研究計画書
仮想ネットワーク上で匿名性と相手の特定を両立するシステムの構築

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 18 日

概要

本研究では、IP ネットワーク上に構築した仮想的なアプリケーション層の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システムを設計・実装する。特に実時間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。
インターネット上で匿名性を保ちながら特定の相手と通信を行いたいという要求が高まっているが既存の技術でその両方を実現しているものは存在しない。それを解決するために新しいシステムを構築する。さらに、そのシステム上で動作するアプリケーションを実装し、運用および評価を行う。

1 背景

非常に多くの人が参加するコミュニケーション手段としてインターネットが利用さ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や住所や電話番号の漏洩によるストーカー被害等からそれらを隠して意見交換や情報公開をしたいという要求は多い。例えば大規模な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。しかし特定のサービスに依存することはサービス運営者による恣意的な削除や改変という危険につながる。また通信量やサーバ運営などのコストから非常に多くの人が参加するシステムとしては規模性を欠く。

特定のサーバ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。

2 目的

本研究では、IP ネットワーク上に構築した仮想的なアプリケーション層の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システムを設計・実装する。特に実時間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。

3 既存の技術とその問題点

以上のような要求に関連する既存の技術として Peer-to-Peer モデルと匿名通信路がある。

3.1 Peer-to-Peer モデル

Peer-to-Peer モデルの特徴 Peer-to-Peer モデルは、ある特別な役割を持つサーバの存在に依存せずそれぞれのノード同士が自律的に協調動作を行うことで何らかのサービスを行うモデルである。このモデルを利用するアプリケーションの例として、IP ネットワーク上に仮想的なアプリケーション層のネットワークを構築しその上で通信を行うファイル交換ソフトウェア等があげられる。ADSL や光ファイバなどの高速なネットワーク基盤が多くの家庭で利用されるようになった結果、Peer-to-Peer モデルによる仮想ネットワークを利用したアプリケーションが広く使われている。

また厳密には Peer-to-Peer モデルではないが Napster[1][2] に代表されるようなノードやデータの発見を索引サーバに依存する Index 集中型とよばれる折衷的なモデルも存在する。

既存のアプリケーション 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 つがあげられる。

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し、実

際のデータの転送は直接接続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。

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。

3.2 匿名通信路

匿名のまま通信を行う匿名通信路を実現する手法として mixnet[7] がある。mixnet では全てのノードが公開鍵対を持ち、情報を送信するノードはあらかじめ中継させるノードの公開鍵でメッセージと次の中継先のアドレスを暗号化する。これを中継ノードの数だけ繰り返し、中継するノードではその暗号化を一段階ずつ復号して次の中継者に送信することで、送信者の匿名性を提供している。

mixnet 自体は暗号化メールを利用することでメールシステムでの匿名性を確保しているが、同様の手法を Peer-to-Peer モデルに適用することができる。

3.3 問題点

以上にあげた技術は背景で述べた要求を部分的に満たすものであるが、匿名性を保ちながら相手を特定できるものは存在しない。

サーバ依存 全ての参加者の通信がサーバを経由するため利用者数が増えた場合に通信量などの点で規模性に欠ける。また、匿名性はサーバやその管理者に対する信頼に大きく依存している。

Index 集中型 サーバに依存するのと同様に通信内容そのものを送信者と受信者で直接交換するため規模性は高いが、その代償として匿名性が無い。

gnutella Index 集中型と同様に匿名性がないほか、ある相手を指定して通信するという概念が無い。

Freenet Freenet ではデータの匿名性を保証しているが、その発信者や取得者を特定することはできないため特定の相手とコミュニケーションをとることができない。

mixnet mixnet では送信者の匿名性は提供されるが受信者の匿名性は提供されていない。また匿名のままメッセージを送信するだけでなく送信者が中継者の公開鍵によって多段に暗号化された返送先ノードを指定することができるが、送信者や中経ノードが静的に存在することを前提にしているためそれらの IP アドレスが動的に変わり得る実際の環境では使いづらい。

4 要件定義

本研究では、こうした問題を解決し、匿名と相手の特定を両立できるシステムを構築する。そのための要件として、以下があげられる。

1. 規模性

   利用者数が増えた場合に特定のサーバの存在がボトルネックとならないように処理を仮想ネットワーク上のノードに分散しなければならない。また特定のサーバに依存することは運営者あるいは運用者に対する圧力により内容が歪められてしまうことを避けられない。

2. 匿名性

   発言者の実世界での属性が明らかになることで差別的な誹謗中傷やさまざまな組織からの圧力、ストーカー被害といった危険に巻き込まれる危険がある。そういったものから発言者を守るためにその匿名性が守られなければならない。

   通信を行う際には相手の IP アドレスを特定して行う。IP アドレスは組織に対して割り当てられているため使用している IP アドレスから所属する大学、企業あるいは利用している ISP が特定できる。また、組織内で IP アドレスをユーザに割り当てる際認証を行っている多くの組織ではネットワーク管理者は個人を特定することが可能である。IP アドレスから所属組織を調べたり個人を特定することが可能であるため、発言者の IP アドレスを誰にも知られてはならないものとする。

3. 相手の特定

   コミュニケーションを取るためには、匿名が守られつつ同時に特定の相手に対して継

表 1: 既存の技術

	規模性	匿名性	相手の特定
サーバ依存	×	○	○
Index 集中型	×	×	○
gnutella	○	×	×
Freenet	○	◎	×
mixnet	○	△	△
本研究	○	○	○

続して通信が行えなければならない。そのため IP アドレスとは別の識別子によって“ある匿名の相手” を識別する必要がある。また、IP アドレスが動的に変わり得る環境においてもこの匿名識別子を用いてネットワーク上に居るであろう相手を見つけだせなければならない。

既存の技術との違いを表 1 に示す。

5 設計

5.1 設計方針

本研究ではノードの識別子としてホスト名や IP アドレスのかわりにノードの公開鍵対を利用することで匿名性と相手の特定を両立させる。

特定のサーバに依存しない 本システム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。この基盤となる仮想ネットワークは、検索要求を仮想ネットワーク上に送出し要求を満たすノードまで転送する gnutella と同様のモデルを想定している。

匿名性 システム上でそれぞれのノードは、匿名識別子となる公開鍵とそのノードの IP アドレスの組であらわされる。各ノードが自分に適応しない検索要求を別のノードに転送する時に送信者の IP アドレスを中継ノード自身の IP アドレスで書き換えることで匿名性を提供する。さらに書き換えたノードは元の送信者の IP アドレスと匿名識別子の組を保存しておく。この情報を利用して相手の特定を行う。

中継者が介在するため、当事者あるいは第三者がデータの経路を追跡することが難しい。ただし、全てのノードで書き換えを行うと効率が悪いため確率的に書き換えを行い、匿名性と効率のバランスをこの確率の調整によっておこなう。

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トラフィック解析と呼ばれる攻撃が存在する。この種の攻撃に対しては意図的な遅延の挿入やダミートラフィックの生成などを検討する。

相手の特定 特定の相手にメッセージを送る際には、上記の逆をたどり、書き換えを行ったノードを順にたどることである匿名識別子を持つノードにまでたどりつくことができる。

検索要求に対し応答として通信路の暗号化に用いる秘密鍵を返送することで、匿名識別子のみで識別されるノード同士で通信が可能となる。

5.2 動作例

仮想ネットワーク上で匿名性と相手の特定を提供する動作例を図 1 に示した。この図で A B C D はそれぞれノードをあらわし、A から送られた検索要求が B、C を経て D に到達し最終的に暗号化通信路が結ばれるまでを示したものである。

図 1: 処理の概要

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復号する。

   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。

6 評価方針

本研究で提案するシステム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。

- 定性的評価
  通信主体に十分な匿名性が提供されているかどうか、匿名識別子から仮想ネットワーク上の相手を発見できるか定性的に評価する。
- 定量的評価
  さまざまな規模の仮想ネットワークを想定し、十分な匿名性を保つために必要なオーバヘッドおよび相手を発見するのに必要なオーバヘッドを各ノードの利用帯域、スループット、RTT 等により定量的に評価する。

7 期待される成果

7.1 想定される応用例

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。例えば以下のようなアプリケーションが考えられる。

- 掲示板
  昨今、匿名掲示板を利用した企業や政府などの組織の告発が行われるようになったが、これはその匿名掲示板の運営者に匿名性を依存している。本システムではシステムとして匿名性を提供しているため、掲示板の運営者やそのサーバのセキュリティ等によらず発言をすることができる。
- 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。
- 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。

7.2 将来への展望

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。

8 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[8],sprng[9] 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[10] 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 [11][12] 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。

9 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する。

10 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://opennap.sourceforge.net/napster.txt.

[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] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms, February 1981.

[8] 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/.

[9] 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/.

[10] 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/.

[11] 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.

[12] 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.