4U-4

IPv6通信におけるプライバシー向上のための ワンタイムアドレスの実現

桜井 敦史† 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

次世代のインターネットプロトコルであるIPv6は、アドレス長を128ビットに拡大することでIPv4に比べてグローバルアドレスの割り当てについて高い自由度を持っている。特にルータから受け取るネットワークプレフィックスとノードのインタフェースIDから一意にアドレスを生成するステートレスアドレス自動設定[1]は、特別な設定なしにグローバルアドレスを割り当てることができ、アドレス管理のコストを軽減できる。しかしこのグローバルアドレスは固定的なアドレスであり、ホストの断定・追跡が容易になるため、例えペイロードが暗号化されていてもアドレスから盗聴者によってホストの動向が追跡されてしまう恐れがあるというプライバシーの点で懸念がある。この問題に対して通信のプライバシーを確保するために時間と共に変化するランダムな一時アドレスがRFC3041[2]で定義されている。この一時アドレスは通信を開始する側の送信元として使用することができるが、End-to-Endの通信において接続先の変化する一時アドレスに直接アクセスすることは現実的ではない。よってアクセスされる側は変化しない永続的なアドレスを使用する必要があり、通信のプライバシー保護が制限されるという問題があげられる。

本研究でIPv6通信におけるプライバシー向上のために、通信を開始するノード（以下、発信ノード）が通信を受け付けるノード（以下、着信ノード）の一時アドレスにアクセスする仕組みを提案する。またIPv6の特徴である広大なアドレス空間を利用して、着信側が使用するアドレスをワンタイムにすることで通信者の断定・追跡を困難にしプライバシー向上を図る。

2 着信側アドレスのワンタイム化

発信ノードが着信ノードのワンタイムな一時アドレスにアクセスするために次の機能を実現する。

1. 発信ノードは宛先である着信ノードの一時アドレスを決める
2. 着信ノードは発信ノードが決めたアドレスに対するアクセスを受け入れるためオンデマンドにアドレスを割り当て、通信終了時にはアドレスを削除する
3. 盗聴による許可しないノードからのアクセスを防ぐ

このようにワンタイムなアドレスにするために互いのノードに複数のアドレスをリスト化したアドレスリストを持たせる。これを他のノードからは知られていない秘密のアドレスリストとして共有し、リストの先頭から順に使用していく。また着信ノードは複数の発信ノードからのアクセスに対応できるようにするが、許可しないノードからのアクセスは受け付けないようにする。

2.1 アドレスリストの生成と共有

アドレスリストを共有化するために着信ノードはアドレス生成に必要なネットワークプレフィックスとインタフェースIDの基になる値（以下、ダミーアドレス）をDNSによって公開する。DNSを利用することで発信ノードはどこからでも着信ノードの新しいダミーアドレスを手に入れることができる。そしてあらかじめ共有した両ノードだけが持つキーによって秘密のアドレスリストを生成する。

アドレスリストはMD5などの非可逆型ハッシュ関数を使用して生成する。生成手順は図1のようにダミーアドレスのインターフェースID0とキーからインタフェースID1を生成し、次にインタフェースID1とキーからインタフェースID2を生成する。アドレスリストの使用順序は生成順序とは逆の順番で使用していく。これによってアドレスを盗聴されてもハッシュ関数の非可逆性から次に使用するアドレスの推測を困難にすることができる。またアドレスリストをすべて使用したら再び新しいダミーアドレスを登録する。

以上のアドレスリストの生成からアクセスまでの処理をまとめたものを図2に示す。

One-Time Address Generation for Privacy Extensions in IPv6 Communications.

†Atsushi SAKURAI, Graduate School of Engineering, Takushoku University
‡Takashi MINOHARA, Department of computer Science, Takushoku University

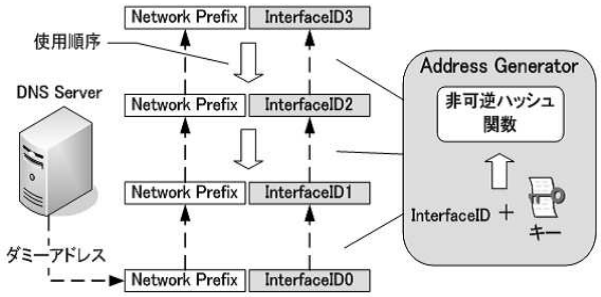

図 1: アドレスリストの生成と使用順序

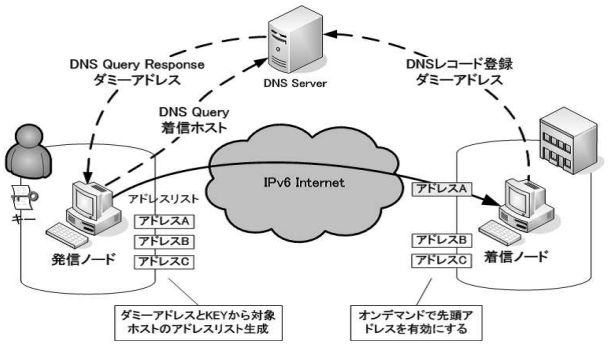

図 2: 発信ノードから着信ノードへのアクセス

2.2 オンデマンドなアドレスの割り当てと削除処理

着信ノードはアドレスリストの全てのアドレスを NIC に割り当てておくのではなく、次の通信が発生したときに割り当てを行なう。

IPv6 ではアクセスを受ける前にアドレス解決である ICMPv6 の NS（近隣探索）パケットがマルチキャストで送信される。NS パケットのターゲットアドレスが着信ノードのアドレスリストに存在し、NIC に割り当てていない未使用なアドレスだった場合、そのアドレスを NIC に割り与え通信を開始する。また TCP 通信に限り FIN パケットの受信によって通信は終了と判断し、宛先アドレスを NIC とアドレスリストから削除する。

オンデマンドなアドレスの割り当てと削除処理を行なうために着信ノードは受信したすべてのパケットの宛先アドレスがアドレスリストに存在するか探索を行なう必要がある。さらに着信ノードは複数の発信ノードからのアクセスに対応するために、それぞれ違った値のキーから生成した複数のアドレスリストを持つ。この複数のアドレスリストの探索はそれぞれのアドレスリストの先頭アドレスを探索していく。このことから図 3 のように使用済みとなったアドレスは削除し、リンクの付け替えを行なう。このため先頭アドレスは双方向のリスト構造をとる。またアドレスリスト内は使用済みを削除していくため単方向リストをとる。

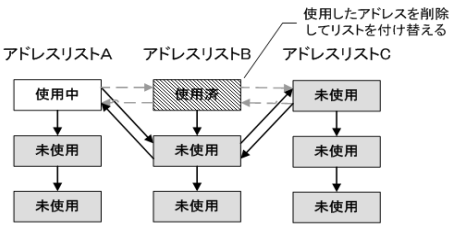

図 3: アドレスリストのデータ構造

2.3 発信ノードの認証

通信の盗聴による不正なアクセスを考慮し、許可する発信ノードからのアクセスを徹底させる必要がある。広大なアドレス空間において秘密のアドレスに最初にアクセスできるのは許可した発信ノードであると判断できる。よって着信ノードは最初にアクセスしてきた発信ノードのアドレスを記憶しておき、他のアドレスからのアクセスを拒否することで許可しないユーザからの不正なアクセスを防ぐ。

3 実装

これまでに Linux 用の IPv6 プロトコルスタック USAGI カーネル[3](スナップショット 20060918 版) を変更し、着信ノードのオンデマンドなアドレスの割り当て・削除処理を実現した。アドレスリストを共有した発信ホストからの TCP 接続に対して着信ホストの一時アドレスが正しく割り与えられた。またコネクションの切断と同時にアドレスを NIC 及びアドレスリストから削除し、ワンタイムアドレスを実現することができた。

4 おわりに

本稿では IPv6 のグローバルアドレスの使用時にノードの断定・追跡が容易になる問題に対して、許可する発信ノードからワンタイムで変化する一時アドレスにアクセスできる仕組みを提案した。そして実際のカーネルに機能を組み込むことで提案した方法によるプライバシー向上のためのワンタイムアドレスが実現可能であることを確認した。

参考文献

[1] T. Narten, R. Draves, ”IPv6 Stateless Address Autoconfiguration”, RFC2462, December 1998

[2] S. Thomson, T. Narten, ”Privacy Extensions for Address Configuration in IPv6”, RFC3041,January 2001

[3] USAGI Project - Linux IPv6 Development Project, http://www.linux-ipv6.org/