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 [7]. 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[12] 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 [9].

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[4] の Darknet モード [3] であり, 基本的なプロトコルは Sandberg[10] 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 [6] 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) と呼ばれるルーティングアルゴリズムが採用されている. 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 [8] [9]. 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[5] 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効率性に着目する. 以下ではスモールワールド性, スケールフリー性, クラスタ性等の現実の F2F ネットワークに現れる構造を Kleinberg モデルよりもさらに正確に反映し, かつ greedy ルーティングが高確率で成功する Serrano et al. のモデル [11] [1] を採用し, Sandberg の埋め込み写像生成アルゴリズムを改良することにより, 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を目指す.

参考文献

[1] Marián Boguná, Dmitri Krioukov, and Kimberly C Claffy. Navigability of complex networks. *Nature Physics*, 5(1):74–80, 2009.

[2] Dan Bricklin. Friend-to-friend networks, 2000.

[3] Ian Clarke, Oskar Sandberg, Matthew Toseland, and Vilhelm Verendel. Private communication through a network of trusted connections: The dark freenet. *Network*, 2010.

[4] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Designing Privacy Enhancing Technologies*, pages 46–66. Springer, 2001.

[5] Nathan S Evans, Chris GauthierDickey, and Christian Grothoff. Routing in the dark: Pitch black. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pages 305–314. IEEE, 2007.

[6] Jon Kleinberg. The small-world phenomenon: An algorithmic perspective. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 163–170. ACM, 2000.

[7] Eng Keong Lua, Jon Crowcroft, Marcelo Pias, Ravi Sharma, and Steven Lim. A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys & Tutorials*, 7(2):72–93, 2005.

[8] Stefanie Roos and Thorsten Strufe. Provable polylog routing for darknets. In *2012 32nd International Conference on Distributed Computing Systems Workshops*, pages

140–146. IEEE, 2012.

[9] Stefanie Roos and Thorsten Strufe. Dealing with dead ends: Efficient routing in darknets. *ACM Transactions on Modeling and Performance Evaluation of Computing Systems*, 1(1):4, 2016.

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

[11] M Angeles Serrano, Dmitri Krioukov, and Marián Boguná. Self-similarity of complex networks and hidden metric spaces. *Physical review letters*, 100(7):078701, 2008.

[12] Ion Stoica, Robert Morris, David Karger, M Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. *ACM SIGCOMM Computer Communication Review*, 31(4):149–160, 2001.