平成21年度　　卒業研究論文

匿名通信における経路制御方式の違いによる匿名性の評価

指導教官
齋藤 彰一 准教授

名古屋工業大学　情報工学科
平成18年度入学　18115071番

酒井 衛

目 次

第1章

はじめに

近年，インターネットが普及するに伴い，電子メールやウェブサイト，掲示板システム (BBS) などインターネットを用いたコミュニケーション手段が多く使われるようになった．これに伴い，内部告発や医療相談などプライバシーの保護が重要な行為やサービスが，インターネットを用いて行われることも考えられる．

プライバシーの保護が必要な情報をやりとりする場合，実社会では匿名を前提とした仕組みがいくつもある．しかし，インターネットではIP アドレスと時間から個人の特定が可能であり，プライバシーの保護が十分とは言えない．インターネットでのプライバシーを保護するためには，通信における匿名性 [1] 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 種類が挙げられる．

- 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

上記の通信における匿名性を考慮した既存の匿名通信路にはTor(The onion router)[2], Cashmere[4]，Bifrost[7] などがある．本論文では，匿名通信路の匿名性を評価し，匿名性の高い匿名通信路を実現するにあたって必要な要素について考察する．

以下， 2 章では今回比較する 3 つの匿名通信路とその評価方法について述べ， 3 章で実際に匿名通進路に評価を適用する． 4 章ではその評価の結果と考察をして， 5 章で結論をまとめる．

第2章

関連研究

本章では，今回評価する3つの匿名通信路Onion Routing[3](Tor)，Cashmere，Bifrostとその評価方法について述べる．

2.1 匿名通信路

2.1.1 Onion Routing

Onion Routingは送信者と受信者，複数の中継ノードにより構成される．送信者がメッセージを受信者に送信する際，送信者は受信者に直接メッセージを送信するのではなく，複数の中継ノードを経由して受信者にメッセージを送信する．そのとき，送信者はメッセージと次のノードへの宛先を鍵（経路構築時は各ノードの公開鍵，構築後は共通鍵）で多重に暗号化して送信する．中継ノードは，メッセージを受信すると自分の鍵でメッセージを復号し，次のノードへメッセージを送信する．これが繰り返し行われることで，最終的にメッセージは受信者へ届けられる (図2.1参照)．

上記方法により，メッセージを多重暗号化することで中継ノードは，自分の前後のノード情報しか得ることができず，送信者や受信者を特定することができない．例えば，図2.1に示すようにメッセージがやりとりされるとすると，ノードxは前後のノード情報しか得られないので，送信者や受信者を特定できない．そのため，匿名性が保たれる．

Onion Routingは，多重暗号により匿名性を保っているが，それぞれのメッセージ

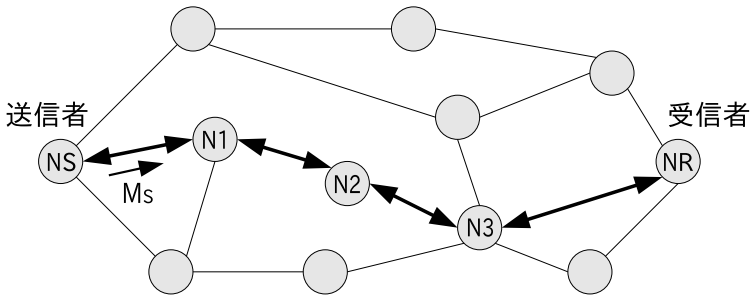

図 2.1: Onion Routing

を復号できるノードは1つのメッセージに対して1つしかないため，1つでも中継ノードがネットワークから離脱すると通信を行うことができなくなってしまう．また，全体のノードを中央サーバが集中管理しているため，ネットワークのノード数が増加すると中央サーバの負担が大きくなり，ノードの管理が難しくなるという欠点がある．

2.1.2 Cashmere

Cashmere は Onion Routing にその欠点であるノードの離脱とノード管理の難しさを解消するために，DHT(Distributed Hash Table) である Pastry[5] を導入した匿名通信路である．Onion Routing と同様に送信者によって多重暗号化されたメッセージを複数のノードを経由させ，受信者にメッセージを届けることで匿名性を確保し，それと同時にノード管理を容易にする．また，図 2.2 に示すように中継をグループ化することでノードの離脱耐性を向上させている．グループ内のメッセージはグループで最初にメッセージを受け取ったノード (root ノード) が自グループにメッセージを行き渡らせる．

中継グループの作成方法

Cashmere の中継グループの作成方法を述べるために，Pastry の構造とメッセージの伝達方法を説明する．Pastry は各ノードに割り当てられた ID の prefix をもとにネットワークを構築する．上位ビットは prefix を基本としてネットワークを構築し，下位

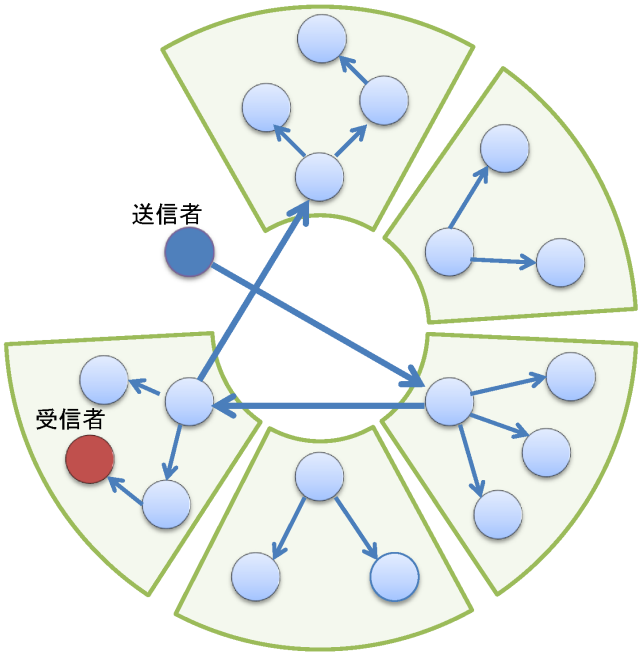

図 2.2: Cashmere

ビットは各ノードが leaf set と呼ばれるノードリストを用いてメッセージをやりとりしやすくする．そして，Cashmere の中継グループは任意の prefix 以下のノードから成る．図 2.2 の扇形に囲まれているノード郡は同じ ID の prefix を持つノード郡であり，中継を行う際に 1 つの中継ノードのように動作する．

バックアップ作成方法

メッセージをやりとりする上で通信を継続的に行うためには，通信に参加しているノードが離脱したときに備えてノードのバックアップをする必要がある．Cashmere におけるバックアップは，root ノードが自ノードが所属するグループに対して行う．root ノードが離脱したときは，自グループに所属するノードが代理で通信を継続する．

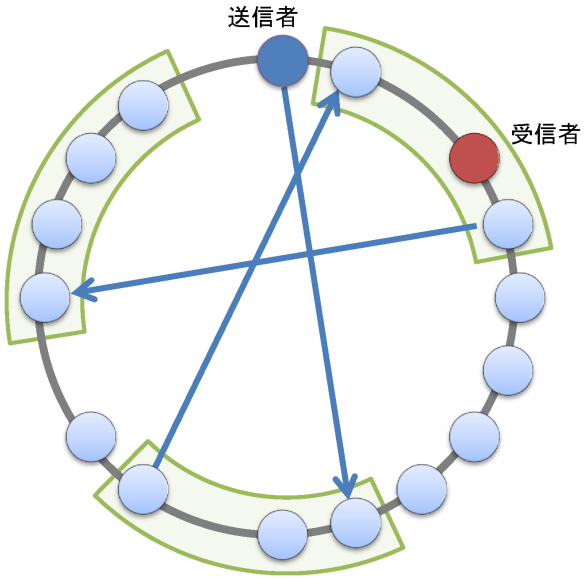

図 2.3: Bifrost

2.1.3 Bifrost

Bifrost は Cashmere と同様に Onion Routing の欠点を補うために DHT の 1 つである Chord[6] を導入した匿名通信路である．Onion Routing と同様，メッセージは送信者によって多重暗号化され，複数の中継ノードを経由し受信者に届けられる．グループ内のメッセージは順次となりのノードに伝達されてグループ全体に行き渡る．

中継グループの作成方法

Bifrost の中継グループの作成方法を述べるために，まず Chord の構造とメッセージの伝達方法について説明する．Chord は円形のネットワークを構築しており，各ノードは ID 順に配置る (図 2.4)．メッセージは自ノードの次に大きい ID のノード (Successor) とやりとりされる．またメッセージをショートカットさせるために，finger table というノードリストを用いる．そして，Bifrost の中継グループは Chord 上で連続したいくつかのノードから成る (図 2.3 参照)．

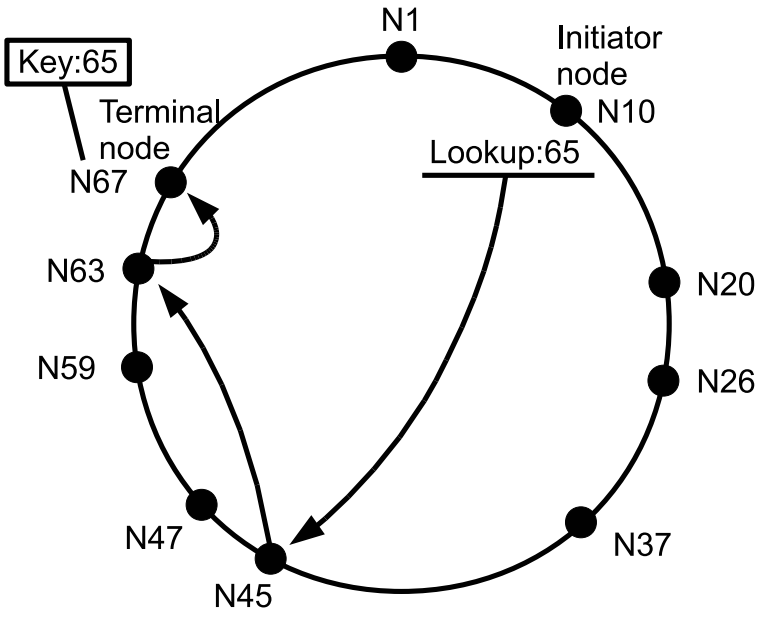

図 2.4: Chord

バックアップ作成方法

Bifrost におけるバックアップは，他中継グループにメッセージを中継する役割を担っているグループの末端のノードだけが行う．末端ノードは，通信を継続するために必要なデータを自グループ外のノードに 2 分割して渡す．末端ノードが離脱したときは，Chord の機構で離脱を検知し，Bifrost が情報を統合して通信を継続するための代理ノードを作る．

2.1.4 各匿名通信路まとめ

3 つの通信路に共通していることは，メッセージを多重暗号化していることである．暗号化されたメッセージをやりとりすることで，各ノードは自ノードの前後のノードの情報しか得られないため，送信者及び受信者を特定しにくくしている．Cashmere と Bifrost に共通していることは，中継をグループ化していることである．グループ化することで，Cashmere はノードの離脱耐性と匿名性の向上を図っている．Bifrost はノードの離脱耐性よりも匿名性の向上を重視している．

2.1.5 問題点

Onion Routing，Cashmere，Bifrost は中継を繰り返すこと，また Cashmere，Bifrost は中継をグループ化することで匿名性を確保している．しかし，それらのパラメータが匿名性を確保するためにどのような効果があるかはっきりとした評価がなされていない．そのため，中継グループを導入することで匿名性が確保できるように思える Cashmere と Bifrost でも，本当に匿名性を確保できているのか分かっていない．そこで，本論文では中継回数と中継グループというパラメータを考慮し，さらには各匿名通信路のネットワークの構築方法の違いを考慮しながら匿名性を評価する．

2.2 匿名性評価

本節では中継グループノード数と中継回数を変化させたときに，匿名性にどのように影響を及ぼすかを数値化するために，Towards measuring anonymity[9] で提示されているエントロピーをもとにした匿名度を用いて比較する．そのために， 2.2.1 に匿名度の求め方， 2.2.2 に求め方を適用した例を示す．

2.2.1 匿名性評価方法

匿名度はエントロピーを用いて求められることができ，ある状態における匿名通信路で各ノードの情報エントロピーの総和を求めることで算出する．エントロピーとは事象の不確かさを示すものであり，不確かなほど高い値となる．全ノード数を N，各ノードが送信者及び受信者である確率を p_i とした場合の式を式 (2.1) に示す．式 (2.1) により，ある状態におけるエントロピーの総和を求めることができる．さらに，$H(X)$ を最大のエントロピー H_M で割ることにより $H(X)$ を正規化する．H_M は，各ノードが等確率で送信者及び受信者である場合の確率をもとに算出する．すなわち，各ノードが $1/N$ の確率で送信者及び受信者であるものとして式 (2.1) に当てはめたとき，式 (2.2) となる．算出した最大のエントロピーをもとに $H(X)$ を正規化すると式は式 (2.3) に示すようになる．式 (2.3) が匿名度 d を算出するために必要な基本的な式である．匿名度 d は $0 \leq d \leq 1$ の値を取り，1 に近いほど匿名性が高いことになる．また，匿名度 d

を算出する際，場合分けが必要なときは，それぞれの場合の確率 q_t としたとき，期待値を求めるときと同様に式を求めると式 (2.4) のように期待値の形として求める．以降，式 (2.4) を用いて匿名度を求る．

エントロピーの総和

$$H(X) = -\sum_{i=1}^{N} p_i log_2(p_i) \tag{2.1}$$

匿名度の最大値

$$H_M = -\sum_{i=1}^{N} \frac{1}{N} log_2(\frac{1}{N}) = log(N) \tag{2.2}$$

基本的な匿名度

$$d = \frac{H(X)}{H_M} = \frac{-\sum_{i=1}^{N} p_i log_2(p_i)}{log(N)} \tag{2.3}$$

匿名度の期待値

$$d = \sum_{j=1}^{K} q_j d_j \tag{2.4}$$

2.2.2 匿名度算出例

前節の匿名性評価方法を簡単な例を挙げて説明する．全 16 ノード，そのうち不正者が 4 ノードいる匿名通信路における送信者の匿名度を求める．簡単化のために，匿名通信路のネットワーク内でメッセージのやりとりが行われたが不正者が検知できなかったものとする．このとき，不正者は送信者には成り得ないため，送信者に成り得るノードは 12 ノードであるから．不正者がメッセージを観測できなかったとき，12 ノードすべてが同じ確率 $p_i = 1/12$ で送信者に見える．また，全体のエントロピーは不正者も含めてのノード数であるから，H_M, $H(X)$, d は次のようになる．

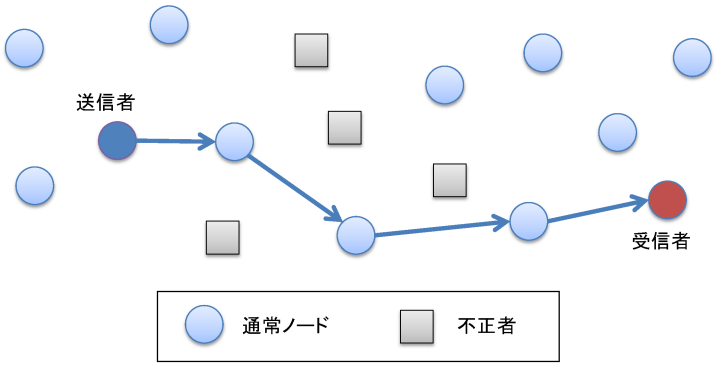

図 2.5: 全 16 ノード，うち不正者 4 ノード

匿名度算出例

$$
\begin{aligned}
H_M &= log_2(16) \\
H(X) &= -\sum_{i=1}^{12} \frac{1}{12} log_2(\frac{1}{12}) = log(12) \\
d &= \frac{H(X)}{H_M} = \frac{log_2(12)}{log_2(16)} = 0.89624
\end{aligned}
$$

第3章

匿名性評価の適用

本章では 2 章で取り上げた匿名通信路に匿名性評価をどのように適用するかを説明する．匿名度を求めるときに使われる要素は次のとおりである．N, L, ρ は定数とし，$f, n, |S|$ を変化することで匿名度を求める．

$\boldsymbol{N}$ ネットワーク中の全ノード数

$\boldsymbol{L}$ 1 回の通信で経由する中継回数

$\boldsymbol{\rho}$ 中継グループ 1 つのノード数

$\boldsymbol{f}$ ネットワーク中の不正者の割合

$\boldsymbol{n}$ 不正者によって判明した中継ノードもしくはグループ数 $(n \leq L)$

$\boldsymbol{|S|}$ 不正者によって判明した中継内にいるノード数

3.1 送信者

送信者の匿名度は，送信者と受信者のメッセージのやりとりの間に不正者が参加している場合と参加していない場合に分けをし確率を求め，エントロピーを用いて求められる．送信者の確率 p_u は，3 つの匿名通信路に共通して次のようになる．

$$p_u = \begin{cases} \dfrac{1}{L-n+1} & \text{(一連の通信で判明している最初のノード)} \quad (3.1) \\ \left(1-\dfrac{1}{L-n+1}\right)\cdot\dfrac{1}{(1-f)N-1} & \text{(上記以外の場合)} \quad (3.2) \end{cases}$$

Onion Routing の性質上，メッセージの送信者は一連の通信の始点であることは明らかである．よって，中継が不正者によって判明しているとき，送信者はその中継よりも前にいるノードであると考えられるため，確率 p_u は式 (3.1) となる．それ以外のノードが送信者であると考えられる確率は式 (3.2) のようになる．式 (3.2) は式 (3.1) の場合とは異なり，送信者を特定する情報がないため不正者以外のノードを均等に送信者と見立てた場合の確率である．確率 p_u は Onion Routing，Cashmere，Bifrost に共通したものとなる．匿名度を算出するためには，式 (3.1)(3.2) それぞれの起こる確率を求め，式 (2.3) に当てはめて特定の場合の匿名度を算出し，式 (2.4) で最終的に匿名度を求める．

3.2 受信者

受信者の匿名度も送信者のときと同様に 2 つの場合に分けて求められる．不正者が一連の通信に参加している場合と参加していない場合である．それぞれの確率 p_u は次のようになる．

$$p_u = \begin{cases} \dfrac{1}{L\rho - f|S|} & \text{(不正者が一連の通信に参加している場合)} \quad (3.3) \\ \left(1-\dfrac{(1-f)|S|}{L\rho-f|S|}\right)\cdot\dfrac{1}{N-|S|} & \text{(上記以外の場合)} \quad (3.4) \end{cases}$$

不正者が一連の通信に参加している場合，受信者である確率は参加したすべてのノードから不正者を除いた確率であるため，式は式 (3.3) となる．不正者が参加していない場合，特定できている中継以外のすべてのノードが受信者である可能性があるため，式は式 (3.4) となる．受信者の匿名度も式 (3.3)(3.4) を用いて送信者の匿名度を求めるときと同様に求める．式 (3.3)(3.4) がそれぞれ起こる確率は特定できた中継数に依存する．Onion Routing の場合，グループ化してないため中継ノードそのものの 1 点，

Cashmere はグループの作成方法を考えるとグループの root ノードの 1 点，Bifrost はグループの 2 つの端点を特定すれば中継を特定できたと判断する．

第4章

評価

本章では3章で各匿名通信路に適用した送信者と受信者の匿名性評価の結果をグラフに示し，考察する．評価パラメータを表4.1に示す．基本では1回のメッセージのやりとりに参加するノード数は16ノードであり(以降，基本状態と呼ぶ)，変化後の参加ノードは32ノードとなるように中継回数と中継グループノード数をそれぞれ4増やした場合を評価する．ただし，中継回数をもとに評価したため，中継グループの概念がないOnion Routingでは，中継グループ内ノード数のパラメータを変化させても意味がないものとする．

4.1 送信者

本節では送信者の匿名性について各匿名通信路，中継グループノード数を増加指せた場合，中継回数を増加させた場合の3つの比較及び考察をする．

4.1.1 匿名通信路の比較

図4.1に基本状態における送信者の匿名度の評価結果を示す．すべての匿名通信路で同一の評価結果となった．これは送信者の動作が他の中継ノードに比べて特異であるためである．CashmereとBifrostでは匿名性を確保するため中継をグループ化しているが，ある中継グループから他の中継グループへメッセージを中継する動作は，中継グループの形を取っていないOnion Routingが中継ノードから他の中継ノードにメッ

表 4.1: 評価パラメータ

	基本	中継グループノード数	中継回数
全ノード	16,384	16,384	16,384
中継グループ内ノード数	4	**8**	4
中継回数	4	4	**8**

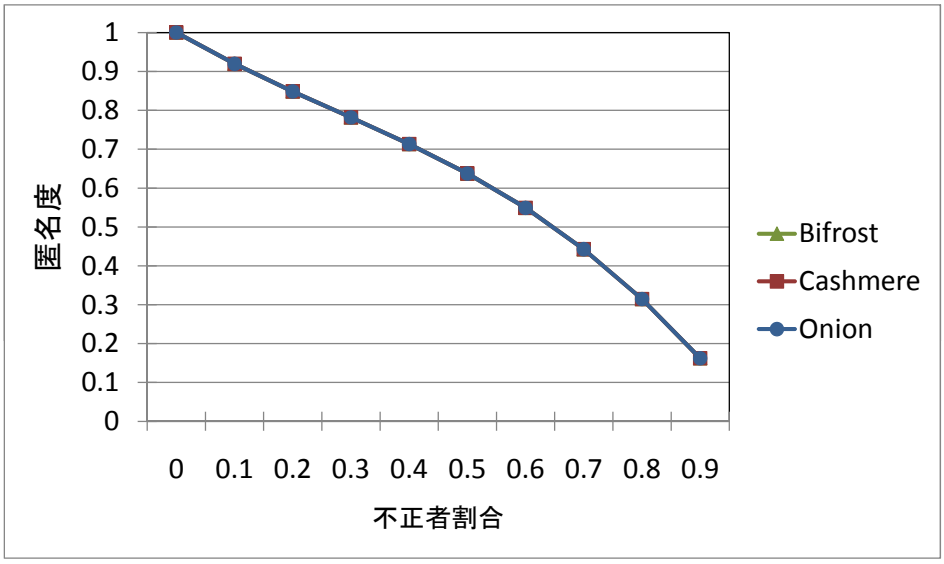

図 4.1: 送信者匿名性

セージを中継する動作と同様であるためである．

4.1.2 中継グループノード数変化時

中継グループ内ノード数を 4 増やしたときの送信者の匿名度の評価結果を図 4.2 に示す．図 4.2 からは分かりにくいが変化させても基本状態と同じ匿名度である．これは 4.1.1 で述べたとおり中継をグループ化しても送信者が通信において特異であることにより，送信者であると思われるノードに偏りが発生するためであり，3 つの匿名通信路すべてに共通することであるため，すべて同じ匿名度となる．

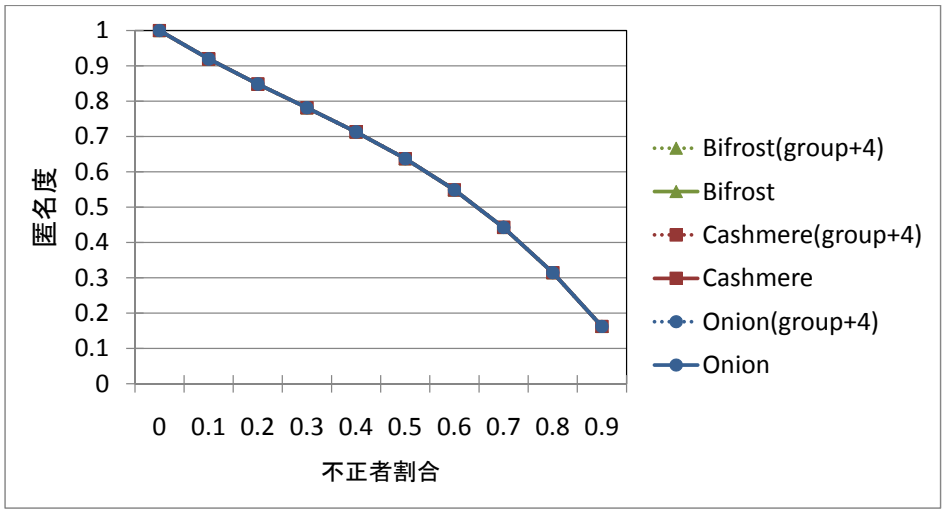

図 4.2: 送信者匿名性 (中継グループ内ノード数増加)

4.1.3 中継回数変化時

中継回数を 4 回増やしたときの送信者の匿名度の評価結果を図 4.3 に示す．図 4.3 からは分かりにくいが 4.1.1 と同様に 3 つの匿名通信路すべてが基本状態より高い匿名度となる．その理由は，中継回数が増加したことでその通信路の経路が長くなり，経路全体を把握するために特定する必要のある中継グループの数が増加するため，確率的に中継を特定することが難しくなるためである．前述の理由により，すべての匿名通信路で同一の匿名度となる．

4.2 受信者

本節では送信者の匿名性について各匿名通信路，中継グループノード数を増加指せた場合，中継回数を増加させた場合の 3 つの比較及び考察をする．

4.2.1 匿名通信路の比較

受信者の匿名度の評価結果を図 4.4 に示す．図 4.4 から匿名度が高い順に Bifrost，Cashmere，Onion Routing である．まず，Onion Routing が最も低い匿名度となった理由は，メッセージの中継をグループ化していないためである．中継回数をもとに比

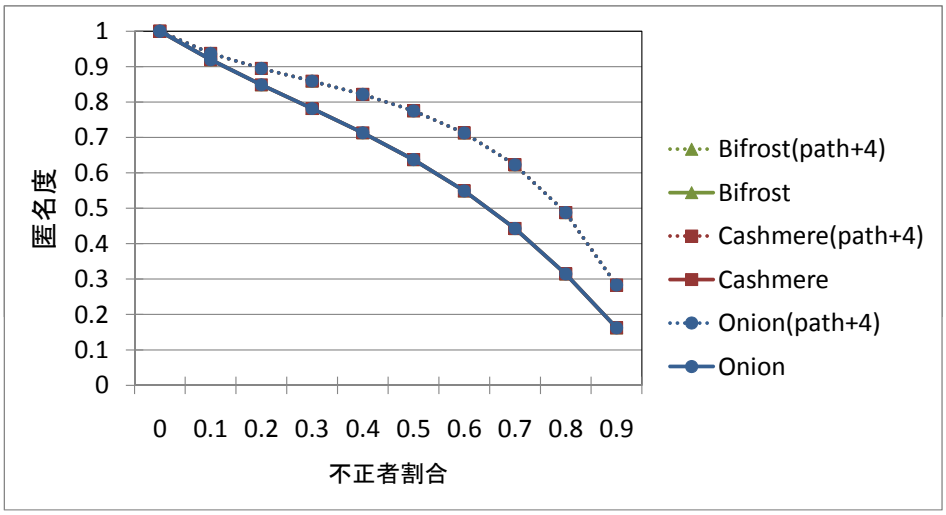

図 4.3: 送信者匿名性 (中継回数増加)

較すると Onion Routing は他の匿名通信路に比べて 1 つのメッセージのやりとりに参加するノードが少ない．そのため，受信者となりうるノードの数が少なくなり，匿名度を求めるときに送信者である確率が高くなるため，匿名度が低くなる．

次に，中継をグループ化している Cashmere と Bifrost で，Bifrost の匿名度が高くなった理由を考える．2 つの匿名通信路の違いは，中継グループの作り方にある．図 2.2 の Cashmere と図 2.3 の Bifrost で不正者が中継グループを特定することを考える．Cashmere はグループの root ノードを特定すれば，同じ prefix を持つノードが同じグループに属することが分かる．それに対して，Bifrost はグループの端点を特定しただけではグループがそれ以降どれだけ続くか分からないため，グループの両端を特定したときにはじめてそのグループを特定できる．つまり，Bifrost の中継グループの方が特定されにくい作りになっているため，確率的に匿名度が良い結果となる．

4.2.2 中継グループノード数変化時

中継グループ内ノード数を 4 増やしたときの受信者の匿名度の評価結果を図 4.5 に示す．Onion Routing を除いて匿名度が若干良くなっていることが分かる．Onion Routing に変化がない理由は，そもそも Onion Routing が中継をグループ化していないため，中継グループ内ノードを増やすことによる影響がないためである．一方，中継をグルー

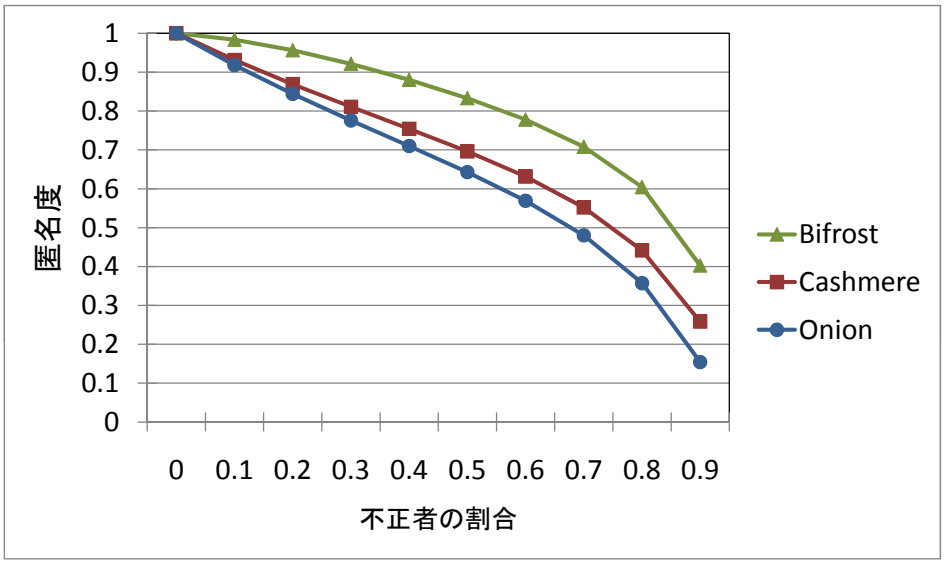

図 4.4: 受信者匿名性

プ化している Cashmere と Bifrost はともに若干匿名度が向上している．匿名度が向上している理由は，ある中継グループが特定されたときを考えると分かる．そのとき，中継グループ内ノード数が増えていると受信者と思われるノードの候補が増加するため，確率的にどのノードが受信者であるか分かりにくくなる．そのため，中継グループ内ノード数を増加させると匿名度が高くなる．

4.2.3 中継回数変化時

中継回数を 4 回増やしたときの送信者の匿名度の評価結果を図 4.6 に示す．すべての匿名通信路において匿名度が向上している．匿名度が高くなる理由は，中継回数を変化させたときの送信者の匿名度 (4.1.3 参照) と同様の理由である．

そして，中継グループ内ノード数と比較すると中継回数を増加したときの方が匿名度が高くなる．その理由として，それぞれの要素を増加したときの確率を考える．中継回数を増やしたときの確率は Onion Routing の場合，元の受信者である確率に対して $\frac{1}{N}$ の影響がある．また，中継をグループ化している Cashmere と Bifrost でも同様に影響がある．それに対して，中継グループ内ノード数を増やしたときの確率は元の確率において，中継グループ内に受信者がいる確率が $\frac{1}{\rho}$ から $\frac{1}{\rho+1}$ に変化する．全ノード

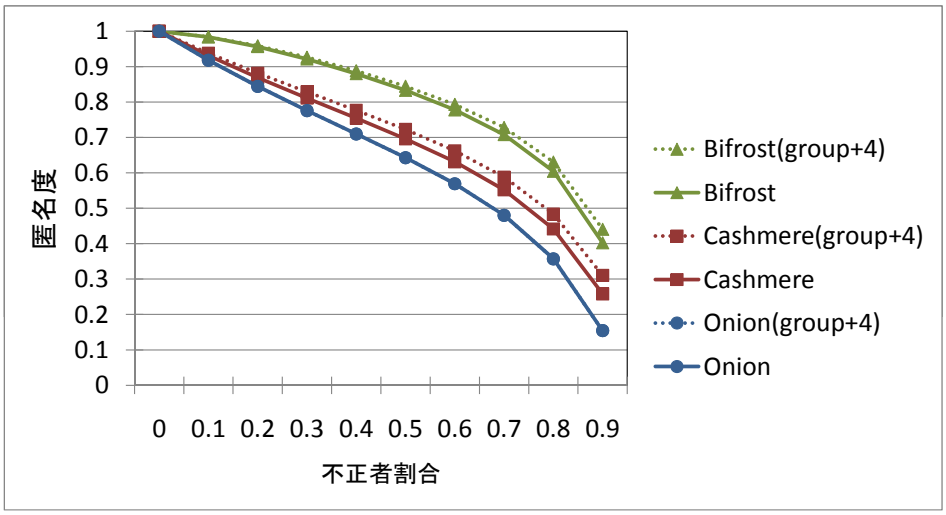

図 4.5: 受信者匿名性 (中継グループノード数増加)

数 N は，中継グループノード数 ρ と比べて明らかに大きいため，中継回数を増加したときの確率の影響が大きいといえる．そのため，中継回数の増加の方が中継グループ内ノード数増加よりも匿名度を高くする影響を与える．

4.3 バックアップ作成時

前節では，バックアップを考慮しない匿名度を評価した．本節では，バックアップを考慮したときの匿名度を評価する．バックアップを考慮すると，Cashmere は中継グループが 1 つの中継ノードと考えることができるので，グループの中に不正者が 1 つでも存在するとそのグループは安全ではない．Bifrost は実際に他ノードに中継を行うノードのみがバックアップをするので，そのノードのバックアップによる匿名性の低下を考えればよい．Onion Routing はバックアップの機構がないが，匿名度の比較参考のために図中には表記する．また，図中凡例の”-min” はバックアップありのそれぞれの匿名通信路の匿名度を表している．

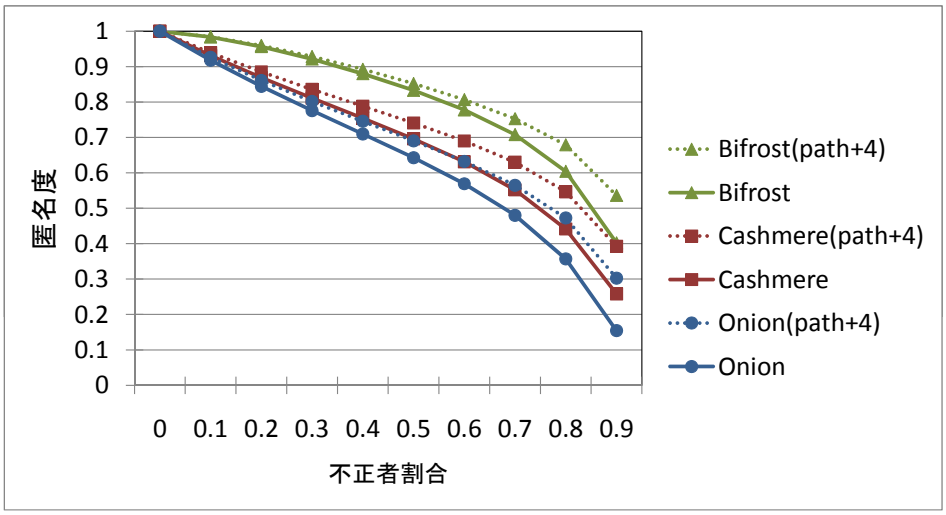

図 4.6: 受信者匿名性 (中継回数変化時)

4.3.1 送信者

匿名通信路ごとの送信者の評価結果の比較を図 4.7 に示す．Cashmere の匿名度が著しく低下していることが分かる．前述したとおり，グループ内に不正者が 1 つでも存在することが中継を特定につながると考えられるためである．Bifrost は他グループにメッセージを中継するノードのみがバックアップを作成するため，バックアップに参加するノード数が少ないため，Cashmere ほどの匿名度の低下に至っていない．

4.3.2 送信者 (中継回数変化時)

中継回数を 4 回増やしたときの送信者の評価結果を図 4.8 に示す．バックアップなしの Cashmere，Bifrost は Onion Routing と同じ匿名度である．バックアップありのとき，Cashmere，Bifrost ともに匿名度は低下している．バックアップなしのときと同様，匿名度の低下率は抑えられているがバックアップを作成することで匿名度は低下しやすくなることが分かる．

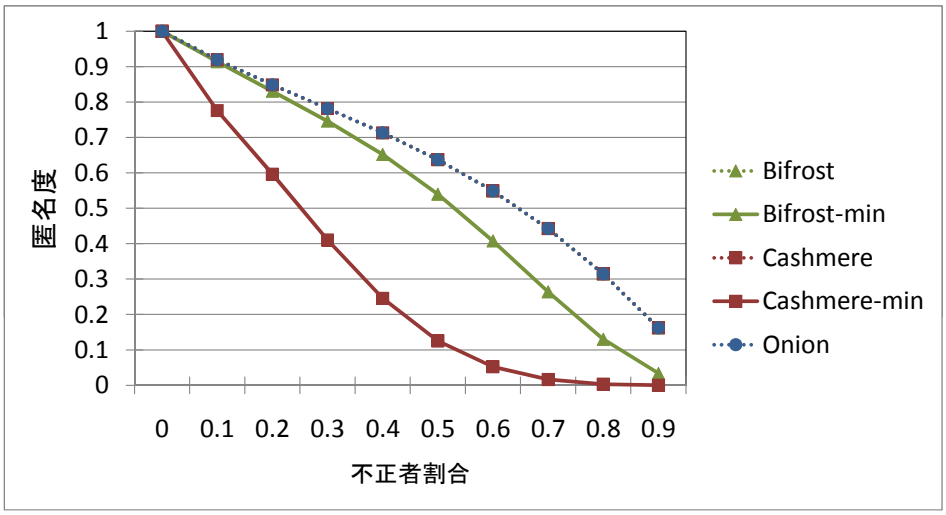

図 4.7: 送信者匿名性 (バックアップあり)

4.3.3 送信者 (中継グループノード数変化時)

中継グループ内ノード数を 4 増やしたときの送信者の匿名度の評価結果を図 4.9 に示す．バックアップありの Cashmere の匿名度の低下が顕著である．Cashmere のバックアップは自グループに対して行うので，グループ内ノード数を増やすほど不正者が居る確率が上がり，グループが特定されやすくなるため，匿名度が著しくていかしている．一方，Bifrost はグループに対してバックアップを行わないので Cashmere と同様の結果にならず，バックアップ行っても匿名度はある程度保たれている．

4.3.4 受信者

匿名通信路ごとの受信者の評価結果の比較を図 4.10 に示す．送信者のときと同様，Cashmere の匿名度の低下が著しい．それに対して，バックアップありの Bifrost はバックアップなしよりも匿名度は低下しているものの，バックアップを考慮しない Cashmere を上回る匿名度を保っている．Bifrost の匿名度が高い理由は，受信者の匿名度の評価には中継グループの特定のしやすさが影響しているためと考えられる．

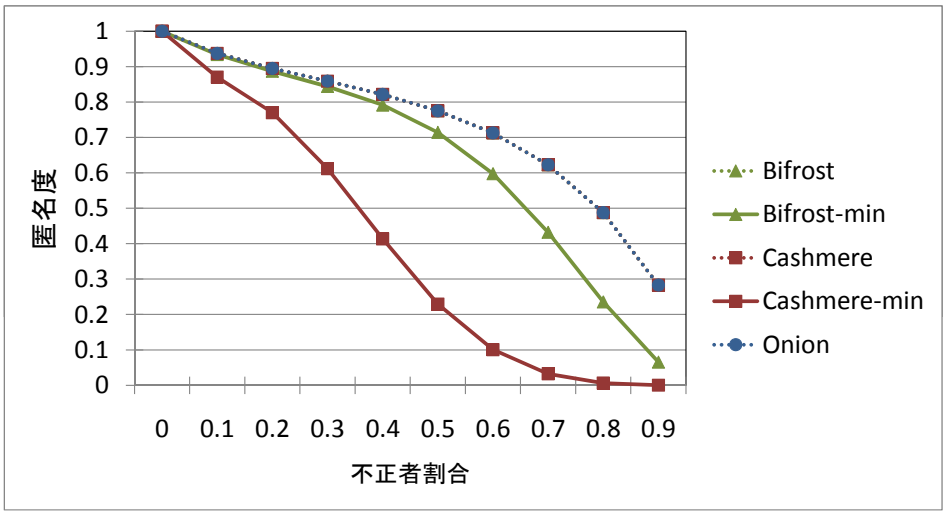

図 4.8: 送信者匿名性 (中継回数増加/バックアップあり)

4.3.5 受信者 (中継回数変化時)

中継回数を 4 回増やしたときの受信者の評価結果を図 4.11 に示す．中継回数を増加していないときと比べ，匿名度は全体的に高い結果となる．すべての中継回数変化時の図 (図 4.3，図 4.6，図 4.8，図 4.11 参照) から中継回数の増加は，送信者，受信者，バックアップの有無に関係なく匿名度を高くすることが分かる．

4.3.6 受信者 (中継グループノード数変化時)

中継グループ内ノード数を 4 増やしたときの受信者の匿名度を図 4.12 に示す．Cashmere の匿名度の低下が著しいが送信者のときと比べ (図 4.9 参照)，低下率は緩やかなものとなる．これは中継グループを特定しただけではグループ内に受信者の可能性があるノードがいることが分かっても，受信者そのものを特定することは困難なためである．

4.4 匿名性評価結果まとめ

前節までの評価結果をもとに匿名通信において望ましい構成を考察する．本論文では，多重暗号を扱った匿名通信について評価したため，多重暗号において望ましい匿

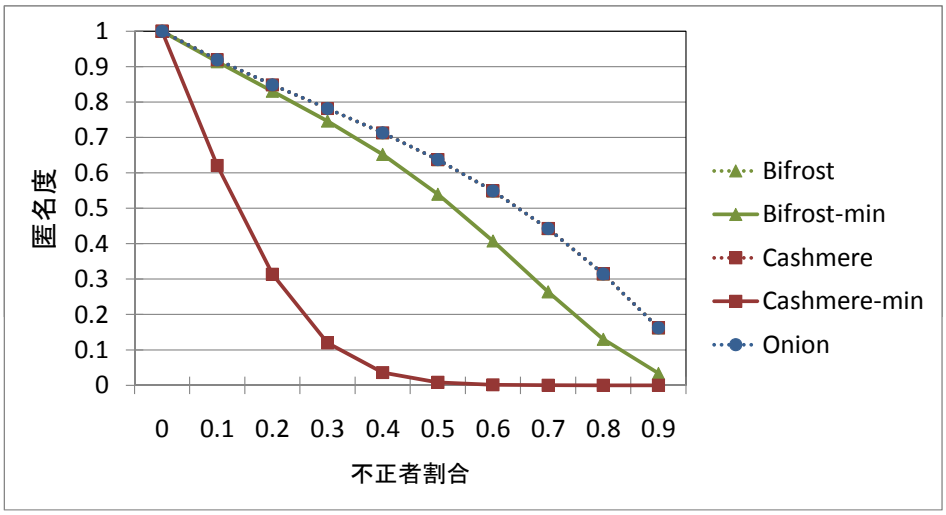

図 4.9: 送信者匿名性 (中継グループノード数増加/バックアップあり)

名通信をまとめる．匿名通信としての要素は，グループ化，メッセージ伝達方法，バックアップが考えられる．本節では，それぞれの要素について考察する．

4.4.1 グループ化

多重暗号を用いる通信において中継を行うことは必須事項である．中継が行われるということは，中継に参加するノードは他ノードに比べ，特異な通信を行うことになり，匿名性が低下する要因となる．そこで，通信に参加するノード数を増やすことで特異な通信を行うノードを増やすことができる．したがって，中継をグループ化するということが，通信に参加するノード数を増やすことになり有用である．参加ノード数を増やすだけなら，単純に多重暗号の中継回数を増やすことでも実現できるが，中継をグループ化することで，暗号及び復号回数の削減とノードの離脱耐性が向上するという利点がある．また，固定的なグループよりも自由にグループ内ノード数を決定できることが，中継の特定することを困難にするためには望ましい．以下，メッセージ伝達方法とバックアップの考察ではグループ化を行うものとして考察を行う．

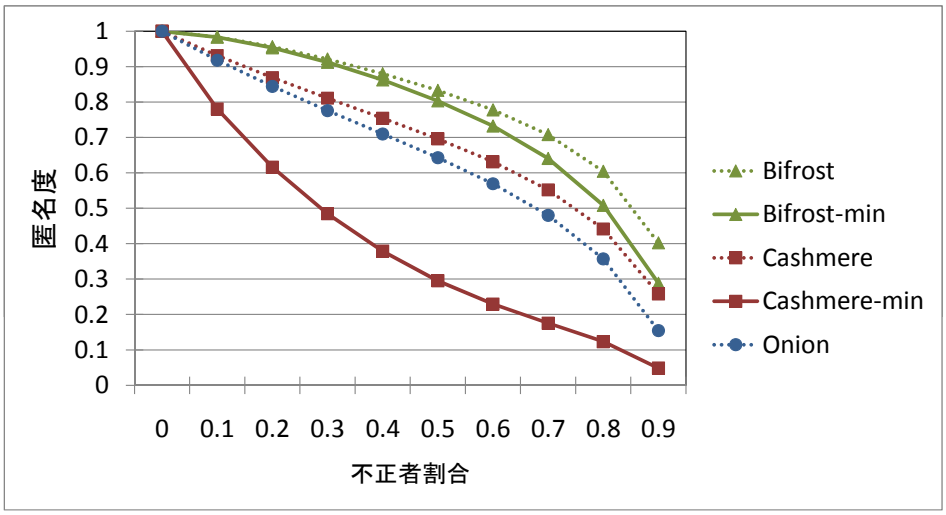

図 4.10: 受信者匿名性 (バックアップあり)

4.4.2 メッセージ伝達方法

多重暗号と中継グループにおける通信には 2 種類の通信がある．(i) 中継グループから他中継グループにメッセージへの伝達と (ii) 中継グループ内のメッセージ伝達の 2 種類である．(i) はメッセージを送信するということであるため，送信者の匿名性に影響する．Onion Routing，Cashmere，Bifrost の匿名通信路の他中継へのメッセージ送信は単一のノードが行うため，中継の一点を特定すれば送信者である可能性のあるノードを特定できる．特定を防ぐためには送信者に見えるノードを増やす必要があり，それを実現するために本来の中継を行うノードの他に中継をしているように見せかけるノード必要がある．(ii) はグループの特定につながる要素のため，送信者及び受信者の匿名性に影響する．グループの特定という観点から考えると，これまで述べてきたことと同様，特異な動作を行うことは避けるべきである．したがって，Cashmere のようにメッセージを受け取った root ノードが自グループにメッセージを伝達することは望ましくない．

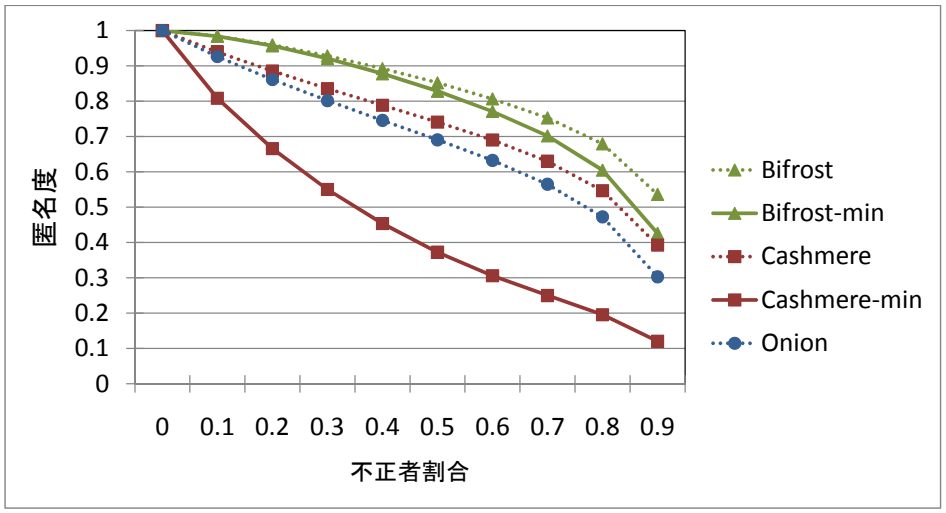

図 4.11: 受信者匿名性 (中継回数増加/バックアップあり)

4.4.3 バックアップ

安定した通信を継続的に行うためには，通信のバックアップを行うノードが必要である．バックアップは Cashmere と Bifrost において大きな匿名性の違いを生じさせる結果となる．Cashmere は，バックアップを自ノードが所属するグループに作成するため，通信が行われると自グループに自分が通信に参加していることを通知すると同時に自分がグループの root ノードであることを知らせている．通信の特異性を考えると，root ノードとグループの端点は他ノードと特に異なる動作をするため匿名性に大きく影響する．したがって，Cashmere のように root ノードであることを他ノードに通知することは匿名性を低下させる要因となる．よって，Bifrost のようにバックアップはグループに関与しないノードが行うべきである．

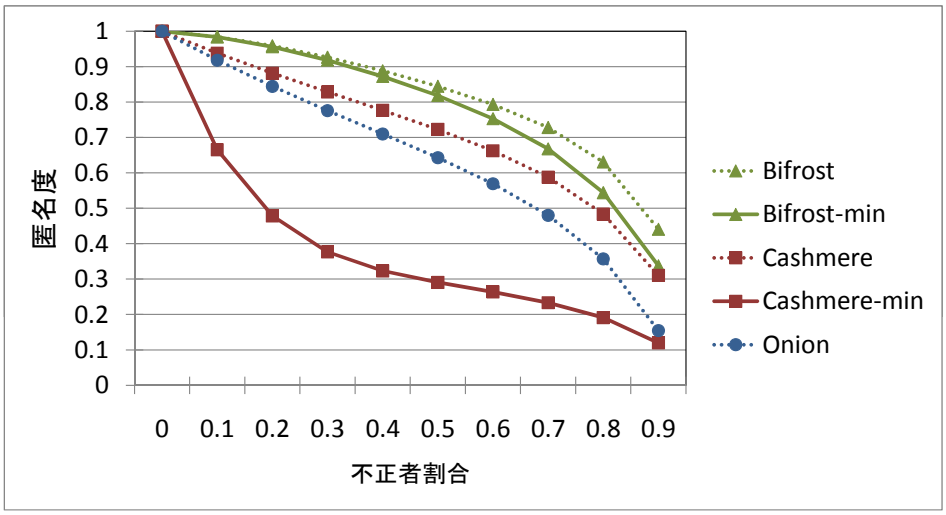

図 4.12: 受信者匿名性 (中継グループノード数増加/バックアップあり)

第5章

まとめ

本論文ではエントロピーをもとにOnion Routing，Cashmere，Bifrostの3つの匿名通信路の匿名性を評価した．その結果，匿名性が高い順に送信者と受信者ともにBifrost，Cashmere，Onion Routingとなった．また，3つの匿名通信路に共通したパラメータとして中継回数，CashmereとBifrostに共通したパラメータとして中継グループノード数を変化させたときに，匿名性にどのような影響があるかを評価した．その結果，中継回数の増加は送信者及び受信者の匿名性向上に結び付いた．中継グループノード数の増加は受信者の匿名性を向上させるのみとなった．しかし，ノードの離脱耐性つまり継続的な通信を行うためのバックアップを考慮すると，Cashmereは匿名性が著しく低下した．

以上の結果をもとに高い匿名性を実現するために望ましい通信方法は，中継のグループ化及び特定しにくいグループ，送信者の可能性があるノードを増やすこと，バックアップを行うノードがメッセージ通信に関与しないことであると考えられる．

謝辞

本研究のために多大な御尽力を頂き，日頃から熱心な御指導を賜った名古屋工業大学の齋藤彰一准教授ならびに齋藤研究室の皆様に深く感謝致します.

また，本研究の際に多くの助言，協力をして頂いた松尾啓志教授，津邑公暁准教授，松井俊浩助教，及び松尾・津邑研究室の皆様に深く感謝致します。

参考文献

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

[2] Dingledine, R., Mathewson, N. and Syverson, P. : Tor: The Second-Generation Onion Router, Proceedings of the 13th conference on USENIX Security Symposium, Vol. 13, pp. 303–320 (2004).

[3] 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).

[4] Li Zhuang, Feng Zhou, Ben Y. Zhao, Antony Rowstron : Cashmere: Resilient Anonymous Routing, In Proc. of Nerworked System Design and Implementation(2005).

[5] Antony Rowstron, Peter Druschel : Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems, the 18th IFIP/ACM International Conference on Distributed Systems Platforms (Middleware 2001). Heidelberg, Germany, November 2001.

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

[7] 近藤 正基, 齋藤 彰一, 石黒 聖久, 田中　寛之, 松尾 啓志 : Bifrost: A Novel Anonymous Communication System with DHT, Second International Workshop on Reliability, Availability, and Security (WARS 2009)

[8] 石黒 聖久, 田中　寛之, 近藤 正基, 齋藤 彰一, 松尾 啓志：通信路の部分的な再構築が可能な匿名通信方式の設計と実装, CSEC コンピュータセキュリティシンポジウム (CSS 2009).

[9] Claudia Diaz, Stefaan Seys, Joris Claessens, Bart Preneeliaz : Towards measuring anonymity, Proceedings of Privacy Enhancing Technologies Workshop, LNCS 2482