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

2006－CSEC－34 (53)
2006／7／21

多重暗号化と確率的動作選択に基づく匿名通信方式：3MN

三宅 直貴† 伊藤 義道† 馬場口 登†

† 大阪大学工学部 〒565-0871 大阪府吹田市山田丘2-1
E-mail: †miyake@nanase.comm.eng.osaka-u.ac.jp, ††{ito,babaguchi}@comm.eng.osaka-u.ac.jp

あらまし プライバシー保護のため通信者を秘匿にする匿名通信方式は，Onion Routing や Crowds 等，数多く提案されている．多重暗号化を行う Onion Routing では，送受信者双方の匿名性を保持できるが，暗号化・復号化処理の回数が多いという問題がある．また，メッセージを他の中継ノードに中継させるかどうかを確率に基づき選択する Crowds では，通信に要する負荷は小さいが，受信者の匿名性に問題がある．本稿では，確率的動作選択と多重暗号化方式を併用することで，少ない暗号化・復号化処理回数で送受信者双方の匿名性を保持できる新たな匿名通信方式 3MN（3-Mode Net）を提案する．

キーワード プライバシー保護，匿名通信，多重暗号化，Crowds, Onion Routing

3MN: An Anonymous Communication System Based on Multiple Encryption and Probabilistic Selections of Actions

Naoki MIYAKE†, Yoshimichi ITO†, and Noboru BABAGUCHI†

† Faculty of Engineering, Osaka University Yamadaoka 2-1, Suita-shi, 565-0871 Japan
E-mail: †miyake@nanase.comm.eng.osaka-u.ac.jp, ††{ito,babaguchi}@comm.eng.osaka-u.ac.jp

Abstract This paper proposes a new anonymous communication system called 3MN (3-Mode Net). The system can be regarded as an extension of the Crowds-based anonymous communication system where each node in the communication path decides its action by probability; whether the node sends a message to the proper recipient, or to another node. In addition to these two actions, 3MN can choose the third action, that is, to encrypt the whole data set and to rewrite the temporal destination. By adding the third action, we can show that 3MN preserves the anonymity of the proper recipient, and reduces the load for encryption and decryption compared to the Onion-based anonymous communication system.

Key words Privacy Protection, Anonymous Communication, Multiple Encryption, Crowds, Onion Routing

1. はじめに

現在，数多くのサービスがインターネットを介して提供されており，インターネット上でのプライバシー保護に関する問題が注目を集めている．個人情報漏洩を防ぐため，クレジットカード番号や氏名，住所といった個人にとって重要な情報は，Secure Socket Layer（SSL）などのセキュリティ技術を用いて暗号化されていることがほとんどである．したがって，通信データの内容に関しては，暗号化することにより秘匿することが可能である．しかし，IP パケットのヘッダには送信元，および送信先の IP アドレスが含まれているため，通信を行っている送信者，および受信者の IP アドレスを秘匿にすることはできない．そのため，現在の標準化されている通信システムでは送受信者の特定が可能であり，他の電子メールなどの情報と関連が付き，その結果，それらの情報をもとに個人を特定する氏名や職業，または住所などが他人に公開されるといったように，個人のプライバシーが守られない可能性がある．

これらを背景に，通信の送信者を秘匿にしつつ通信を行うことで個人のプライバシーを保護する匿名通信方式は，数多く提案されている[1]～[3]．匿名通信方式を用いると，通信データの内容と通信を行っている送信者，および受信者の IP アドレスとの結びつきがわからなくなるため，電子投票や，匿名での WEB アクセス，メッセージ送信などに利用されている．

匿名通信方式のひとつである Crowds [4], [5] は，送信メッセージを Crowds のメンバにランダムに中継することで送信者の匿名性を保持するが，中継したメンバ全員に最終的な受信者が公開されるという問題がある．また，別の匿名通信方式である Mix-Net [6], [7] は，複数の送信者が中継するサーバの公開

鍵により送信メッセージを多重暗号化してサーバへ送り，サーバが多重暗号化された複数のメッセージを復号化し，メッセージの順序を入れ替えることで送受信者双方の匿名性を保持する．しかし，それにともなう暗号化・復号化処理の回数が多いといった問題や，経路が固定されているため攻撃の対象になりやすいといった問題がある．Onion Routing [8], [9] は，経路上にある全ノードの暗号鍵により送信メッセージを多重暗号化することで送受信者双方の匿名性を保持するが，Mix-Net と同様，それにともなう暗号化・復号化処理の回数が多いという問題がある．

本稿では，送受信者双方の匿名性を保持し，かつ暗号化・復号化処理の回数が少ない新たな匿名通信方式である 3MN (3-Mode Net) を提案し，その数学モデルを導出する．また，従来の匿名通信方式である Crowds，および Onion Routing との比較を，理論値，およびシミュレーションの両方から行う．

以下に本稿の構成を示す．第 2 節では，従来の匿名通信方式である Crowds や Onion Routing の仕組みと，その利点および欠点を述べる．第 3 節では，本稿で提案する 3MN の動作について述べる．第 4 節では，3MN の数学モデルを導く．第 5 節では，理論値，およびシミュレーション結果から，3MN を評価する．第 6 節では，本稿をまとめ，今後の展開について述べる．

2. 従来の匿名通信方式

一般に匿名通信においては，メッセージ送信者から最終的な受信者への通信は複数の中継ノードを介して行われる．その際，中継ノード間で送られる情報はデータと中継ノードが次に送るべき相手の宛先である．本稿では，これらデータと宛先の 2 つをまとめたものをデータセットとよぶ．以下 2 節では，すでに提案されている匿名通信方式である Crowds と Onion Routing を紹介し，それらの利点および欠点を述べる．

2.1 Crowds

Crowds では，送信者 S が最終的な受信者 R を宛先としたデータセットを Crowds のメンバに送り，データセットを受け取ったメンバは，図 1 のように受信者 R に送るか別のメンバに送るかを確率的に決定する．最終的な受信者に送るかどうかの選択とデータセットの転送は，受信者 R に届くまで続けられる．

次に，Crowds の動作例を図 2 に示す．図 2 の例では，送信者 S はメンバの一人である A に，宛先を最終的な受信者 R としたデータセットを送る．データセットを受け取った A が，別のメンバに送ることを選択したとすると，メンバの一人である B に宛先を受信者 R としたデータセットを送る．同様に，データセットを受け取った B が，別のメンバに送ることを選択したとすると，メンバの一人である C に宛先を受信者 R としたデータセットを送る．ここで，データセットを受け取った C が，受信者 R に送ることを選択した場合，R にデータセット内のメッセージを送って通信が完了する．

Crowds において，送信者 S からデータセットを受け取ったメンバは，ノード S がメッセージ送信者であるのか，中継メンバであるのか区別できないため，送信者 S の匿名性を保持できる．また，Crowds は多重暗号化処理を行わないことから，処理が軽快であるといった利点を持つ．しかし，最終的な受信者が，データセットを中継するメンバ全員に対して公開されるため，最終的な受信者の匿名性は失われるといった欠点をもつ．

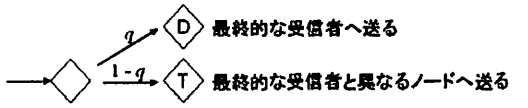

図 1 メンバの行動

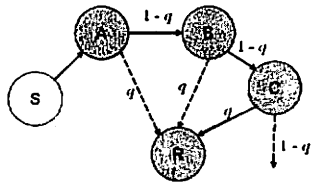

図 2 Crowds の動作例

2.2 Onion Routing

Onion Routing は，メッセージ送信者が最終的な受信者までの経路情報をあらかじめ定め，経路上のノードそれぞれに別々の共通鍵を配送し，それをもとに送信メッセージを多重暗号化した後，経路上にある複数の中継ノードを介して最終的な受信者にメッセージを送る匿名通信方式である．

Onion Routing は共通鍵を配送するステージと，メッセージを配送するステージの 2 つからなる．送信者 S が最終的な受信者 R にメッセージを送る際，中継ノードとして，A，B を選んだ場合，Onion Routing は以下のように動作する．

まず，共通鍵配送ステージにおいて，S は以下の手順に基づき，A，B，R へ，それぞれ S との共通鍵 K_A，K_B，K_R を送る（図 3 参照．ただし，(X, K_Y) は，次の宛先が X であるという情報と，共通鍵 K_Y の情報を含んでいることを意味する）．

(1) 共通鍵 K_R を R の公開鍵 P_R で暗号化し，宛先を R としたデータセットを作成する．

(2) (1) で作成したデータセットに共通鍵 K_B を付け加え，これらをまとめて B の公開鍵 P_B で暗号化する．このデータに対する宛先を B としたデータセットを作成する．

(3) (2) で作成したデータセットに共通鍵 K_A を付け加え，これらをまとめて A の公開鍵 P_A で暗号化する．このデータに対する宛先を A としたデータセットを作成する．

S はこうして作成したデータセットを A へ送信する．A は受け取ったデータセットを自身の秘密鍵で復号化することで，B の公開鍵 P_B で暗号化されたデータと共通鍵 K_A を得るとともに，次の宛先が B であることを知る．A はその暗号化データを B に送信し，B は受け取った暗号化データを自身の秘密鍵で復号化することで，R の公開鍵 P_R で暗号化されたデータと共通鍵 K_B を得るとともに，次の宛先が R であることを知る．B はその暗号化データを R へ送信し，R は受け取ったデータを復号化することで共通鍵 K_R を得ることができる．また，S から R までの経路上の中継ノードはメッセージ送信のため，一定期間，前後のノードとの接続を維持しておく．

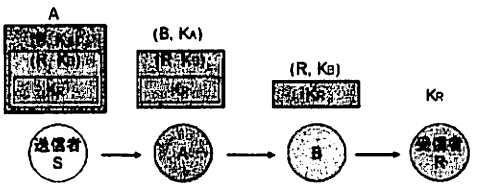

図 3　Onion Routing の経路設定と共通鍵の配送例

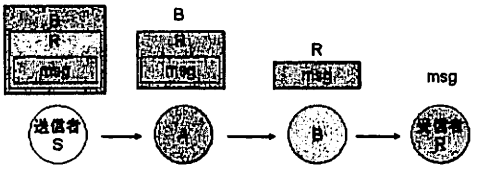

図 4　Onion Routing のメッセージ送信例

メッセージ配送ステージでは，S はこれらの共通鍵を用いてメッセージを多重暗号化する（図 4 参照．ただし，メッセージを msg と表記する）．

(1)　メッセージを R の共通鍵 K_R で暗号化し，そのメッセージの宛先を R としたデータセットを作成する．

(2)　(1) で作成したデータセットを B の共通鍵 K_B で暗号化し，その宛先を B としたデータセットを作成する．

(3)　(2) で作成したデータセットを A の共通鍵 K_A で暗号化する．

こうして作成された多重暗号化データを S は A に送信する．A は受け取ったデータセットを，既に受け取っている共通鍵 K_A で復号化することで，B の共通鍵 K_B で暗号化されたデータを得るとともに，次の宛先が B であることを知る．A はその暗号化データを B に送信し，B は受け取った暗号化データを共通鍵 K_B で復号化することで，R の共通鍵 K_R で暗号化されたデータを得るとともに，次の宛先が R であることを知る．B はその暗号化データを R へ送信し，R は受け取ったデータを復号化することで S からのメッセージを得ることができる．

データセットを受け取った中継ノードは自ノードの前後のノードの情報しか得られず，データセットを送信したノードが送信者であるのか，また，次のノードが最終的な受信者であるのか判別できないため，送受信者の匿名性を保持できるといった利点をもつ．しかし，多重暗号化処理や復号化処理のため，各ノードの負荷が大きいという欠点を持つ．

3.　匿名通信方式 3MN

従来の匿名通信システムでは，最終的な受信者の匿名性保持と多重暗号化によるノード負荷の低減を両立することは困難であった．本節ではこの問題を解決する 3MN の動作を説明する．

3.1　概　　要

Crowds はデータセットの宛先が常に最終的な受信者であるため，メッセージを中継するメンバ全員に最終的な受信者が公開されてしまうという欠点があった．これに対し，3MN では 2 節で説明した Crowds の 2 つの選択肢に加え，宛先以外のノードの暗号鍵で暗号化した後，そのノードを宛先としたデータセットを新たに作成し，異なるノードへ送るという選択肢も加える．したがって，中継ノードは図 5 のように 3 つの選択肢から行動を選択することになる．この操作を加えることで中継ノードは，宛先が最終的な受信者であるかどうかの区別ができなくなるため，最終的な受信者の匿名性を保持できる．また，送信者 S からメッセージを受け取った中継ノードは，Crowds と同様に S がメッセージの送信者であるのか，単に中継ノードであるのかを区別できないため，送信者の匿名性も保持できる．

以下では，共通鍵 K_X でデータセットを暗号化し，その共通鍵 K_X をノード X の公開鍵 P_X で暗号化することを，暗号鍵 K_X，P_X によりデータセットを暗号化するという．また，ノード X の公開鍵 P_X で暗号化された共通鍵 K_X を K'_X と表記する．これに対し，暗号化された共通鍵 K'_X をノード X の秘密鍵 S_X で復号化し，得られた共通鍵 K_X でデータセットを復号化することを，復号鍵 K_X，S_X によりデータセットを復号化するという．

3.2　メッセージ送信者の動作

送信者 S は，R への送信メッセージを R の暗号鍵 K_R，P_R によって暗号化し（すなわち，送信メッセージを共通鍵 K_R で暗号化し，共通鍵 K_R を公開鍵 P_R で暗号化する），受信者 R を宛先としたデータセットを作成する．さらに，作成されたデータセットを任意に選んだノード（図 6 ではノード A）の暗号鍵で暗号化し，そのノードを宛先としたデータセットを作成する．このようにして作成したデータセットを，データセットの宛先とは異なるノード（図 6 ではノード B）に転送する．

3.3　中継ノードの動作

中継ノードは，受け取ったデータセットの宛先が自ノードであるかどうかの確認を行う．データセットの宛先が自ノードである場合，暗号化されている共通鍵を自身の秘密鍵で復号化し，その共通鍵を用いて暗号化データを復号化する．こうして，受信時とは異なる新たな宛先と暗号化データからなるデータセットを得た後，次のステップに進む．一方，データセットの宛先が自ノードでない場合は，宛先と暗号化データをそのままにして次のステップに進む．

次のステップでは，データセットに対する暗号化処理の有無や転送先決定という行動の選択を行う．行動には図 5 のように，宛先にデータセットを転送する D-Mode，宛先と異なるノードに転送する T-Mode，および宛先と異なるノードの暗号鍵で暗号化し，他のノードに転送する E-Mode の 3 通りが存在する．中継ノードは行動として，確率 m で D-Mode，確率 e で T-Mode，確率 p で E-Mode を選択するものとする（ただし，$m+e+p=1$）．

3.4　3MN の動作例

図 6 を用いて 3MN の動作例を示す．ただし，図 6 における msg は送信メッセージを意味する．また，図 6 において，宛先とともにデータセットに付加される共通鍵については，宛先のノードの公開鍵で暗号化されていることに注意する．データセット内での四角の枠は，共通鍵により暗号化されていることを意味している．

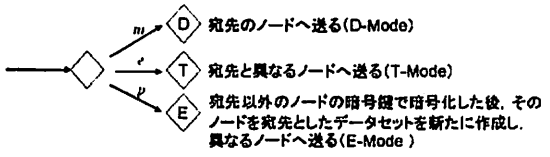

図 5　中継ノードの行動

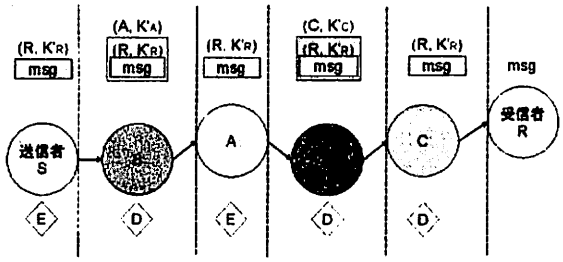

図 6　3MN の動作例

送信者 S は，送信メッセージを共通鍵 K_R で暗号化したデータと，データセットの暗号化に使用した共通鍵 K_R を R の公開鍵 P_R で暗号化した K'_R とともに，受信者 R を宛先としたデータセットを作成する．

送信者 S はデータの送信時には必ず E-Mode を選択するものとし，任意に選んだ中継ノード A の暗号鍵 K_A，P_A を用いて，宛先を A としたデータセットを作成した後，B へ転送する．B は宛先が自ノードでないことを確認した後，D-Mode を選択したとする．この場合，B はデータセットを宛先である A へ転送する．ノード A は，受け取ったデータセットの宛先が自ノードであるため，復号鍵 S_A，K_A を用いてデータセットを復号化する．こうして，A は宛先が R である新たなデータセットを得る．その後，E-Mode を選択したとすると，R とは異なる C を宛先とし，その暗号鍵 K_C，P_C で暗号化したデータセットを作成し，宛先 C とは異なるノード F へ転送する．このように復号化処理と行動の選択，および転送を繰り返し，最終的に R のもとへ転送される．R は宛先が自ノードであるため共通鍵 K_R を得た後，データセットを復号化する．これにより多重暗号化されていた暗号化データの復号化処理が全て終わり，受信者 R は送信メッセージを得ることができる．

4.　3MN のモデル化

3.3 節の説明からわかるとおり，3MN では D-Mode，T-Mode，E-Mode を選択すると，暗号化の多重度は，それぞれ，1 つ減った状態，変化しない状態，1 つ増えた状態へと遷移する．このことに着目すると，データセットの多重度を状態に選ぶことで，3MN の振る舞いをマルコフモデル [10] に帰着させることができる．

本節では状態遷移図から状態遷移行列を求め，全中継ノード数，および暗号化処理回数の期待値を導く．その際，メッセージの通過したノード数（送信者・最終的な受信者・現在のノードは含まない）を s とおく．また，多重度は各ノードにおいて，データセットを復号化できる場合は復号化した直後，すなわち，

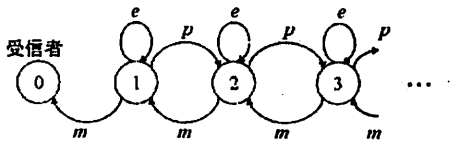

図 7　状態遷移図

行動の選択を行う直前の多重度とする．

4.1　遷移確率行列の導出

最終的な受信者にメッセージが届いた状態，すなわち多重度が 0 のときは同じ状態を維持し続ける．多重度が 1 以上のときは，確率 m で D-Mode，確率 e で T-Mode，確率 p で E-Mode を選択し，D-Mode，T-Mode，E-Mode を選択すると，暗号化の多重度は，それぞれ，1 つ減った状態，変化しない状態，1 つ増えた状態へと遷移する．このように状態が遷移する状態遷移図を図 7 に示す．以上から遷移確率行列 P は

$$P = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots \\ m & e & p & & & & \\ 0 & m & e & \ddots & & & \\ \vdots & & \ddots & \ddots & \ddots & & \\ 0 & & & \ddots & e & p & \\ 0 & & & & m & e & \ddots \\ \vdots & & & & & \ddots & \ddots \end{bmatrix}$$

となる．ただし，ij 成分は多重度 $i-1$ から多重度 $j-1$ に遷移する確率を表す．

4.2　全中継ノード数，および暗号化処理回数の期待値

メッセージの通過したノード数が s であるときの多重度についての状態分布を行ベクトル π_s で表す．ただし，状態分布 π_s の i 番目成分 $\pi_s(i)$ は，多重度が $i-1$ である確率を表す．このとき，状態遷移は

$$\pi_{s+1} = \pi_s P$$

と表現できる．送信時には送信者は必ず多重度 2 で暗号化することを考慮すると，初期状態分布 π_0 は $\pi_0 = (0\ 0\ 1\ 0\ \dots\ 0)$ となり

$$\pi_{s+1} = \pi_0 P^s$$

を得る．

以下本節では，以上に述べたモデルに基づき，全中継ノード数の期待値 Ep，暗号化処理回数の期待値 Ee，および宛先が最終的な受信者と一致するノード数の期待値 Er を導く．

メッセージの通過したノード数が s となる時点で最終的な受信者にメッセージが届いている確率，すなわち多重度が 0 である確率は $\pi_s(1)$ である．このことからメッセージが届くまでに通過したノード数が s となる確率 r_s は

$$r_s = \pi_s(1) - \pi_{s-1}(1)$$

となる．ここで，$0 \leqq p < m$ であれば，メッセージはいずれ最終的な受信者に届くため，

$$\lim_{l \to \infty} \pi_l(1) = 1$$

である．これらのことから，$0 \leqq p < m$ という条件下で全中継ノード数の期待値 Ep は

$$\begin{aligned} \mathrm{Ep} &= \sum_{s=1}^{\infty} s \cdot r_s \\ &= 1 \cdot \{\pi_1(1) - \pi_0(1)\} + 2 \cdot \{\pi_2(1) - \pi_1(1)\} + \cdots \\ &= \lim_{l \to \infty} \left(l\pi_l(1) - \sum_{s=0}^{l-1} \pi_s(1) \right) \\ &= \sum_{s=0}^{\infty} \{1 - \pi_s(1)\} \end{aligned}$$

となる．

次に，共通鍵による暗号化処理回数について考える．暗号化処理は，初めに送信者によって 2 回行われ，その後，最終的な受信者にメッセージが届くまで，確率 p で行われる．よって，暗号化処理回数の期待値 Ee は

$$\begin{aligned} \mathrm{Ee} &= 2 + p \cdot \sum_{s=0}^{\infty} \{1 - \pi_s(1)\} \\ &= 2 + p \cdot \mathrm{Ep} \end{aligned}$$

となる．一方，復号化処理回数は暗号化処理回数と必ず一致するため，それぞれの期待値は同じ値をとる．復号化処理は，最終的な受信者にメッセージが届くまで，確率 m で行われることから

$$\mathrm{Ee} = m \cdot \mathrm{Ep}$$

と表すこともできる．以上から，

$$\begin{aligned} \mathrm{Ee} &= 2 + p \cdot \mathrm{Ep} \\ &= m \cdot \mathrm{Ep} \end{aligned}$$

となり，$\mathrm{Ep} = 2/(m-p)$，$\mathrm{Ee} = 2m/(m-p)$ を得る．

次に，宛先が最終的な受信者と一致するノード数の期待値 Er を求める．受け取ったデータセットの宛先が最終的な受信者と一致するのは多重度が 1 となるときである．よって Er は

$$\mathrm{Er} = \sum_{s=1}^{\infty} \pi_s(2)$$

となる．ところで，メッセージの通過したノード数が $s-1$ のときに，多重度が 1 である状態から D-Mode を選択して多重度が 0 となる確率と，全中継ノード数が s である確率 r_s は等しいため，r_s は

$$r_s = m\pi_{s-1}(2)$$

と表すこともできる．これより，

$$\begin{aligned} \mathrm{Er} &= \lim_{l \to \infty} \sum_{s=1}^{l} \frac{1}{m} \cdot \{\pi_{s+1}(1) - \pi_s(1)\} \\ &= \frac{1}{m} \end{aligned}$$

を得る．

表 1　3MN と他の匿名通信方式の理論値

	3MN	Crowds	Onion Routing
Ep	$2/(m-p)$	$1/q$	N
Ee	$2m/(m-p)$	0	$N+1$
Er	$1/m$	$1/q$	1

5. 他の匿名通信方式との比較，および評価

5.1 理論値での比較

本節では 3MN と Crowds，および Onion Routing を，前節で求めた理論値に基づいて比較し，3MN の特徴について考察する．ただし，比較の際は 3MN における全中継ノード数の期待値が Crowds，および Onion Routing における全中継ノード数と等しいと仮定し，その際の暗号化処理回数の期待値や宛先が受信者となる回数の期待値を比較する．

3MN，Crowds，Onion Routing における，全中継ノード数の期待値 Ep，暗号化処理回数の期待値 Ee，データセットの宛先が最終的な受信者と一致する中継ノード数の期待値 Er を，表 1 に示す．ここで，表 1 での m, p はそれぞれ，3MN における D-Mode を選択する確率，E-Mode を選択する確率である．また，N は Onion Routing における全中継ノード数，q は Crowds における最終的な受信者に送る確率である．

表 1 において，全中継ノード数の期待値 Ep を全て N とした場合，Onion Routing における，暗号化処理回数の期待値 Ee は $N+1$，3MN での暗号化処理回数の期待値 Ee は $m \cdot N$ となる．$1 > m > 0$ であるため，3MN は Onion Routing よりも暗号化処理の回数が少ないという利点を有することがわかる．暗号化処理回数と復号化処理回数は等しいことから，復号化処理の回数についても同じことがいえる．また，メッセージ送信者が行う暗号化処理回数においては，Onion Routing では $N+1$，3MN では 2 であり，3MN は Onion Routing よりも送信者の負荷が小さいことがわかる．

次に，最終的な受信者が特定されるリスクについて考える．比較のため全中継ノード数の期待値 Ep を全て $2/(m-p)$ とした場合，3MN におけるデータセットの宛先が最終的な受信者と一致する中継ノード数の期待値 Er は $1/m$ であり，Onion Routing におけるデータセットの宛先が最終的な受信者と一致する中継ノード数 Er は，最終的なメッセージ受信者の直前のノード 1 つのみである．3MN におけるデータセットの宛先が最終的な受信者と一致する中継ノード数 Er は Onion Routing の 1 よりも大きな値をとることから，最終的な受信者が特定されるリスクは Onion Routing の方が低いと考えられる．また，最終的な受信者が特定されてしまう Crowds においては，Er は Ep と同じ $2/(m-p)$ である．一方，3MN の Er は $1/m$ であり，$1 > p \geqq 0$ から，$2/(m-p)$ の半分以下の値であることがわかる．そのため，3MN において最終的な受信者が特定されるには至らないと考えられる．

また，送信者が特定されるリスクについては，3MN，Crowds，Onion Routing ともに，送信者から直接メッセージを受け取るノード数は 1 なので，送信者が特定されるリスクは変わらない

表 2　シミュレーションによる他の匿名通信方式との比較

	3MN		Crowds	Onion Routing
	実験値	理論値	理論値	理論値
Ep	20.07	20.00	20.00	20.00
Ee	6.01	6.00	0.00	21.00
Er	3.33	3.33	20.00	1.00

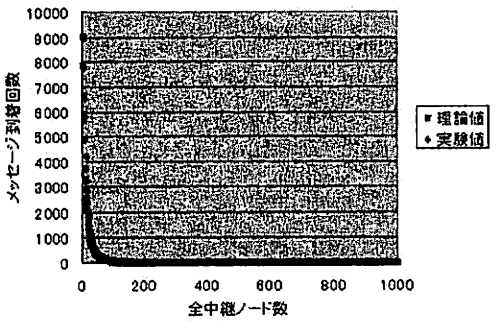

図 8　全中継ノード数に対するメッセージ到着回数の分布（$m = 0.3$, $e = 0.5$, $p = 0.2$ シミュレーション回数 10 万回）

と考えられる．

5.2　シミュレーション結果

$m = 0.3$, $e = 0.5$, $p = 0.2$ としてシミュレーションを 10 万回行った．シミュレーションから得られた全中継ノード数の期待値 Ep，暗号化処理回数の期待値 Ee，およびデータセットの宛先が最終的な受信者と一致する中継ノード数の期待値 Er の実験値を理論値とともに表 2 に示す．また，比較のため，全中継ノード数の期待値を，3MN の全中継ノード数の期待値である 20.00 とした場合の，Crowds，および Onion Routing のそれぞれの値も表 2 に示す．その際の 3MN の全中継ノードにおけるメッセージ到着回数の分布を図 8 に示す．

表 2 より，3MN における全中継ノード数の期待値 Ep，暗号化処理回数の期待値 Ee，およびデータセットの宛先が最終的な受信者と一致する中継ノード数の期待値 Er において，実験値は理論値にほぼ一致していることがわかる．

また，3MN の暗号化処理回数の期待値は Onion Routing に比べ 1/3 程度であることがわかる．3MN のデータセットの宛先が最終的な受信者と一致する中継ノード数については，Onion Routing の 3 倍以上であるが，Crowds と比べると 1/6 の値であることがわかる．以上から，3MN は，暗号化処理回数については Onion Routing よりも小さく，データセットの宛先が最終的な受信者と一致する中継ノード数は Crowds よりも小さいことがわかる．

また，図 8 より，理論値と実験値とのメッセージ到着回数の分布は非常に似ていることがわかる．メッセージ到着回数の分布において理論値と実験値の適合度検定を行うため，カイ二乗分布検定を有意水準 0.05 として行った結果，実験値の分布は理論値の分布に適合することがわかった．m, e, p を 0.1 刻みに値が存在する全ての組み合わせでシミュレーションを行ったが，Ep，Ee，Er，における理論値と実験値との差は誤差の範囲内であり，全中継ノード数に対するメッセージ到着回数の分布においては，カイ二乗分布検定を有意水準 0.05 として行った結果から，実験値の分布は理論値の分布に適合することがわかった．以上から 4 節で与えた 3MN のモデル，および導出した理論値は 3MN を考察する上で妥当なものであることがわかる．

6. おわりに

本稿では，中継ノードの行動として，Crowds における 2 通りの選択肢に加え，データセットを暗号化して転送するという選択肢を加えた新しい匿名通信方式である 3MN を提案した．また，これにより，送受信者双方の匿名性が保持できること，および，多重暗号化処理や復号化処理によるノードへの負荷が低減できることを，理論とシミュレーションによって示した．

今後の課題として，実際のネットワークを用いた実装と評価，および，3MN を用いて双方向通信を行う枠組みを構築することがあげられる．

文　献

[1] Ronggong Song and Larry Korba, Review of Network-based Approaches for Privacy, Proceedings of the 14th Annual Canadian Information Technology Security Symposium, vol.44905, 2002.

[2] Brian N. Levine and Clay Shields, Hordes: A Multicast Based Protocol for Anonymity, Journal of Computer Security, vol.10, no.3, pp.213–240, 2002.

[3] David L. Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, vol.1, no.1, pp.65–75, 1988.

[4] Michael K. Reiter and Aviel D. Rubin, Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security, vol.1, no.1, pp.66–92, 1998.

[5] Michael K. Reiter and Aviel D. Rubin, Anonymous Web transactions with Crowds, Communications of the ACM, vol.42, no.2, pp.32–48, 1999.

[6] David L. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Predonyms, Communications of the ACM, vol.24, no.2, pp.84–88, 1981.

[7] 尾形わかは, 黒沢馨, 高谷和伯, "(k, n) 閾値匿名通信路とその応用, " The 1997 Symposium on Cryptography and Information Security, SCIS'97-27F, 1997.

[8] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, Hiding Routing Information, 1st International Workshop on Information Hiding, vol.1174, pp.137–150, 1996.

[9] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag, Anonymous Connections and Onion Routing, IEEE Journal on Specific Areas in Communications, vol.16, no.4, pp.482–494, 1998.

[10] 羽鳥裕久, 森俊夫, 有限マルコフ連鎖, 培風館, 1982.