社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（28）
2008 / 7 / 25

DHTを用いた双方向匿名通信路の提案

近藤 正基† 齋藤 彰一† 松尾 啓志†

† 名古屋工業大学院情報工学専攻 〒466-8555 愛知県名古屋市昭和区御器所町
E-mail: m_kondo@matlab.nitech.ac.jp, {shoichi,matsuo}@nitech.ac.jp

あらまし 近年インターネットの普及により莫大な情報量がネットワークを介して処理されている．このため，個人情報の流出などの問題が深刻となり，プライバシの確保の必要性が高まっている．そこで，ユーザの匿名性の保護が重要となっており，いくつかの匿名通信方式が研究されてきた．しかし，動的なネットワーク上で何らかの双方向通信を行う際，送信時の経路を返信時に利用できない状況が考慮されるべきであるが，従来の匿名通信方式では十分に考慮されていない．本論文では従来の匿名通信方式である多重暗号化に，分散ハッシュテーブルのChordを用いた経路制御を組み合わせることで，新たに可用性を有した通信方式を提案する．

キーワード 匿名通信路，分散ハッシュテーブル，Chord

Proposal of Anonymos Routing Technique with DHT

Masaki KONDO†, Shoich SAITO†, and Hiroshi MATSUO†

† Graduate School of Engineering, Nagoya Institute of Technology
Showa-ku, Nagoya-shi,Aichi 466-8555 Japan
E-mail: m_kondo@matlab.nitech.ac.jp, {shoichi,matsuo}@nitech.ac.jp

Abstract The immense amount of information is processed on the network by the spread of the Internet. Therefore problems such as leaking out personal information became serious, and then necessity of privacy protection is increasing. The researches protecting anonymity have become important and have been studied. Anonymous communication systems should think over a situation of unable to use the same routes in the round trip. However the existing systems exclude it. This paper proposes the new high-availability anonymous communication method combining the existing multiplex encryption method and Chord, Distributed Hash Table.

Key words Anonymos Routing,DHT,Chord

1. はじめに

近年，高度情報化社会の高まりによって，商業，行政，医療，家庭など，あらゆる分野においてコンピュータとインターネットの利用が一般化している．このため，医療相談や社内告発といった行為をインターネットを介して行うことが考えられる．このような行為は，「だれ」が「どこ」へ通信を行ったかが分からないような，強固な匿名性が必要である．

一般に通信における匿名性については次の3種が挙げられる[1]．

- 送信者匿名性
- 受信者匿名性
- 送信者と受信者のつながりの匿名性

これらの匿名性を確保するさまざまな匿名通信手法が研究されている．中でも代表されるのはMix-net[2]や，Crowds[3]，オニオンルーティング[4][5]である．これらのシステムは，電子投票や社内告発などのユーザの匿名性や，位置情報，プライバシを保護するために，匿名性を備えた通信を必要とするアプリケーションの基盤として用いられている．この3種の匿名性の中で，ユーザが最も重視するものは送信者の匿名性とされ，どの従来研究も送信者の匿名性は実現している．しかし，先に挙げたとおり医療相談や社内告発といったものを行う際は3種の匿名性すべてを実現する必要がある．

匿名通信手法には，いくつかのノードを中継して匿名性を実現する手法と，ブロードキャストやマルチキャストを使って匿名性を実現する手法がある．いくつかノードを中継して匿名性を実現する手法とは，送信者と受信者の間にいくつかのノードを経由させることによって，匿名性を実現する手法である．ここで，匿名通信を行う際，医療相談に代表されるような匿名性を確保しつつ双方向に通信が必要なケースを考える．双方向通信では，中継ノードの故障や消滅などにより送信時の経路が返信時には辿ることができない場合を考える必要がある．しかし，

送信者と受信者のつながり，特に送信者の秘匿に重きをおく匿名通信においてはこの問題の解決は簡単ではない．この問題について，これまで提案されてきた方式では十分に考慮されているとは言いがたい．先に挙げた Mix-net，オニオンルーティング，Crowds のいずれも，送信時の経路上にある中継ノードが 1 つでもその位置を離れたとき，返信データが送信者に届かない．また，2 章で述べるが Crowds とオニオンルーティングは比較的小規模なネットワークを想定した設計である．

ブロードキャストやマルチキャストを利用して匿名性を得る手法が提案されている [6]．この手法はグループ全員，もしくは数ノードに対して直接通信を行う．このため，先に挙げた中継ノードを用いる手法に比べ，通信遅延を生じず，送信時と返信時の経路も保証されている．しかし，定期的にすべてのノードがブロードキャストもしくはマルチキャストを行うため，通信の帯域幅を大きく消費し，小規模なネットワークでしか用いることができない．

我々は，分散型の P2P システムを用いて，多重暗号化と分散ハッシュテーブルである Chord [8] のアルゴリズムを組み合わせることにより，柔軟な経路選択を行う匿名通信路の提案をする．

本論文の構成は次のとおりである．2 章では匿名通信路の既存手法の問題点を述べる．3 章で我々が提案する多重暗号化と Chord の組み合わせた手法の説明を行い，4 章で検討を行う．また，提案手法が一定の匿名性を確保したまま可用性，スケーラビリティを向上させうることを示す．そして最後に 5 章でまとめる．

2. 匿名通信の従来研究

本章では従来研究として，多重暗号化を用いて送受信者ともに秘匿するオニオンルーティングと，多重暗号化を用いない方法の Crowds の 2 つの手法について説明する．以下，匿名通信の始点となるノードを送信者，終点となるノードを受信者という．

2.1 オニオンルーティング

オニオンルーティングは，ネットワーク上に複数配置された中継ノードで構成される．送信者は各中継ノードとの共通鍵を用いて，メッセージの多重暗号化を行う．各中継ノードは，受信した暗号文に対して復号処理を行う．これを，受信者まで繰り返し行う．以上により，通信経路の特定を困難にする．すなわち，オニオンルーティングは送受信端末間の全通信経路を暗号技術により秘匿する技術である．通信路全体を傍受することができないという仮定で，任意の攻撃者によるメッセージ送信者の特定を困難にしている．

オニオンルーティングは経路生成，メッセージの送受信，経路破棄の 3 つのフェーズを持つ．経路生成フェーズでは送信者が受信者に至る各中継ノードと共有する鍵を送信時と返信時用に 1 組ずつ生成し，各中継ノードと共有する．これによって送受信の経路を確立する．送受信フェーズでは共通鍵を用いてメッセージを多重暗号化する．図 1 のように，送信者 NS から受信者 NR までの間に中継ノード N_i(i=1, 2, 3) を有し，それぞれ

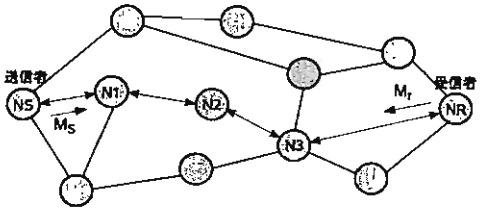


図 1 オニオンルーティングの動作

との共通鍵を K_i(i=1, 2, 3)，通信内容を V すると，多重暗号化メッセージ Ms は以下に示す再帰的計算で得られる．また，A||B は A と B を結合したものを表し，IP_n はノード n の IP アドレスを示す．

$$Ms = IP_1||K_1(IP_2||K_2(IP_3||K_3(IP_{NR}||K_{NR}(V))))$$

上記により得られたメッセージを経路上の各ノードが共通鍵を用いて復号しながら受信者まで届ける．受信者の NR は，メッセージを共通鍵を用いて復号することでデータ V を得る．返信時も同様に多重暗号化したメッセージを復号しながら送信者 Ns まで届ける．最後に，経路破棄フェーズは，経路上のノードが抜ける際に，そのノードは前後のノードに経路破棄用のコマンドを送信し，前後のノードが経路情報から対応する情報を削除する．

2.2 Crowds

Crowds はいくつかの協調しあうノードのグループで構成される分散システムである．ユーザが匿名性を確保するためには Crowds のグループに加入しメンバリストを受け取る．それぞれのノードは中継ノードとしての役割も果たす．何かしらのデータを匿名性を確保して送る場合，受信者を記述したデータを宛先として Crowds のメンバに送る．動作の概要を図 2 に示す．送信者 NS はメッセージを p の確率で受信者 NR へ，(1 − p) の確率で他の Crows のメンバに送る．リクエストを受けとったメンバは，NS 同様に確率 p で受信者へ，確率 (1 − p) で他のメンバにメッセージを送信する．この処理を繰り返すことにより，最初にリクエストを発信したノードを容易に特定できなくする．また，返信の際には直前のノードに対して各ノードが返信メッセージを返すことで通信が可能となる．

2.3 問 題 点

オニオンルーティングに代表されるメッセージを多重暗号化を利用する方式は，メッセージを中継するノードが一つでも信頼できるものであれば匿名性が破られることはない．しかし，受信者までの経路を送信者が固定的に決めるため，中継ノードが故障などで一つでも通信できなくなった場合には，メッセージを届けることができない．例えば，送信時にいずれかの中継ノードが通信できない場合には，再度経路生成フェーズからやり直せばよい．しかし，返信時の各中継ノードは，送信時にメッセージを送ってきた直前のノードしか知ることができず，送信者が分からない．返信時にいずれかの中継ノードの通信が途絶えることは，ネットワークの変化やアプリケーション等の処理

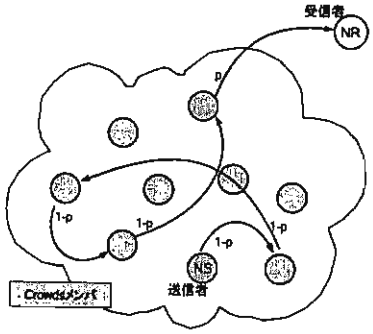


図 2 Crowds の動作

に要する時間によっては，送信時よりも発生しやすい．このように多重暗号化による高い匿名性ゆえに経路選択の柔軟性が極めて低いと言える．また，オニオンルーティングは経路生成の際に一時利用の公開鍵を用いて探索要求をブロードキャストすることで，受信者への経路と各中継ノードとの共通鍵を得る．しかし，ブロードキャストは大規模なネットワークにおいては実用的でないため，スケーラビリティが高いとは言えない．

Crowds の場合，送信時における経路選択の柔軟性は高い．しかし，確率的な経路選択においてメッセージの到達性を保証するために，中継ノードに受信者を隠すことができない．よって匿名性は多重暗号化を使う方式と比べて低いと言える．また，返信時にはそれぞれのノードはメッセージが送られてきた直前のノードしか知ることがないため，当該中継ノードが返信前に離脱すると返信することができなくなる．さらに，Crowds のメンバシップは Crowds 専用のサーバによって集中管理される．このため，ノード数の増加に対してスケーラブルに動作することが難しく，スケーラビリティが低いと言える．

3. 提案手法

匿名性 1 章で挙げたは 3 種の観点から計ることができる．これら 3 種の匿名性はそれぞれ独立したものではない．送信者と受信者のつながりの匿名性は，送信者か受信者のどちらかの匿名性を満たすならば，満たされるという関係にある．この観点から Crowds などを代表とする匿名通信手法は，送信者の匿名性を満たすことで送信者の匿名性と送信者と受信者のつながりの匿名性を確保している．しかし，自分が属するネットワークの管理者が送信者を特定できる場合，匿名性は大幅に低下する．

これら 3 種の匿名性のうち，ユーザにとって最も満たされるべきと考えられるものは送信者の匿名性である．しかし，医療通信など受信者も知られたくない通信の場合はこれの限りではない．つまり，強固な匿名性が必要な通信を行う場合，送信者と受信者共に匿名性が満すことが必要である．オニオンルーティングは，多重暗号化を用いることで高い匿名性を実現している．しかし，IP アドレスによる固定的な経路設定により可用性が低い．また 2.1 に示したとおりスケーラビリティも低い．そこで本稿では分散ハッシュテーブルである Chord に多重暗号化を組み合わせる手法を提案する．提案手法は,IP アドレスに変

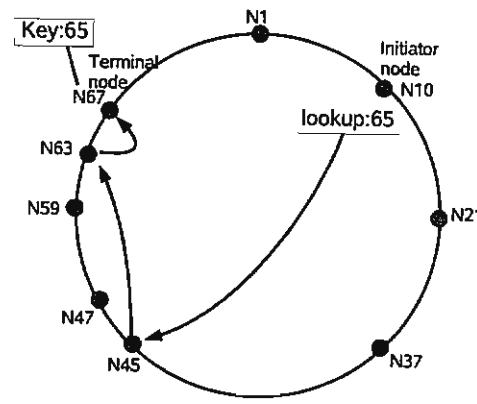


図 3 Chord よる探索

えて，Chord で用いられる ID 空間で各ノードを管理することにより，送受信者の匿名性を損なうことなく可用性とスケーラビリティを向上させる手法である．

3.1 本手法の特徴

送受信者が共に匿名システム内に存在した双方向匿名通信路手法として，以下のような特徴をもつ匿名通信方式を目標とする．

(1) 匿名性
送信者と受信者ともに秘匿し，通信のつながりの匿名性を確保する．

(2) 可用性
従来手法より，柔軟な経路選択を可能にする．

(3) スケーラビリティ
従来手法よりも大規模なネットワークで利用できる．

3.2 Chord

本手法で用いる分散ハッシュテーブルは Chord [8] である．Chord は，環状の ID 空間を用いることから，ID の始点と終点がないという特徴がある．環状空間は，[9]，文献 [10] でも使用されており，匿名通信路において始点と終点を秘匿するのに適している．Chord は，システムに参加する各ノードに ID を割りふり環状な ID 空間を形成する．そして，コンテンツをハッシュ関数用いて一意な ID との組に変換し、各ノードはそれぞれが受け持つ範囲の ID を一意に決め対応するデータ項目を管理する手法である．また各ノードがそれぞれ小さな経路表 (fingertable) を保持している．キーの配置されたノードを発見するために各ノードが経路表に基づいて繰り返し問い合わせを行う必要がある．

図 3 に Chord の動作を示す．あるノード (N10) があるキー (Key:65) を探索する場合，N10 は自分が保持している fingertable の中から key:65 に一番近いノード (N45) に対して問い合わせを送る．N45 が key:65 を管理していない場合，同様に自分が保持している fingertable の中から key:65 に一番近いノード (N45) に対して問い合わせを送る．このようにして検索キーを管理するノードにリクエストを送り，コンテンツを得る

手法である．また，N ノードの中から目的のノードの発見する問い合わせの回数は，最悪でも O(logN) 回となる．

以後，最初にリクエストを開始するノードを開始ノード (initiator)，あるノード X に対して大きい ID を持つノードの中で最も X に近いノードを X の Successor，X に対して小さい ID を持つノードの中でもっとも X に近いノードを X の Predecessor と呼ぶ．また P2P における分散ネットワークでは，ノードが離脱する場合には，持っているコンテンツごと離脱するため，以後そのコンテンツを参照できなくなる問題がある．Chord ではその問題に対して，あらかじめコンテンツのレプリカを Successor に渡しておくことで解決をしている．

3.3 Chord とオニオンルーティングを用いた単純な匿名通信路

オニオンルーティングに Chord の経路選択を用いた場合を考える．まず，オニオンルーティングの各ノードに ID を割り当て，Chord の ID 空間に配置する．そして，中継を行うノードを ID で指定し，多重暗号化を用いてメッセージを送信する手法が考えられる．この手法の場合，各ノードを ID で管理することで可用性とスケーラビリティが高くなると考えられる．しかし，受信者が中継ノードに含まれていることは明らかであり，かつ中継ノード数はメッセージサイズが上限となる．さらに，Chord の経路制御のために経由する中継ノードに，現在の宛先を知られる．これらのために，匿名性がオニオンルーティングより低下する．

次にすべてのメッセージを Successor に送るという手法が考えられる．この場合，全ノードにメッセージを送ることになるため，送信者または受信者の可能性はシステムに参加している全ノードとなり，高い匿名性を持つ．しかし，スケーラビリティが低いのは明らかである．

そこで，Chord の ID 空間を利用しつつ，**受信エリア**と呼ぶ Successor にメッセージを送る区間を設けることで，可用性とスケーラビリティを確保したまま，高い匿名性を確保する手法を提案する．なお，メッセージの多重暗号に用いる公開鍵は，各ノードの公開鍵を公開鍵サーバに登録し，送信者は公開鍵サーバに問い合わせることとする．

3.4 構成要素

Chord に加えた提案方式の構成要素について述べる．

送信者 Ns: 匿名通信の始点ノード
受信者 Nr: 匿名通信の終点ノード
受信エリア $A_i(i = 0,\ 1,\ 2,\ ...,\ n)$: Chord の ID 空間上で Ns が任意に指定した n 個の ID 部分空間．$A_i(i = 1 \sim n)$ のどれかに Nr が含まれる必要がある．
受信エリアの最小 ID $ID_{min}(A_i)$: 受信エリア A_i の始点 ID
受信エリアの最大 ID $ID_{max}(A_i)$: 受信エリア A_i の終点 ID
受信エリアの始点ノード A_is: $ID_{min}(A_i)$ を管理するノード
受信エリアの終点ノード A_it: $ID_{max}(A_i)$ を管理するノード
受信エリア内ノード $A_iN_k(k = 0,\ 1,\ ...,\ m_j)$: 受信エリアに存在するノード．$A_iN_1$ の Successor が A_iN_2 となる
公開鍵サーバ PDS: Chord に存在するノードの公開鍵 $(P_{node},\ K_{node})$ のデータベースを管理する機関
ヘッダ用公開鍵暗号化データ $P_{node}(Y)$: データ Y をノード $node$ のヘッダ用公開鍵 P_{node} で暗号化したデータ
データ用公開鍵暗号化データ $K_{node}(Y)$: データ Y をノード $node$ のデータ用公開鍵 K_{node} で暗号化したデータ
送信メッセージ Ms: Ns が Nr へ送る送信時のメッセージ
返信メッセージ Mr: Nr が Ns へ送る返信時のメッセージ
メッセージヘッダ H_s: 送信メッセージのヘッダ部
メッセージヘッダ H_r: 返信メッセージのヘッダ部
通信内容 V: メッセージに含まれる通信内容部
中継ノード $R_{i,j}(j = 0,\ 1,\ 2,\ ...,\ l)$: メッセージを受信エリア A_i へ Chord アルゴリズムに従い中継するノード

また，文字列 A と B の結合を A‖B で表す．

3.5 提案方式

本提案手法は，多重暗号化したヘッダ部とデータ用公開鍵で暗号化したデータ部からなるメッセージを，Chord を基盤とした経路制御方式で配送する．本節では，提案手法のメッセージ生成と送信と返信の各フェーズについて述べる．最後に全体の動作の概要を示す．

3.5.1 メッセージ生成フェーズ

本手法のメッセージは，ヘッダ部とボディ部に分かれる．ヘッダ部は，受信エリア群の始点ノード ID を多重暗号化して作成する．ボディ部は，さらに返信用ヘッダ部と通信内容に分かれる．以下，メッセージのヘッダ部とボディ部に分けて生成方法を述べる．

(ヘッダ部)

(1) 送信者は受信エリア $A_i(i \geq 1)$ を決める．受信エリアは最小 ID と最大 ID を指定して定める (Nr がいずれかの受信エリアに含まれている必要がある)．

(2) 選択した受信エリアを任意の順に並び替える．このとき，送信者 Ns から通信順に $i = 1, 2, 3$ とする．またヘッダ部の多重暗号化のために A_it の公開鍵 P_{Ait} を得る．

(3) 各エリアの最小 ID を次に示す再帰的計算により多重暗号化する．

$$H_i = P_{i+1}(ID_{min}(A_{i+2}) \parallel H_{i+1})$$

以上によりヘッダ部 Hs $(= H_0)$ が求まる．

(ボディ部) ボディ部は，さらに返信用ヘッダ部 H_r と通信内容 V に分けられる．

(1) ヘッダ部の生成 (1)〜(3) と同様の処理を返信用に行い，H_r を作成する．これは返信時の経路を送信者が指定するためである．

(2) Nr との一時的な共通鍵 C_{Ns} を生成する．これは返信時のボディ部の暗号化を送信者が指定するためである．

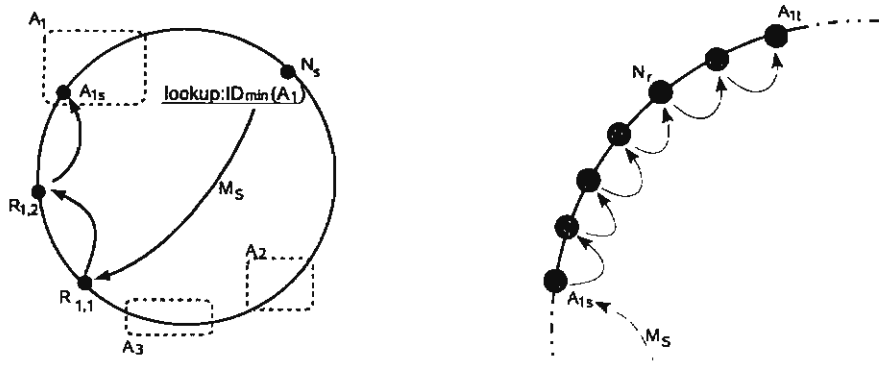
(3) ボディ部 (B_s) を次に示すとおり暗号化を行う．

$$B_s = K_{Nr}(H_r||C_{Ns}||V)$$

(4) ヘッダ部 H_s と結合する．これを送信メッセージ M_s とする．

3.5.2 送信フェーズ

提案手法の経路制御は主に受信エリア外と受信エリア内に分けられる．メッセージ送信フェーズの動作を以下に示す．



(a)受信エリア外　　(b)受信エリア内

図 4　提案方式の経路制御

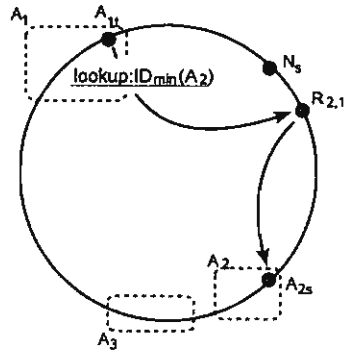


図 5　受信エリア間の経路制御

(受信エリア外)

(1)　送信者 Ns は生成した Ms のヘッダ部に従って，$ID_{min}(A_1)$ へ Chord のアルゴリズムに従い，メッセージを送信する．

(2)　M_s を受け取った中継ノード $R_{i,j}$ は，ヘッダ部に従って，以下のいずれかの処理を行う．

- 自身が $ID_{min}(A_i)$ を管理するノードでなければ，Chord のアルゴリズムに従いメッセージを $R_{i,j}(j=j+1)$ に送信する．
- 自身が $ID_{min}(A_i)$ を管理するノードであれば，ヘッダ部の復号を試みる．復号できなければ受信エリアであることを示すフラグ (以下，受信フラグ) を立て，Successor にメッセージを送信し，受信エリア内処理 (2) を実行する．このときヘッダ部から $ID_{min}(A_i)$ を指した情報を削除する．

(受信エリア内)

(1)　受信エリアフラグが立った状態で Predeseccor からメッセージを受けとった場合は，中継ノードは以下のいずれかの処理を行う．

- ヘッダ部の復号を試み，復号できなければ Successor へメッセージを送信する．
- ヘッダ部の復号を試み，復号できれば次の宛先 $(ID_{min}(A_{i+1}))$ を得る．ここで，このノードは初めて自分が A_it であることを知る．A_it は新たに initiator となって $R_{i+1,1}$ に M_s を送る (受信エリア外処理 (2) へ戻る)．
- ヘッダ部の復号を試み，復号できたとき，次の宛先 ID が無ければメッセージの送信を終了する．

(2)　(1) の動作を行った後，データ用秘密鍵を用いてメッセージのデータ部の復号を試みる．このとき復号が可能ならば，メッセージ受信となる．

3.5.3　返信フェーズ

提案手法の返信フェーズの動作を以下に示す．

(1)　送信時のデータ部に含まれていた返信用ヘッダ H_r を返信メッセージのヘッダ部とする．Mr は返信通信内容 V と H_r を結合することで構成する．

(2)　送信フェーズと同様に通信を行う．

3.5.4　動作の概要

図 4 と 5 に受信エリア数 3 の動作を示す．まず，送信者 Ns は最初の受信エリアの始点ノード A_1s にメッセージ Ms を Chord のアルゴリズムに基づいて送信する (図 4(a) 参照)．A_1s からは Successor にメッセージを送信する (図 4(b) 参照)．受信エリア内のノードは，自身の通信用秘密鍵を用いてヘッダ部の復号を試みる．そして，復号できなければ Successor に送信する．もし復号できた場合は，次のエリアの始点ノードの $ID_{min}(A_2)$ を知ることができるので，initiator となって Chord のアルゴリズムに従いメッセージを送信する (図 5 参照)．これを繰り返し行うことで，ヘッダ内に受信エリアがなくなるまでメッセージを送信する．

また，受信エリア内のノード (A_iN_k) はメッセージ中継後に，データ部をデータ用秘密鍵を用いて復号を試みる．復号できた場合，当該ノードが受信ノード N_r であることが判明する．返信は，送信メッセージのデータ部に含まれていた返信用ヘッダを用いて同様に送信する．

データ部とヘッダ部を独立に暗号化することと，返信時のヘッダを送信者が用意すること，さらに受信後もすべての受信エリアについて送信が続くことで，送受信者の匿名性と送受信者の

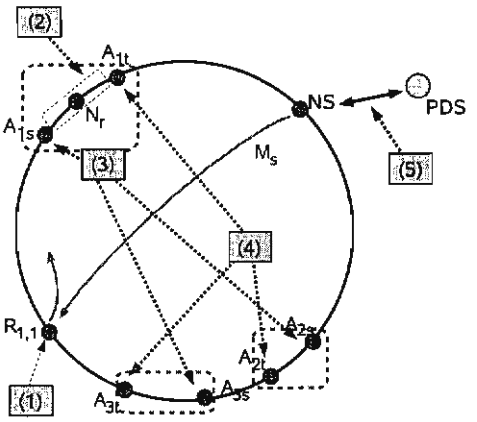


図 6　攻撃者の位置

つながりの匿名性を確保する.

中継ノード故障などの場合, 受信エリア外では Chord のアルゴリズムに従い各々が自立的に次の中継ノードを選ぶ. また, Chord のアルゴリズムは Successor と常に接続していることから, 受信エリア内では Successor に正しくメッセージを送信できる. しかし, 受信エリアの終点ノード (A_it) が故障などにより利用できない場合が考えられる. この場合は, ヘッダ部を復号すべきノードがなくなるため, 次の受信エリアにメッセージを送信ができなくなる. このため, Chord のアルゴリズムに習い, Successor にヘッダ用秘密鍵のレプリカを渡しておく. これより A_it の離脱に対処する.

4. 検討と比較

本章では提案手法の特徴を挙げた後, 匿名性, 可用性, スケーラビリティと結託攻撃の検討を行う. また, 既存の匿名通信路手法である Crowds とオニオンルーティングとの比較を行う.

4.1 本手法の考察

本手法を送信者匿名性, 受信者匿名性, 送信者と受信者のつながりの匿名性の各観点から評価を行う. なお, 文献 [10] を参考に, 攻撃者を中継ノードと, 通信を盗聴した第三者ノードを仮定し, 以下の (1)〜(5) に分類する (図 6 参照).

(1)　Chord のルーティングを行う際の中継ノード (受信エリア外)

(2)　受信エリア内 (A_i) かつ A_it, A_is でないノード

(3)　受信エリアの始点ノード (A_is)

(4)　受信エリアの終点ノード (A_it)

(5)　送信者とヘッダ部とデータ部公開鍵サーバとの通信

しかし, (5) に関する通信は暗号化されていること, さらに PDS は十分に信頼できると仮定する. よって, ここでは対象外とする.

4.1.1 送信者の匿名性

送信者の匿名性を考える. まず (1) のノードが得られる情報を考える. (1) のノードが得られる情報は, メッセージを送信してきたノードと現在目指しているノード (A_is) の 2 つのみである. このノードが送信者を知るということは, 言い換えると, 送信してきたノードが Ns であるかを判断できるかと言うことである. 全 ID 空間を $2^k(0 \leq k)$ をすると, Chord の fingertable に登録されるノードは当該ノードから ID で 2^0 から 2^{k-1} だけ離れた各ノードである. つまり, 2^{k-1} 以上離れたノードにメッセージを送る場合は, 必ず 2^{k-1} 離れたノードにメッセージを送る. この 2^{k-1} 離れたノードへの通信は, initiator 以外では発生しない. このため, 通常の Chord では 2^{k-1} 離れた通信を受信したノードは, 当該通信相手が Ns であると推測できる [9].

しかし, 本手法の場合, 受信エリアによって Chord のルーティングを繰り返し行うため, たとえ (1) が受信エリア数 (i) を知っていると仮定しても, 直前のノードが Ns である最大確率は $1/i$ でしかない. さらに, 受信エリア数が含まれるヘッダ部は多重暗号化されているため, 受信エリア数を特定すること自体が困難である. よって (1) のノードが Ns を特定する確率は 1/(全ノード数−自ノード数), つまり 1/(全ノード数− 1) である.

次に (2), (3), (4) のノードも (1) のノードと同様に, 得られる情報はメッセージを送信してきた直前のノードに関する情報のみである. (1) のノードと同様に, 送信してきたノードが Ns と推定するのは, メッセージのヘッダ部の多重暗号化により困難であり Ns を特定する確率は 1/(全ノード数− 1) である.

4.1.2 受信者の匿名性

受信者の匿名性を考える. まず (1) のノード通信から受信者に関して知ることのできる情報は, 現在目指している受信エリアの始点ノード (A_is) のみである. このとき, 全受信エリア内にあるノードの総数を AN_{max} とすると, A_is が Nr である可能性は, $1/AN_{max}$ である. しかし, 他の受信エリアは多重暗号化により秘匿されており, 知ることが困難な上, それぞれの受信エリアの範囲はユーザが決めることができるため, 理論上 AN_{max} は全ノード−自ノード数 と考えることができる. 自ノード数は 1 であるから, A_is が Nr である確率は 1/(全ノード数− 1) となる.

次に (2) のノードについて述べる. (2) が得られる受信者の情報は, 自分の Predesessor と Successor は受信エリアに含まれており, それらのノードが N_r の可能性があるということである. (2) が知った受信者の可能性をもつノード数は 2 であるため, Nr である確率は, $2/AN_{max}$ である. しかし, これも (1) の場合と同様, 理論上 AN_{max}は全ノード− 1 と考えることができる. つまり (2) のノードが知ることができた中継ノードが N_r である可能性は高々2/(全ノード数− 1) である. また (3) のノードは自分の Successor が受信エリアに含まれることしか知ることができないため, Nr に関する情報は 1/(全ノード数− 1) となる.

(4) のノードの場合, 受信エリアの終点のため Predesessor が受信エリアであることが分かる. また, ヘッダ部の復号を行うため, 次の受信エリアの始点も知ることになる. しかし, 知ることができる受信者の可能性があるノードはこの 2 つのみであるため, Nr に関する確率は $2/AN_{max}$ となる. さらに, 上記と同様に AN_{max}は全ノード数− 1 と考えることができるため, (4) のノードが知ることのできるノードが Nr である可能性は高々2/(全ノード数− 1) となる.

4.1.3 送信者と受信者のつながりの匿名性

4.1.1 と 4.1.2 より，どのノードも送信者か受信者の可能性を秘めたノードを推定することはできるが，推定したノードが真に送信者か受信者である確率は低い．このため，送信者と受信者のつながりを割り出すことも困難である．

また，双方向通信の場合，送信時と返信時のメッセージとの対応関係を推定することで，送信者と受信者のつながりを推定する方法が考えられる．しかし，本手法では，N_s が送信時に作成した返信用のヘッダを使って返信するため，送信時に中継を行ったノードが，返信時も中継するとは限らず，返信時のメッセージを観測することが困難である．また，仮に送信時に中継を行ったノードが返信時も中継を行ったとしても，返信時のメッセージは，送信時のメッセージと完全に異なっており，対応関係を把握することは困難である．そのため，送信者と受信者のつながりの匿名性は確保される．

4.1.4 結託攻撃に関する考察

(1)〜(4) のノードの 2 つが結託をした場合，送信者の匿名性，受信者の匿名性，送信者と受信者の匿名性がどれだ低下するかを検討する．

まず，送信者の匿名性について検討する．送信者の匿名性が確保されるか否かは，メッセージを送信したノードの情報に起因する．4.1.1 で示したように攻撃者は，2^{k-1} 以降 (ID 空間で角度にして 180 °) 離れたノードからメッセージが送られてきた時のみ，直前ノードが送信者であると推測することができる．しかし本手法では，受信エリアの始点ノードが受信するごとに過去のヘッダ情報を削除する．このため，(1)〜(4) のノードがどのように結託した場合であっても，Ns からのメッセージか，それ以前の受信エリアの終点ノード $(A_i l)$ からのメッセージであるか判断することはできない．

次に受信者の匿名性について述べる．(1) のノードが知る受信者の可能性をもつノード数は，4.1.2 に示した通り 1 であり，(2)〜(4) のノード数も高々2 である．そのため，(1) と (2)〜(4) のノードが結託した場合は $3/AN_{max}$ の確率で受信者が推定できる．しかし 4.1.2 に示した通り AN_{max}は (全ノード数− 1) と考えることができるため実質的に 3/(全ノード数− 1) となる．同様に (2) のノード同士が結託した場合もそれぞれが知る受信者の可能性をもつノードは高々2 であり最悪でも実質的に 4/全ノード数 となる．

最も匿名性が低下すると考えられる場合は，(3) と (4) もしくは (4) のノードが同士が結託した場合である．これらのノードが結託した場合，いずれかの受信エリアの始点と終点が知られる．仮に知られた始点と終点のノードが，同じ受信エリアに属するものであった場合，受信エリアの範囲が知られることになる．そのため，知ることのできた受信エリア内のノード数を AN とすると，この結託によって知ることのできる受信者の可能性は AN/AN_{max} である．しかし，多重暗号化により他の受信エリアを知ることができないため AN_{max}は全ノード数 と考えられることができ，結局のところ受信者の可能性は高々AN/(全ノード数− 1) である．

また，2 つ以上のノードが結託行ったとしても，すべての受信エリアの数と範囲までしか特定できない．何度もメッセージ交換を行うことによって徐々に推測される可能性はある．最悪の場合には，すべての受信エリアが特定される．しかし，この場合においても，真の受信者が特定される確率は $1/AN_{max}$ である．

4.2 可 用 性

本手法は 3 章で示したとおり，匿名通信を行うノードを Chord のアルゴリズムを用いて ID 空間に配置し，ID を宛先として指定することでメッセージの経路を動的に選択する．これにより，3.5.4 に示したとおり中継ノードが故障などにより離脱したとしても，Chord のアルゴリズムにそって次ノードを選びなおしメッセージの送信を進めることができる．また，受信エリア内のルーティングの際も，ヘッダ復号のための秘密鍵のレプリカを Successor に渡しておくことで，秘密鍵を持ったノードすべてが同時に離脱しない限り，メッセージの中継が止まることはない．

返信時も ID で指定したヘッダを用いて返信用のメッセージを送信時と同様に送信するため，ヘッダ復号の秘密鍵を持ったノードすべてが同時に離脱しない限り返信をすることができる．

4.3 スケーラビリティ

本手法で探索方式として使用している Chord では，3.2 で示した様に完全分散型 P2P システムでありながら，中央サーバなしで動作する．そのため高いスケーラビリティを持つと考えられる．

しかし，本手法では Chord のアルゴリズムで構成されるノードの他に，公開鍵管理サーバが必要である．このサーバがスケーラビリティの上でボトルネックとなることが予想される．しかし，仮に信頼できるサーバをいくつか用意し，それらのサーバに分散させて公開鍵を保有させることで，この問題対処することができる．この問題の解決は今後の課題である．

4.4 検討のまとめと課題

以上より，本提案手法は送信者と受信者をともに秘匿しつつ，高い可用性とスケーラビリティを有していると言える．また，多重暗号化と Chord による動的な経路生成により結託攻撃に対しても高い匿名性を確保する．

問題点として，メッセージの暗号化と復号はすべて公開鍵暗号で行うこと，さらに，受信エリア間の通信に Chord による中継を行うため，遅延が大きいと考えられる．また，各ノードが意図的にメッセージの転送を怠ったり，誤ったルーティングをしたり，メッセージを改変することが考えられる．これらの攻撃の対処法としては，異なった受信エリアを選択したメッセージを用いて多重にメッセージを送ることで解決できるが，今後検討が必要である．

5. 既存手法との比較

オニオンルーティングと Crowds との，送信者の匿名性，受信者の匿名性，送受信者のつながりの匿名性，可用性とスケーラビリティを比較する．それぞれの比較をまとめたものを表 1 に示す．

表 1　既存手法との比較

手法	Crowds	オニオンルーティング	提案手法
送信者匿名性	○	○	○
受信者匿名性	×	○	○
つながりの匿名性	△	○	○
可用性	△	×	○
スケーラビリティ	×	△	○
応答時間	○	△	△

5.1 Crowds

Crowds は 2.2 に示した通り，ある確率で受信者か中継ノードかを選んでメッセージを送信することで，送信者の匿名性を確保する手法である．確率によって次のノードを決めるため，一度も他のノードを経由せず，直接受信者と通信を行った場合であっても，送信者の匿名性は確保される．しかし，受信者に到達することを保証するために，受信者の情報は秘匿されない．つまり，受信者の匿名性の確保は考えられていないため，受信者は中継したすべてのノードに知られる．

次に可用性について述べる．Crowds は確率によって次のノードを決めるため，動的に受信者までの経路を確保することができることから，高い可用性があると言える．しかし，返信は，送信時に中継したノードが送られてきたノードに返すことで行う．つまり，中継ノードのどれか 1 つでも離脱した場合，通信が途絶える．この場合，送信者がタイムアウト処理等を行い，再送信を行わなければならない．以上のことから，送信時においては高い可用性があるが，双方向通信に着目した場合，可用性が高い通信を行えるとは言えない．

スケーラビリティについて述べる．Crowds はグループのメンバシップを専用のサーバによって集中的に管理する．サーバによって集中管理する方式は，ノード数の増加に対してスケーラブルに動作することができない．このためスケーラビリティは低いと言える．

5.2 オニオンルーティング

オニオンルーティングは 2.1 に示した通り，メッセージを多重暗号化することで送信者と受信者を共に秘匿させる手法である．これにより，1 つでも信頼できる中継ノードがある場合，送信者と受信者を共に知ることができない．そのため，送信者と受信者のつながりの匿名性も確保される．また，経路生成時にそれぞれの中継ノードとの共通鍵を生成するため，本手法に比べ高速であると考えられる．

しかし，経路生成時に固定的に経路を決めるため，可用性が低い．送信時と返信時ともに中継ノードが一つでも離脱した場合，メッセージを復号することができず，再度経路生成からやりなおす必要がある．また，経路生成では，受信者までの経路を受信者がどのノードか知られることなく生成する必要があるため，ブロードキャストが使われる．そのため，動的なネットワークでは何度もブロードキャストが行われることから，本手法に比べ可用性が低いと考える．

また，スケーラビリティは，先述のとおり経路生成時にブロードキャストを行うことがボトルネックとなり，本手法で挙げるような大規模なネットワークでは，帯域を大きく消費するため，使用が難しいと言える．このためスケーラビリティは低いと言える．

6. ま と め

本論文では，オニオンルーティングなどで扱われる多重暗号化に分散ハッシュテーブルである Chord の経路選択を用いる手法を提案した．IP アドレスを Chord の ID に写像し，メッセージの宛先を ID で管理することで高い可用性とスケーラビリティを満たすことができる．また，受信エリアを付加することで強固な匿名性を満たすことを示した．本提案手法は双方向通信を行いつつ，送受信者の匿名性の維持が求められるアプリケーションに有効であるといえる．

今後は，各種攻撃に対する防御策を検討する．その上で高い匿名性を確保できるよう改良を行う．また，大規模な実験環境を用いた性能評価実験を行う計画である．

謝辞　本研究は財団法人堀情報科学振興財団の研究助成によるものである．

文　献

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

[2] Chaum, D.L:Untraceable electronic mail, return address, and digital pseudonyms, Comm.ACM, Vol.24, No.2, pp.84-88, ACM Press(1981).

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

[4] 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)

[5] 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).

[6] 井上 大介，松本 勉:マルチキャストを用いた匿名通信方式，電子情報通信学会技術報告，ISEC-99-29 (1999).

[7] Kikuchi, H.: Sender and Recipient Anonymous Communication without Public Key Cryprography, 情報処理学会研究報告書，98-CSEC-1-8 (1998).

[8] 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).

[9] 阿部 洋丈，加藤和彦:Aerie:www のための完全分散匿名プロキシ，情報処理学会論文誌，Vol. 46 No. SIG3, pp. 51-61 (2005).

[10] 北澤 繁樹，長野 悟，双紙 正和，宮地 充子:初等的な環状経路を用いた匿名通信方式，情報処理学会論文誌，Vol. 41 No.8, pp.2148-2161 (2000).