1)) \\
&= 1-p(n_{v,t}=0)) \\
&= 1-(1-p(v,t))^{k_v}) \\
&\approx 1-Poisson(0;k_v p(v,t))) \\
&= 1-e^{k_v p(v,t)}
\end{aligned} \tag{1}
$$

よってある隣接ノード v が $E(l(v,t))$ が最小化することは, $1/k_v p(v,t)$ を最小化することと同値であるからヒューリスティック関数 $f(v)$ を

$$f(v) = \frac{1}{k_v p(v,t)} \tag{2}$$

と定義すれば, 「メッセージを持つノード u は (2) 式で定義される $f(v)$ を最小化するような隣接ノード $v \in N(u)$ にメッセージをフォワードする」というシンプルなルーティングアルゴリズムにより, 隣接ノード中最もターゲットに近い可能性の高いノードを選択することができる.

3 問題設定

2.5 節に述べた F2F ネットワークにおける分散ルーティング効率を向上するための大まかな方針として (1) 埋め込みアルゴリズムの改良 (2) 分散ルーティングアルゴリズムの改良 の 2 通りを挙げることができる．本研究では後者の方針を選択する．つまり Sandberg による SWAP が greedy embedding でないという前提の上で, SWAP 適用後のネットワークにおけるルーティング効率を改善させるための方法を模索する．
その上で今回我々は F2F ネットワークが持つスケールフリー性に着目し, 2.6 節で述べた Şimşek, Jensen のヒューリスティックスを取り入れることで Freenet プロトコルにおける分散ルーティングのパフォーマンスを向上させることを試みる．つまり, 今回我々が検証する仮説は「greedy embedding でない SWAP 適用後の F2F ネットワークにおいて, 単純なノード間距離に応じたヒューリスティックを用いる代わりに, 隣接ノードの次数とノード間距離を共に考慮したヒューリスティックスを用いることで, ルーティングのパフォーマンスを向上させることが可能である」とまとめることができる．以下この仮説検証のために, D^2-DFS と EVN を統合したルーティングアルゴリズム, degree-and-distance-directed depth-first search (D^3-DFS) の提案とパフォーマンス評価を行っていく．

4 提案手法

まず D^3-DFS において用いるヒューリスティックスを定義する．Sandberg の手法に従い, ネットワークが Kleinberg モデルに従って生成されたとすると隣接ノード $v \in N(u)$ がターゲットノード t と隣接する確率は正規化定数 Z を用いて $p(v,t) = 1/d(v,t)Z$ であるから, これを 2.6 節で導いた (2) 式に代入するとヒューリスティック関数 $f(v)$ は次のような形で表される．

$$f(v) = \frac{d(v,t)}{k_v} \tag{3}$$

よって D^3-DFS において, メッセージを持つノード u は (3) 式を最小にするような $v \in N(u)$ にメッセージをフォワードすることが基本的な動作となる．これは通常の距離のみを用いた greedy ルーティングに次数の重み付けを付加したものと見なすことができる．
次に, u の全ての隣接ノードが以前にメッセージを受け取ったことがあるような状況を考える．このような場合 [**?**] では次ノードを隣接ノードの中からランダムに選択するとしているが, ランダムなノード選択では同様に隣接ノードが全て訪問済みであるようなノードに何度も到達する可能性があり無駄なステップが増えることが予想されるため, D^3-DFS ではその

名前が表すように, u に初めてメッセージをフォワードしたノード (predecessor) にメッセージを戻すとする.

以上 D^3-DFS の動作に関する概略を述べた. 詳細なアルゴリズムは以下の擬似コード Algorithm 1 に示す. ただし擬似コードの記述スタイルについては [13] を参考にした.

Algorithm 1 D^3-DFS(Node u, Node p, ID t, Set B, TTL c)

```
# u: current message holder, p: previous message holder
# t: target node ID, B: set of nodes who have seen the message before
if id(u) == t then
    routing succeeded; terminate
end if
if c == 0 then
    routing failed; terminate
end if
if u.predecessor == null then
    u.predecessor = p
end if
S = {v ∈ N(u) | v ∉ B}
if S == ø then # all the neighbors have seen the message before
    B = B ∪ {u}
    next = u.predecessor
else
    next = arg min_{v∈S} d(u, v)/k_v
    B = B ∪ {next}
end if
if next == null then # this happens only if a current node is the source
    routing failed; terminate
else
    D^3-DFS(next, u, t, B, c − 1)
end if
```

最後に D^3-DFS において各ノードが利用可能な情報をまとめると以下のようになる.

1. 自分と隣接ノードの ID

2. ターゲットの ID
3. メッセージを自分に最初に送ってきたノード (predecessor)
4. これまでにメッセージをフォワードした隣接ノード
5. 隣接ノードの次数

上記の 1. から 4. は先行研究の D^2-DFS が利用する情報と同様であるが, 5. のみが新たに追加された利用可能な情報である．実際の F2F ネットワークにおける実装においては, 各ノードが互いに現在の接続ノード数に関する情報を隣接ノードと共有し合う状況ということになる．5. の条件は [8] における分散ルーティングの定義には含まれないものだが, [14] や [15] 等 1. から 4. 以外の局所的な情報を利用する方式も「分散的 (decentralized)」なアルゴリズムと呼ばれているので, 今回提案するアルゴリズムも広義の分散ルーティングとして捉えることとする．また隣接ノードの単なる次数情報はグラフ全体のトポロジーを明らかにするものではなく, また信頼するノード以外に対してアイデンティティを明かすことにもなりえないため, D^3-DFS はプライバシーコントロールやセキュリティ面を重視する Freenet などの F2F ネットワークに十分適用可能であると考えられる．

5 評価

5.1 シミュレーション手法

D^3-DFS のパフォーマンス評価を行うために 5.3 節で述べる実データに対するシミュレーション実験を行った. 実験の基本的な流れは先行研究と同様 (1) 埋め込みの生成 (2) 距離空間における分散ルーティングの実行 という 2 つのステップから成る.
(1) においては 2.5 で述べた Sandberg の埋め込みアルゴリズムを適用し, 各ノードに対する ID の割り当てを行った. ただし, [7] に従い Metropolis-Hastings アルゴリズムの反復を $6000|V|$ 回, [10] に従い SWAP におけるランダムウォークの試行回数を 10 と設定した.
ID 割り当ての終了後, (2) においては全てのノードを出発点として, 各ノードにつき 5 つのターゲットノードをランダムに選びルーティングのシミュレーションを行った. ただし [7], [16] に従いホップ数上限 $TTL \approx \log^2 |V|$ とし, ホップ数が TTL を超えたルーティングを失敗とみなした. 以上の条件下で $5|V|$ 回 D^3-DFS のルーティングシミュレーションを行い, 比較のために既存の 5 つのルーティングアルゴリズムに対しても同様の実験を行い, 各ルーティングアルゴリズムについて, ルーティングの成功率, 成功したルーティング試行の平均ホップ数を集計した.
また成功率の異なるルーティングアルゴリズム間で平均ホップ数の大小を比較するのは不適切であるため, TTL を長めに (恣意的ではあるが本研究では 500 とする) 設定してルーティング実験を同様に $5|V|$ 回行った場合の「各ホップ数以下で成功したルーティング試行の割合」を集計した.

5.2 各ルーティングアルゴリズムの説明

(a) FAIL: 純粋な greedy ルーティング. dead-end に達したらその時点でルーティング失敗とする [7]
(b) CONT: FAIL より緩い条件での greedy ルーティング. dead-end に達したも隣接ノード中で最もターゲットに近いノードにフォワードする. 隣接ノードが全て訪問済みの場合ルーティング失敗とする. [7]
(c) EVN: ノード選択に D^3-DFS と同様のヒューリスティックを用いる. 隣接ノードが全て訪問済みの場合ルーティング失敗とする.
(d) EVNR: ノード選択に D^3-DFS と同様のヒューリスティックを用いる. 隣接ノードが全て訪問済みの場合, 隣接ノードからランダムに選んだノードにフォワードして続行する. [12]

(e) D^2-DFS: ノード選択は CONT と同様. 隣接ノードが全て訪問済みの場合, predecessor にメッセージをフォワード (backtracking) して続行する. [6], [3]

5.3 使用データ

先行研究の多くは埋め込みやルーティングのアルゴリズムのパフォーマンス評価のため, 実世界のソーシャルネットワークデータを使用している. 本研究もそれに習い F2F ネットワークの実データとして, 2016 年 12 月 11 日時点における Pretty Good Privacy (PGP) の Web of Trust (WoT) を用いた. PGP は暗号化プログラムであり, WoT は PGP 公開鍵の信頼性を非中央集権的な方法で担保するための仕組みである (詳細は [17], [18] を参照). WoT の形成するネットワークは現実世界における人同士の信頼関係ネットワークの部分グラフであり, 公開鍵の所有者はノードに, 公開鍵に対するデジタル署名がエッジに対応する. 例えば「Alice が Bob の公開鍵にデジタル署名した」場合 Alice から Bob へのエッジが存在しているといった具合である. WoT は本来有向グラフであるが, 先行研究に従い「公開鍵の所有者間で相互にデジタル署名が行われている」ことを「ノード間に信頼がある」と定義し, 元のネットワークデータから単方向の署名に対応するエッジを削除したものから giant component (最もノード数の多い連結部分グラフ) を抽出し, これを無向グラフとして扱うこととする. 以上のような操作によって得られたグラフを $G = (V, E)$ とする. ネットワークデータの処理, ネットワークデータ解析は全て NetworkX 1.11[19] を用いて行った.
WoT G の解析の結果得られた基本情報を表 1 に示す. 表 1 と WoT の次数分布をプロットした図 1 から, WoT は典型的なスモールワールドネットワークかつスケールフリーネットワークの特徴を持つことが確認できる.

総ノード数 $\|V\|$	48983
総エッジ数 $\|E\|$	183840
平均最短経路長	6.60
平均次数	7.51
最大次数	885
クラスタリング係数	0.31
スケーリング指数 γ	1.92

表 1: 2016 年 12 月 11 日時点における Web of Trust の基本情報
使用データセット: `https://wot.siccegge.de/download/2016-12-11.wot`

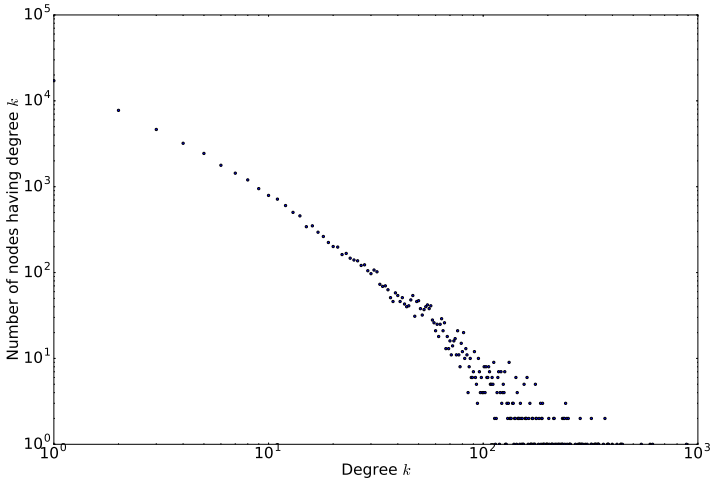

図 1: Web of Trust ネットワークの次数分布

5.4 シミュレーション結果

5.4.1 未処理のデータに対する結果

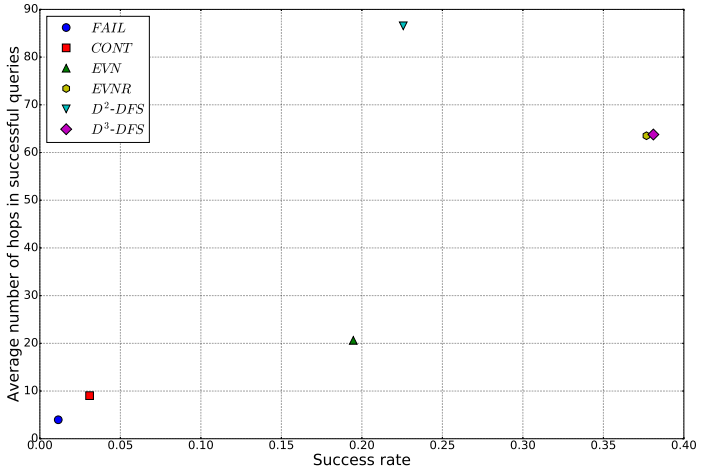

図 2: ID 割り当て後の Web of Trust ネットワークにおける各ルーティングアルゴリズムの成功率と平均ホップ数

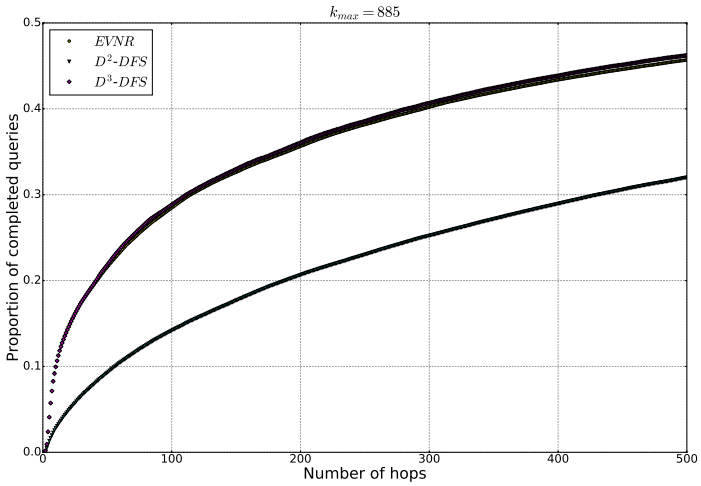

図 3: ID 割り当て後の Web of Trust ネットワークにおける各ホップ数以下で成功したルーティング試行の割合

5.4.2 ハブを除いたデータに対する結果

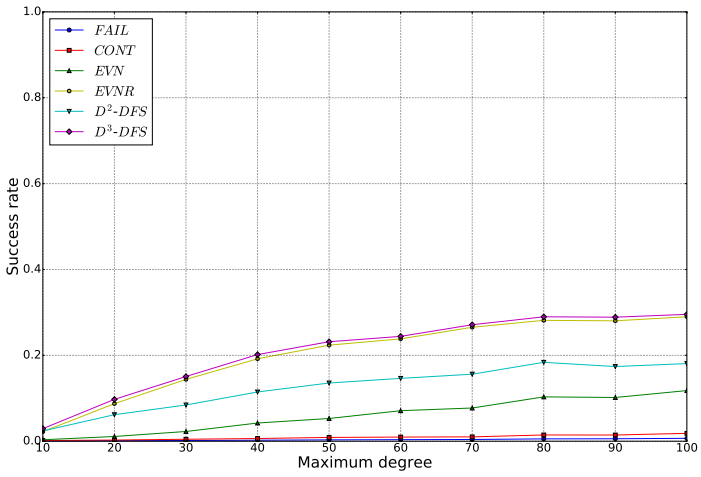

図 4: 次数上限を設定した Web of Trust ネットワークにおける各ルーティングアルゴリズムの成功率

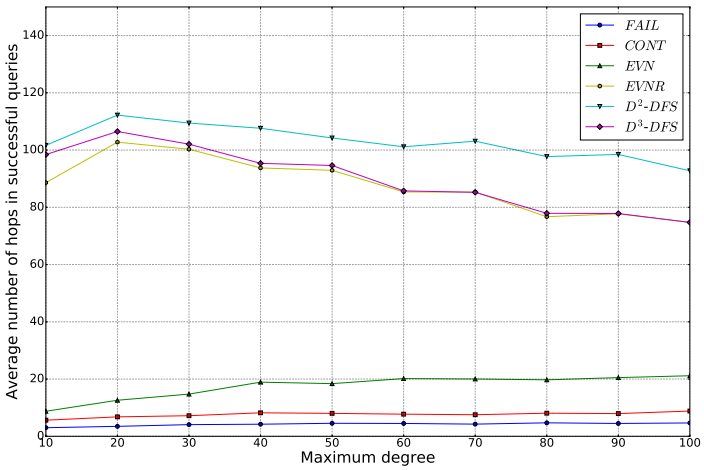

図 5: 次数上限を設定した Web of Trust ネットワークにおける各ルーティングアルゴリズムの平均ホップ数

6　結論と今後の展望

TBD

謝辞

参考文献

[1] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 2, pp. 72–93, 2005.

[2] D. Bricklin, "Friend-to-friend networks." `http://www.bricklin.com/f2f.htm`, 2000.

[3] I. Clarke, O. Sandberg, M. Toseland, and V. Verendel, "Private communication through a network of trusted connections: The dark freenet," *Network*, 2010.

[4] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 149–160, 2001.

[5] 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.

[6] 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.

[7] O. Sandberg, "Distributed routing in small-world networks," in *Proceedings of the Meeting on Algorithm Engineering & Expermiments*, pp. 144–155, Society for Industrial and Applied Mathematics, 2006.

[8] 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.

[9] S. Roos and T. Strufe, "Provable polylog routing for darknets," in *2012 32nd International Conference on Distributed Computing Systems Workshops*, pp. 140–146, IEEE, 2012.

[10] D.-M. S. Roos, *Analyzing and Enhancing Routing Protocols for Friend-to-Friend Overlays*. PhD thesis, TU Dresden, Germany, 2016.

[11] N. S. Evans, C. GauthierDickey, and C. Grothoff, "Routing in the dark: Pitch black," in *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pp. 305–314, IEEE, 2007.

[12] 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.

[13] S. Roos and T. Strufe, "A contribution to analyzing and enhancing darknet routing," in *INFOCOM, 2013 Proceedings IEEE*, pp. 615–619, IEEE, 2013.

[14] G. S. Manku, M. Naor, and U. Wieder, "Know thy neighbor's neighbor: the power of lookahead in randomized p2p networks," in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pp. 54–63, ACM, 2004.

[15] E. Lebhar and N. Schabanel, "Almost optimal decentralized routing in long-range contact networks," in *International Colloquium on Automata, Languages, and Programming*, pp. 894–905, Springer, 2004.

[16] B. Schiller, S. Roos, A. Hofer, and T. Strufe, "Attack resistant network embeddings for darknets," in *Reliable Distributed Systems Workshops (SRDSW), 2011 30th IEEE Symposium on*, pp. 90–95, IEEE, 2011.

[17] P. R. Zimmermann, *The official PGP user's guide*. MIT press, 1995.

[18] A. Abdul-Rahman and S. Hailes, "A distributed trust model," in *Proceedings of the 1997 workshop on New security paradigms*, pp. 48–60, ACM, 1998.

[19] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using NetworkX," in *Proceedings of the 7th Python in Science Conference (SciPy2008)*, (Pasadena, CA USA), pp. 11–15, Aug. 2008.

付録 A　用語集

Glossary

F2F Friend-to-friend. 1, 2

local contact 距離空間上に配置されたグラフにおいて最も近距離にあるノード間を接続するエッジ. 2

SWAP TBD. 3

埋め込み TBD. 1

特別研究報告書

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

指導教員　　宮崎修次　講師

京都大学工学部情報学科
数理工学コース
平成 24 年 4 月入学

高橋　彰

平成 29 年 1 月 XX 日提出

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

高橋　彰

平成28年度

特別研究報告書

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

指導教員　　宮崎修次　講師

京都大学工学部情報学科
数理工学コース
平成 24 年 4 月入学

高橋　彰

平成 29 年 1 月 XX 日提出

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

高橋　彰

摘要

本研究では, ネットワークトポロジーのスモール・ワールド性を利用し, 効率的かつ非中央集権的なルーティングを実現するための手法を提起する.