研究計画書
匿名性と相手の特定を両立する仮想ネットワークの構築

慶應義塾大学環境情報学部
自署：_____
学籍番号 79956832
平成 14 年 10 月 11 日

概要

本研究では、仮想ネットワーク上で匿名性を保ったまま特定の相手との間に暗号通信路を提供するアーキテクチャを設計・実装する。特にリアルタイムなコミュニケーションを対象とし、データではなくノードの匿名性を提供する。
人間の実世界での属性を隠して行動したいという要求から匿名性を提供するサービスが広く使われているが、サービスの内容や匿名性はそのサービスの提供者に全面的に依存している。さらに、高速なネットワークインフラが多くの家庭で利用されるようになり、Peer-to-Peer モデルを利用したネットワークアプリケーションが広く使われるようになったため、特定のサーバに依存しない仮想ネットワーク上で匿名を保ったままコミュニケーションを成立させるシステムに対する要求が高まっている。本研究の応用例として、匿名による共同創作活動を支援するグループウェアや後から回答者と匿名のまま連絡の取れるアンケートなどが考えられる。

1 背景

インターネット上でさまざまなコミュニケーションが行われるようになったが、自分の名前や性別、職業といった属性による差別等を嫌がりそれらを隠して意見交換や情報公開をしたいという人は多く、大規模な匿名掲示板や個人間商取引に使われるエスクローサービスなどの匿名性を提供するサービスが広く使われるようになっている。

しかしそれらはそのサービスの提供者に全てを依存しているため、特定のサーバの存在に依存せずに匿名を保ったままコミュニケーションを成立させるシステムに対する要求が高まっている。

幸いにして ADSL や光ファイバなどの高速なネットワークインフラが多くの家庭で利用されるようになり、Peer-to-Peer モデルによる仮想ネットワークを利用したネットワークアプリケーションが広く使われるようになった。

そこで本研究では、こうした要求に応える仮想ネットワークのアーキテクチャを構築する。

2 既存の技術

2.1 Peer-to-Peer モデルの特徴

Peer-to-Peer モデルは、ネットワーク層の IP によるネットワーク上に仮想的なアプリケーションを構築しその上で通信を行う通信モデルである。

Server-Client モデルによってもサーバが匿名と相手の特定を提供することができるが、匿名性をサーバに対する信頼に依存している、サービスとしてサーバが提供している以外の利用方法ができないという 2 点から、本研究では Server-Client モデルを採用しない。

Peer-to-Peer モデルには大きく 2 つの方式が存在する。1 つはノードやデータの発見を索引サーバに依存する Index 集中型であり、もう 1 つは仮想ネットワーク上の複数のノードに検索要求を送出することで検索を行う完全分散型である。

Napster[1][2] をはじめとした Index 集中型では各ノードがあらかじめ索引サーバに所有しているデータの一覧を登録し索引サーバ上で検索を行うが、索引サーバの存在から既に述べた Server-Client 型の欠点を同様に持っている。よって本研究では Index 集中型は採用しない。

2.2 既存のアプリケーション

完全分散型の Peer-to-Peer モデルを利用した特徴的なアプリケーションとして以下の 2 つが挙げられる。

Gnutella[3][4] 仮想ネットワーク上で求めるデータを見つけるまで検索要求を転送するという完全分散型としてごく基本的な構成をしている。データの転送は直接行うため匿名性は提供されない。また、特定の個人に対する通信という概念もない。

freenet[5][6] 匿名の情報保存・検索ネットワークとして設計されたネットワーク基盤で、アップロードされたデータをネットワーク全体のノードに分散して保存してデータの提供者や取得者が分からないように設計されている。この Freenet ではデータの匿名性を保証しているが、本研究ではノードの匿名性が対象であり、データの提供者や取得者を一切特定できない点でコミュニケーション目的には利用し難い。

3 研究の概要と設計

3.1 概要

本研究では、以下に示す 2 つの要件を満たす新しい仮想ネットワークのアーキテクチャを設計・実装する。

1. 匿名性

   ノードの匿名性を確保するため、互いの通信相手も含めて実際に通信を行っているノードを特定できてはいけない。

2. 相手の特定

   通信を行う際にノードを特定する匿名識別子を利用して安全な通信路を確保することができ、そのノード以外が通信を傍受したりなりすましたりできてはいけない。

既存のアプリケーションとの違いを表 1 に示した。

3.2 設計

本研究で提供する仮想ネットワークは、既存の完全分散型の仮想ネットワークモデルに対する拡張として設計する。

表 1: 既存の技術

	サーバ依存	匿名性	相手の特定
Server-Client	×	○	○
Index 集中型	×	×	○
gnutella	○	×	×
Freenet	○	◎	×
本研究	○	○	○

図 1: 処理の概要

仮想ネットワーク上で匿名性と相手の特定を提供する機構のおおまかな動作を図 1 に示した。

検索要求及び検索結果の送信者を途中のノードが書き換え、データを転送する際にそれらのノードを中継することにより匿名性を確保しつつ、各ノードはそれぞれ公開鍵対を保持しその公開鍵をノードを示す匿名識別子として用いることでノードを特定する。

また、検索要求や検索結果メッセージごとに書換を禁止することで、自己を証明することもできる。

動作の詳細は以下のとおりである。

1. A が検索要求メッセージを投げる。

   メッセージには検索要求のほか、A の識別子すなわち公開鍵 K_A が含まれる。

2. C が検索要求を受け取る。C は検索条件に適合しないため、検索要求をそのまま他のノードへと転送する。

   D も同様に検索要求を受け取り転送するが、中継する毎に確率的にメッセージの送信者の IP アドレスを自ノードのアドレスへと書き換えて転送する。

   さらに、書換を行ったノードは書換前の匿名識別子 K_A とその送信元である A の IP

アドレスの対を記憶する。

3. B が検索要求を受け取り、条件に適合した。B は K_A と D のアドレスを保存する。

   次に暗号通信路のセッション鍵 K_S を生成し、K_A で暗号化する。この $K_A[K_S]$ と K_B を検索結果として、K_B に対応するノード D に返す。

4. D が検索結果を受け取る。D は K_A に対応するノード A に検索結果を転送する。この場合も 3 と同様に確率的にメッセージの送信者を書き換え、K_B 及び B のアドレスの対を記憶する。

5. A が検索結果を受け取り、K_A と対となる自分の個人鍵を使って K_S を復号する。K_B 及び D のアドレスの対を記憶する。

   A は K_B と通信を始めるため、K_B に対応するノード D に接続する。ただし、通信内容は K_S によって暗号化する。

6. D はさらに K_B に対応する B に接続し、A から送られた通信内容を B に中継する。

7. B は K_S によって通信内容を複合する。

   同様に、B から A に対しても K_S で暗号化することで安全かつお互いに匿名性を保ったまま通信を行うことができる。

   また通信路が失われた後も、仮想ネットワーク上で相手の匿名識別子 K_B を検索することで通信路を再生することができる。

3.3 想定される問題点と解決策

3.3.1 オーバヘッド

匿名性を維持するために中経者を利用するため、トラフィック的に大きなオーバヘッドが存在する。

本システムではメッセージの書き換えをノードごとに確率的に行っているが、実際の動作状況をもとに確率パラメータを変動させることで十分な匿名性を確保しつつオーバヘッドを最小限に抑える手法が考えられる。

3.3.2 トラフィック解析

複数地点で収集したトラフィックを解析することで通信路を推測する攻撃が存在する。

この攻撃に対しては、ダミートラフィックの生成や意図的な遅延の挿入などが考えられる。

4 評価方針

本研究で提案するアーキテクチャが要件を満たしていることを確認するため、実際に運用を行い以下の点から評価を行う。

4.1 匿名性

- 通信主体が互いの通信相手のノードを特定できない。
- 第三者がトラフィック解析などにより通信主体のノードを特定できない。
- 十分な匿名性を保証するために必要なオーバヘッド

4.2 相手の特定

- 匿名識別子から通信相手と暗号通信路を確保できる。
- 第三者がトラフィック解析などにより通信主体のノードを特定できない。

5 期待される成果

5.1 アプリケーション例

以下に、本研究で構築する仮想ネットワーク上で実現できるアプリケーションの例を挙げる。

5.1.1 グループウェア

インターネット上での匿名の創作行為を支援するため、このシステムを利用してグループウェアのような情報共有ツールを実現することができる。具体的な機能としては掲示板、ファイル転送などがある。

5.1.2 アンケート

様々な主体が社会調査をはじめとしたアンケートを実施しているが、無記名のアンケートをこのシステム上で行うことでアンケートの実施主体を信用せずとも匿名を保ったまま回答することができる。

また、アンケートの実施主体が特定の回答者に後からインタビューを行うこともできる。

5.2 将来への展望

これまでインターネット上で匿名で行動するには何らかのサービスの力を借りる必要があり、それが匿名での行動には限界となっていた。本研究によって実現されるシステムを利用することで、自分の情報を自分で制御することができるようになる。

利用者が増えさまざまなアプリケーションが開発されることで、単なる匿名性の確保という機能をこえてより大規模かつ一般的な通信基盤となる可能性もある。

6 これまでの活動

徳田・村井・楠本・中村・南合同研究会 環境情報学部入学当初より徳田・村井・楠本・中村・南合同研究会に所属し、高度なネットワークインフラの構築及び運用に携わっている。

pie[7],sprng[8] 学部 1 年春学期よりインターネットの普及に関する研究グループに所属し、インターネットインフラが普及する上での問題点や、普及が社会に与える影響について研究を行っている。

neco[9] 学部 3 年春学期よりネットワーク上のコミュニケーションに関する研究グループに所属しネットワーク上で行われるコミュニケーションの新しい形態の研究に携わっている。

P2P モデルの研究 [10][11] P2P モデルを利用したネットワーク測定に関する研究に携わっている。

7 志望理由

本研究では、新しい情報流通ネットワークモデルを提案し、構築する。これを実現するためには、ネットワーク技術のみならず、アプリケーションとしてより多くの人に使ってもらうためのユーザインターフェースに関する議論が必要不可欠である。このように多角的な面から研究を進めるにあたり、これらの分野の研究が盛んに行われている政策・メディア研究科を志望したい。

8 共同研究者・関連団体

本研究では、慶應義塾大学大学院政策・メディア研究科 “モービル広域ネットワーク (MAUI)” プロジェクトにおいて、村井純教授、楠本博之助教授、中村修助教授の指導のもとに行う。

また、以下の団体と協力しながら研究を進める。

- 慶應義塾大学村井研究会内ワーキンググループ neco
- WIDE Project

参考文献

[1] napster messages http://www.clip2.com/gnutellaprotocol04.pdf.

[2] Napster Inc. Napster http://www.napster.com.

[3] Clip2. The gnutella protocol specification v0.4. http://www.clip2.com/gnutellaprotocol04.pdf.

[4] Jnutella.org http://www.jnutella.org/.

[5] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Workshop on Design Issues in Anonymity and Unobservability*, pages 46–66, 2000.

[6] Freenetproject.org http://www.freenetproject.org.

[7] インターネットの普及に関する研究グループ http://www.sfc.wide.ad.jp/kg/pie/.

[8] 通信基盤としてのインターネット整備戦略、およびその上での政策・社会環境の整備に関する研究グループ http://www.sfc.wide.ad.jp/kg/sprng/.

[9] ネットワーク上のコミュニケーションに関する研究グループ http://www.sfc.wide.ad.jp/kg/neco/.

[10] 豊野剛, 仲山昌宏, and 杉浦一徳. P2p model を用いたエンドノード間トラフィック測定. In **分散システム/インターネット運用技術シンポジウム** *2002*, March 2002.

[11] 豊野剛, 仲山昌宏, 石橋啓一郎, and 村井純. Network traffic measurement and database conversion by the user point of view. In **情報処理学会第** *63* **回全国大会講演論文集 分冊** *3*, page 269, September 2001.