修論実装の進捗

ARCH meeting 2014/11/06

bhangra

実装の進捗

- ノードリストの管理
- △新規ノードの接続
  - dns seed
  - dns round robin
  - version / verack ハンドシェイク
  - ×getaddr / addr メッセージ
- △採掘したブロックの伝搬
- △受信したブロックの処理
- ×悪しきノードと乗っ取りを受けたノードの挙動
- ×ネットワーク全体の模倣
  - ×接続の片方向性の割合
  - ×新規ノードの生成、TTLを見てのノード殺害等

現状のシミュレーション

- ノードを複数固定で最初期のみに生成
- DNSラウンドロビンで他のノードと接続
- ×getaddr / addr メッセージは未だ未使用

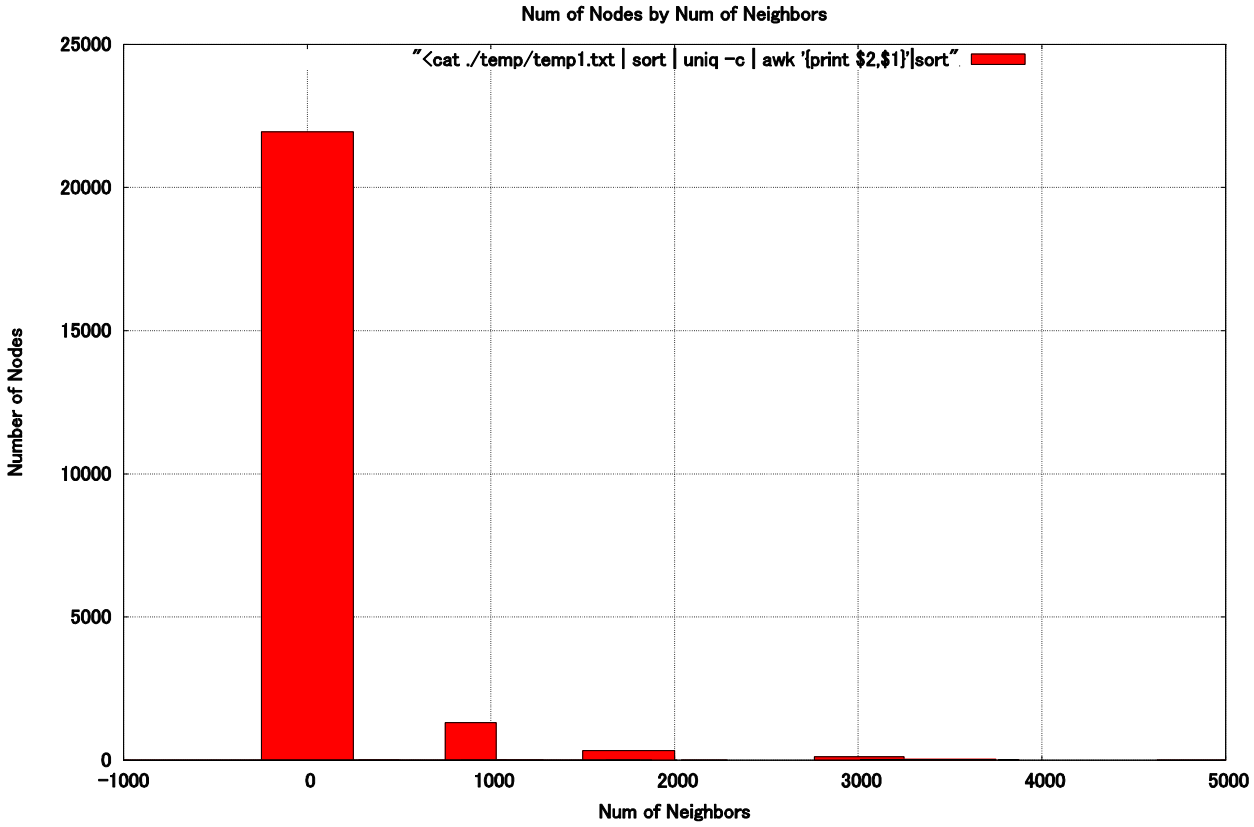
- △主に全てのノードが最新かそれに近いブロックを同じタイミングで持てているかを見ている

実際のBitcoinネットワーク？

- Hole punching機能が無いからNATの向こうに居るノードは
  - 他所からの接続を受け付けない
  - 接続ノード数が最低限？

- 新規接続出来るノードは
  - 殆どがデフォルトの最大接続数の1000?
  - 後はユーザが気まぐれで設定した最大接続数？

ノード数	隣接ノード数
21947	リスト取得失敗(接続失敗)
2	1
1	46
1	87
1	500
1305	1000
331	2000
1	2001
1	2047
112	3000
30	4000
11	5000
2	6000
4	7000



データが微妙

- TCP接続がそもそも出来なかったケースと、versionハンドシェイク出来なかったケース混ざってるから
  - 接続数が設定された最大値で新規接続出来なかったケースの割合がわからない

- 再度データ取得する必要あり

データ取得方法

1. 原始的なプログラムとスクリプトを使った再帰的なデータ収集
   - 既にやった手法なので直ぐ取り掛かれる
   - 新規接続ノードの隣接ノードリストが入手出来ない
2. ビットコインクライアントを改造
   - seedする事で新規接続ノードの隣接ノードリストが手に入る
   - getaddr送信の高頻度化、ブロック・トランズアクション伝搬の無効化、ログの取り方の実装等少々手間