様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月１５日現在

機関番号：32638
研究種目：基盤研究（C）
研究期間：2009～2011
課題番号：21560413
研究課題名（和文）IPv6 通信アドレスに関するプライバシー保護

研究課題名（英文）Privacy Enhancement in IPv6 Address

研究代表者
蓑原　隆（MINOHARA Takashi）
拓殖大学・工学部情報工学科・教授
研究者番号：80239334

研究成果の概要（和文）：本研究では広大なアドレス空間を持つ IPv6 通信を対象としてアドレスに関するプライバシーを高める方法として，複数の中継ノードを利用するアドレス変換，および，Mobile IPv6 におけるホームエージェントの多重化による位置プライバシーの保護の方法を提案した．また，Linux 上に提案手法を実装し，そのオーバヘッドがネットワークの遅延速度に比べて許容範囲内であることを実験ネットワークで確認した．

研究成果の概要（英文）：In this study, we have proposed two methods for enhancing privacy concerning the IPv6 addresses: receiver address translation using distributed relay service, and multiple home agents of Mobile IPv6. We have implemented the prototype of proposed methods on Linux system, and conducted some experiments. The result shows that the overheads are negligible compared to typical delay time in the Internet communications.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,000,000	300,000	1,300,000
2010 年度	400,000	120,000	520,000
2011 年度	400,000	120,000	520,000
総　計	1,800,000	540,000	2,340,000

研究分野：通信・ネットワーク工学
科研費の分科・細目：工学，電気電子工学，通信・ネットワーク工学
キーワード：セキュアネットワーク，ディペンダブルコンピューティング

１．研究開始当初の背景

インターネットが広く一般に利用されるに伴い，通信当事者のプライバシーの保護に対する関心が高まっている．インターネット通信で送受されるパケットは，最終的な送受信者間で伝達される情報と，アドレスに代表されるパケットの配送に使われる情報で構成される．前者は封書に入れられた手紙のように暗号化によって第三者から保護することができるが，後者については封書の表書きのように情報の伝達に携わるものが使用することから，暗号化によって当事者以外に秘密にすることが困難である．このため，通信当事者が特定のアドレスを使用し続けた場合，アドレスを手掛りに複数の通信を関連付けることが可能になる．すなわち，第三者は容易に特定の個人の通信を取り出すことができ，その通信状況を知ることができるようになる．さらに，通信アドレスを特定されることは，正当な通信対象以外からのアクセスを

受ける可能性の増大に繋がる．よって，アドレス情報の保護は，単にプライバシーの問題だけでなく不正アクセス等に対する安全面からも重要な意味を持つ．

アドレス情報の保護には，本研究が対象とするものも含めて 3 つの方法が考えられる．

①多数の中継ノードと多重の暗号化を用いる方法

Goldschlag らによって提案された Onion Routing では，パケットを中継ノードのアドレスも含めて多重に暗号化し，中継ノードでタマネギの皮をむくように逐次復号化して次の中継先のアドレスを取り出すという方法で受信者のアドレスを秘匿する．郵便に例えれば，それぞれ別のあて先を指定した封筒に多重にメッセージを封入し，封書を受取ったものが一番外側の封筒を取り去って次に送るという方法である．送信者はパケットごとに中継経路を変更することが可能でアドレス情報の漏洩に関する強度は高いと考えられるが，多数の中継と全中継ノード分の暗号化，復号化の処理によるオーバヘッドが大きいと考えられる．また，あらかじめ多数の協力ノードを必要とする点で導入も難しい．

②複数ノードへの同報(マルチキャスト)通信を用いる方法

Waters らは正当な受信者だけが復号できるように暗号化したメッセージを複数のノードに対して同報通信として送り，復号化に失敗したノードではメッセージを破棄する方法を提案している．同報通信を受取った複数のノードのうち，どのノードで復号化に成功したかは当該ノード以外には分らないため，実際にメッセージを受取ったノードを秘匿することができる．また，どのノードに対する通信も同じ同報通信アドレスを使って送信されるため，アドレス情報による関連づけは困難になる．しかし，本来の受信者以外にメッセージが送られることのコストと，さらに各受信ノードで復号化処理が行われるコストという点でオーバヘッドが大きいと考えられる．

③アドレスを頻繁に変更する方法

特定のアドレスを使い続けることがアドレス情報の保護にとっての問題であり，短時間であれば複数のメッセージに同じアドレスが使われても構わないと考えれば，情報の保護としてアドレスを頻繁に変更していく方法が考えられる．不要(SPAM)メールを避けるために電子メールアドレスを変更する考え方に近い．アドレスを動的に変えていく方法としては，DHCP のようにサーバに割当てさせるもの，RFC3041 のように自身でアドレスを変更していくものが使用できるが，メールアドレスの場合と同様に，アドレスが変更されたことを正規の通信相手だけにいかにして伝えるかという問題がある．

２．研究の目的

本研究の目的は，インターネット通信の当事者に関する情報のうち，特に通信者を特定するアドレス情報が，通信を傍受する第三者によって窃用されることの防止である．

本研究は，次世代インターネット通信プロトコルとして普及が見込まれる IPv6 通信が広大なアドレス空間を有することに注目し，背景で述べた③の方法，すなわち通信アドレスを一時アドレスとして頻繁に変更することで，特定のアドレスと通信の当事者との関連付けを困難にすることを目的とする．このとき，アドレスの変更によって，正規の通信の当事者同士での通信が困難にならないように，当事者同士が協調してアドレス変更を行う方法を実現する．また，アドレス情報の保護としてアドレス空間の広さや計算機の持つメモリ空間の広さといった空間的な広がりを利用し，中継や暗号化などの時間的なオーバヘッドを小さくする．

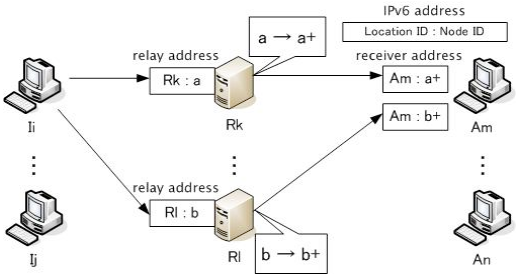
IPv6 のアドレスは, そのアドレスで指定されるノードが接続された LAN を識別するネットワークプリフィックス部と, LAN 内で当該ノードを識別するインターフェース ID 部から構成される．研究開始時までの研究成果として，以下の方法によって，インターフェース ID 部について，送受信者が協調してアドレスを変更するメカニズムを提案し，Linux システムをベースにプロトタイプシステムを構築している．

- 送受信者間であらかじめ共有した暗号化キーを用い, 第三者が推定できないアドレス系列(インターフェース ID 系列)を，それぞれのノードが独立に生成．
- 送信者が通信(セッション)を開始する度にアドレス系列から新しいアドレスを取り出して使用することで, アドレスを頻繁に変更．

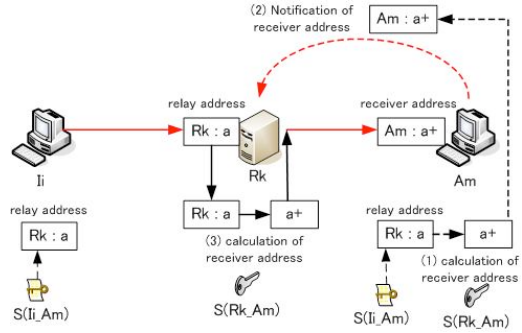
しかし，アドレス情報の保護としてはインターフェース ID の保護だけでは十分ではなく，プリフィックス部の保護が必要である．本研究では，送受信者間に 1 段の中継ノードを挟み，中継ノードを頻繁に切り替えることでプリフィックス部による関連付けを防ぎ，IPv6 アドレス全体について第三者がアドレスの変更をトレースすることが困難な通信方法を実現する．また，MobileIPv6 が使用されている場合には，新たに中継ノードを設けるのではなく，MobileIPv6 のホームエージェントにプライバシー保護のためのアドレス変換機構を統合する．

３．研究の方法

本研究では次の図に示すように，複数の中継ノードをインターネット上の異なった場所に設置し，それらを順次切り替えて使用することで，アドレスの変化の追跡を困難にする．通信を開始する側のノードは，新しい接続を開始する度に中継のためのアドレスを変更し，中継ノードにパケットを送信する．中継ノードはそのパケットをあたかも自分が送信したかのように加工して，受信側のノードに再送信する．



パケットの転送を成功させるためには，中継ノードにおいてパケットの宛先アドレスを変換する必要があるが，このとき中継の前後のアドレスの関係を第三者に知られないようにしなければならない．本研究では，次の図に示すように，中継の前後のアドレスに関数関係を持たせることで，中継の前後のアドレス対の情報をネットワーク上で交換しなくてもよいようにする．

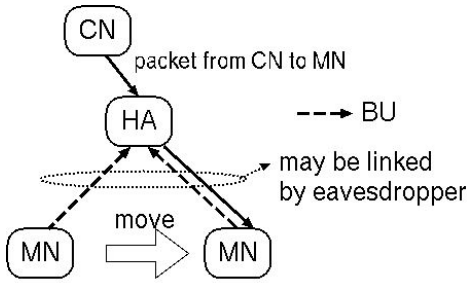


具体的には，通信の両端の送受信ノードは暗号化鍵 S(I,A)を共有し，それを利用して第三者に知られないアドレス系列を生成する．一方，中継ノードと受信ノードも暗号化鍵 S(R,A)を共有する．受信ノードは送信ノードと同期したアドレス系列からアドレスを取り出し，S(R,A)を使ってインターフェース ID 部 a を変換し，その結果 a+を中継ノードに登録する．中継ノードは新しい通信を受信すると受信ノードと共有した鍵を使って宛先アドレスのインターフェース ID 部 a を変換し，登録済みのアドレスから一致するものを検索する．検索によって受信ノードのネットワークプリフィックス部が分かるので，その宛先にパケットを転送する．

中継ノードの使用によって通信アドレスの対応関係を秘匿するには，複数の送受信ノードによって中継ノードが共有されなければならない．このとき異なった受信ノードによって登録されたアドレスのインターフェース ID 部が偶然一致してしまう可能性がある．しかし，インターフェース ID 部の重複は中継ノードあるいは受信ノードによって検出可能であることから，重複した際にアドレス系列を１つ進めることで重複による問題を回避する．

通信を行っているノードが移動ノードである場合，移動によってアドレスが変化するが，変化したアドレスの関連が第三者に分かってしまうと移動ノードの移動状況の追跡をおこなわれてしまう危険性が生じる．本研究では移動ノードへの通信プロトコルとして一般的な MobileIPv6 が使用されている場合について，アドレス履歴の追跡を困難にする方法を提案する．

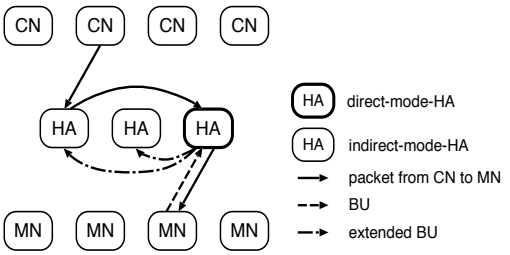
MobileIPv6 においては移動ノード（MN）に対して変化しないアドレス（ホームアドレス）を管理するホームエージェント（HA）を設置し，通信相手からの通信をホームエージェントが取り持つことで通信相手に対して移動ノードのアドレスが変化していないように見せることができる．このときホームエージェントが移動ノードの移動先のアドレスを知っている必要があるため，次の図に示すように，移動ノードは移動の度にホームエージェントに対して自分のアドレスをバインディングアップデートと呼ばれる通信を行って通知する．よって第三者が移動の前後のバインディングアップデートを宛先であるホームエージェントによって識別し関連付けることで，移動ノードのアドレスの変化を追跡できる可能性がある．



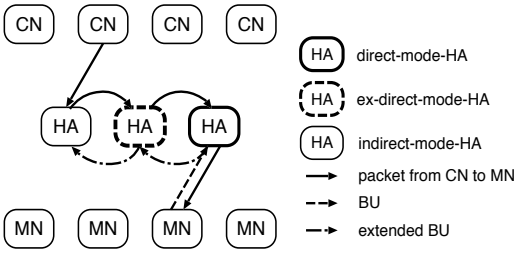
(a) single home agent

本研究ではホームエージェントを多重化し，移動ノードが複数のホームエージェントを切り替えて使用することでバインディングアップデートの宛先を変化させ，移動アドレスの追跡を困難にする．しかし，移動ノードの最新のアドレスを知っているのはバインディングアップデートを受け取ったホームエージェントのみなので，通信相手ノードが他のホームエージェントに対して通信を

起動した場合は移動ノードへの接続ができないことになる．したがって，移動ノードの移動先のアドレスを通信相手が通信を行ったホームエージェントに通知する仕組みが必要になる．本研究では，次の図に示す２つの方法を提案する．



(a) BU multicast



(b) on demand BU relay

第１の方法は，移動ノードからのバインディングアップデートを受信したホームエージェントが受信後ただちに他のホームエージェントに受信したことを通知する方法である．この方法では通信相手ノードが通信を始める前にホームエージェント間で情報を共有しているため通信遅延時間は少なくなると考えられるが，ホームエージェント数が大きくなったときに通知のための通信量が増大するという欠点がある．

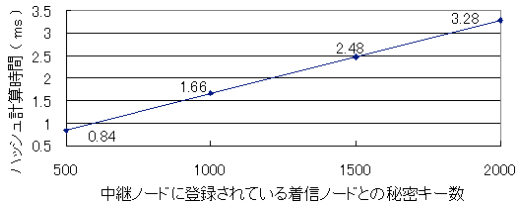
第２の方法は，通信の待ち合わせ場所として１つ前の通信で使用したホームエージェントを使用する方法である．まず，移動ノードからのバインディングアップデートを受信したホームエージェントは，１つ前の通信で使用されたホームエージェントにだけ通知を行う．一方，通信相手からの通信を受け取ったホームエージェントは受け取った時点で１つ前の通信で使用されていたホームエージェントに通信を転送する．この方法では，少なくとも初回は３つのホームエージェントによる中継を必要とすることになり通信遅延が大きくなるが，実際に通信が発生するまでバインディングアップデートの通知を行わないため，不要な通信量の増大を抑えることが期待される．本研究では，これらの方法について実際にプロトタイプシステムを作成し，その性能を評価する．

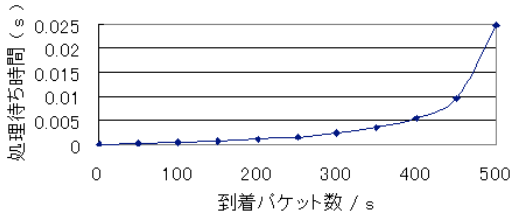
４．研究成果

次の２種類のシステムを開発し，平均的なPC上に実装したシステムを用い実験ネットワークで通信遅延の測定を行い，転送経路の増加による遅延以外の処理の遅延は許容される範囲内であることを確認した．

1) 分散中継サービスによるアドレス変換システム：IP アドレスによる関連づけを防ぐためには送受信者が頻繁に自身のアドレスを変更する必要がある．しかし IP アドレスには通信経路選択に必要なネットワーク識別情報が含まれるため，ネットワーク情報も隠蔽するには，複数のネットワークに中継ノードを配置してアドレス変換を行う必要がある．このとき，中継の前後のアドレスの関係を第三者から秘匿しなければならない．この問題に対して，一方向性関数関係をアドレス間に持たせる方式を考案し，提案手法による中継システムの実装を行った．

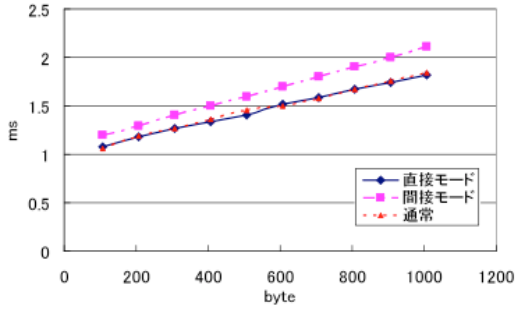
さらに実装したシステムを用いて実験ネットワークを構築し，性能評価を行った．中継ノードでは複数の送受信ペアの通信を扱うため，中継パケットが到着したときにどの受信ノード宛であるのかを検索するために受信ノード分の一方向関数の計算を行う必要がある．したがって検索時間は受信ノード数が増える，すなわち保存されている秘密キー数が増えるに従って増大する．実装したシステムにおいて測定した秘密キー数と一方向性関数の計算時間の関係は次の図のようになり，実装システムにおける検索処理が十分に最適化されていないにも関らず数ミリ秒の遅延で数千の受信ノードをサポートできることが分かる．また，測定した結果をもとにパケットの到着率に対する処理待ち時間を推定したところ，秘密キー数 1000 の場合をプロットした次の図に示すように，数十ミリ秒の範囲に納まることが確認された．検索処理は送受信ペアが通信を開始するときのみ起動され，継続する通信については再探索する必要がないことから，上記の遅延は許容範囲内であると考えられる．





2)MobileIPv6 のホームエージェントの多重化システム：移動端末のインターネット接続において，モバイルノードのアドレスの変化を隠蔽し，固定的なアドレスでのアクセスを可能にする Mobile IP では，固定的なアドレスを管理するホームエージェントにモバイルノードが移動先を通知するバインディングアップデートを傍受することで，移動履歴の追跡が可能になってしまう危険性が存在する．この問題に対し複数の固定アドレスを用い，バインディングアップデートの通知先を複数のホームエージェントから選択できるようにすることで，移動履歴の追跡を困難にする方法を考案し，プロトタイプシステムとしてバインディングアップデートを受信したホームエージェントが他のホームエージェントに通知する方式について Linux 上の Mobile IPv6 スタックである UMIP に対する拡張として実装した．

実装したシステムを用いて実験ネットワークを構成し，性能評価として ICMP Echo パケットを用いてラウンドトリップタイムを測定した．測定結果は次の図に示すようになり，バインディングアップデートを受け取ったホームエージェントと通信相手からの通信を受け取ったホームエージェントが同一の場合には，通常の MobileIPv6 の処理との差がみられないこと，ホームエージェントが異なり，中継処理が 1 段多く入る場合も，遅延時間の増加は，ホームエージェント間の通信遅延時間に限定されることが確認された．



５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

① H. Takahashi, T. Minohara, “Enhancing Location Privacy in MobileIPv6 by using Redundant Home Agents”, Proceeding of Work In Progress Workshop at PerCom 2012, 査読有, 2012, 457-460

② 高橋弘行，蓑原隆，複数のホームエージェントによる Mobile IPv6 のプライバシーの向上，電子情報通信学会技術研究報告，査読無, DC2009-88, 2010, 477-482

〔学会発表〕（計 3 件）

① 高橋弘行，蓑原隆，MobileIPv6 におけるロケーションプライバシーの向上，第 74 回情報処理学会全国大会，2012 年 3 月

② H. Takahashi, T. Minohara, “Enhancing Location Privacy in MobileIPv6 by using Multiple Home Agents”, 12th Symposium of Engineering of North China University of Technology and Takushoku University, 2011 年 10 月

③ T. Minohara and R. Sato, “Enhancing Unlinkability on IPv6 Receiver Address with Distributed Relay Service”, ACM Conference on Wireless Network Security, 2010 年 3 月

〔その他〕
ホームページ等
http://www.cs.takushoku-u.ac.jp/dcl/

６．研究組織
(1)研究代表者

蓑原　隆（MINOHARA Takashi）
拓殖大学・工学部・教授
研究者番号：88239334