L-025

位置アドレスを用いたネットワークのプライバシー保護

Privacy protection on the network using positional addresses

青木　太一†　佐藤　直†
Taichi Aoki　Naoshi Sato

1. まえがき

筆者らは，パケットの送受信アドレスに位置情報を使用する位置アドレスネットワークの構成法を検討している[1]. 本稿では，最初に位置アドレスネットワークの研究背景と概要を述べる．さらに，同ネットワークの実用化にあたり課題となるプライバシー問題[2]を取り上げ，解決策を検討する．

2. 位置アドレスネットワークの研究背景と概要

2.1 研究背景

インターネットで広く採用されている IP アドレスは特定の論理空間から当局がユーザに払いだす形態をとっている．この論理空間は有限であるため，アドレスの割り当て管理が必要で，アドレスの枯渇問題も生じる．また，グローバルなアドレスは有料であるため，ユーザが自由に使用しにくいという問題がある．

運用面の問題としては，パケットが最終的に物理層で転送されるにも関わらず，アドレス体系が論理的であるため，その対応を調べるための情報交換や記憶するためのアドレステーブルが必要であり，ネットワーク規模の増大に伴いルータなどの通信機器の負荷も大きくなる，という問題がある．

さらに，情報セキュリティの面では，アドレスが物理的な位置と対応していないため，アドレス詐称や障害が発生してもその位置を正しく特定しにくいのが現状である．

2.2 概要

（1）位置アドレスの概要

研究背景に述べたような，論理アドレスが有する問題の解決策として，物理アドレスを使用することを提案する．

具体的に，物理アドレスとして，緯度・経度・高度といった地理情報に基づく位置アドレス（以下 PA と示す）を提案する．PA には GPS 等の位置情報システムから取得した位置情報をアドレスとして用いることが考えられる．PA は，例えば，地球表面上の全てのエリアを 1m 単位で表わす場合，緯度・経度に対して，各々26 ビット・27 ビットを割当てることで表現できる．また、高度の範囲として，地球の中心から人工衛星の静止軌道までを対象とする場合，同様に 26 ビットで表現できる[1].

ネットワークを構成する機器は原則として GPS 衛星などから算出した位置情報を自らのアドレスとして使用する．位置情報の精度は必ずしも高い必要はないが，アドレスビット数が有限な場合隣接する機器が同一の PA を適用しようとする場合が発生するので，重複しないように調整する．この重複をさけるための調整方針としては，該当する機器同志間の緯度・経度・高度の大小関係が維持されるよう自律的に行う，ことが考えられる．

（2）位置アドレスを用いたパケット転送網の概要

PA を用いたパケット転送網（位置アドレスネットワークと呼ぶ）の概要を図 1 に示す．同図において，位置アドレスネットワークが有する主要な機能を図 1 の吹き出しに示した．以下，各機能の概要を示す．

・ユーザ登録・認証機能

位置アドレスネットワーク利用者（端末）を登録し，認証する機能である．本機能は，さらに，移動通信網の LR(Location Register)[3]の機能を有し，位置情報の登録・管理を行う．

・名前解決機能

利用者（端末）の名前から PA を解決する機能である．これは，インターネットにおける DNS（Domain Name Service）に相当する．

・位置アドレスによる経路制御機能

PA を用いて経路制御する機能である．経路制御のためのプロトコルとしてはインターネットで広く採用されている OSPF（Open Shortest Path First）[4]を想定する．すなわち，物理的に近接する領域を経路制御の単位（エリア）とし，このエリアを多段階に構成して経路制御する．

以上のような経路制御機能は基本的に従来のインターンシップと同一であるが，位置情報自体が階層構造を有するため，効率的に経路情報の集約および削減を図ることが可能になると考えられる．

・ユーザセキュリティ機能

この機能は情報セキュリティの向上を図るための機能である．本機能では PA の真正性をチェックし，その結果に従ってパケットフィルタリングする．本機能により，不正な（なりすまし）送信を防止でき，送信元を特定することが可能になる．このように，全てのネットワーク機器が

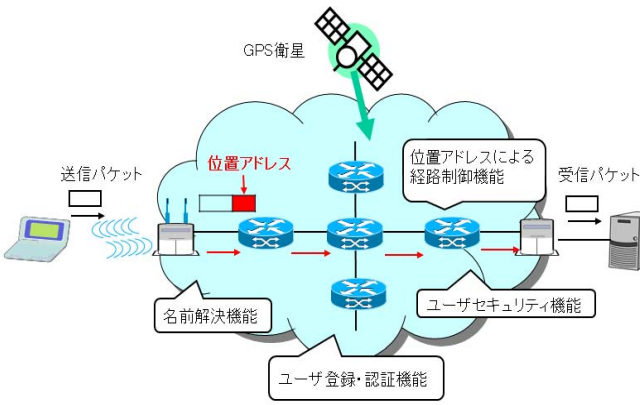


図 1　位置アドレスネットワークの概要

† 情報セキュリティ大学院大学

PA を用いることによって，高効率なネットワークセキュリティの実施が期待される．

3. 位置アドレスの匿名化

位置アドレスネットワークはこれまで述べたような利点を有するが，他方，この PA をエンド・エンドで適用するとユーザの位置が判明し，プライバシーが侵されるという問題が生じる．このため，以下では，PA の適用範囲を中継系に限定することを想定して，位置アドレスの匿名化を検討する．

アクセス系では，PA の署名付きのハッシュ値を代理アドレス SA として用いてパケット転送する．エッジルータは SA を PA に変換することによって，PA による経路制御を実現するとともに，プライバシーを保護する方式を提案する．

3.1 検討モデルと前提条件

検討モデルを図２に示す．同図において，両ホスト端末はそれぞれエッジルータを介してパケット通信する．

ホスト端末は位置情報から自身の PA，SA を作成・保持できるものとする．また，アクセス系において，ホスト端末はデジタル署名が可能であるとする（以下，このデジタル署名の詳細については説明を省略する）．また，中継系のセキュリティは確保されており，PA が漏えいすることはないものとする．

3.2 名前，位置および代理アドレスの登録

図２において，ホスト端末は自身の名前，PA および SA をエッジルータに伝え，エッジルータはこれらを名前解決機能（以下 DNS と示す）に登録する（①）．ここで，完全性を保つため，ホスト端末が自身の PA をデジタル署名したハッシュ値を SA とする．この DNS への登録は移動通信網と同様に定期的に実施される．

3.3 名前解決とパケット転送

ホスト端末が通信する場合は，最初にエッジルータを介して相手側ホスト端末の名前解決要求を行う．この結果，DNS により相手の SA が検索され，送信側ホスト端末に伝えられる（②）．同時に送受両ホスト端末の PA が検索され送信側・受信側エッジルータに伝えられる（③）．送信側ホスト端末は自身および相手の SA を送受信アドレスとしてパケットに付与し，送信側エッジルータに送信する．送信側エッジルータは SA を PA にアドレス変換して送信する．受信側エッジルータでは PA を SA にアドレス変換して受信側ホスト端末に送信する．

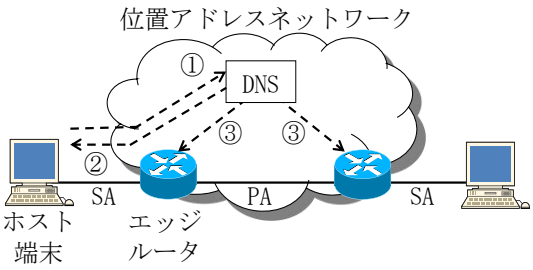
以上より，アクセス系（ホスト端末～エッジルータ）では SA を用いたパケット転送が，中継系（エッジルータ～エッジルータ）では PA を用いたパケット転送がそれぞれ実施され，ホスト端末には相手側の PA が転送されないため，プライバシー問題が解決できる．

4. まとめ

本稿では，最初に，IP アドレスのような論理的アドレスをパケット転送網のアドレスとして使用することの課題を指摘し，その解決策として，物理アドレス，すなわち，位置情報をアドレスとして用いる位置アドレスネットワークを提案した．

提案によれば，位置情報自体が階層構造を有するため，位置アドレスにより経路制御することで，効率的に経路情報の集約および削減できると考えられる．また，位置アドレスを認証することで，なりすまし防止や送信元特定がネットワークレベルで簡易に行うことができることを示した．

一方，本提案の位置アドレスにより，ユーザの位置が判明し，プライバシーが侵されるという問題に着目し，解決方法を提案した．具体的には，位置アドレスの適用範囲を中継系に限定するとともに，名前解決機能を利用し，代理アドレスを用いて位置情報を隠ぺいするネットワーク構成法を提案した．今後本提案の評価を行う．



①ホスト端末の名前，位置および代理アドレスの登録
②代理アドレスの取得
③位置アドレスの取得
SA；代理アドレスによるパケット転送
PA；位置アドレスによるパケット転送

図２ 位置アドレス匿名化方式

文 献

[1] 岡崎成寿，小宮康裕，佐藤直，″位置アドレスを用いた経路制御の基本検討″, FIT2008, L-021, 2008 年 9 月
[2] 青木太一，佐藤直，″位置アドレスを用いたネットワークにおけるプライバシー保護手法の提案″, 信学技報, NS2014-101, 2014 年 9 月
[3] 弓場英明，澤田政弘，薮崎正実，″移動通信網間ゲートウェイロケーションレジスタ″, 信学技報, IN2001-36, 2001 年 7 月
[4] 友近剛史，池尻雄一，小早川知昭，″インターネットルーティング入門″, 翔泳社，第 3 章，2001 年 9 月