IPv6通信の関連付け防止のための受信者アドレスのワンタイム化

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

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．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．

これまでに，我々は，アドレス変更の範囲を広範囲に利用できるIPv6通信を対象に，受信ノードのアドレスに関する非関連性の実現を目的として，送信ノードと受信ノードが連携することで受信ノードのアドレスを変更するワンタイムアドレスを提案している[1][2]．この方法は，暗号化キーを送受信者で共有しておき，誰でも入手可能なダミーアドレスと暗号化キーをパラメータとして，秘密のアドレス系列を独立に生成し，アドレスを順番に使用することでアドレス情報に対する関連付けを防ぐ．しかし，提案したワンタイムアドレスはインターフェースID部分のみを変更するためプレフィックス部分による関連付けの問題が残されている．

本研究では，プレフィックス情報による関連付けを防ぐ方法として，送信ノードと受信ノードの間に中継ノードを設置し，複数の中継ノードを切り替えることでプレフィックス部もワンタイム化する方法を提案する．

2 中継による関連付け防止

信頼できる中継ノードにおいてアドレス情報の付け替えを行うことで，以下のいずれか一方の非関連性を達成する方法について提案する．

- アドレス情報から特定のネットワーク宛ての通信であることを推定できないようにする (受信ネットワークの関連付け防止)
- アドレス情報から特定のネットワーク発の通信であることを推定できないようにする (送信ネットワークの関連付け防止)

One-Time IPv6 Address with Translation via Relay Node.
[†]Graduate School of Engineering, Takushoku University
[‡]Department of computer Science, Takushoku University

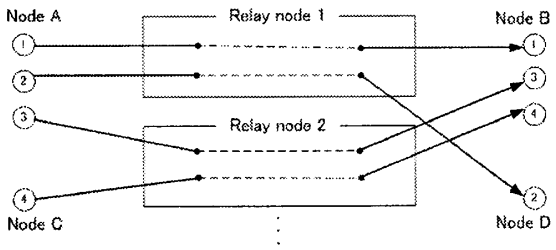

図 1: 中継ノードによるアドレス情報の関連付け防止

中継ノードを使うことによるプレフィックス部の関連付け防止の例を図1に示す．ここで，各ノードは別々のネットワークに所属しているとする．ノードAはノードBに2回(①，③)，ノードDは1回(②)の通信を行い，ノードCはノードBに1回(④)の通信を行っている．中継ノードより手前の部分では，送信先アドレスのプレフィックスは中継ノードのネットワークを指すことになり，どの受信ネットワークへの通信か区別できない．中継ノードよりも先の部分では，送信元アドレスのプレフィックスは中継ノードのネットワークを指すことになり，どの送信ネットワークからの通信かを区別できない．さらに，中継ノードを複数利用することで，1つの中継ネットワークを監視された場合に，アドレス情報を関連付けられることを防ぐ．

3 中継ノードでのワンタイムアドレス変換

中継ノードでのアドレス変換では，中継ノード以外はアドレスがどう付け替えられるのかがわからなく，中継ノードだけがアドレス変換の対応関係を知る必要がある．そこで，中継ノードは，中継先ノードごとに異なる受信アドレスを用意し，送信ノードがアクセスした受信アドレスによって中継先を決定する．このとき，複数の送信ノードで同じ受信アドレスを使用すると，別の送信ノードに中継先がわかることになるので，受信アドレスは送信ノードごとに用意する．さらに，受信アドレス及び，中継先アドレスを固定すると，同じアドレスを使っている通信の関連付けができてしまうため，これらのワンタイム化を行う．

アドレスのワンタイム化には，先に提案した IPv6 ワンタイムアドレス同様に，ダミーアドレス，暗号化キーをパラメーターとして順次生成したアドレス系列を用いる．今，送信ノード S と中継ノード P 及び，受信ノード R がそれぞれ共有鍵 $K_S(SP)$，$K_S(PR)$ を共有し，全ノードが受信ノード R の公開鍵 $K_P(R)$ と各ノードのダミーアドレスを入手していると仮定する．送信ノード S と中継ノード P は，受け入れアドレス系列のパラメーターとして，中継ノード P のダミーアドレス (Pr_P : I_{P0}) と $K_S(SP)$+$K_P(R)$ を用いることで受信ノードごとに異なる受け入れアドレス系列を生成，共有する．また，中継ノード P と受信ノード R は，受信ノード R のダミーアドレス (Pr_R : I_{R0}) と $K_S(PR)$+$K_P(R)$ をパラメーターとする中継先アドレス系列を生成，共有する．中継ノードでは，同じ公開鍵 $K_P(R)$ をパラメータに使った受け入れアドレス系列と中継先アドレス系列を対応付ける (図 2)．上記により，2 つの共有鍵を取得できるのは中継ノード P だけであり，中継ノード P 以外が両方のアドレス系列を生成することはできず，対応付けることもできない．

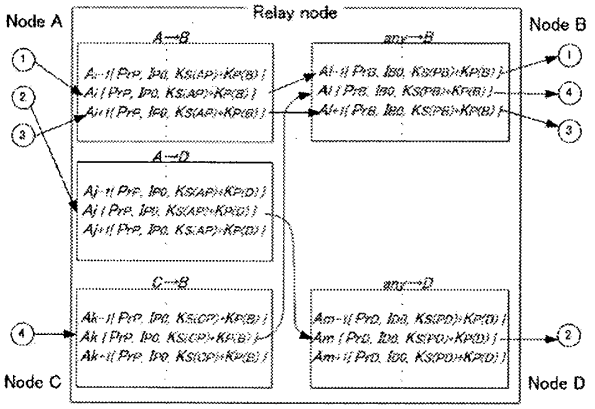

図 2: 中継ノードによるアドレス系列の対応付け

中継ノードでのアドレスの変換によって，上位層のチェックサムの計算結果が合わなくなることを防ぐため，中継ノードの送信元アドレスの値の選択に自由度が残されていることを利用し，チェックサムが保存されるように中継ノードの送信元アドレスを調整する．

4 動作実験と性能評価

中継ノードでは各送信ノードに対して中継先受信ノード数の受け入れアドレス系列を用意する必要がある．中継ノードは，受信したパケットの宛先を受け入れアドレス系列から探索するため，受け入れアドレス系列の数が多い場合，アドレス付け替えのオーバーヘッドが大きくなると考えられる．そこで，オーバーヘッドを評価するための実験を行った．図 3 に示す構成のネットワークにおいて，送信ノードと受信ノード間の RTT を ping6 で測定した結果を図 4 に示す．プロトタイプの中継ノードではアドレス系列の検索に線形探索を用いているため，アクセスしたアドレス系列の先頭からの位置によって処理時間が変化する．中継を使用しない場合の RTT の値は 1.9ms で，最初のアドレス系列をアクセスした場合の中継オーバーヘッドは約 0.1ms と極めて小さい．また，送信ノード数，受信ノード数がともに 100 ノードの場合の最悪値 (10000 番目のアドレス系列) でも 5ms 程度のオーバーヘッドで中継できる．

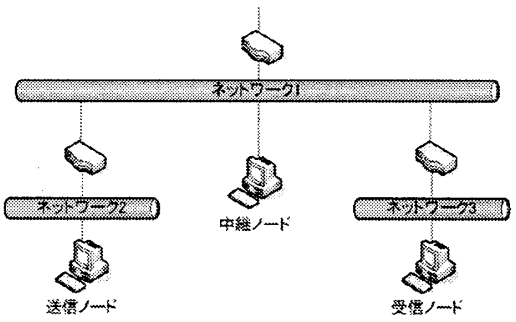

図 3: 実験環境

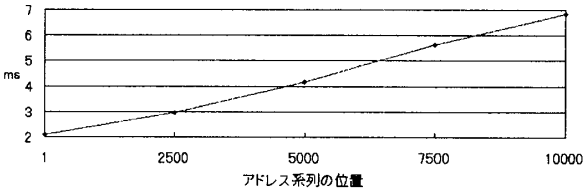

図 4: アクセスしたアドレス系列による RTT の差

5 おわりに

本稿では IPv6 通信におけるネットワークレベルでの関連付けを困難にする手法について提案した．また，提案手法のアドレス付け替えを行う中継ノードを実装し，プレフィックスによる関連付け防止対策が実現可能なことを確認した．さらに，アドレスの付け替えを少ないオーバーヘッドで実現可能なことを確認した．

参考文献

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

[2] 桜井敦史，蓑原隆，佐藤良太：IPv6 における着信側のプライバシー向上のためのワンタイムアドレスの実現, WIT2007, pp.30-35, (2007).