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の実装

佐藤 良太† 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．プライバシー保護の対象として，通信の内容は IPSec などの暗号化技術によって保護できるが，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はできない．アドレス情報を知られることによる問題の 1 つに非関連性 (Unlinkability) の喪失がある．これはアドレス情報を元に複数のメッセージが関連付けられること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という問題である．

インターネットの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 [1] が提案されている．しかし，始点アドレスを変更しただけでは非関連性は十分に得られない．例えば，社内ネットワークへ VPN 接続するための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，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可能性がある．

本稿で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に通信を行う状況において，パケットの終点アドレスによるメッセージの関連付けを防ぐための中継サービスについて具体的な実装と評価を示す．

2 アドレス変更による関連付けの防止

アドレス情報が常に固定であることは通信を関連付けられる原因となる．そこで，我々は図 1 のように送信先アドレスを変更するために複数の中継者 (中継ノード) を分散配置し，中継ノードの受信するアドレス (被中継アドレス) 及び，受信者 (着信ノード) のアドレス (着信アドレス) を適宜変更する方法を提案している [2]．アドレス変換を行なうためには変換前後のアドレスの対応が必要となる．提案手法では変換前後のアドレスの一部 (ノード指定子) に秘密キーによる一方向性の関係を持たせる．図 2 に示すように，アドレス変換は事前に変換後のアドレスを計算して中継ノードに登録し (①②)，中継時に同じ計算を行い登録アドレスから一致するものを検索する (③)．

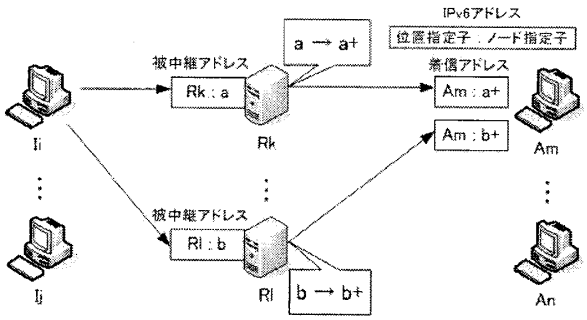

図 1: 中継者の分散配置

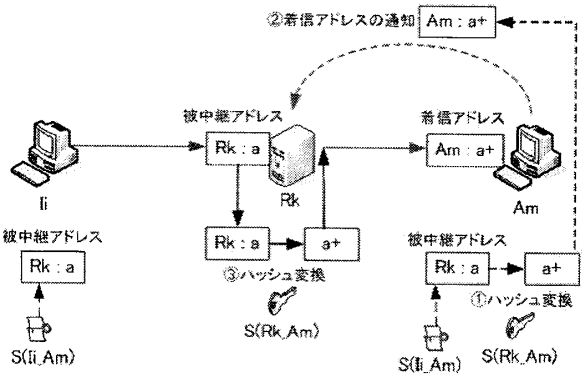

図 2: 中継者での着信アドレスの生成

提案手法は発信ノードと中継ノードの間では事前にアドレス変換に関する情報を通知せずに済むという利点がある．また，盗聴者は着信アドレスを受信しただけでは，アドレスの変換関係を知ることができない．

Implementation Distributed Relay Service for Providing Unlinkability of One-time Destination Addresses in IPv6 Communications.

†Ryota SATO, Graduate School of Engineering, Takushoku University
‡Takashi MINOHARA, Department of computer Science, Takushoku University

3 システムの実装

提案手法を実現するためにアドレス情報の通知方法など，詳細な仕様を定め，LinuxPC 上に中継システムを実装した．

3.1 中継ノードの実装

中継ノードの処理はユーザ空間のプロセスとして実装した．同一通信の 2 パケット目以降のハッシュ変換処理を軽減するために，被中継アドレスが初めて使われたとき (初回パケット到着時) に変換前後のアドレス情報を対応付けて保存し，同じ被中継アドレス宛ての場合は保存しておいたアドレス情報に基づいて転送する．

3.2 発着信ノードの実装

中継ノードでアドレスを変換することで，TCP のチェックサムなどの上位層で問題になる場合がある．そこで，発着信ノードの処理は OS のパケットフィルタ機能 (ip6tables) を拡張し，上位層では固定のアドレスを見せておき，下位層では固定アドレスと変化するアドレスにマッピングすることとした．

4 性能評価

中継処理を行なうことで余分な経路を通ることによるオーバヘッドと中継処理によるオーバヘッドが生じる．前者はネットワーク構成に依存するため，本稿では後者について，図 3 に示す実験ネットワークを使って測定を行なった．

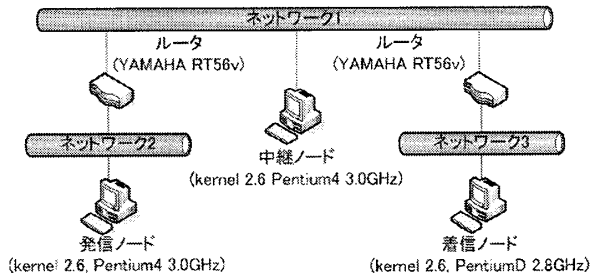

図 3: 実験ネットワーク

4.1 ハッシュ計算のオーバヘッドの測定

中継処理において初回パケット到着時には登録されている着信ノードの秘密キーの数分のハッシュ計算のオーバヘッドが生じる．秘密キーの数に対するハッシュ計算処理時間の測定を行なったところ，図 4 に示すように，秘密キー数に対して線形に増加するが，秘密キー数が数千個以内であれば数ミリ秒となることがわかった．さらに，秘密キー数が 1000 個の場合のハッシュ計算時間を M/M/1 モデルにあてはめ，到着初回パケット数/秒に対する処理待ち時間を計算すると図 5 のようになった．この結果から，中継ノードに登録されている秘密キーが 1000 個の場合，到着初回パケット数が 500 パケット/秒以下であれば，数ミリ秒程度の処理待ち時間で中継処理を行なうことができる．

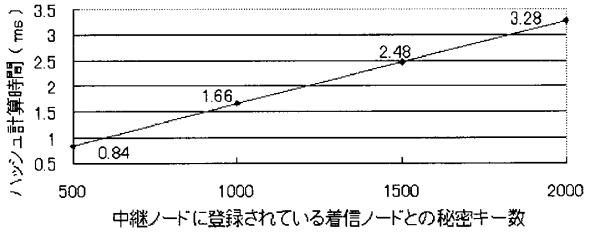

図 4: 着信ノードとの秘密キーによるハッシュ計算時間

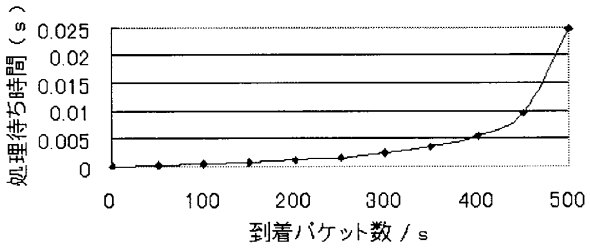

図 5: 到着パケット数に対する処理時間の変化

4.2 中継処理のオーバヘッドの測定

中継処理のオーバヘッドの測定として，Ping6 を用いて RTT の測定を行なった．中継を利用しない場合 (発信ノードが直接着信ノードにアクセスする場合) と，中継を利用した場合について行なった．測定の結果，2 パケット目以降の中継によるオーバヘッドは約 0.2ms 程度で中継処理できることを確認した．

5 おわりに

本稿では終点アドレスによるメッセージの関連付けを防ぐ提案手法の実装について述べた．実装したシステムの中継処理に要するオーバヘッドを測定した結果，アドレスの付け替えを少ないオーバヘッドで実現可能なことを確認した．

参考文献

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

[2] 佐藤 良太，桜井 敦史，蓑原 隆，“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”，インターネットテクノロジーワークショップ (WIT2008), (Jun 2008).