匿名掲示板の開発

-完全に匿名な通信を目指して-

1　背景

情報化社会において，誰もが実名で発言できるほど強く生きているわけではない．様々な弱い立場の人ほど，匿名性を必要としている．日々の生活の不平不満，心の悩み，大声で言えない身体の悩みなどは匿名性が担保されて初めて安心して語ることができる．

しかし，インターネット上に存在する匿名性は，本当の意味の匿名ではなく，システムの運営側がサービスで名前を伏せておいてくれているだけである． 例えば，システムの内部の誰かが通信ログを外部に持ち出す，ふとしたミスで通信ログが外部の人間の手に渡る，などという事態になれば世の中は大混乱に陥ってしまう．

2　目的

人の命にも関わる社会情報基盤は，それを運営する人間の裁量のみに委ねられるべきではなく，その中でも匿名性は，社会を支えるためにも，可能な限り属人性の無い所に成立されるべきである．また，情報技術が発達するに伴って情報の保存・共有・調査にかかるコストが飛躍的に下がっており，生半可な努力では簡単に匿名性は破られてしまう．そのような事態を避けるため，アルゴリズム的に保証された匿名性をネットワークの上に実現する事を目的とする．

3　開発内容

本プロジェクトでは，全ての通信が傍受された上でもなお発信者の匿名性を維持できる匿名プロキシを実装した．この匿名プロキシでは，Chord[1] と呼ばれるDHT を利用した．匿名化のためにはパケットの内容の隠蔽・中継経路の隠蔽・発信タイミングの隠蔽を行う必要がある．それぞれについて説明する．

3.1 内容の隠蔽

通信内容は全て暗号化される．P2P に参加する際に必ず自身の IP アドレス・ポート番号・公開鍵をセットで公開し，そのピアへの送信パケットは全てそのピアに対応する公開鍵による暗号化を行なった上で送信されるため，その暗号化されたデータを取得しても解読は不可能となる．暗号化は常に新しい共通鍵をランダムに生成し，その鍵を用いて鍵ごと埋め込むため，同一の内容であっても全く異なるデータとして送信される．

3.2 中継経路の隠蔽

全ての送受信は目的のピアに向けて複数のピアを経由していく．しかし中継する際に受信したパケットと送信したパケットとの対応関係を追われてしまうと発信者を特定できてしまうため，中継する際には到着した順ではなく常にランダムな順序で送信を行う．

暗号化されたパケットのサイズで対応関係を追われる事を避けるため，全てのパケットは 4KB にパディングした上で暗号化して送信する．前述したように中継する際にパケットは受信者の公開鍵を用いて暗号化され直すため特定のピアの送受信を監視してもなお受信したパケットと送信したパケットの対応関係は割り出せない．

3.3 タイミングの隠蔽

情報発信を行なおうとしたピアの何らかの挙動の変化が観測された場合に，そのピアが発信者として疑われる可能性があるため，全てのピアは情報の発信の有無にかかわらず外から見た挙動を変化させないようにする．その為に Chord の fix finger メソッドを図 1 のように改変する．

通常の経路維持と全く同じ素振りで情報を伝搬させるため挙動から情報のリレーされたタイミングを追うことができない．

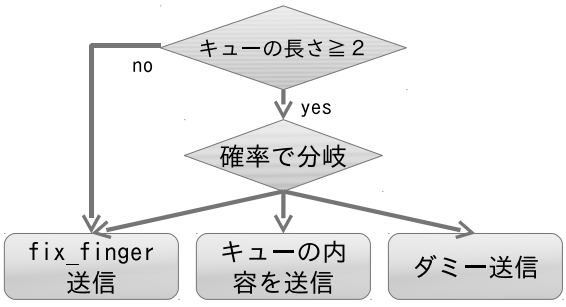

図 1: 隠蔽のため改変した fix finger

3.4 ユーザーインタフェース

AnonyMe そのものにも UI を取り付けた．これは現状でこのピアが知っている終端点の名前と，現時点で自分から見えている自分以外のピア，最近 10 秒間での通信ログが表示されている．これは AnonyMe を立ち上げた状態でブラウザに「127.0.0.1:4567」と入力することで表示できる．ポート番号は起動時のオプションで自由に変更できる．自分以外のピアの台数が多いほど，P2P として匿名性の観点からも安定性の観点からもより良い状態となっている事を意味するため，GUI の中に自分以外の参加ピア数を表示する欄を設けた．

4 従来の技術との相違

4.1 通常の電子掲示板との違い

インターネット上で一般に掲示板と言った場合，電子掲示板（BBS）を指すことが多い．これは個人が容易に作成でき，至る所でホストされているサービスである．この BBS には自分の名前を入力する欄があり，ハンドルネームや匿名での投稿が可能であるが，そこでの入力と関係なく第三者が通信を監視すれば容易に個人と書き込みの対応関係を知ることが出来る．
しかし AnonyMe の提供する匿名性は第三者が通信履歴を解析・分析した上でもなお個人と書き込みの対応関係を得ることができない物であり根本的に異なる．

4.2 匿名プロキシとの違い

P2P 通信を用いた匿名プロキシは既に実装例がある．既存の匿名プロキシは複数のピアと共通鍵を用いてマルチホップな通信を行い通信経路を匿名化するものであるが，ネットワーク全体を監視した場合はそもそもの通信の有無や，入力・出力の比率を調査する事により一次発信者を突き止める事が可能である [2]．しかし AnonyMe の提供する匿名性では，常に発信者でないピアもフィンガーテーブルの更新に合わせて送信を続ける上，情報の送受信によって入力・出力の比率が偏らないため同様の手法による発信者の特定は不可能である．

4.3 Wikileaks との違い

Wikileaks(http://wikileaks.org) は匿名で情報を公開できるサービスである，これは Wikileaks にアップロードする際にも 4.2 章で触れた匿名プロキシなどの方法を用いた匿名化が推奨されている上，ホスティングサービスが意図的に最小限の通信ログしか記録しないといった人為的な工夫によって発信者の匿名性を高めている．しかしこれによって匿名化がなされるのは Wikileaks の管轄に入っている部

分だけであり，その外側の匿名性は保証されない．すなわち監視者は情報の発信者を特定する事が可能である．
しかし AnonyMe は通信のアルゴリズムレベルでの匿名性を実現しており，特定のホスティングサービスに依存しない．また，所属するネットワークに関わらず発信者の匿名性を保つ事が出来る．

4.4 MixNet との違い

MixNet とはパケットが複数のサーバを経由する中で，意図的に複数のパケットをすれ違わせる事で対応関係を追えなくするアルゴリズムである．しかしこれは予め MixServer という専用のサーバを複数立ち上げておく必要があり，そのサーバの通信間での匿名性はあるものの，クライアントからそのサーバ群に接続するまでの匿名性は保たれない，クライアントが一つしか無い場合には，その MixServer 群への入力と出力から容易に発信者を特定できてしまう．
しかし AnonyMe は各ピアが中継サーバとしての役割も果たすため専用のサーバを立てる必要が無い上，AnonyMe に複数のピアさえ参加していれば情報発信を行うクライアントが 1 台しか無い場合でも発信者の情報を隠す事が可能である．

5 期待される効果

完全に匿名で通信が行える事による作用を具体的に見積もる事は難しい．しかし，より自由なインターネットの世界を形作っていくために匿名は必要な技術であり，インターネットが人間の社会とより密接に関わっていくための重要な足がかりになると考えている．

6 クリエータ名 (所属)

熊崎宏樹（名古屋工業大学大学院工学科創成シミュレーション工学専攻）

参考文献

[1] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. Chord: A scalable p2p lookup service for internet applications. In *ACM SIGCOMM Conference*, 2001.

[2] Steven J. Murdoch and George Danezis. Low-cost traffic analysis of tor. In *IEEE Symposium on Security and Privacy*, pages 183–195, 2005.