送信先アドレスによる関連付けを防ぐための分散型中継サービス

佐藤 良太† 蓑原 隆‡ 桜井 敦史†
拓殖大学大学院工学研究科† 拓殖大学工学部‡

概 要

近年インターネットにおいてプライバシーを保護することが重要になっているため，メッセージを保護する暗号化技術が数多く提案されている．しかし，配送に用いるアドレス情報は暗号化によって保護することができない．そのため，通信アドレス情報を元に複数の通信を関連付け収集することが可能であり，本来は第三者に知られたくない情報を窃用される恐れがある．通信アドレス情報による関連付けを防ぐにはアドレスを適宜変更する必要があり，これまでに，送信元アドレスを変更する方法が提案されている．しかし，関連付け防止は送信元アドレスを変更しただけでは不十分であり，送信先アドレスの変更が必要となる．そこで，我々は送信先による関連付けを防ぐ方法として，送信者と受信者の間にアドレス変換のための複数の中継者を並列に設置し，中継者及び送信先アドレスを変化させる方法を考える．また，送信者が信用できないアクセスポイントなどを利用している状況を想定し，送信者と中継者の間でアドレスの対応関係を通知するような事前通信をせずに中継者を利用する方法について提案する．

1 はじめに

近年，インターネットの利用者および利用目的の拡大に伴い，利用者のプライバシーの保護が重要になってきている [1]．インターネットで送られるメッセージをプライバシー面から見ると，メッセージの内容自体は IPSec[2] などの暗号化技術によって保護できるが，アドレス情報については隠蔽するとメッセージの配信自体が困難になるため容易に保護することができない．

メッセージのアドレス情報を知られることによる問題としては，非関連性 (unlinkability)[3] の喪失が考えられる．これはアドレス情報をもとに複数のメッセージを関連付けられてしまうという問題で，盗聴者に対して本来知られたくない情報を漏らしてしまう原因になる．したがって，通信のプライバシーを確保するにはアドレスを変更する必要がある．

インターネット通信のパケットには送信元のアドレス (始点アドレス) と送信先のアドレス (終点アドレス) が付加される．このうち，始点アドレスについては，動的に変更する方法 [4][5] が提案されている．しかし，始点アドレスのみを変更しただけでは十分ではなく，終点アドレスによってメッセージを関連付けられてしまう可能性がある．受信者が公共のサービスを提供するなどして，比較的多数のノードからのアクセスを受けている場合は，そのノードに送信されるパケットの終点アドレスによる関連付けは難しいと考えられるが，社内ネットワークへ VPN 接続するためのサーバや，個人で自分だけが使用する目的のために設置しているサーバのように，利用者が限定されるノードに送信されるパケットについては，例え始点アドレスを変更したとしても終点アドレスからメッセージを関連付けられる危険性がある．例えば，外出先で自分のコンピュータをネットワークに接続して通信を行った後で別の地点に移動して同様に通信を行ったとすると，2 地点のアクセスポイントの情報を照合することで，通信の終点アドレス等から 2 つの通信を関連付けることができ，送信者の 2 地点間での移動を知られてしまう．したがって，関連付けを防ぐためには始点アドレスだけでなく，終点アドレスの変更が必要である．

終点アドレスを変化する方法としては，終点アドレスをマルチキャストにする方法 [6] と中継を用いる方法 [7][8] が提案されている．また，我々は IPv6 アドレスのインターフェース ID 部をワンタイム化する方法 [9] を提案している．

[1]Distributed Relay Service for Providing Unlinkability of Destination Addresses in IPv6 Communications
[2]Ryota SATO, Graduate School of Engineering, Takushoku University
[3]Takashi MINOHARA, Department of Computer Science, Takushoku University
[4]Atsushi SAKURAI, Graduate of Engineering, Takushoku University

マルチキャストを用いる方法では，暗号化したメッセージをマルチキャストで複数のノードに送る．このとき，Incomparable Public Key という公開鍵暗号の一種で正しい着信ノードのみが復号できる方法を使用する．復号に失敗したノードはメッセージを破棄し，正当な受信者以外はどのノードが受け取ったかを知ることができない．この方法で終点アドレスの推定を困難にするためには，マルチキャストグループのノード数が多いことが前提となる．しかし正当な受信者以外においてもメッセージの復号は試行されるため，ノード数が多くなるとその分オーバヘッドが増大する．

中継を用いる方法では，中継経路の設定をパケットのアドレス情報に付加する Onion-Routing や中継でのパケット付け替え前後のアドレス情報の対応関係を事前に通知する Stealth-LIN6 が提案されている．Onion-Routing は送信者から送信されたパケットを複数の中継者を経由し受信者に届ける方法である．Onion-Routing では，複数の中継者を経由するために，送信者が事前に複数の中継者を選択し，パケットを経由する中継者ごとの公開鍵で各区間でのアドレス情報を含めて多重にパケットを暗号化する．パケットを受け取った中継者は自身の秘密鍵でパケットを復号し次のノードへ転送する．この方法では，複数の中継者で復号を行う必要がある．Stealth-LIN6 は送信者から送信されたパケットをランダムに指定した 1 つの中継者を経由することで受信者に届ける．Stealth-LIN6 では，アドレス情報の対応関係を事前に送信者，中継者および受信者で交換する．アドレス情報の対応関係を交換することで，中継者はどのアドレスに対するパケットをどの受信者に転送するかの対応関係を得る．送信者は中継者を切り替えて利用することで通信ごとに終点アドレスを変更する．この方法では，事前にアドレスの対応関係を通知しておく必要がある．

我々が提案したワンタイムアドレスは，送信者と受信者で同一の受信者のアドレス系列を生成し，送信者が順番にアクセスする方法であるが，アドレスのプレフィックス部分が固定であるという問題がある．

本研究は広範囲のアドレス空間を利用できる IPv6 通信を対象に特定のノードだけがアクセスするサーバが存在する状況において，パケットの終点アドレスによりメッセージの関連付けができてしまう問題を対象とする．我々は送受信者間にアドレスを付け替える複数の中継者を分散配置し終点アドレスを変更する方法を考える．このとき，送信者と中継者の間での盗聴が特に問題だと考え，この間でのアドレスの対応関係の事前通信をせずに中継を利用する方法を提案する．

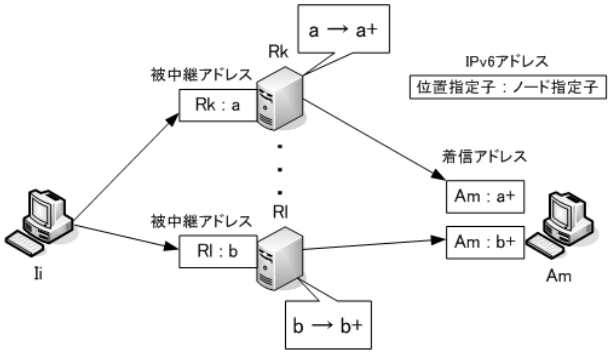

図 1: 中継の切り替え

2 中継サービス

インターネットの通信の多くは，2 つのノード間で相互に送受信されるものだと考えられる．そこで，2 ノード間の一連の通信を最初に開始するノードを「発信ノード」，発信ノードからの通信を受け取るノードを「着信ノード」と呼ぶこととする．我々が想定する状況は着信ノードにアクセスするノードが特定の発信ノードに限定される状況である．このような状況において，発信ノードが送信元アドレスを変化させたとしても，終点アドレスによってメッセージを関連付けることができると考えられる．

そこで，本研究では図 1 に示すように，発信ノードと着信ノードの通信を媒介するノードを複数設置してアドレス変換を行うことで発信ノードが用いる終点アドレスを変化させ，通信の関連付けを防ぐ．このとき両者の通信を媒介するノードを中継ノード (relay) と呼ぶ．また，発信ノードから中継ノードに送られるパケットを発信パケット，アドレス変換が行われて中継ノードから着信ノードに送られるパケットを着信パケットと呼ぶ．インターネットアドレスは，下位層のプロトコルの配信が可能な位置までパケットを転送するための情報と，下位層のプロトコルでの配信時にノードを指定あるいは探索するための情報からなると考えられる．以下，前者の情報を「位置指定子」，後者の情報を「ノード指定子」と呼ぶ．また，以降の表記を簡潔にするために，発信パケットの始点アドレスを「発信アドレス」，終点アドレスを「被中継アドレス」と呼び，着信パケットの始点アドレスを「中継アドレス」，終点アドレスを「着信アドレス」と呼ぶことにする．

中継ノードでは被中継アドレスから着信アドレスへの変換を行う必要がある．このとき，被中継アドレスのノード指定子が固定であると中継を行った場合でも発信パケットの関連付けが行われる可能性がある．そこで，発信ノードが用いる被中継アドレスは一時的なものとし，着信ノードと中継ノードが等しい場合にも被中継アドレスを変更できるようにする．着信ノードから発信ノードに対して返信が行われる場合には，返信対象のパケットと同じ中継ノードを経由させ中継アドレスから発信アドレスへ逆方向のアドレス変換を行うことでパケットを配信する．

本研究では，関連付け防止の対象として，攻撃者は発信パケットあるいは着信パケットのいずれか一方を傍受できるものとする．ただし，中継の前後でのパケットの時間関係を利用した関連付けや，攻撃者自身がパケットを送って，中継後のパケットを監視するような能動的な攻撃は対象外とする．発信ノードと着信ノードおよび着信ノードと中継ノードは事前に安全な場所で情報を交換することができるものとする

3　中継ノードでのアドレス変換方法

中継ノードにおいての被中継アドレスを着信アドレスに変換する具体的な方法として，被中継アドレスの位置指定子で中継ノードを指定し，ノード指定子で着信アドレスを指定することにする．すなわち，中継ノードにおいて被中継アドレスのノード指定子を着信アドレスに変換できるようにする．このときのアドレス変換にはハッシュ計算を用いることにする．

図 2 に示すように，着信ノード A_m は，発信ノード I_i から中継ノード R_k に被中継アドレス R_k：a 宛ての初回の発信パケットが届く前に変換結果である着信アドレス A_m：a+を中継ノード R_k に登録する．中継ノード R_k は発信パケットが到着すると，まず被中継アドレス R_k：a のノード指定子 a をハッシュ関数で変換し a+ = h(a, S(R_k-A_m)) を得る．次に事前に登録された着信アドレスの中からノード指定子 a+が一致するものを検索し着信アドレス A_m：a+を得る．この変換がうまく働くには，着信ノードにおいて被中継アドレスのハッシュ計算の結果が必要となる．ハッシュ計算には中継ノード R_k と着信ノード A_m の秘密情報 S(R_k-A_m) を用いて，第 3 者に a と a+の関係がわからないようにする．これにより，着信ノードにおいても同じハッシュ計算を行うことが可能なので，この問題は発信ノードと着信ノードで同じ被中継アドレスを生成することで解決できる．両ノードであらかじめ交換した秘密情報 S(I_i-A_m) を元に同一の被中継アドレス系列を生成する．生成方法については 5 章で説明する．また，複数のノードによる通信を考えた場合に生成したアドレスあるいは変換したアドレスが一致してしまう可能性についても考える必要がある．このアドレス重複の問題とその解決策については 6 章で説明する．

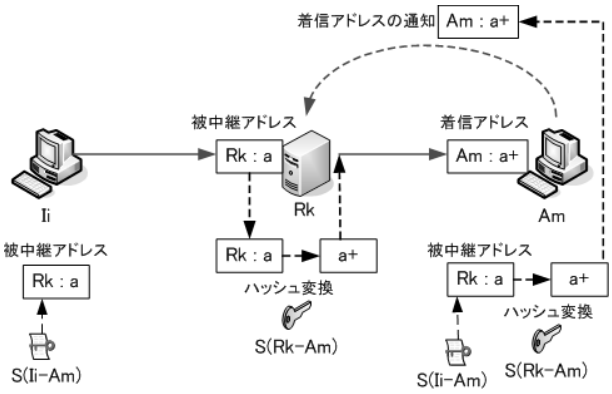

図 2: 中継ノードでの着信アドレスの生成

この方法は着信ノードと中継ノードの間で通知される情報に被中継アドレスの情報を含まないという利点を持つ．着信アドレスを受信しただけでは，アドレスの対応関係を知ることができないため，盗聴者が着信アドレスを取得しても，どの発信ノードとこれから通信を行うかを導くことはできない．一方，問題点としては，中継ノードにおいてアドレス変換の計算を行い，複数の着信アドレスから検索しなければならない点があげられる．中継ノードは複数の着信ノードごとの変換方式を用いて変換し，それぞれの複数の着信アドレスと比較しなければならない点があげられる．そこで，中継ノードは着信ノードが着信アドレスを通知するための固定アドレスを着信ノードごとに用意しておくことで，着信ノードがどの固定アドレスに通知したかによって，着信ノードとの秘密情報と着信アドレスを対応付けることができる．これにより，中継ノードは被中継アドレスをその着信ノードとの秘密情報を用いて生成した結果を，他の着信ノードから通知されたアドレスと比較せずに済む．また，中継処理の効率化のために，被中継アドレスが始めて使われたときに変換前後のアドレス情報を対応付けて保存する．これにより，同じ被中継アドレス宛ての 2 回目以降のパケットは保存しておいたアドレス情報に基づいてパケットを転送することで，ハッシュ変換・検索処理を削減できる．

4　発信ノードと着信ノードのアドレス変換

発信ノードは，中継ノードに発信パケットを送信し，着信ノードは，中継ノードから転送された着信パケットを受け取る．このとき，着信パケットのアドレス情報は，発信パケットのアドレス情報と異なっているため，TCP のヘッダチェックサムのように上位層での通信に問題が発生する可能性がある．そこで，発信ノードと着信ノードにおいて，上位層で固定のアドレス (以下，ダミーアドレスと呼ぶ) を見せておき，IP 層以下では通信ごとに変化するアドレスを用いることで上位層での問題を解決する．

着信ノードは受信した着信パケットの着信アドレスから発信ノードを特定できるように，事前に発信ノードと共有しておいた秘密情報から被中継アドレス系列を生成し，被中継アドレス系列から着信アドレスを生成する．これを行うために，発信ノードと着信ノードはあらかじめ安全に秘密情報とダミーアドレスを交換しておく必要がある．具体的な方法としては，図 3 に示すように，発信ノードからの行きのパケットでは，上位層において始点アドレスを発信ノードのダミーアドレス I_0，終点アドレスを着信ノードのダミーアドレス A_0 を見せておき，IP 層以下ではそれぞれのダミーアドレスを発信アドレス I_x と被中継アドレス R_x にマッピングしパケットを送信する．このとき，帰りのパケットのために対応関係 (Src:$I_0 \rightarrow I_x$，Dst:$A_0 \rightarrow R_x$) を保存しておく．着信ノードでは受け取ったパケットの終点アドレス A_y がどの被中継アドレス系列から生成された着信アドレスかによって，パケットのアドレス情報を発信された状態に戻し，上位層には発信ノードのダミーアドレス I_0 と着信ノードのダミーアドレス A_0 を見せる．このとき，帰りのパケットのために対応関係 (Src:$R_y \rightarrow I_0$，Dst:$A_y \rightarrow A_0$) を保存しておく．着信ノードからの帰りのパケットでは，図 4 に示すように，保存しておいた対応関係に基づいてアドレス情報を変更する．

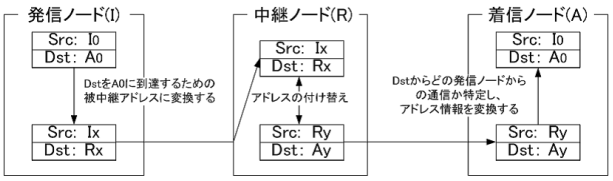

図 3: 行きのパケットのマッピング

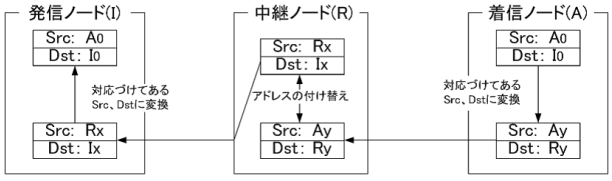

図 4: 帰りのパケットのマッピング

5　被中継アドレス系列の生成方法

中継ノードでの対応関係の生成の方法では，発信ノードと着信ノードで事前に秘密情報として共有鍵と複数の中継ノードの位置指定子を交換しておき，図 5 に示すように，被中継アドレス系列を生成する．被中継アドレス系列の生成の方法について以下に示す．

1. 履歴バッファから前回の計算で求めた値 (初回は 0 を使用) に共有鍵を足し合わせた値を結合する
2. ステップ 1 で生成した値を MD5 を使用して 128bit のハッシュ値を計算する
3. ステップ 2 で生成した値の左 64bit と中継ノード数との mod 値を計算し，取得してある中継ノードの位置指定子のリストの mod 値番目を被中継アドレスの位置指定子とする
4. ステップ 2 で生成した値の右 64bit の 6bit 目 (最も左の bit を 0bit 目とする) を 0 にセットし，これを被中継アドレスのノード指定子とする
5. ステップ 2 で生成したハッシュ値を取り出し，これを履歴バッファに格納し，次回の計算に使用する

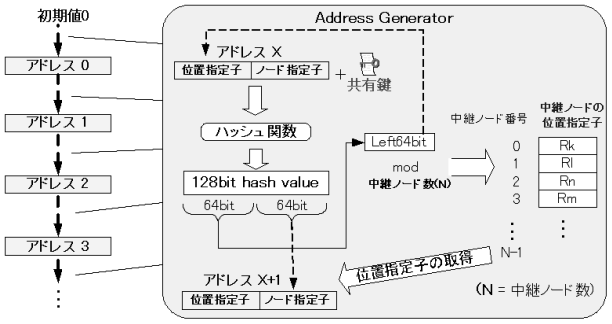

図 5: 被中継アドレス系列の生成

この方法により，共有鍵を持っている発信ノードと着信ノードだけが生成可能なアドレス系列を生成できる．また，第 3 者が系列内の被中継アドレスを取得したとしても，その被中継アドレスから前後のアドレスを生成することはできない．

6　アドレスの重複についての考察

IPv6 のアドレス空間は複数のアドレスを次々と生成していく本方式を実現する上で十分に広いと考えられるが，生成されたアドレスが偶然に一致してしまう可能性についても考える必要がある．アドレスの重複として，被中継アドレスの重複と，着信アドレスの重複が考えられる．被中継アドレスの重複は別々の発信ノードで生成した被中継アドレスが一致した場合に発生する．着信アドレスの重複は同一または別々の着信ノードで被中継アドレスをアドレス変換した着信アドレスが一致した場合に発生する．アドレスの重複にはそれぞれ発生パターンがあるので，それらについて説明する．ここで，前提条件として発信ノードと着信ノードが通信を行いたいとき，着信ノードから中継ノードへの着信アドレスの通知は，発信ノードの被中継アドレスに対するアクセスよりも先に行われるものとする．

6.1　着信アドレスの重複

着信アドレスの重複は同一ネットワークの着信ノードが異なる被中継アドレスに対して同一の着信アドレスを生成した場合に発生する．このとき，中継ノードでのハッシュ変換も同一の着信アドレスとなり，2 つの通信の区別が困難になる．そこで，着信アドレスの重複が発生した場合には，これを検出し重複した通信の一方あるいは両方について，発信ノードに通知し発信ノードが次の被中継アドレスを使うことで対応する．

着信アドレスの重複は図 6 に示す 4 つのパターンに分類できる．以下それぞれの場合について検出と通知の方法を示す．

図 6(1) の状況は，同一着信ノード A_m で着信アドレスが重複し複数の中継ノードに着信アドレスを通知しようとする場合である．着信ノード A_m は先に通知した着信アドレスを A_m : h(a, S(R_k-A_m)) とし，同じ着信アドレス A_m : h(a', S(R_l-A_m)) を生成したときに重複を検知できるので後者の通知を止める．すると，中継ノード R_l では着信アドレスが通知されていないので発信ノード I_j からの通信に対してエラーを通知する．

図 6(2) の状況は，同一着信ノード A_m で着信アドレスが重複し中継ノード R_k に着信アドレスを通知しようとする場合である．着信ノード A_m は先に通知した着信アドレスを A_m : h(a, S(R_k-A_m)) とし，同じ着信アドレス A_m : h(a', S(R_k-A_m)) を生成したときに重複を検知できるので後者の通知を止める．しかし，この場合は最初の通知を使って発信ノード I_j からパケットが転送されてくる可能性があるので着信アドレス A_m : a+に送られてきた通信を拒否する．

図 6(3) の状況は，着信ノード A_m と着信ノード A_n が同一ネットワークに所属し，別々の着信ノードで生成した着信アドレスが重複した場合である．この場合は着信アドレスの重複を NS/NA メッセージなどで検知できるので後者の通知を止める．すると，中継ノード R_l では図 6(1) と同様にエラーを通知する．

図 6(4) の状況は，着信ノード A_m と着信ノード A_n が同一ネットワークに所属し中継ノード R_k に着信アドレスを通知する場合である．先に通知した着信アドレスを A_m : h(a, S(R_k-A_m)) とし，同じ着信アドレス A_n : h(a', S(R_k-A_n)) を生成したときに着信アドレスの重複を図 6(1) と同様に検知でき，後者の通知を止める．すると，中継ノード R_k では，S(R_k-A_n) を用いたハッシュ変換の結果 A_m : (a', S(R_k-A_m)) は登録されないので発信ノード I_j からの通信に対してエラーを通知する．

6.2　被中継アドレスの重複

被中継アドレスの重複は図 7 に示すように別々の発信ノードで同一の被中継アドレスを生成した場合に生じる．このとき，中継ノードでは重複した被中継アドレスのハッシュ変換結果が複数の着信アドレスと一致してしまい，中継先の区別が困難になる．そこで，中継ノードは被中継アドレスの変換結果が複数の着信アドレスと一致した場合に，これを検出して，発信ノードに通知する．通知された発信ノードは次の被中継アドレスを使うことで対応する．

被中継アドレスの重複と着信アドレスの重複が同時に生じる場合も考えられる．例えば，図 7 において a+ = a-の場合である．この場合，着信アドレスの重複が検出されて，着信アドレスの通知は片方しか行われないため，被中継アドレスの変換結果が複数の着信アドレスと一致することでの重複検出ができない．しかし，この場合複数の着信ノードとの共有鍵による変換結果が 1 つの着信アドレスに一致するので，これを検出して発信ノードに通知する．通知された発信ノードは次の被中継アドレスを使うことで対応する．

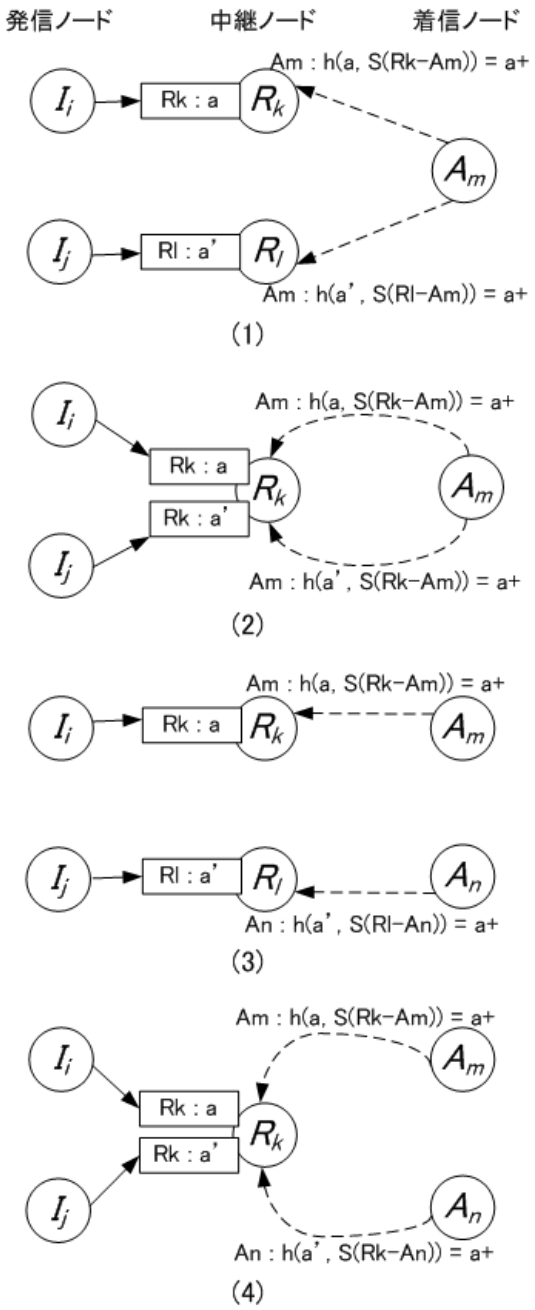

図 6: 着信アドレスの重複パターン

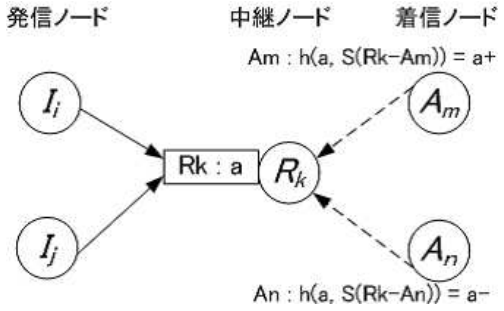

図 7: 被中継アドレスの重複

7 中継ノード処理のオーバヘッドの評価

7.1 中継ノードの実装

提案した方法では被中継アドレスが初めて使われるときに中継ノードでハッシュ変換と着信アドレスの検索を行う必要がある．これらの処理のオーバヘッドを測定するために中継ノードの実装を行った．実装において 2 回目以降の中継処理の効率化のために，発信パケットと着信パケットのアドレス情報を対応付けて保存しておくことにした．これによって，発信ノードから既にハッシュ変換をしたことがあるアドレス情報を持つパケットが届いた場合は，ハッシュ変換せず，その保存しておいたアドレス情報に基づいてパケットを転送することができる．

7.2 測定環境

中継ノードのアドレス変換を実装し，中継オーバヘッドの測定を行った．実験環境としては図 8 に示すように各ノードを別々のネットワークに設置した．また，中継ノードが位置指定子で表されるネットワークへのルータに見える経路を設定した．測定では 1 つの着信ノードとの共有鍵に対して通知されている着信アドレスは 1 つと設定して，中継を利用する場合と利用しない場合について Ping6 を用いた RTT の測定を行った．

7.3 測定結果

測定の結果を図 9 に示す．中継を利用しない場合の RTT は約 1.75ms であった．中継を利用した場合では被中継アドレスに対する初回のパケットにおいて着信ノードとの共有鍵数に比例してオーバヘッドが増加し

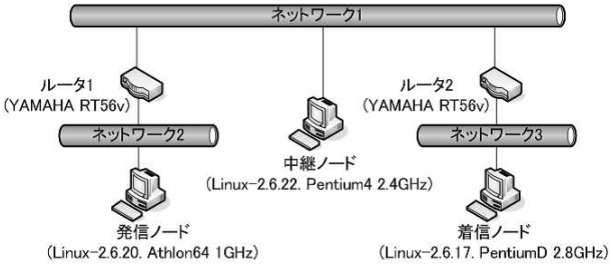

図 8: 実験環境

たが，共有鍵数が 1000 個の場合であっても約 2ms 程度のオーバヘッドであった．一方，同じ被中継アドレスに対する 2 回目のパケットでは変換前後のアドレス情報を保存しているためハッシュ変換や検索処理を行わない．そのため，着信ノード数によらず RTT はほぼ一定であった．

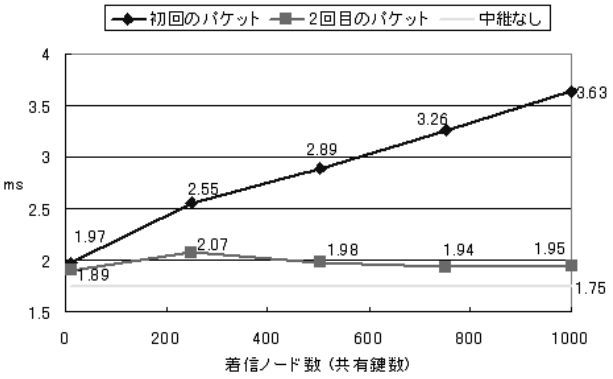

図 9: 測定結果

8 おわりに

本研究では送信先アドレスによるメッセージの関連付けの問題に対して，アドレスを変換する複数の中継を分散配置し，送信者 (発信ノード) と中継者 (中継ノード) の間でアドレス変換の対応関係のための事前通信を行わずに，中継ノードがアドレスを変換する方法を提案した．提案した方法により，送信先アドレスによるメッセージの関連付けを防ぐことができ，発信ノードと中継ノードの間で事前通信を行わないことでメッセージの関連付けの可能性を軽減することができる．実装した中継ノードを用いた RTT の測定により，中継による通信のオーバヘッドが数ミリ程度に抑えられることを確認した．

実際の運用にあたっては発着信ノードでのオーバヘッドや複数の通信が同時に行われる時のスケーラビリティを考慮する必要があるので，今後，発着信ノードの実装を行い，これらの評価を行う．

参考文献

[1] Goldberg, I., “Privacy-enhancing technologies for the Internet, II, five years later”, In, Proceeding of the Workshop on Privacy on Privacy Enhancing Technologies, LNCS 2009, San Francisco, CA, USA, 2002, pp.1-12.

[2] Kent, S., Seo, K. ”Security architecture for the Internet protocol” RFC 4301, 2005.

[3] Haddad, W., Nordmark, E. ”Privacy Aspects Terminology draft-haddad-alien-privacy-terminology-03”, Network Working Group, Internet-Draft, 2007.

[4] T. Narten and R. Draves: “Privacy extensions for stateless address autoconfiguration in IPv6”, RFC 3041, 2001.

[5] M.Gruteser and D.Grunwald: “Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis”, Mobile Networks and Applications 10, 2005, pp.315-325.

[6] Waters, B.R., Felten, E.W., Sahai, A.: Receiver anonymity via incomparable public keys. In: CCS ’03: Proceedings of the 10th ACM conference on Computer and Communications Security, Washington D.C., USA, 2003, pp.112-121.

[7] Goldschlag, D., Reed, M., Syverson, P. ”Onion Routing”, Communications of The ACM, Vol.42, 1999, pp.39-41.

[8] 市川 隆浩，坂野 あゆみ，寺岡 文男: “匿名性のある IPv6 モビリティ通信プロトコル”，第 8 回インターネットテクノロジーワークショップ, 2007, pp.36-44.

[9] Sakurai, A., Minohara, T., Sato, R. and Mizutani, K.: One-Time Receiver Address in IPv6 for Protecting Unlinkability, *Proc. ASIAN 2007*, pp.240-246.