通信経路を論理的に隠蔽する匿名通信方式

The anonymous communication mode from which a communication process is concealed logically

大浴寛之† 吉田富美男‡
Hiroyuki Oeki† Fumio Yoshida‡

†長岡技術科学大学　経営情報システム工学専攻
‡長岡技術科学大学　経営情報系

†Department of Management and Information Systems Engineering, Nagaoka University of Technology.
‡Department of Management and Information Systems Science, Nagaoka University of Technology.

要旨

情報システムが日常生活に浸透するにつれて，情報システムを介したコミュニケーションにおける匿名性の確保も重要な課題の１つとなってきている．しかし従来の匿名通信方式は基本的に通信経路の複雑化によって匿名性を確保しているため，経路上の管理者などが協力すれば送信者と受信者を特定する事が可能である．そこで本研究では，通信経路を論理的に隠蔽することにより，送信者が協力しない限り匿名性が損なわれない方式を提案する．

1. 背景

情報システムの急速な発展につれて，日常生活の多くの場面でも情報システムを利用するようになっているが，その一方でプライバシーの保護も重要な課題となっている．このようなプライバシーの問題では，情報そのものだけでなく情報の通信経路も対象に含まれており，電子投票や社内告発，医療相談などの分野では，通信における匿名性の確保が重要な課題の１つとしてあげられている．

さらにビジネスの分野でも，インターネットを介して様々な情報交換が行われている．特に最近では人間同士だけではなく，様々な業務システムがインターネットを介して連携しており，業務システムの構築においても匿名性の確保は重要な課題であると考えられる．

このような匿名性を確保するための通信方式として，Mix-Net[1]やオニオン・ルーティング[2], Crowds[3]などが知られている．しかし，これらの匿名通信方式は善意の関係者を仮定し，通信経路を複雑にすることにより匿名性を確保しているため，経路上のすべての管理者や中継者が協力することで，送信者と受信者の繋がりを特定する事が可能となってしまうという問題もある．

2. 研究目的

本研究では，善意の管理者または中継者の存在を仮定せずに，通信経路を論理的に隠蔽することにより，送信者が協力しない限り匿名性が損なわれない方式を提案することを目的とする．

3. 提案方式

3.1. 概要

本方式では図1に示すように，送信者Sが送信した情報を，送信者が選んだ他の利用者と管理者が交互に情報を転送して受信者Rに届ける．その際，送信者自身が中継者の１人として参加するとともに，複数の情報転送を一括して行うことにより通信経路を隠蔽する．

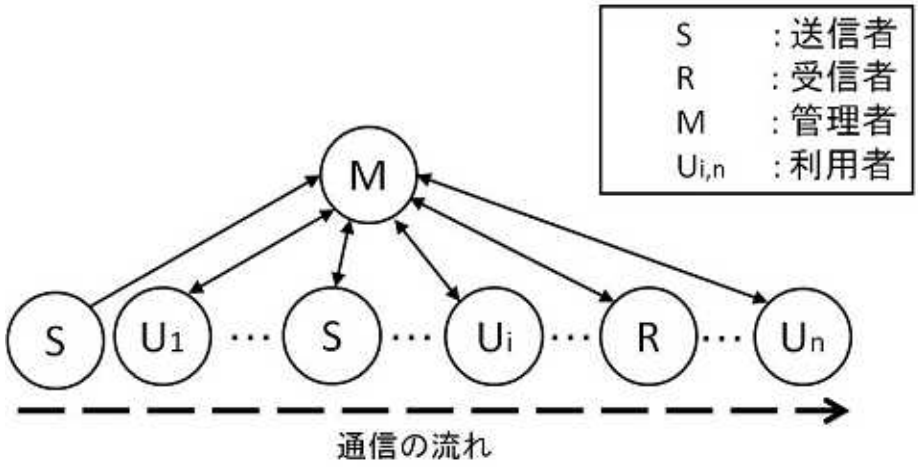

図 1　提案方式の通信例

3.2. 準備

本方式で通信を行いたい利用者は，以下の準備を行う．

（1）自身の公開鍵・秘密鍵を作成する．

（2）管理者に自身の公開鍵を登録し，管理者から ID を取得する．

（3）全利用者の ID と公開鍵を管理者から取得する．

3.3. 通信手順

本方式で通信を行いたい利用者は，以下の手順に従って情報を送信する．

（1）通信経路の決定

送信者は，以下のルールに従って中継者と中継順を決定する．

①中継者には，自分自身と受信者の他に，３人以上の任意数の利用者を加える．

②受信者よりも先に自分自身が中継するようにする．

（2）送信情報の作成

送信者は，決定した中継順の最後から順番に以下の操作を行って送信情報を作成し，管理者の公開鍵で暗号化して管理者に送信する．

①はじめに「送信情報」を空にしておく．

②当該中継者が，受信者ならば送信したい情報を，そうでなければダミーの情報を用意する．

③用意した情報を「送信文」として「送信情報」に付加し，当該中継者の公開鍵で暗号化して，これを新たな「送信文」とする．

④「送信文」に当該中継者のＩＤを付加し，管理者の公開鍵で暗号化して，これを新たな「送信情報」とする．

⑤中継者がそれ以外いなければ終了する．中継者がまだいれば次の中継者に進み②へ戻る．

一方管理者は，常に以下の処理を繰り返し，情報の中継を行う．

（1）管理者は受け取った情報を自分の秘密鍵で復号し，次の中継先 ID を調べる．次の中継先がなければその情報は破棄する．

（2）中継先 ID の利用者宛の「送信情報」があらかじめ定められた一定数になるまで待つ．

（3）一定数の「送信情報」が集まったら一括してその利用者へ送信する．

また利用者は全員，常に以下の処理を繰り返し，情報の中継及び受信を行う．

（1）利用者は受け取った「送信情報」を自分の公開鍵で全て復号する．

（2）自分宛の「送信文」を取り除く，残った「送信情報」を一括して管理者に送信する．

3.4. 匿名性

ここでは提案方式の匿名性について考察する．本論文では「受信者は送信者の特定が困難」「管理者は受信者と送信者の繋がりの特定が困難」という 2 つの要件を満たす通信方式を匿名通信と考える．

はじめに受信者による送信者の特定について考える．受信者が送信者を特定するためには，自分の取得した情報をもとに管理者と協力して，通信経路を遡っていく必要がある．しかし，通信経路の途中には必ず送信者が存在する．匿名通信を行いたい送信者が自分の通信経路情報を教えない限り，受信者はそれ以上の通信経路情報を取得することができない．よって受信者は，送信者を特定することが困難となる．

次に，管理者による受信者と送信者の繋がりの特定を考える．管理者は，情報の送信者を知ることができる．よって，その通信経路のメンバと協力して情報の流れを順に見ていくことにより，受信者を特定することが可能となる．しかし，さきほどと同じく通信経路の途中には必ず送信者が存在する．よって，管理者は受信者までの通信経路情報を取得することができない．

さらに本提案方式では，中継者が一度に複数の通信に関わることによって「通信経路情報を教えない中継者 = その情報の送信者」という関連がつけられないようになっている．

4. 結論

通信経路を論理的に隠蔽する通匿名通信方式を提案した．今後は，今回の研究に基づいて実際にシステムを構築し，既存の方法との比較実験を行う予定である．

参考文献

[1] Chaum, D., “Untraceable electronic mail, return addresses, and digital pseudonyms.” *Comm. ACM*, Vol.24, 1981, pp.84-88.

[2] Goldschlag, D., Reed, M. and Syverson, P. “Onion routing for anonymous and private internet connections.” *Comm. ACM*, Vol.42, 1999, pp.39-41.

[3] Reiter, M.K., and Rubin, A.D. “Crowds : Anonymity for web transactions.” *ACM Trans. Information and System Security*, 1998, pp.66-92.