IPv6ワンタイムアドレスにおけるMACアドレス変換

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

1 はじめに

近年インターネットの普及に伴いプライバシーの保護が重要になっている．プライバシー保護において，IPsecなどを用いて暗号化することにより，メッセージそのものの内容は保護できるが，配送に使用されるアドレスによって複数のメッセージの関連付けが行われてしまうという問題が残っている．この問題に対して，我々はIPv6を対象としてIPレベルでアドレスを切り替えていくIPv6ワンタイムアドレス[1]を提案したが，Ethernetのように複数のノードがデータリンクレベルを共有している場合にMACアドレスでの関連付けが出来てしまうという問題がある．そこで本研究ではMACアドレスを秘匿化し，イーサヘッダ及びIPヘッダの情報による異なるパケットの関連付けを困難にすることを目的とする．

2 ブロードキャストアドレスを用いたMACアドレスの秘匿化

MACアドレスの秘匿化として，まずブロードキャストアドレスを利用する方法を考案した．ブロードキャストアドレスを用いて送信を行うことで全てのノードに送信が行われることになるが，全ノードが同じアドレス情報を使用することになるため，MACアドレスからはそのパケットが誰から送信されたものなのか，またはそのパケットは誰に宛てたものなのかといった情報が知られることはない．正当な受信ノードはMACアドレスから自分宛のデータであるか判断出来ないが，IPアドレスから自分宛と知ることが出来る．

パケット内のMACアドレスをブロードキャストアドレスに変換して通信を行うには，まずパケットを送信するノードがイーサヘッダ内に含まれる送信元MACアドレスをブロードキャストアドレスに変更する必要がある．また，相手から送信されてくるパケットに実際のMACアドレス情報が使われることを防ぐために，MACアドレスをノード間で交換し合うために送信される近隣要請(NS)メッセージや近隣応答(NA)メッセージに含まれるMACアドレスもブロードキャストアドレスに変更する．これらのアドレス変換によって，送信と受信の両パケットで架空のMACアドレスとしてブロードキャストアドレスを用いることが可能である．

プロトタイプの実装として，Linuxのブリッジ機能を用いて仮想インターフェイスを作成し，仮想インターフェースと実際のインターフェイスとの間においてカーネルレベルでパケットの監視を行って条件に合致したパケットの変更を行うシステムを作成した．パケットの監視・変更の機能はカーネルモジュールとして作成している．

プロトタイプの実装によりブロードキャストアドレスを用いた秘匿化が可能であることを確認したが，この手法では全ての端末へ情報の送信が行われると共にルータからのリダイレクトメッセージが送信されるので無駄なパケットが増大するという問題がある．

3 動的アドレス変更によるMACアドレスの秘匿化

MACアドレスの秘匿化として，次にMACアドレスを変化させる方法を考案した．具体的には，IPv6ワンタイムアドレスから一対一の関係でMACアドレスを生成し，IPv6ワンタイムアドレスの変更に同期させてMACアドレスの変更を行う．生成するMACアドレスはIPv6ワンタイムアドレスの下位48bitを使用し，I/GbitとG/Lbitは0にする．

MACアドレス長はIPv6ワンタイムアドレスにおいて重複確認が可能な下位64bitよりも短いためアドレスが重複する可能性がある．そこで本研究ではIPv6ワンタイムアドレスの重複検出処理を拡張して，MACアドレスの重複が発生した場合にもIPv6ワンタイムアドレスの再設定を行うようにした．このとき，重複確認時のNSメッセージのMACアドレスの衝突を避けるために，送信元MACアドレスとしてG/Lbitを1にしたMACアドレスを使用する．NSメッセージを受信したノードは相手のMACアドレスを取り出しG/Lbitを0に戻した後に自分自身が使用しているMACアドレスリストと比較する．もしMACアドレスがリスト内に存在した場合はIPv6アドレスの重複の有無にかかわらずNAメッセージを送信して，重複を通知する．

MAC Address Translation in IPv6 One-Time Address.
†Department of computer Science, Takushoku University
‡Graduate School of Engineering, Takushoku University

プロトタイプの実装として前説同様仮想インターフェースを利用したカーネルモジュールを作成した．このとき本来のMACアドレス以外のパケットを受信するために，インターフェイスをプロミスキャスモードで起動して自分以外のMACアドレス宛てのパケットも受信するようにした．また，カーネルレベルのMACアドレスチェックでパケットが破棄されることを防ぐために，受信したパケットのMACアドレスがアドレスリストに登録されていた場合は実際のMACアドレスに書き換えて受信が行えるようにした．

4 実験による評価

提案したアドレス変換処理のオーバーヘッドを評価するために通常カーネル，ブロードキャストアドレス使用，動的アドレス変更使用のそれぞれの性能を測定した．動的アドレス変更については通信に使用するアドレスのアドレスリスト中の位置による違いも評価した．

4.1 遅延時間の測定

同一リンク内の実装を行っていないノードからping6を送信して応答時間(RTT)の測定を行った．

表1: 応答時間の測定結果(ms)

通常カーネル

送信回数	1	2	3	4
平均値	1.223	0.127	0.127	0.126
標準偏差	0.055	0.006	0.006	0.006

拡張カーネル(ブロードキャストアドレス使用時)

送信回数	1	2	3	4
平均値	1.245	0.133	0.132	0.132
標準偏差	0.059	0.004	0.005	0.003

拡張カーネル(動的アドレス変更，アドレスリスト先頭のアドレス使用時)

送信回数	1	2	3	4
平均値	1.240	0.131	0.131	0.131
標準偏差	0.052	0.005	0.006	0.005

拡張カーネル(動的アドレス変更，アドレスリスト10番目のアドレス使用時)

送信回数	1	2	3	4
平均値	1.241	0.131	0.131	0.131
標準偏差	0.050	0.006	0.005	0.005

拡張カーネル(動的アドレス変更，アドレスリスト100番目のアドレス使用時)

送信回数	1	2	3	4
平均値	1.260	0.134	0.134	0.134
標準偏差	0.051	0.005	0.005	0.006

対象アドレスへの最初の通信ではNS，NAメッセージによるアドレス解決処理が発生するため2回目以降に比べてRTTが大きくなる．提案したアドレス変換によるオーバーヘッドは，この最初の通信に対してブロードキャストアドレス，動的アドレスともに20μsec程であった．また，動的アドレス変更の100番目に対するアクセスでは更に20μsec程度のオーバーヘッドが加算されている．一方，2回目以降の通信のオーバーヘッドはいずれの場合も数μsec程度であった．これらの結果から，アドレス変換が通信速度に与える影響は実用上問題ない範囲であるといえる．

4.2 メモリ使用量の測定

通常カーネル，拡張カーネルについて同一リンク内の2ノード間のスループットを測定したところ，動的アドレス変更においては通常カーネルとの差はみられなかったがブロードキャストアドレスでは著しい性能低下が観測される場合があった．これは前述のルータからのリダイレクトメッセージが原因であると考えられる．

4.3 メモリ使用量の測定

メモリ使用量は，他プロセスの影響を抑えるためにCUI環境での計測を行った．通常カーネルや拡張カーネルの動的アドレス変更使用時においてアドレスリストに100個のアドレスを登録して計測を行ったが，メモリ使用量は約71MBのままほとんど変わらなかった．よってアドレスリスト使用時におけるメモリ使用量の増加は僅少である．

5 おわりに

IPv6ワンタイムアドレスにおけるMACアドレス変換としてMACアドレスを秘匿する方法についてブロードキャストアドレスを用いる方法と，動的アドレス変更を用いる方法の提案を行い，実装を行った．実装したシステムを用いて，実際にMACアドレスの秘匿化が可能であることを確認した．

ブロードキャストアドレスによる秘匿化では，ルータからのリダイレクトメッセージが送信されるとき，性能が低下する．そのためMACアドレスを秘匿する場合には動的アドレス変更を用いることが望ましい．

参考文献

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