初等的な環状経路を用いた匿名通信方式

北澤繁樹[†] 長野悟[†,☆]
双紙正和[†] 宮地充子[†]

近年コンピュータおよびインターネットの普及により，莫大な量の情報がネットワークを介して処理されるようになってきている．これにともなって，意図しない個人情報の流出などが問題となり，プライバシの確保が重要となってきた．そこで，ユーザの匿名性を保護するために様々な研究が行われてきた．しかしながら，従来方式では暗号化を多重に行うことによるコストが大きくなったり，ブロードキャストを効率的に行うためのネットワークアーキテクチャを必要としたりするという問題があった．そこで，1999年，我々は，環状経路には始点と終点が存在しないという特徴があり，これを利用することで通信の始点（送信者）と終点（受信者）の特定を困難にした匿名通信方式を提案した．この提案方式においては，通信路情報を暗号化する必要がなくなり，鍵配送や暗号化と復号にかかるコストを小さくすることができる．本論文では，提案方式のプロトコルを形式的に定義し，さらに，その安全性と運用に関して評価する．その結果，経路上の結託者の攻撃に対する安全性はCrowdsとして提案されている従来方式より提案方式の方がつねに高く，経路長に関してもCrowdsの方式より効率的にできる場合があることを示す．また，環状経路の運用に関してはメッセージの到達確率について議論し，提案方式の耐故障性について評価する．

Anonymous Communication with Elementary Cyclic Routes

Shigeki Kitazawa,[†] Satoru Nagano,[†,☆] Masakazu Soshi[†]
and Atsuko Miyaji[†]

In today's computer networks, it is one of the utmost concerns to provide anonymity for protecting users' privacy. However previous anonymous communication protocols have such disadvantages that additional cost like repeated encryption is required, or that receiver anonymity is not realized. Therefore, we propose a new anonymous communication scheme with cyclic routes. Cyclic routes have a good feature that there exist neither starting points nor end points. This feature would be useful to realize anonymous communication where identities of senders (starting points) and receivers (end points) must be made unknown. Thus our scheme reduces the cost of key distribution, encryption, and decryption, maintaining anonymity of both senders and receivers. In this paper, we formally define our protocol and discuss its various aspects including anonymity. Especially, we show that our scheme can generally provide higher degree of anonymity than Crowds system proposed recently.

1. はじめに

現代のような高度情報化社会では，商業，家庭，医療，行政，軍事など，あらゆる分野において莫大な量の様々な情報がコンピュータによって処理される．これにともなって，個人の意図しない情報の流出などの新しい課題が生じてきている[3]．特に，近年インターネットが急激に普及したことでこのような傾向に拍車がかかり，ユーザの嗜好や位置情報など様々な個人情報の漏洩が問題になっている[11),13)]．そこで，ユーザの匿名性を確保しつつ，ある程度のサービスを提供することの必要性がますます高まっている．

ネットワーク上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，数々の研究が行われてきた．1981年，Chaumによって，電子メールにおける匿名通信方式として，複数のMIXと呼ばれる中継ホストを経由して匿名通信を行う方式が提案された[1)]．この方式では，送信者は通信内容とその宛先を入れ子にして，いくつかの中継するMIXの公開鍵を用いて暗号化しておく．メッセージはMIXを経由するごとに復号され，経路の最後でMIXから受信者へ通信内容が

† 北陸先端科学技術大学院大学情報科学研究科
School of Information Science, Japan Advanced Institute of Science and Technology
☆ 現在，NTTアドバンステクノロジ株式会社
Presently with NTT Advanced Technology Corporation

送られる．中継するノードは，メッセージを送ってきたノードとメッセージをこれから送るノードのアドレスしか分からない．この MIX の方式を応用したものもいくつか提案されているが[10),15)]，これらの方式では，多重の暗号化によるシステムパフォーマンスの低下が問題となる．

また，既存のネットワーク通信方式であるブロードキャストやマルチキャスト[14),16)]を利用して匿名性を得る方式が提案されている[4),5)]．ブロードキャストを用いる方式[5)]では，グループ全員にダイレクトに通信するので，MIX のような中継ノードを経由することによる通信遅延が生じないことが利点である．しかしながら，定期的にすべてのノードがブロードキャストするので，通信の帯域幅を多く消費する傾向がある．マルチキャストを用いた方式[4)]は，ブロードキャストほどには帯域幅を消費しないが，高い匿名性を実現するためにはメッセージ数が多くなり，オーバヘッドが大きくなる．拡張性の面からみると，ブロードキャスト，マルチキャストともに小規模なネットワークを想定した設計となっており，通信に参加するグループやメンバの数が増えた場合にはそれを処理するための特別なネットワークアーキテクチャが必要となる[17)]．

一方，送信者情報の秘匿を暗号化やブロードキャストなどに頼らず，“人を隠すなら群衆の中” というアイデアで，メッセージを中継するマシンが確率的に次の経路を決定することにより匿名性を実現する方式（Crowds）を，1998 年，Reiter らが提案した[11),12)]．しかしながら，確率的に経路を決定するので通信遅延が大きくなる．さらに，メッセージを中継したノードすべてに宛先が知られてしまうという問題点もある．

1999 年，我々は，匿名通信方式方式として，汎用性があり，かつ送信者および受信者の匿名性を維持するためのコストが低いシステムを目的とし，メッセージ配送経路として環状経路を用いた方式を提案した[8)]．この方式では環状経路には経路の始点と終点が存在しないという性質を利用することで，匿名通信路の送信者（始点）と受信者（終点）の特定を困難にしている．環状経路の性質を利用した匿名通信方式としては，1984 年，Pfitzmann によって SBNS（Switched/Broadcast Network Structure）が提案されている[9)]．しかしながら，SBNS では，物理的につながった環状経路を用いることや，最初の通信においてレスポンダの公開アドレスを含まなければならないことなどから，環状経路の性質を十分利用しているとはいえない．提案方式では，環状経路を形成するのにルーティングエージェントと呼ばれる匿名通信代行ルータを用いる．ユーザはただ 1 つのルーティングエージェントに所属し，所属しているルーティングエージェントを介して匿名通信をやりとりする．したがって，ユーザに関する情報を環状経路と匿名通信代行の 2 重で保護することで，送信者および受信者の匿名性を確保することができる．また，情報の秘匿に必要な暗号化プロセスを減らすことが可能であるため，鍵共有や暗号化と復号を繰り返すことで生じるシステム性能の低下を防ぐことができる．さらに，提案方式は特別な用途を仮定していないので，World Wide Web（WWW）やその他の様々な通信プロトコルに応用が可能である．加えて，提案方式では一対一通信ができればよいため，特定のネットワークアーキテクチャに依存することなく実現できる．

本論文では，提案方式の安全性と運用に関して評価を行う．その結果，経路上の結託者の攻撃に対する安全性は Crowds より提案方式の方がつねに高く，経路長に関しても Crowds の方式より効率的にできる場合があることを示す．また，環状経路の運用に関してはメッセージの到達確率について議論し，提案方式の耐故障性について評価する．

本論文の構成は次のとおりである．2 章では，代表的な匿名通信方式の 1 つとして Crowds に着目し，議論する．3 章では環状経路を用いた匿名通信方式を提案する．さらに 4 章および 5 章で提案方式に関する安全性とシステムの運用について評価する．6 章では，提案方式と Crowds との比較を行う．最後に 7 章で本論文の結論を述べる．

2. Crowds の概要

この章では，代表的な匿名通信方式の 1 つとして Crowds に注目し，議論する．

WWW 上で匿名通信を実現する方式として，1998 年，Reiter らにより Crowds が提案された[11),12)]．Crowds では，匿名性を確保するためにユーザは “crowd” と呼ばれる匿名通信を実現するためのグループに “jondo” という匿名ユーザとして参加する．匿名通信を行うとき，通信の始動者となる jondo は，最初に crowd 内の自分以外の jondo へメッセージを送信する．メッセージを受け取った jondo は crowd の中から無作為に選んだ jondo またはメッセージの最終的な宛先に転送する．他の jondo に転送する確率を p_f $(> 1/2)$ とし，crowd 内の全 jondo の数を N_{jondo}，crowd のメンバのうちで結託しているメンバの数を C_{jondo} とする．このとき，crowd のメンバの結託により通信の始動者の jondo が知られてしまう確率 $P_1(N_{jondo}, C_{jondo})$ は，

$$P_1(N_{jondo}, C_{jondo}) = \frac{N_{jondo} - p_f(N_{jondo} - C_{jondo} - 1)}{N_{jondo}}$$

で与えられる[11]．また，平均経路長 $l_1 = (2-p_f)/(1-p_f)$ である．

Web サーバから見た crowd のメンバ（jondo）はすべて一様であり，実際にメッセージを発したユーザを確率的にしか特定することができない．しかしながら，Crowds ではメッセージの経路を確率的に決定するので，メッセージの到達性を保証するために，メッセージを中継するメンバに対して宛先を隠すことができない．また，システムの盗聴者からメッセージ内容を隠すために crowd のメンバは crowd 内のすべてのメンバと鍵共有を行い，メンバ間の通信を暗号化しているが，メンバの更新のたびに鍵も更新しなければならないので，頻繁に crowd メンバの更新があると鍵更新にかかるコストも無視できなくなる．

3. 提案方式

ここでは，環状経路を用いた匿名通信プロトコルを提案する．

3.1 概　　要

図 1 に提案方式の概要図を示す．提案方式は，ユーザの匿名性を確保するために，環状経路によって通信の始点と終点のアドレスの特定を困難にする．その結果，経路情報を暗号化する必要がないので，システム性能の劣化を防ぐことができる．

提案方式で実際に環状経路にするのは 3.2 節で述べるルーティングエージェント間でメッセージをやりとりする部分である．ユーザはそれぞれ決まったルーティングエージェントに所属しており，所属しているルーティングエージェントを介して匿名通信を行う．したがって，ユーザはプロキシ[2),7)]となるルーティングエージェントを介して匿名通信路にアクセスすることになり，2 重に匿名性が保護されている．また，このようなシステム構造を持つことにより，ファイアウォール[2)]を利用したネットワークに対して容易に応用することが可能である．

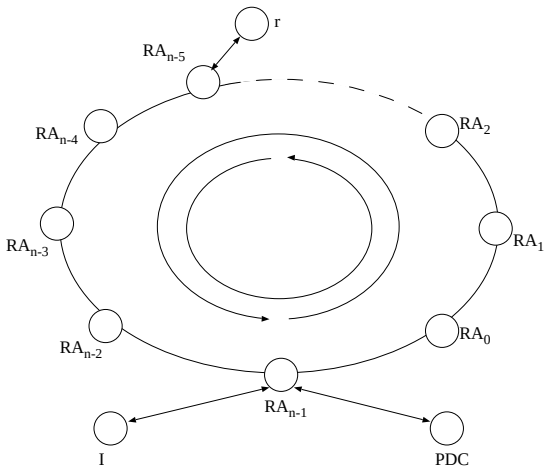

図 1　提案方式の概要図
Fig. 1　System overview.

3.2 エンティティ

提案方式におけるエンティティについて説明する．

イニシエータ I： 通信内容 V を送信するユーザ．

レスポンダ r： イニシエータが出す通信内容 V の宛先ユーザ．

ルーティングエージェント（RA）： 各ユーザのメッセージ通信のルーティングを司るエージェント．プロトコルにおけるルーティングエージェントの総数を N_{RA} とする．各ユーザに対して，ただ 1 つのエージェントが必ず存在する．逆に 1 つのルーティングエージェントには複数のユーザが存在してもよい．また本論文では，イニシエータ I のルーティングエージェントを R_I，レスポンダ r のルーティングエージェントを R_r と表記する．

公開鍵データベースセンタ（PDC）： ユーザ u のユーザ ID（ID_u），ユーザ u のルーティングエージェントの ID（ID_{RA_u}），ユーザ u のルーティングエージェントの公開鍵（PK_{RA_u}）のデータベースを管理する機関．

3.3 メッセージ形式

イニシエータ I がレスポンダ r に匿名通信により通信内容 V を送信するとし，環状経路は同じルーティングエージェントを 2 回以上通らない初等的な有向閉路[6)]と仮定する．このときのメッセージ形式 $\mathcal{M}$ は以下のようになる．

$$\mathcal{M} = ((ID_{RA_0}, ID_{RA_1}, \cdots, ID_{RA_{n-1}}), E/C, V)$$

$(ID_{RA_0}, ID_{RA_1}, \cdots, ID_{RA_{n-1}})$ はメッセージが送信される（環状の）経路順を表している．ここで，n は経路長を表しており，システムで固定のパラメータである（$n \leq N_{RA}$）．ただし，必ずしも RA_0 および RA_{n-1} がそれぞれ R_I および R_r であるとは限らない．環状経路であるため，R_I，R_r を $RA_0, RA_1, \cdots, RA_{n-1}$ の中の，任意の位置に配置することができるので，R_I と R_r の特定を困難にすることができる．R_I が，$RA_0, \cdots, RA_{n-1}$ の途中にあるとき，RA_{n-1} に送られたメッセージは RA_0 に送られる．E/C フィールドには，CID（コミュニケーション ID），あるいはレスポンダの所属するルーティングエージェント R_r

の公開鍵 PK_{R_r} により $(ID_{R_r}||ID_r||CID||rand)$ を暗号化した $\mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand))$ のいずれかが入る．$rand$ は乱数を表す．暗号化関数 E の入力において，PK_{R_r}，ID_{R_r}，ID_r，CID は，いずれも送信者および受信者以外でも入手可能な値であるので，組合せからレスポンダを特定することを防ぐため，乱数（$rand$）をパディングしている．また，$\mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand))$ と CID を見かけ上区別できないようにするため，両方を同じ長さにする．

3.4 データベース

すべてのルーティングエージェントは，受信メッセージを処理するために必要な情報を格納しておくため，3つのデータベースを持つ．

EDB： R_I が生成したメッセージの E/C フィールドを格納するデータベース．受信メッセージが自分が生成した往信メッセージであるかの判定に用いる．

SCDB： R_I が生成したメッセージの CID とそのメッセージのイニシエータの ID（ID_I）を格納するデータベース．受信メッセージが自分が生成した往信メッセージに対する返信であった場合，どのイニシエータに返信メッセージを送るかを決定するときに用いる．

RCDB： R_r がレスポンダに送信したメッセージの CID と経路情報を格納するデータベース．レスポンダから返信内容を受信し，イニシエータへの返信メッセージを生成するときに用いる．

3.5 提案方式

本節では，提案プロトコルについて説明する（図1）．ここでは，経路上の各ルーティングエージェントは通常稼働しているとする．

往信フェーズ

(1) イニシエータ I はレスポンダ r の ID（ID_r）と通信内容 V を I のルーティングエージェント R_I へ渡す．

(2) R_I は PDC からレスポンダが所属するルーティングエージェントの ID（ID_{R_r}）と，その公開鍵（PK_{R_r}）を入手する．

(3) R_I は ID_{R_r} と PK_{R_r} を受け取った後に，R_I と R_r を含んだ環状経路をランダムに生成し，次のようなメッセージ $\mathcal{M}$ を作成する．

$$\mathcal{M}=((ID_{RA_0},ID_{RA_1},\cdots,ID_{RA_{n-1}}),\ \mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand)),V)$$

(4) R_I は $\mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand))$ を送信メッセージの識別のために EDB へ保管し，ID_I と CID を SCDB へ保管する．メッセージ $\mathcal{M}$ を経路上次の RA_i へ送信する．

(5) メッセージを受信した RA_i は E/C フィールドを SCDB，RCDB，EDB に保管されている値と照合する．RA_i が R_I でない場合は E/C フィールドと同じ値がそれらのデータベースにはないので，次に自分の秘密鍵を用いて復号を試みる．しかし，PK_{R_r} と対応する秘密鍵ではないので，得られた文字列の先頭には ID_{R_r} が含まれない．そこで，メッセージ $\mathcal{M}$ は自分に向けられたメッセージではないと判断し，経路上次の RA_{i+1} へ転送する．メッセージが R_r に到達するまで，同様の手順が繰り返される．

(6) R_r は，他のルーティングエージェントと同様の処理を行う．しかしながら，R_r だけは E/C フィールドの復号後，ID_{R_r}，ID_r，CID を得ることができる．そこで，レスポンダ r へ通信内容 V と CID を送信する．同時に，CID と経路情報を RCDB に保管する．メッセージ $\mathcal{M}$ を次の経路へ転送する．メッセージ $\mathcal{M}$ が R_I に到達するまで同様の操作が繰り返される．

(7) R_I も，他のルーティングエージェントと同様の処理を行う．このとき，EDB に $\mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand))$ の値が見つかるので，メッセージ $\mathcal{M}$ は自分が作成したメッセージであると判断し，メッセージ $\mathcal{M}$ を破棄し，EDB から $\mathsf{E}(PK_{R_r},(ID_{R_r}||ID_r||CID||rand))$ を削除する．

返信フェーズ

(1) レスポンダ r は，先に受け取った匿名の通信内容 V に対する返信 V' を作成し，r が所属するルーティングエージェント R_r へ，V' と CID を送る．

(2) R_r は RCDB に保持していた CID と経路情報を利用して次のメッセージ $\mathcal{M}'$ を作成し，環状経路上で次のルーティングエージェントへ転送する．

$$\mathcal{M}'=((ID_{RA_0},ID_{RA_1},\cdots,ID_{RA_{n-1}}),CID,V')$$

(3) メッセージ $\mathcal{M}'$ を受信したルーティングエージェントは送信フェーズと同様に E/C フィールドを SCDB，RCDB，EDB に保管されている値と照合する．R_I でないときには，データベースに E/C フィールドの値と同じデータがないので，次に自分の秘密鍵で復号を試みるが得られた文字列の先頭には自分の ID が含まれないので，メッセージ $\mathcal{M}'$ は自分宛のメッセー

ジではないと判断し，経路上次のルーティングエージェントへ転送する．メッセージ $\mathcal{M}'$ が R_I に到達するまで同様の操作が繰り返される．

(4) R_I は他のルーティングエージェントと同様の処理を行うが，SCDB，RCDB，EDBに E/C フィールドの値が格納されているかどうかチェックしたとき，SCDBに E/C フィールドの値（CID）が見つかるので，$\mathcal{M}'$ は自分が作成したメッセージに対する返信であると判断し，通信内容 V' をイニシエータ I へ送信し，SCDBから ID_I と CID を削除する．同時に，経路上次のルーティングエージェントへメッセージを転送する．転送は，R_r まで繰り返される．

(5) R_r は，他のルーティングエージェントと同様の処理を行うが，E/C フィールドをチェックしたとき，RCDBに保管してある CID から自分が出した返信メッセージであると判断できるので，メッセージ $\mathcal{M}'$ を破棄し，RCDBから CID と経路情報を削除する．

3.6 プロトコル

3.5節では提案プロトコルに関する全体的な流れに関して述べた．ここでは，ルーティングエージェントの詳細な処理について記述する．

まずはじめにプロトコルで使われている記号について説明する．

u：ユーザ；
U：ユーザの集合；
I：イニシエータ；
r：レスポンダ；
ra：プロトコルを実行するルーティングエージェント；
m：メッセージ；
M：メッセージの集合；
V：通信内容；
n：経路長；
RA：ルーティングエージェントの集合；
ID：識別子の集合；
$\mathsf{id}(\varepsilon)$：入力エンティティ ε ($\in$U$\cup$RA) の IDを返す関数；
$\mathrm{ID_{RA}}$：$\mathsf{id}(ra)$ ($ra \in$ RA) の集合；
CID：コミュニケーション ID；
CID：コミュニケーション IDの集合；
PK：公開鍵の集合；
PATH：$\mathrm{ID_{RA}}^n$ の部分集合；
$\mathsf{rt}(\mathsf{id}(u))$：$u$($\in$U) のルーティングエージェントを返す関数；
$\mathsf{cid}(m)$：m($\in$M) のコミュニケーション IDを返す関数；
$\mathsf{pk}(ra)$：ra ($\in$ RA) の公開鍵を返す関数；
$\mathsf{E}(key, value)$：$value$ を key で暗号化した値を返す関数；
$\mathsf{D}(key', value')$：$value'$ を key' で復号した値を返す関数；
EDB：$\{\mathsf{E}(\mathsf{pk}(\mathsf{rt}(\mathsf{id}(r))), (\mathsf{id}(\mathsf{rt}(\mathsf{id}(r)))||\mathsf{id}(r)||\mathsf{cid}(m)||rand)) \mid r \in$U, $m \in$M $\}$ の部分集合；
SCDB：ID $\times$ CID の部分集合；
RCDB：PATH $\times$ CID の部分集合；

プロトコルは以下のように定義される．

```
1   procedure ra_send(id(I), id(r), V);
2     begin /* process messages sent by I */
3       send id(r) to PDC;
4       receive (id(r), id(rt(id(r))),
5         pk(rt(id(r)))) from PDC;
6       P := (n − 2) routing agents randomly
7         chosen from RA−{rt(id(I)), rt(id(r))};
8       P := P∪{rt(id(I)), rt(id(r))};
9         /* note that rt(id(I))=ra holds */
10      PATH := ();
11      for i := 1 to n do
12        begin
13          a := a routing agent
14            randomly chosen from P;
15          P := P−{a};
16          PATH := (PATH, id(a));
17        end
18      CID := random();
19      rand := random();
20      E := E(pk(rt(id(r))), (id(rt(id(r)))||id(r)||
21        CID||rand));
22      EDB := EDB∪{E};
23      SCDB := SCDB∪{(id(I), CID)};
24      dest := ID of the next routing agent
25        of rt(id(I)) in PATH;
26      send (PATH, E, V) to dest;
27    end;
28
29  procedure
30    ra_relay(PATH, E_or_CID, V, sk);
31    /* procedure for relaying messages */
32    begin
33      if (∃(id(I), cid(m))∈SCDB:
34        cid(m)=E_or_CID) then
35        begin
36          send V to I;
37          SCDB := SCDB−{(id(I), cid(m))};
38        end
39      else if (∃(PATH, cid(m))∈RCDB:
40        cid(m)=E_or_CID ) then
41        begin
42          RCDB := RCDB−{(PATH, cid(m))};
43          return;
44        end
```

```
45      else if (∃e ∈EDB: E=E_or_CID) then
46        begin
47          EDB := EDB−{E};
48          return;
49        end
50      else
51        begin
52          (id(rt(id(r))), id(r), cid(m)) :=
53            D(sk, E_or_CID); /* decrypt */
54          if (id(rt(id(r)))=id(ra)) then
55            begin
56              send (V, cid(m)) to id(r);
57              RCDB :=
58                RCDB∪{(PATH, cid(m))};
59            end
60        end
61      dest := ID of the next routing agent
62        of ra in PATH;
63      send (PATH, E_or_CID, V) to dest;
64    end;
65
66  procedure ra_receive(V, cid(m));
67    /* procedure for replying */
68    begin
69      search RCDB for a pair of PATH
70        and cid(m′) where cid(m)=cid(m′);
71      dest := ID of the next routing agent
72        of ra in PATH;
73      send (PATH, cid(m), V) to dest;
74    end;
75
76  procedure
77    routing_agent(id(ra), sk, received_data);
78    begin /* sk is the secret key of ra */
79      if (received_data=(id(I), id(r), V))
80        then
81        ra_send(id(I), id(r), V);
82      else if (received_data=
83        (PATH, E_or_CID, V))then
84        ra_relay(PATH, E_or_CID, V, sk);
85      else if (received_data=(V, cid(m)))
86        then
87        ra_reply(V, cid(m));
88    end;
```

procedure ra_send は，ルーティングエージェントがイニシエータからリクエストを受け取った場合の処理である．11〜17 行目の処理で長さ n の環状経路を生成する．

procedure ra_relay は，ルーティングエージェントが他のルーティングエージェントからメッセージを受け取った場合の処理である．33，34 行目の条件式は，メッセージの E/C フィールドと SCDB の内容とを照合し，受け取ったメッセージが以前そのルーティングエージェントで作成したメッセージの返信であるかどうかを判断している（23 行目参照）．39，40 行目の条件式は受け取ったメッセージが，以前そのルーティングエージェントが受け取ったメッセージの返信が環状経路を経て自分に戻ってきたメッセージであるかどうかを RCDB を用いて判断している（57，58 行目参照）．45 行目の条件式では，受け取ったメッセージが，以前そのルーティングエージェントで作成した送信メッセージであり，それが環状経路を経て自分に戻ってきたものであるかどうかを EDB を用いて判断している（22 行目参照）．SCDB，RCDB，EDB の照合にすべて失敗した場合に，メッセージを自分の秘密鍵を用いて復号を試みる．復号手続きを一番最後としているのは，復号処理には計算コストがかかるので無駄な復号処理を避けるためである．

procedure ra_receive は，ルーティングエージェントがレスポンダからのメッセージ形式でメッセージを受け取った場合の処理である．返信の際は，以前 RCDB に CID と対応づけて保管しておいた環状経路を用いる．

4. 安全性の評価

ここでは送信フェーズにおいて，“環状経路”，“モニタ”，“R_r”，“ルーティングエージェントの結託” の攻撃を想定し，各々の攻撃によって，どのような情報が漏洩するのかを考察し，得られた結果と Crowds との比較を行う．ただし，R_I や R_r に関する情報はメッセージの環状経路のみに含まれているとし，通信内容 V には R_I や R_r を特定できるような情報を含まないものとする．

4.1 環状経路

ここでは，メッセージの経路情報を知ることのできる経路上のルーティングエージェント，および盗聴により経路情報を知ることのできる第 3 者を攻撃者とし，攻撃者は経路情報のみから R_I，および R_r を特定を試みるものとする．本提案方式において，環状経路を用いる利点として以下の点があげられる．

(1) R_I と R_r を他のルーティングエージェントが確率的にしか特定できず，たとえ R_r であっても R_I を確率的にしか特定できない．

(2) 経路情報を暗号化しなくて済むので，経路暗号化にかかる負担が少ない．

(1) に関して，他のルーティングエージェントから通信メッセージを受け取ったルーティングエージェントは，送ってきたルーティングエージェントが R_I，R_r であるのか，または中継ルーティングエージェントなのかを，メッセージからは判断することができない．さらに，メッセージの宛先である R_r でさえも，自分宛のメッセージであると判断はできるが，R_I が環状経路の何番目にいるのかを特定できない．さらに，

環状経路とユーザの間にルーティングエージェントを介在させることによって，ユーザの特定がより困難となる．ただし，その場合でも経路情報を隠さないために，R_I および R_r が，環状経路を形成するいくつかのルーティングエージェントのどれかであることまでは知られてしまう．経路上の R_I と R_r を除いたルーティングエージェントは，少なくとも自分自身は R_I や R_r ではないことが分かる．したがって，経路上のルーティングエージェントが経路長 n の経路情報を受け取ったとき，R_I または R_r が分かる確率は，$1/(n-1)$ となる．また，R_I と R_r の両方が分かる確率は $1/((n-1)(n-2))$ となる．

(2) に関して，一般に直線的な経路を隠すためには，イニシエータ I はすべての中継ノードの公開鍵を入手し，それぞれの転送先ノードを公開鍵を用いて暗号化するといったアプローチがとられる[1),15)]．このとき，返信も考慮した場合返信経路も I が作成し暗号化する．よって，暗号化とそれにともなう鍵配送のコストは大きくなる．一方，提案方式では R_r の公開鍵で宛先情報を 1 回暗号化するだけである．したがって，暗号化を多用した従来方式[1),15)]と比べ，低いコストで匿名通信路を実現することが可能である．

環状経路のある 1 点を盗聴している攻撃者が，経路情報を入手した場合は，R_I または R_r が分かる確率は，$1/n$ となり，R_I と R_r どちらも分かる確率は $1/(n(n-1))$ となる．

4.2 モニタリング

モニタとは個々のマシンから発せられる通信のタイミングやメッセージ $\mathcal{M}$ の内容そのものを見ることができる攻撃者である．これにより，モニタはモニタリングしている対象が匿名通信プロトコル上でどのような働きをしているのか判断することができる．モニタが得られる情報は，モニタリングしているマシンが匿名通信においてどのような働きをしているかによって異なる（**図 2**）．

(1) 通信経路上の，ある中継ルーティングエージェントに関する，別のルーティングエージェントとのすべての通信
(2) イニシエータ I のルーティングエージェント R_I に関する，別のルーティングエージェントとのすべての通信
(3) レスポンダ r のルーティングエージェント R_r に関する，別のルーティングエージェントとのすべての通信
(4) イニシエータ I のマシンと R_I との間のすべての通信

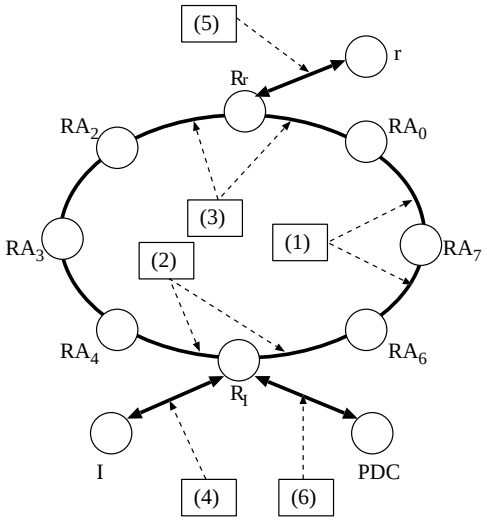

図 2 モニタリングの位置
Fig. 2 Locations of monitoring.

(5) レスポンダ r のマシンと R_r との間のすべての通信
(6) R_I と公開鍵データベースセンタ（PDC）との間のすべての通信

(1) の場合，モニタが得られる情報は，メッセージの経路情報である．R_I，R_r を特定することはできない．(2)，(3) の場合は (1) で得られる情報のほかに，ルーティングエージェントから誰かに向けてメッセージが送信されたことを知ることができる．(4) の場合は，モニタはイニシエータ I とレスポンダ r を特定することができてしまう．(5) の場合にモニタが得られる情報は ID_r であり，I に関する情報は何も得られないが，あるユーザと r の間で匿名で何らかの交信を行われたことが分かってしまう．(6) の場合，モニタが得られる情報は，ID_r，ID_{R_r}，および R_r の公開鍵 PK_{R_r} であり，このルーティングエージェントが r に対して匿名で情報を伝えようとしていることが分かる．

これらのうち，(4)，(5)，(6) に関する通信は通常ファイアウォールなどで守られている通信であると仮定してもよいのでここでは考えない．したがって，(1) 中継ルーティングエージェント RA_j，(2) R_I，(3) R_r，のそれぞれに関してモニタが知りうる情報について次に詳細を示す．

4.2.1 RA_j をモニタリングしている場合

中継ルーティングエージェント RA_j をモニタリングしているモニタは，RA_j が他のルーティングエージェントからの入力を次のルーティングエージェントへ転送したことを知ることしかできない．また，メッ

セージ $\mathcal{M}$ 内の経路情報を知ることができるが，R_I あるいは R_r を特定することはできない．これは，中継ルーティングエージェントをモニタリングしているモニタは，通常中継ルーティングエージェントが知りうる情報（メッセージ $\mathcal{M}$ 内の環状経路の情報や RA_j がメッセージ $\mathcal{M}$ の中継ルーティングエージェントであるという情報）以外の情報については何ら知ることができないことを示している．

4.2.2 R_I をモニタリングしている場合

R_I がメッセージ $\mathcal{M}$ を送信するとき，モニタは，R_I がメッセージを受信していないのにもかかわらず $\mathcal{M}$ を送信しているということを知ることができる．これにより，モニタには R_I であることが知られてしまう．このとき，モニタが経路の長さ n である経路情報を含むメッセージから R_r を特定する確率は，$1/(n-1)$ である．しかし，R_r から受信者 r を知ることはできない．

4.2.3 R_r をモニタリングしている場合

R_I と同様，R_r に関するすべての送受信メッセージをモニタリングできるとする．R_r は受け取ったメッセージを他の中継ルーティングエージェントと同じように転送するので，モニタはメッセージの入出力からは R_r かどうか判断できない．したがってモニタは“R_r が通信内容 V の匿名通信を受け取った”ことしか知ることができない．

4.3 R_r

ここでは，R_r が単独で攻撃者である場合を考え，R_I を受信メッセージから特定しようとしているものとする．受け取ったメッセージから R_I を特定できる確率は経路上の中継ルーティングエージェントと等しく，$1/(n-1)$ である．これは，R_r ですら R_I を特定することはできないことを示している．

4.4 ルーティングエージェントの結託

この節では，経路上の悪意のあるルーティングエージェントが結託して R_I あるいは R_r を特定しようとする攻撃について議論する．

4.4.1 結託のモデル化

はじめに，この攻撃に関してのモデル化を行う．まず，表記として N_{RA} を存在するルーティングエージェントの総数とし，C_{RA} を N_{RA} のうち結託しているルーティングエージェントの数とする．ただし，C_{RA} には R_I は含まないものと仮定する $(0 < C_{RA} \leq N_{RA}-1)$．$n$ は生成される環状経路の経路長を表す $(2 < n \leq N_{RA})$．また，環状経路は初等的な閉路とする．よって，ルーティングエージェントは同じメッセージを 2 回以上受け取ることはない．

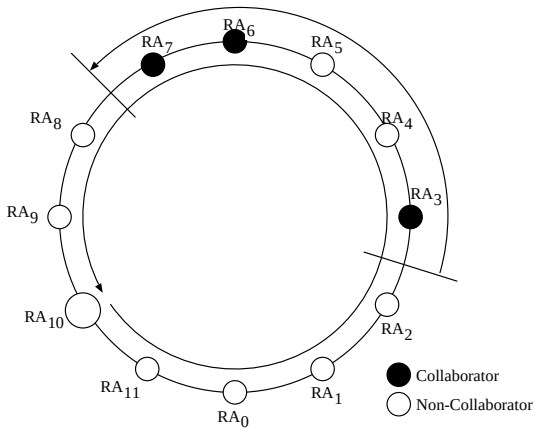

図 3 ルーティングエージェントの結託
Fig. 3 Example of collaboration attack by routing agents.

ここでは，結託ルーティングエージェントどうしが事前にお互いの存在を確認し，メッセージを受け取った経路上の結託ルーティングエージェントは，結託している他のルーティングエージェントが経路上にどのように配置されているかを特定できるものとする．たとえば，**図 3** のように RA_3，RA_6，RA_7 のルーティングエージェントが結託しているとする．この場合，RA_3 がメッセージを受け取ったとき，RA_7 と連絡をとることによって，RA_3 は RA_7 がまだそのメッセージを受け取っていないということを知ることができる．すなわち，RA_3 は R_I からの経路上における最初の結託ルーティングエージェントであり，RA_8，RA_9，RA_{10}，RA_{11}，RA_0，RA_1，RA_2 のうちどれか 1 つが R_I であることを知ることができる．また，Pfitzmann らによって提案された SBNS[9] の環状経路は固定であるので，このような攻撃は特に有効である．

4.4.2 結託攻撃に関する解析

4.4.1 項で述べた結託攻撃のモデルにおいて，結託ルーティングエージェントが R_I を特定できる確率を求める．

定理 1 全ルーティングエージェント（N_{RA}）のうち，C_{RA} 個のルーティングエージェントが結託しているとき，結託ルーティングエージェントが R_I を特定できる確率 $P_2(N_{RA}, C_{RA})$ は以下のようになる：

$$P_2(N_{RA}, C_{RA}) = \frac{C_{RA}}{N_{RA}-1} .$$

証明 全ルーティングエージェント（N_{RA}）から n 個のルーティングエージェントを用いて環状経路を構成するとき，環状経路の種類は，

$$\frac{(N_{RA}-1)!}{(N_{RA}-n)!}$$

である．

（i）環状経路上に結託ルーティングエージェントが 2 つ以上存在するとき

経路上最初と最後の結託ルーティングエージェントで分けられた経路のうち，R_I を含む方に a 個の非結託ルーティングエージェントが並ぶとすると，すべての非結託ルーティングエージェントの中から R_I を含んで a 個に並べる場合の数は，

$$\frac{(N_{RA}-C_{RA})!}{(N_{RA}-C_{RA}-a)!}-\frac{(N_{RA}-1-C_{RA})!}{((N_{RA}-1)-C_{RA}-a)!} = \frac{a(N_{RA}-C_{RA}-1)!}{(N_{RA}-C_{RA}-a)!}$$

通りある．その両端に最初と最後の結託ルーティングエージェントが来るので，それも含めた組合せは，

$$\frac{a(N_{RA}-C_{RA}-1)!}{(N_{RA}-C_{RA}-a)!}C_{RA}(C_{RA}-1)$$

通りとなる．残りの部分は結託しているかしていないかは関係ないので，最終的な経路の並べ方の組合せは，

$$\frac{a(N_{RA}-C_{RA}-1)!}{(N_{RA}-C_{RA}-a)!}C_{RA}(C_{RA}-1)\frac{(N_{RA}-(a+2))!}{(N_{RA}-n)!}$$

通りとなる．

ここで，すべての非結託ルーティングエージェントの総数 $N_{RA}-C_{RA}$ の値によってさらに（i-1）$n-2<N_{RA}-C_{RA}$，（i-2）$N_{RA}-C_{RA}\le n-2$ の 2 つに場合分けをして考える．

（i-1）$n-2<N_{RA}-C_{RA}$ のとき

このとき，経路上に非結託ルーティングエージェントがならぶ数 a は最大 $n-2$ までとることができ，$1\le a\le n-2$ となる．よって，このときの結託攻撃により R_I が特定できる確率 $P_2^{(\mathrm{i}-1)}(N_{RA}, C_{RA})$ は，

$$\begin{aligned}
&P_2^{(\mathrm{i}-1)}(N_{RA}, C_{RA})\\
&= \frac{1}{\frac{(N_{RA}-1)!}{(N_{RA}-n)!}}\sum_{a=1}^{n-2}\left(\frac{a(N_{RA}-C_{RA}-1)!}{(N_{RA}-C_{RA}-a)!}\right.\\
&\quad\left.\times C_{RA}(C_{RA}-1)\,\frac{(N_{RA}-a-2)!}{(N_{RA}-n)!}\,\frac{1}{a}\right)\\
&= \frac{C_{RA}(C_{RA}-1)(N_{RA}-C_{RA}-1)!}{(N_{RA}-1)!}\\
&\quad\times\sum_{a=1}^{n-2}\frac{(N_{RA}-a-2)!}{(N_{RA}-C_{RA}-a)!}\\
&= \frac{C_{RA}}{N_{RA}-1}-\frac{C_{RA}(N_{RA}-C_{RA}-1)!(N_{RA}-n)!}{(N_{RA}-1)!(N_{RA}-C_{RA}-(n-1))!}
\end{aligned}$$

となる．

（i-2）$N_{RA}-C_{RA}\le n-2$ のとき

このとき，a は最大でも $N_{RA}-C_{RA}$ までしかとることができない．すなわち，$1\le a\le N_{RA}-C_{RA}$ になる．よって，このときの結託攻撃により R_I が特定できる確率 $P_2^{(\mathrm{i}-2)}(N_{RA}, C_{RA})$ は，

$$\begin{aligned}
&P_2^{(\mathrm{i}-2)}(N_{RA}, C_{RA})\\
&= \frac{1}{\frac{(N_{RA}-1)!}{(N_{RA}-n)!}}\sum_{a=1}^{N_{RA}-C_{RA}}\left(\frac{a(N_{RA}-C_{RA}-1)!}{(N_{RA}-C_{RA}-a)!}\right.\\
&\quad\left.\times C_{RA}(C_{RA}-1)\frac{(N_{RA}-a-2)!}{(N_{RA}-n)!}\,\frac{1}{a}\right)\\
&= \frac{C_{RA}(C_{RA}-1)(N_{RA}-C_{RA}-1)!}{(N_{RA}-1)!}\\
&\quad\times\sum_{a=1}^{N_{RA}-C_{RA}}\frac{(N_{RA}-a-2)!}{(N_{RA}-C_{RA}-a)!}\\
&= \frac{C_{RA}(C_{RA}-1)(N_{RA}-C_{RA}-1)!}{(N_{RA}-1)!}\\
&\quad\times\frac{(N_{RA}-2)!}{(C_{RA}-1)(N_{RA}-C_{RA}-1)!}\\
&= \frac{C_{RA}}{N_{RA}-1}
\end{aligned}$$

となる．

（ii）環状経路上に結託ルーティングエージェントがただ 1 つ存在するとき

この場合も結託の特別な場合と考えることができる．このとき $a=n-1$ であるから，$n-1\le N_{RA}-C_{RA}$ となる．よって，このときに R_I が特定できる確率 $P_2^{(\mathrm{ii})}(N_{RA}, C_{RA})$ は，

$$\begin{aligned}
&P_2^{(\mathrm{ii})}(N_{RA}, C_{RA})\\
&= \frac{1}{\frac{(N_{RA}-1)!}{(N_{RA}-n)!}}C_{RA}\frac{1}{n-1}\left(\frac{(N_{RA}-C_{RA})!}{(N_{RA}-C_{RA}-(n-1))!}\right.\\
&\quad\left.-\frac{(N_{RA}-1-C_{RA})!}{((N_{RA}-1)-C_{RA}-(n-1))!}\right)\\
&= \frac{C_{RA}(N_{RA}-C_{RA}-1)!(N_{RA}-n)!}{(N_{RA}-1)!(N_{RA}-C_{RA}-(n-1))!}
\end{aligned}$$

となる．

$n-2<N_{RA}-C_{RA}$ は，すなわち $n-1\le N_{RA}-C_{RA}$ を表しているので，$n-2<N_{RA}-C_{RA}$ のときには，環状経路上の結託ルーティングエージェントの数は 1 つ（$P_2^{(\mathrm{ii})}$），または 2 つ以上（$P_2^{(\mathrm{i}-1)}$）の場合がある．一方で，$N_{RA}-C_{RA}\le n-2$ のとき，非結託ルーティングエージェントは必ず 2 つ以上存在するので，非結託ルーティングエージェントが 1 つ存在するというときはない．以上より，

$$\begin{cases}
n-2<N_{RA}-C_{RA}\text{のとき}\\
\quad P_2(N_{RA}, C_{RA})=P_2^{(\mathrm{i}-1)}+P_2^{(\mathrm{ii})}=\dfrac{C_{RA}}{N_{RA}-1}\\
n-2\ge N_{RA}-C_{RA}\text{のとき}\\
\quad P_2(N_{RA}, C_{RA})=P_2^{(\mathrm{i}-2)}=\dfrac{C_{RA}}{N_{RA}-1}
\end{cases}$$

となり，どのような N_{RA}，C_{RA} においても，

表 1 各エンティティが知りうる情報
Table 1 Learnable information at each entity.

攻撃者	攻撃手段	R_I に関して	R_r に関して
中継ルーティングエージェント	結託なし	$1/(n-1)$ で特定可能	$1/(n-1)$ で特定可能
	結託あり	$C_{RA}/(N_{RA}-1)$ で特定可能	返信時 $C_{RA}/(N_{RA}-1)$ で特定可能
モニタ	中継ルーティングエージェントをモニタリング	モニタがモニタリングしているルーティングエージェントは R_I ではないこと	
	R_I をモニタリング	モニタがモニタリングしているルーティングエージェントは R_I であること	
	R_r をモニタリング	モニタがモニタリングしているルーティングエージェントは R_I ではないこと	
R_r	結託なし	$1/(n-1)$ で特定可能	自分が R_r であること
	結託あり	$C_{RA}/(N_{RA}-1)$ で特定可能	自分が R_r であること

$$P_2(N_{RA}, C_{RA}) = \frac{C_{RA}}{N_{RA}-1}$$

である． ■

これが提案手法において往信時の R_I，および返信時の R_r が結託ルーティングエージェントに知られてしまう確率である．定理 1 の結果から，提案手法において経路長 n は結託攻撃を用いて R_I を特定するには何の影響も及ぼさないことが分かる．ここで，今まで議論してきたように，攻撃者としての中継ルーティングエージェントが R_I を特定するための手段としては，(1) 経路情報により確率的に特定するものと，(2) 結託により確率的に特定するものがある．(1) の攻撃が成功する確率は 4.1 節より $1/(n-1)$，(2) の攻撃が成功するのは，定理 1 より $C_{RA}/(N_{RA}-1)$ である．したがって，$1/(n-1) = C_{RA}/(N_{RA}-1)$ が成り立つときの経路長，すなわち，$n = (N_{RA}-1+C_{RA})/C_{RA}$ よりも経路長が短い場合には (1) が成功する確率が (2) よりも高くなり，逆に長い場合は (2) が成功する確率が (1) よりも高くなる．よって，経路長 n は実際の匿名通信の規模とどれだけの結託を許すかによって決定することができる．

4.5 メッセージの改竄

本提案方式において，現段階では環状経路上を流れる通信データに署名などを用いて内容を保証はしていない．したがって，環状経路情報の改竄，E/C フィールドの差し換え，通信内容の改竄といった手法を用いて不正メッセージを生成し，それを経路上のルーティングエージェントに送り，ルーティングエージェントがメッセージをどのように処理するのかを観察することによって R_I や R_r を特定する攻撃が可能である．このような攻撃を用いても，本提案方式が従来持つ安全性のレベル（すなわち，$n/2$ 回の操作による特定が可能）を下げることはない．しかし，このような攻撃を積極的に回避するには，各ルーティングエージェント間において相互認証を行ったり，証明機関を置きメッセージ全体，またはメッセージの構成要素に対して署名を行うとよい．提案方式において，新たに証明機関を導入してもよいし，PDC が証明機関の役目を兼任してもよい．証明機関は経路上のルーティングエージェントに対して受信メッセージの正当性を保証する．

4.6 安全性のまとめ

攻撃者が得た情報で提案方式における R_I，および R_r についての情報をどこまで知ることができるかを，**表 1** にまとめる．ただし，すべての攻撃者はメッセージ（経路情報，E/C フィールド，通信内容）を手に入れることができるとする．

5. 提案方式の運用

本章では，提案方式の運用面に関して，耐故障性，通信コストなどから評価する．

5.1 耐故障性

環状経路上をメッセージが流通する際，何らかの原因でルーティングエージェント間で通信が途切れた場合，そのメッセージはレスポンダのルーティングエージェント R_r に届かない可能性がある．経路長 n のメッセージ送信において，R_I 以外の f 個のルーティングエージェントの無作為な故障を許したとき，メッセージが R_r に届く確率 $P_3(n, f)$ を求めてみる．R_r が故障していない確率は $1 - f/(n-1)$ であり，R_I から R_r に至るまでのルーティングエージェントが故障しない場合を考えればよいので，$P_3(n, f)$ は，

$$P_3(n,f) = \frac{1}{(n-1)!}\sum_{x=0}^{n-f-2}\left(\frac{(n-f-2)!}{(n-f-x-2)!}(n-x-2)! \times \left(1-\frac{f}{n-1}\right)\right)$$

表 2 Crowds と提案方式の変数
Table 2 Parameters of Crowds and our scheme.

Crowds	提案方式
crowd のサイズ N_{jondo}	ルーティングエージェントの総数 N_{RA}
結託している jondo の数 C_{jondo}	結託ルーティングエージェントの数 C_{RA}
I と r の平均距離 $(2-p_f)/(1-p_f)$	R_I と R_r の平均距離 $n/2$

$$= \frac{(n-f-1)!}{(n-1)(n-1)!}\sum_{x=0}^{n-f-2}\frac{(n-x-2)!}{(n-x-2-f)!}$$
$$= \frac{(n-f-1)}{(f+1)(n-1)}$$

である．

故障時の到達確率を高めるためには，1 つのメッセージについて，複数のメッセージを用意しそれらを送信するとよい．ただし，用意する複数メッセージに（宛先が同じ）環状経路を各々について作成した場合，どの経路情報にも R_I および R_r が含まれるので，R_I をモニタリングしている攻撃者が R_I の通信に関する入出力を保存しておくといった攻撃をした場合，メッセージの経路情報を比較することで高い確率で R_r が特定できてしまう．したがって，どのメッセージに対しても，同じ環状経路を用いる．

R_r は 1 つのメッセージについて複数の複製メッセージを受け取ることになるので，それらが同一のメッセージの複製であることを認識できなければならない．このために，通信内容 V に対する ID（VID）を新たに導入する．そして，複製メッセージを作るたびに CID を新たに割り当てるが，VID は変更しないようにする．こうして，R_r は複数の複製メッセージを受け取ってもそれらが同一のメッセージの複製であると認識できる．ここで，攻撃者が通信内容 V によってメッセージの複製を入手し，それらによってメッセージの宛先を推定することができる状況も可能性としては考えられるが，これは E/C フィールドに添付する暗号メッセージの中に対称鍵暗号のセッション鍵を入れておき，それを用いて暗号化してやればよい．

5.2 通信コスト

変更（署名）提案方式では経路長 n の環状経路を用いているので，I から R まで匿名で V を伝えるのに，環状経路上で n 回，$I \to R_I$ で 1 回，$R_r \to R$ で 1 回，PDC との通信で 2 回，最低計 $n+4$ 回の通信が必要になる．通信保守のために，同じメッセージを d 回送るとすると，最大 $dn+4$ 回の通信が必要になる．

提案方式におけるメッセージ長はルーティングエージェント（ID_{RA}）のアドレス長を A bits，公開鍵暗号の鍵長を 1024 bits とし，その暗号文を 1024 bits とすると，メッセージの大きさは，An+1024+$|V|$ bits となる．このうち，冗長となる部分は A$(n-1)$+1024 bits となる．

また，提案方式で用いている環状経路は初等的な閉路であり，経路構成要素 n の環状経路を生成したとき，その経路上のどの部分にも等しく R_I，R_r が存在する可能性がある．したがって，R_I から R_r までの平均遅延は $n/2$ となり，実際の通信における，即応性（メッセージを送信してから返信を受け取るまでの遅延）という点で見れば一対一通信の，平均 n 倍程度の遅延である．

6. Crowds との比較

ここで，Crowds[11]において，jondo の結託によりイニシエータの jondo が知られてしまう確率と，提案方式においてルーティングエージェントの結託により R_I が知られてしまう確率を比較する．

Crowds において，crowd のメンバが結託によりイニシエータの jondo が知られてしまう確率 $P_1(N_{jondo}, C_{jondo})$ は，2 章で述べたとおり，

$$P_1(N_{jondo}, C_{jondo}) = \frac{N_{jondo} - p_f(N_{jondo} - C_{jondo} - 1)}{N_{jondo}}$$

で与えられる[11]．

ここで，比較に際して，表記の対応づけは**表 2** のとおりである．

このとき，

$$N_{jondo} = N_{RA} = N,\ C_{jondo} = C_{RA} = C$$

として結託攻撃に関する比較を行うと，

$$P_1(N, C) - P_2(N, C) = \frac{N(N-C-1) - p_f(N-C-1)(N-1)}{N(N-1)}$$
$$= \frac{(N-C-1)(N-p_f(N-1))}{N(N-1)} > 0$$

となる．よって，提案方式におけるイニシエータの匿名性は Crowds よりもつねに高いといえる．

次に，提案方式における平均距離 $l_2 = n/2$ と Crowds における平均距離（平均経路長）$l_1 = (2-p_f)/(1-p_f)$ を比較すると，

表 3 Crowds との比較
Table 3 Comparing the proposed scheme with Crowds.

	(1)	(2)	(3)
Crowds	$1/(N_{jondo}-1)$	1	$(N_{jondo}-p_f(N_{jondo}-C_{jondo}-1))/N_{jondo}$
提案方式	$1/(n-1)$	$1/(n-1)$	$C_{RA}/(N_{RA}-1)$

$$\begin{cases} l_1 < l_2 & \left(\text{if } \dfrac{1}{2} < p_f < \dfrac{n-4}{n-2}\right) \\ l_1 \geq l_2 & \left(\text{if } \dfrac{n-4}{n-2} \leq p_f \leq 1\right) \end{cases}$$

という結果を得る．つまり，n（提案方式で経路長）をある値に設定したとき，Crowds において設定する転送確率 p_f の値によっては，イニシエータとレスポンダの平均距離で提案方式の方が有利であることが分かる．p_f は，crowd メンバがイニシエータの jondo を特定するのを困難にするためのパラメータであるので，crowd メンバに対するイニシエータの匿名性を向上させるには，大きな値をとる必要がある．それにともなって，Crowds の平均経路長は増す．

次に，Crowds と提案方式の安全性における比較を**表 3** に示す．表 3 において，以下の 3 つの項目について比較を行った．

(1) 経路上の中継ノードが R_I（または jondo）を特定できる確率
(2) 経路上の中継ノードが R_r（またはエンドサーバ）を特定できる確率
(3) 経路上の結託中継ノードにより R_I（または jondo）を特定できる確率

ただし，比較の条件をそろえるため，以下の条件設定を行った．

(1) 中継ノード間で結託がないときの，中継ノードが R_I（または jondo）を知る確率を比較した．
(2) (1) と同様の条件で，中継ノードが R_r（または jondo）を知る確率を比較した．
(3) 経路上の中継ノードが c 個結託した場合に，結託ノードが R_I（または jondo）を知る確率を比較した．

表 3 から，提案方式は Crowds において提供されているイニシエータの jondo の匿名性を上回る匿名性を持ちつつ，レスポンダの匿名性も確保していることが分かる．これは，ネットワーク上で通信が行われていることは分かるが，いったい誰と誰がその通信をしているのか確率的にしか特定できないということなので，提案方式で提供できる匿名性が強いことを示している．

7. 結　　論

本論文では，環状経路には始点と終点が存在しないという性質に着目し，メッセージの送信者と受信者の特定を困難にする方式を提案した．さらに，その安全性と運用に関して評価した．その結果，Crowds で提案されていた方式よりも，経路上の結託者に対する安全性は，提案方式の方がつねに高く，イニシエータとレスポンダの平均距離に関しては，提案方式の方が効率的にできる場合があることを示した．また，環状経路の運用に関してはメッセージの到達確率について議論し，提案方式の故障に対する耐故障性について評価した．

参 考 文 献

1) Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).
2) Cheswick, W.R. and Bellovin, S.M.: *Firewalls and Internet Security*, Addison-Wesley (1995).
3) 堀部政男：プライバシーと高度情報化社会，岩波新書 (1998).
4) 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研究報告（ISEC-99-29）.
5) Kikuchi, H.: Sender and Recipient Anonymous Communication without Public Key Cryptography, 情報処理学会研究報告（98-CSEC-1-8）(1998).
6) 古林　隆，伊理正夫：ネットワーク理論，日科技連出版社 (1976).
7) Luotonen, A. and Altis, K.: World-Wide Web Proxies, *Computer Networks and ISDN Systems*, Vol.27, No.2, pp.147–154 (1994).
8) 長野　悟，北澤繁樹，双紙正和，宮地充子：環状経路を用いた匿名性と位置情報プライバシの保護，コンピュータセキュリティシンポジウム（*CSS99*），pp.37–42 (1999).
9) Pfitzmann, A.: A switched/broadcast ISDN to decrease user observability, *Proc. 1984 International Zurich Seminar on Digital Communications, Applications of Coding, Channel Coding and Secrecy Coding*, pp.183–190 (1984).
10) Pfitzmann, A., Pfitzmann, B. and Waidner, M.: ISDN-MIXes: Untraceable Communication with Very Small Bandwidth Overhead, *Proc. IFIP/Sec '91*, pp.245–258 (1991).
11) Reiter, M.K. and Rubin, A.D.: Crowds: Anonymity for Web Transactions, *ACM Trans. Info. Syst. Security*, Vol.1, No.1, pp.66–92

(1998).
12) Reiter, M.K. and Rubin, A.D.: Anonymous Web Transactions with Crowds, *Comm. ACM*, Vol.42, No.2, pp.32–38 (1999).
13) 妹尾健史，菊池浩明，藤岡　淳，中西祥八朗：インターネット上の匿名通信路方式の評価，*SCIS98-3.3.E* (1998).
14) Stevens, W.R.: TCP/IP Illustrated, *The Protocols*, Vol.1, Addison-Wesley (1997).
15) Syberson, P.F., Coldschlag, D.M. and Reed, M.G.: Anonymous Connections and Onion Routing, *IEEE Symposium on Security and Privacy*, pp.44–54 (1997).
16) Tanenbaum, A.S.: *Computer Networks*, 3rd edition, Prentice-Hall (1996).
17) Tanenbaum, A.S.: *Distributed Operating System*, Prentice-Hall (1995).

(平成 11 年 11 月 30 日受付)
(平成 12 年 6 月 1 日採録)

北澤　繁樹（学生会員）

1996 年電気通信大学電気通信学部電子物性工学科卒業．1998 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年北陸先端科学技術大学院大学情報科学研究科博士後期課程進学後，エージェントを用いたセキュリティシステムおよびモバイルエージェントのセキュリティ等に興味を持つ．

長野　悟

1998 年法政大学工学部経営工学科卒業．2000 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．同年 NTT アドバンステクノロジ（株）入社．通信における送受信者のプライバシ保護に興味を持つ．

双紙　正和（正会員）

1993 年 3 月東京大学大学院理学系研究科情報科学専攻修了．電気通信大学大学院情報システム学研究科博士後期課程，同研究科助手を経て，1999 年 4 月から現在まで，北陸先端科学技術大学院大学情報科学研究科助手．セキュリティモデル，アクセス制御，分散システムの研究に従事．博士（工学）．

宮地　充子（正会員）

1988 年大阪大学理学部数学科卒業．1990 年同大学院修士課程修了．同年，松下電器産業（株）入社．1998 年北陸先端科学技術大学院大学情報科学研究科助教授．現在に至る．情報セキュリティの研究に従事．博士（理学）．SCIS93 若手論文賞，科学技術庁注目発明賞各受賞．電子情報通信学会会員．