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, F2F 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 $O(\log^2 n)$ 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, 埋め込みの不正確さと, 現実のネットワークに存在する多数のリーフノードに対しロバストなルーティングアルゴリズムを提起する.

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

3 問題設定

TBD

4 提案手法

TBD

4.1 ネットワークモデル

TBD

4.2 ルーティングアルゴリズム

TBD

5 評価

5.1 シミュレーション手法

TBD

5.2 シミュレーション結果

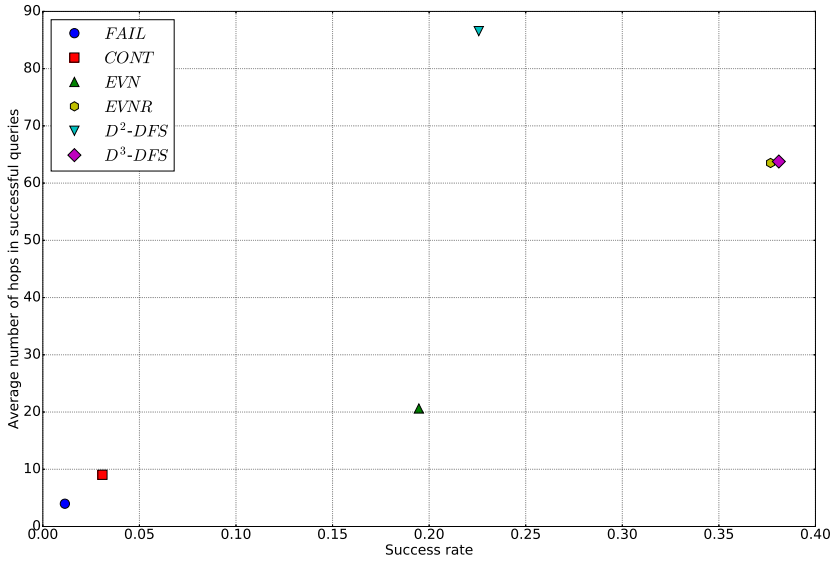

図 1　ID 割り当て後の Web of Trust ネットワークにおける各ルーティングアルゴリズムの成功率と平均ホップ数

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," 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.

付録 A　用語集

表 1　これは意味のない表です.

	A	B
C	70	80
D	100	0

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, F2F 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.