通信用公開鍵配布機能と並列送信機能を有する匿名通信方式の提案と評価

田中 寛之 †　　石黒 聖久 †　　近藤 正基 †　　齋藤 彰一 †　　松尾 啓志 †

† 名古屋工業大学
466-8555 愛知県名古屋市昭和区御器所町

あらまし インターネットの普及により，膨大な量の情報がインターネットで処理されている．そのため，プライバシーの保護の問題の重要性が増しており，匿名性を守るための研究が不可欠である．我々は通信用公開鍵の配布機能とメッセージの並列送信機能を有した匿名通信方式を提案する．提案方式はDHTを用いたノード管理層と，多重暗号化を用いた匿名通信路層の2層で構成され，ノードの急な離脱への耐性が高い匿名通信路を実現している．また，メッセージの並列送信機能により高速なメッセージ伝達を実現している．本稿では，提案方式の構造，公開鍵の配布機能とメッセージの並列送信機能を説明し，提案方式の性能評価の結果を示す.

Proposal and Evaluation of Public Key Distribution and Multiple Anonymous Routes for Anonymous Communication System

Hiroyuki Tanaka †　　Kiyohisa Ishiguro †　　Masaki Kondo †　　Shoichi Saito †
Hiroshi Matsuo †

†Nagoya Institute of Technology
Gokiso-cho Showa-ku Aichi 466-8555 Japan

Abstract As immense amounts of information continue to be processed on the Internet due to its proliferation, the severity of such problems as the disclosure of personal information is increased; privacy must be protected.Research to protect anonymity has become crucial. We propose the anonymous communication system that satisfies public key distribution, multiple anonymous routes, and countermeasures against sudden breakaway of nodes. Our system consists of a Node Management Layer using DHT and an Anonymous Route Layer using multiplex encryption method. Furthermore, multiple anonymous routes allow message to transmit fast. This paper describes its structure, its procedure with multiple anonymous routes and public key distribution, and its performance evaluations.

1　はじめに

インターネットでの通信は暗号化によって秘密にすることができるが，時間とIPアドレスから個人の特定が可能であり，送受信者が誰かということは隠せない．この問題を解決するために匿名通信方式が必要とされている．

匿名通信は，送信者が特定できないこと，受信者が特定できないこと，送受信者間を追跡できないことの3つの要件を満たす必要がある [1]. 以下，これらをまとめて**匿名性**と言い，これら匿名性を備えた通信を**匿名通信**，匿名通信が使用する通信路を**匿名通信路**と言う.

本稿では，通信用公開鍵の配布機能と並列送信機能を有する匿名通信方式を提案する．提案方式は，これらの匿名性を実現するために多重

暗号化を用い，送受信者の情報 (ID や IP アドレス，経路情報) を隠蔽する．提案方式の特徴として，通信用公開鍵の配布機能を持つため，通信用公開鍵サーバが無い．さらに，並列送信機能によって通信速度の向上を図っている．**スーパーノード(Super Node: SN)** を導入することで，この 2 つの機能を実現した．

本稿では，2 章で関連研究について述べ，3 章で提案方式の詳細と動作について述べる．そして 4 章で実装と評価結果を示し，最後に 5 章でまとめる．

2 関連研究

既存の匿名通信方式には Tor [3]，Crowds [4], Cashmere [5] 等がある．以下，これらの方式について述べる．

Tor は Onion Routing [6],[7] の次世代版として開発され，一般公開されている匿名通信方式である．Tor はネットワーク上に分散して存在する多数のノードで構成される．ノードの状態と公開鍵を管理するディレクトリサーバから，送信者は全ノードの情報を入手し，それらから選択した中継ノードと共有鍵を用いてメッセージを多重暗号化する．各中継ノードは，受信したメッセージを復号し，次ノードの情報を得る．これを受信者までの全中継ノードで繰り返し行う．すべてのノードで復号を行うため暗号復号処理に時間を要し，通信に時間を要する．

Crowds はネットワーク上に分散して存在する多数のノードで構成される．各ノードは初めに Crowds のグループに参加してサーバからメンバリストを受け取る．メッセージは Crowds のメンバを中継されて受信者に到達する．メッセージは確率 p で受信者に送られ，確率 $1-p$ で Crowds メンバに送られる．返信時は直前のノードに対してメッセージを返すことで送信者まで中継する．Crowds は受信者の宛先を暗号化せずに，メッセージに記述するため受信者の匿名性はない．

Cashmere は DHT と多重暗号を組み合わせて用いる方式である．Cashmere ではノード ID の上位 m ビットを用いてノードをグループに分ける．各グループは公開鍵と秘密鍵のペアを共有しており，公開鍵は認証局を用いて配布される．経路情報とペイロードが別々に暗号化されており，経路情報を復号するとペイロードを復号するための共有鍵が得られる仕組みとなっている．メッセージは，各グループの 1 つのノードをによって中継され，すべてのグループへ送られる．グループ内のノードへは，中継ノードからグループ内のすべてのノードにメッセージが転送される．この方式ではグループごとの公開鍵の管理と配布を行うサーバが必要となる．

3 提案方式

提案方式は，我々の研究室で提案した既存方式 [8] を改良した方式で，通信用公開鍵の配布機能とメッセージの並列送信機能を持つ．

3.1 既存方式の概要

既存方式はノード管理層と匿名通信路層で構成される．匿名通信とノード管理を分離することで，システムは匿名性を考慮することなく容易にノード管理を行える．ノード管理層では DHT である Chord を用いて，ノードの参加離脱処理と検索処理と公開鍵の配布処理を行う．匿名通信路層は多重暗号を用いて，匿名通信路の構築，メッセージの生成と暗号化，メッセージの送受信を行う．

図 1 に既存方式の動作を示す．既存方式では，図 1 の破線で囲まれた 1 つの連続した ID 空間 (A_i) を，**受信エリア(Receiver Area: RA)** と呼ぶ．まず，送信者が匿名通信路を構成するノード (中継ノード) を選択する．経路決定後，(1) 送信者は最初の受信エリアの始点ノードを検索し，(2) 送信する．送信者からのメッセージは各受信エリアのすべてのノードを経由後，受信エリア終端ノードによってメッセージが復号される．(3) 次の宛先を検索し，(4) 次の受信エリアへメッセージを送信する．受信者の位置は経路に含まれていれば任意である．

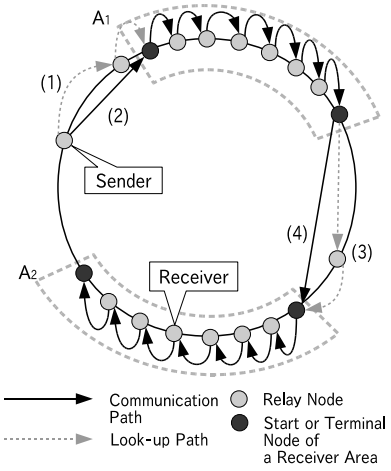

図 1: 既存方式の中継の流れ

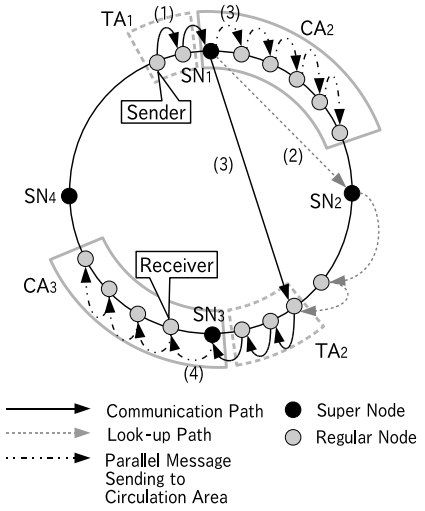

図 2: 提案方式の中継の流れ

3.2 提案方式

提案方式は，既存方式と同様にノード管理層と匿名通信路層で構成される．本節では提案方式の特徴であるスーパーノード，公開鍵の配布機能，並列送信機能について述べる．

3.2.1 スーパーノード

既存方式ではすべてのノードが通信用公開鍵を持つのに対し，提案方式では通信用公開鍵を持つノードを一部のノードに限定している．提案方式の，通信用公開鍵を持つノードをスーパーノードと呼び，通信用公開鍵を持たないノードを通常ノード (Regular Node: RN) と呼ぶ．

スーパーノードは，参加ノードの数に対して一定の割合存在し，ノードがシステムに参加する時に役割が与えられる．また，ノード数が減った場合にはスーパーノードを通常ノードに戻して，数を減らす．

スーパーノードは通信用公開鍵の配布，メッセージの復号，メッセージの並列送信を行う．スーパーノードの数は通常ノードの数に比べて少なく，スーパーノード同士はお互いの状態の把握が比較的容易である．そのため，スーパーノード同士での公開鍵の交換が可能となり，鍵を配布することが出来る．また，スーパーノードは公開鍵と秘密鍵のペアを持ち，メッセージを復号できるため，Successor だけでなく，任意のノードへの送信を並列に行える．

3.2.2 公開鍵の配布機能

経路構築のために送信者が公開鍵を集める処理を無くし，既存方式よりも匿名性を向上させるために公開鍵配布機能を実現する．各スーパーノードは，自ノードから次のスーパーノードまでの連続した ID 空間に含まれるノードへの公開鍵とメッセージの配布を担当する．このエリアを（スーパーノードを含めて）**配布エリア(Circulation Area: CA)** と呼ぶ．公開鍵の配布は以下の 2 つのステップで行われる．(1) 各スーパーノード同士で公開鍵を交換してすべての公開鍵を集める．(2) 各スーパーノードが配布エリアへ公開鍵を配布する．これによりすべてのノードに公開鍵が行き渡る．ここで配る公開鍵は経路情報を暗号化するために用いる．

3.2.3 並列送信機能

提案方式では通信を高速化するためにメッセージの並列送信機能を実現する．受信エリアの終端ではなく，配布エリアの始点であるスーパーノードで復号を行うため，既存方式よりも速くメッセージを次の受信エリアに送ることが出来る．

図 2 に提案方式の動作を示す．提案方式における，通常ノードから次にメッセージを復号するスーパーノードまでの連続した ID 空間を**誘導エリア(TaxiingArea: TA)** と呼ぶ．図 2 では誘導エリアは破線で囲まれた領域 TA_i である．配布エリアは実線で囲まれた領域 CA_i である．提案方式では CA_i と TA_i を合わせた領域を受信エリアと呼ぶ．図 2 の TA_1 は送信者から最初に復号を行うスーパーノードまでの範囲であり，どの受信エリアにも属さない．また，最後の受信エリアは誘導エリアを持たない．

送信者はメッセージ生成後，(1)TA_1 のノードを介して，メッセージを SN1 まで送る．この例では，SN1 はヘッダ部の復号に成功し，次にメッセージを送るべき宛先 ID が得られる．(2) 宛先 ID を担当するノードを Chord を用いて検索し，(3) 得られた宛先 ID のノードと CA_2 への送信を同時に行う．その後，TA_2 を経由して SN_3 受信すると再び復号が行われる．ここで SN_3 は復号したヘッダから次の宛先が無く，終端であることを知り，(4) CA_3 にのみメッセージを送る．

4 実装と評価

本章では提案方式の実装と性能評価の結果について述べる．また，提案方式の匿名性の検証について述べる．

4.1 実装

提案方式の実装はオーバーレイ構築ツールキットである Overlay Weaver [9] を基盤として行った．Overlay Weaver では Chord のオーバーレイネットワーク構築機能，ルーティング機能，メッセージ送受信機能などが提供されている．提案方式は，このメッセージ送受信機能に多重暗号化処理，復号処理，経路制御処理を追加することで実装した．なお，公開鍵暗号には RSA を用い，共有鍵暗号には AES を用いる．

4.2 性能評価

100Mbps のイーサネットにネットワークスイッチを介して接続した 32 台の計算機を用いて，環状のオーバーレイネットワークを構成し，提案方式の評価実験を行った．実験に用いた計算機のスペックは Sempron 2800+/1.6GHz，メモリ 1GB，OS は Linux である．

4.2.1 実験概要

実験の評価パラメータはメッセージサイズ（実験 1），スーパーノードの暗号化の多重度 (実験 2,3) である．実験では 1 つの配布エリアに 8 台のノードを割り当て，TA_1 は送信者が 1 台いる以外は，TA に属するノード 0 台としたため “エリア数 * 8”が中継ノード数となる．また，送信者と受信者がそれぞれ復路と往路の終端に位置するように通信路を設定した．図 3 に往路の通信経路を示す．復路は別経路であるが，同様の構造となっている．

以下に各実験の概要を示す．[実験 1] 往路復路ともに受信エリア数が 2(往復で 4)，16hop の経路 (往復で 32hop) を構築し，送信データサイズを $L_M = 1, 64, 128, 256, 512, 1024, 2048, 4096[KB]$ と変化させた場合の RTT を計測する．[実験 2] 受信エリア数を変化させ，通信路構築に要する時間を計測する．[実験 3] 受信エリア数を変化させ，128KB の送信データに対する処理時間を計測する．

4.2.2 結果

実験 1 の結果を図 4 に示す．図 4 から RTT は，通信データサイズが 1MB の場合で RTT は約 1.4 秒である．既存方式は約 2.6 秒 [8] であり，RTT が約 1.2 秒短くなっている．これは並列送信機能の効果である．

実ネットワークで稼動している Tor では，中継ノード数 4 台，片道 4hop の通信路の生成時間が 7 秒，データ通信時間が約 2 秒である [10]. 提案方式では，片道中継ノード数が 16 台の場合で片道 8hop である．また，既存方式では片道 16hop である．実験では LAN を用い，Tor の性能評価はインターネットで行っているが，中継ノード数を考慮すると，提案方式は十分実用的な性能であると考えられる．また，暗号復号処理が約 3 分の 1 を占めることもわかる．

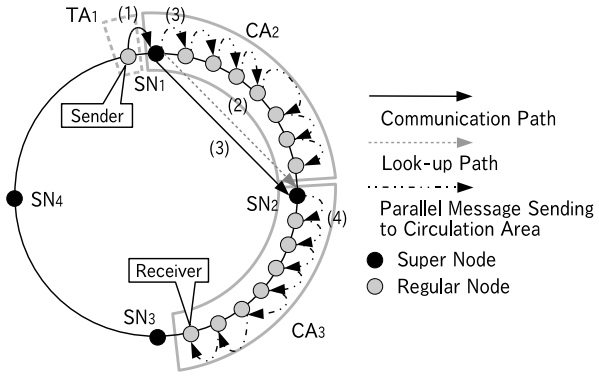

図 3: 実験環境

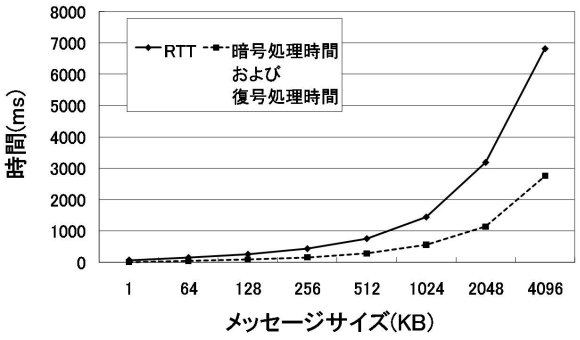

図 4: 実験 1：RTT と暗号復号処理時間 (片道暗号化多重度 2，片道中継ノード数 16)

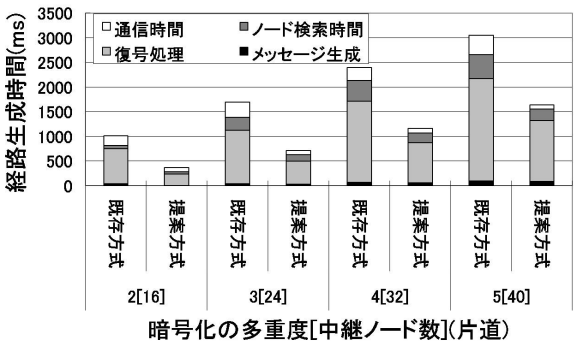

図 5: 実験 2：経路生成時間

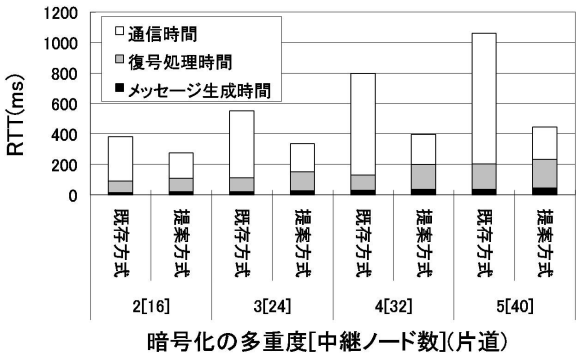

図 6: 実験 3：データ通信時間

次に，経路生成とデータ通信に要する時間の詳細な分析と，メッセージ送信の並列化の効果を分析するために実験 2,3 を示す．実験 2 の結果を図 5，実験 3 の結果を図 6 に示す．

図 5 からは，暗号化の多重度が多いほど復号に要する時間が増え，通信に要する時間が長くなることが分かる．復号処理に要する時間の占める割合が大きいため，復号時間が短い提案方式の方が経路生成時間が短い．提案方式の方が復号時間が短いのは，既存方式ではすべての中継ノードが構築メッセージのヘッダの復号を試みるのに対して，提案方式ではスーパーノードのみ復号するためである．また，既存方式と提案方式には検索時間に差があるのは，ノード管理層での検索の転送回数が異なるためである．

図 6 は匿名通信路構築後のデータ通信時間を表す．データ通信時間が構築に要する時間よりも短い理由は，メッセージの暗号化に共有鍵を用いているためである．通信時間はメッセージが伝搬するのに要した時間である．既存方式は暗号化の多重度が増加すると，通信時間が大きく増加しているのに対し，提案方式はほとんど増加していないことがわかる．既存方式では，SN の暗号化の多重度が 1 つ増えると受信エリア数が 1 つ増え，中継ノード数と hop 数も 8 増加する．しかし，提案方式はメッセージの並列送信機能により，1hop しか増えない．このため，エリア数が増えて中継ノード数が増えても通信時間の増加は既存方式より少なく，増加時間は既存方式の 8 分の 1 程度である．以上から，メッセージ送信の並列化の効果が現れていることが分かる．

4.3 匿名性の検証

複数の攻撃者がシステムに参加し，中継ノードに紛れ込みながら結託して通信解析攻撃を行う場合を考える．このとき，送受信者に関する

情報を得られるかどうかを検証する．通信解析攻撃とはノードの通信を監視し，通信内容を含むメッセージ送受信をすべてログに取り，送受信の関係性を解析することで匿名性をなくす攻撃である．

一つの匿名通信路中の復号を行うすべてのスーパーノードが結託した場合を考える．この場合，すべての受信エリアを知ることが可能である．しかし，送信者の結託を考慮しないとすると，攻撃者は匿名通信路の全体を知ったとしても，送信者より前に受信エリアがあるかどうかが分からないため，それが全体であると確信することは出来ない．

しかし，このままでは送信者の通信を監視されていた場合，前のスーパーノードからの受信が無いメッセージの送信があった場合に送信者だと分かる．そのため，各中継ノード間で単純で高速な暗号化をメッセージに施すことでこれを防ぐ．また，誘導エリアが存在することで，攻撃者は送信者と誘導エリアの始点ノードを区別することが出来ない．さらに，受信者については各中継ノードとの区別をすることが出来ない．よって匿名性が保たれる．

また，提案方式には通信用公開鍵を管理するサーバが存在しないため，鍵サーバとの通信を監視される恐れが無く，既存方式よりも匿名性が向上している．

5　まとめ

本稿では，通信経路を秘匿するための公開鍵の配布機能を有する匿名通信方式を提案した．提案方式では多重暗号化と Chord を組み合わせて用いていることで離脱耐性の高い匿名通信路を実現している．スーパーノードを導入することで，公開鍵の配布機能とメッセージの並列送信を実現した．また，提案方式をオーバーレイ構築ツールキットである Overlay Weaver を基盤に提案方式の実装を行い，評価を行った．その結果，メッセージの並列送信機能により RTT が 1.2 秒短縮されていることを確認した．インターネット環境での評価と，受信者との共有鍵の共有方法が今後の課題である．

謝辞

本研究の一部は，財団法人堀情報科学振興財団の研究助成，および文部科学省科学技術研究補助金基盤研究 C(課題番号:20500064) によるものである．

参考文献

[1] Pfitzmann, A. and Waidner, M.: Networks without user observability, Eurocrypt'85, LNCS 219, pp. 245–253 (1986).

[2] Stoica, I., Morris, R., Karger, D., Kaashoek, F. and Balakrishnan, H.: Chord : A Scalable Peer–To–Peer Lookup Service for Internet Applications, Proc. 2001 ACM SIGCOMM Conference, pp. 149–160 (2001).

[3] Dingledine, R. and Mathewson, N.: Tor: The Second-Generation Onion Router, Proceedings of 13th USENIX Security Symposium, pp. 303-320 (2004).

[4] Reiter, M. K. and Rubin, A. D. : Crowds: Anonymity for web transactions, ACM Trans. Information and System Security, pp. 66–92 (1998).

[5] L. Zhuang., F. Zhou., B. Y. Zhao. and A. Rowstron. Cashmere: Resilient anonymous routing, Proc. NSDI (2005).

[6] Goldschang, D., Reed, M. and Syverson, P.: Onion routing for anonymous and private internet connections, Comm. ACM, Vol.42, No.2, pp. 39–41 (1999).

[7] Reed, M.G., Syverson, P.F. and Goldschlag, D.M: Anonymous connections and Onion routing, IEEE Journal on Specific Areas in Communications, Vol.16, No.4, pp. 482–494 (1998).

[8] 近藤 正基, 田中 寛之, 齋藤 彰一, 松尾 啓志 : 分散ハッシュテーブルによるノード管理を行う匿名通信方式の設計と実装, 情報処理学会研究報告書, 2009–OS–111 No.22 (2009).

[9] 首藤一幸, 田中良夫, 関口智嗣. オーバーレイ構築ツールキット Overlay Weaver. 情報処理学会論文誌, コンピューティングシステム, Vol. 47, No. ACS15 (2006).

[10] Andriy, P., Lexi, P. and Johannes, R.: Performance Analysis of Anonymous Communication Channels Provided by Tor, Third International Conference on Availability, Reliability and Security , pp. 221–228 (2008).