2010 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当PM

原田 康徳 PM
（日本電信電話株式会社 NTT コミュニケーション科学基礎研究所 主任研究員）

2. 採択者氏名

チーフクリエータ： 熊崎 宏樹（名古屋工業大学大学院）
コクリエータ： なし

3. 委託金支払額

1,600,000 円

4. テーマ名

匿名掲示板の開発

5. 関連Webサイト

なし

6. テーマ概要

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、といった事態になれば世の中は大混乱に陥ってしまう。時に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、数学的、アルゴリズム的に証明された匿名性をネットワークの上に実現すべきである。

匿名システムが犯罪に結びつくというのはまったく間違いであり、例えば駅のトイレに犯罪予告や情報のリークが書かれていても誰も信じない。匿名で犯罪予告を行うだけならばテレビ局に郵送するだけで充分で、それもいたずらであると判断されれば無視されるだけに終わる。匿名の発言という物はその媒体に関わらず匿名相応の対応を受けるものであって、電子掲示板という形のみが特異的に危険である理由はない。

本プロジェクトでは、匿名性を得るための手法として Mix-net という技術を応用する。これは匿名の電子投票などの為に発明された技術で、同一サイズにパディング（埋め合わせ）した複数のパケットをサーバ内ですれ違わせる中継を複数経由させる事でパケットの発信元の特定を防ぐ。これ自身は専用のサーバを複数管理しなくてはならず、そのサーバ群への接続自体を監視された場合特定が可能な瞬間も出てくる。それらの問題を避けるため本プロジェクトではP2P 通信の一種であるDHTを応用し、すべてのピアが中継者と発信者を兼ねる事ですべての通信が中継と発信との見分けが付かない形での匿名性と資源管理の問題を解決する。

本プロジェクトでは、高い匿名性を確保する為に投稿帯域を制限した掲示板機能のみを提供する。匿名な情報共有の違法な利用目的としてはファイル交換が有名な例として挙げられるが、本プロジェクトの掲示板ではすべてのユーザの間で情報の流入・流出の量を一定に保つ事で送信者の匿名性を確保する仕組み上、無理にでも違法なファイルをアップロードした場合の送信者の匿名性は自主的に破られるため問題ないと考えられる。

匿名性をアルゴリズムで担保した掲示板を実装し社会にその価値を問う事が本プロジェクトの目標である。

7. 採択理由

アルゴリズムの正しさと、システムとしての実用性を両立させることはなかなか難しい。また、使われる技術が特徴的であり、悪用される恐れがあるほど、研究・開発する人間には、高い倫理観が求められることとなるだろう。

匿名掲示板というと、世の中では悪いイメージでとられているが、熊崎君のいうよう

に、弱い立場の人の小さな声を拾い上げる上で、情報化社会に不可欠なインフラとも言える。監視社会という暗い窮屈な未来の中で、匿名掲示板が一つの光として世の中の役に立つような、そんな開発を期待している。

8. 開発目標

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こと、およびそのサービスの形として匿名掲示板を開発することを目標とした。

9. 進捗概要

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 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。

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。

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。

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挙動を変化させないようにする。その為には Chord の fix finger メソッドを

改変する。観測者からは通常の fix finger の挙動と全く同じ宛先へ全く同じサイズのパケットを送出しているため見分けが付かない。

10. プロジェクト評価

純粋に技術的な開発に専念できれば、もう少し開発が進んだと思うが、技術的な問題だけではなく、社会に対する影響も考慮しなければならなかったため、なかなか大変な開発であったと思う。しかし、その甲斐もあって、一般的なセンスをもった人にでも匿名性の重要さを理解してもらえるシステムを作ることができたのはよいことであった。

11. 今後の課題

プロジェクト期間内では純粋に Ruby で実装を行なったため、Windows への現時点での移植性に難がある。これは Ruby 側が改善する事で解決する可能性も有るが、JRuby に移植する事で JVM が各 OS の差異を吸収できるため、この移植作業を行うことが今後の課題として挙げられる。

今後はこのプロトコルの匿名性の強度を検証した上で、社会の基盤の一部となるよう利便性を高めていく必要がある。