ID・ロケータ分離による新世代ネットワークアーキテクチャ

Ved P. Kafle (ベド　カフレ)
光ネットワーク研究所 ネットワークアーキテクチャ研究室 主任研究員

大学院博士課程修了後、2006年、NICT に入所。現在、新世代ネットワークの設計、実装、評価に基づく研究開発及び標準化に従事。

はじめに ーなぜ新世代ネットワークなのかー

今やインターネットは、私たちの日常生活になくてはならないものになっています。近い将来には、インターネットには、家電製品、乗り物、健康・環境監視センサーなどの多種多様なデバイスが相互接続される日が来るでしょう。しかし、40年前に設計されたインターネットは、当時遠方の知人のコンピューターとの通信をするためのもので、携帯・微小デバイスの無線接続、セキュリティとサービス品質の提供、低消費電力での大容量のデータの効率的な転送などは考慮されていませんでした。アプリケーションがこのような要求をするようになって、様々な機能がオリジナルのインターネットアーキテクチャに、全体の最適化を考えることなく、ランダムに追加されてきました。その結果、現在のインターネットには負荷がかかり過ぎ、本来あった拡張性という特徴が次第に失われてきました。それゆえ、前述した要求を、さらに将来に生じる要求も満たすようにするために、私たちは白紙から新世代ネットワークを設計してきました。

新世代ネットワークは、海外では、“Future Internet”とか“Future Network”などと呼ばれていますが、現在のインターネットでの制約条件は継承しません。新世代ネットワークは、膨大な数の多種多様な移動デバイスを想定し、様々なネットワークプロトコルをサポートします。この記事では、このような目標を達成するために必要なID・ロケータ分離という概念について、現在のインターネットのアーキテクチャと比較しながら説明します。

ID・ロケータ分離の概念

図1 (a) は、現在のインターネットのプロトコルの階層構造を示します。IPアドレスは、アプリケーション層とトランスポート層で、端末やセッションやサービスの識別子 (ID) として利用され、同じIPアドレスが、ネットワーク層ではネットワーク内での端末の接続位置 (ロケータ) として利用されます。1つのIPアドレスをIDとロケータの両方に使用することは、異種のプロトコル、移動通信、マルチホーム接続、セキュリティ、経路制御の拡張などに適していません。端末が、ネットワークを移動した場合、端末のIPアドレス (IDとロケータの両方) が変更され、元のIPを識別子として用いた現在進行中のセッションが切れます。また、マルチホーム接続は、接続しているネットワークが混雑・切断した場合に、別のインターフェースに切り替えるためのものですが、それぞれのインターフェースは独自のIPアドレスを持っているため、接続切り替え時にセッションIDが変更になり、通信セッションの滑らかな継続は困難です。同様に、IPアドレスに紐付いたセキュリティ情報は、端末のIPアドレスの変更で無効になります。さらに、コアネットワークは、それぞれのエッジネットワークまたはアクセスネットワークごとの経路表を作成しますが、エッジネットワークのサイズが小さく、数が非常に多くなった場合には、基幹の経路表のサイズは非常に大きくなり、エッジネットワークのIPアドレスの設定が頻繁に変更になると、基幹の経路表を更新する処理負荷が高くなり、最終的には、基幹の経路制御の機能に支障が出るでしょう。

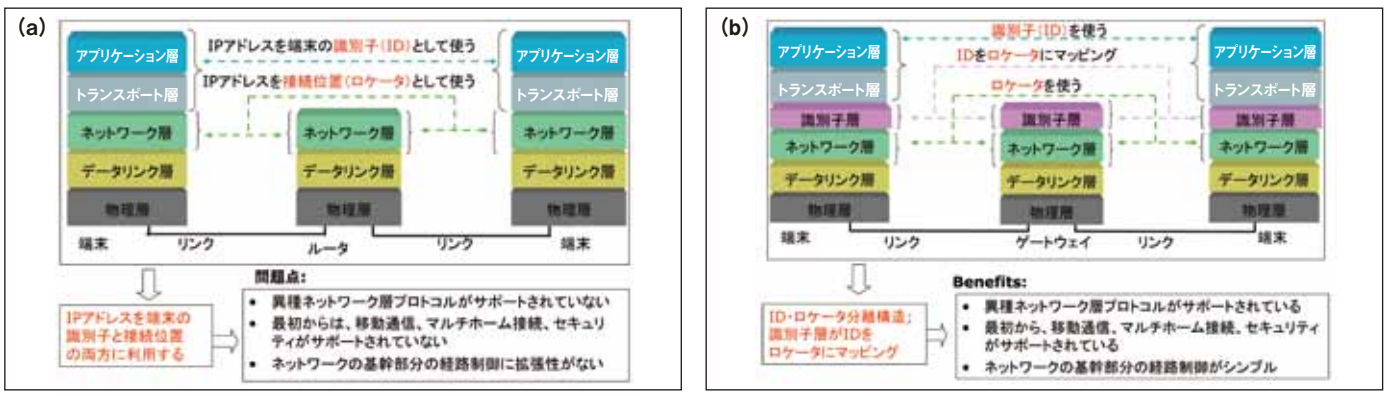

図1●プロトコル階層図　(a) 現在のインターネットの場合　(b) ID・ロケータを分離した新世代ネットワークの場合

従って、新世代ネットワークのプロトコル階層は、図1 (b) に示すようにIDとロケータを切り離す (ID・ロケータ分離) 必要があります。トランスポート層とネットワーク層の間に挿入された識別子層は、IDをロケータにダイナミックにマッピングし、端末の移動やマルチホーミングによってネットワーク層がロケータを変更した場合にも、アプリケーション層やトランスポート層は、端末や通信セッションの識別用に同じIDを使い続けることができます。この特徴は、ネットワーク層で別の種類のプロトコルを使うことを可能とします。データのパケットのヘッダには、送信元と宛先の両方のIDとロケータが含まれています。ゲートウェイは、パケットがエッジネットワークとコアネットワークを横断する際に、IDをヘッダの中のネットワークプロトコルやロケータの値を変換するための参照値として使います。これにより、新世代ネットワークでは、エッジネットワークやコアネットワークで異なるタイプのネットワーク層プロトコルの利用が可能となります。

HIMALISアーキテクチャ

ID・ロケータ分離の概念に基づき、NICTはHIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation: ロケータとIDを分離することによる異質性の許容と移動への適応) アーキテクチャを提案してきました。図2はHIMALISアーキテクチャの主要な構成要素であるエッジネットワーク、コアネットワーク、論理制御ネットワークを示しています。コアネットワークはエッジネットワーク同士を接続するために高速なルータとリンクで構成されています。

●ネットワークアクセス機能

端末 (図2の端末1) がエッジネットワークに接続するとき、DHCP (Dynamic Host Configuration Protocol) 等の初期設定プロトコルの実行やAA、LNS、GWのIDやロケータ等のエッジルータのパラメータを入手します。端末は次に、認証と登録のためにAAにコンタクトします。認証が済むと、端末には新しいロケータが割り当てられます。端末の端末名、端末ID、ロケータ、公開鍵はLNSのホストテーブルに保存され、端末IDとロケータはGWのIDテーブルに保存されます。端末にはアクセスキーも割り当てられ、信頼性の証明やAA、LNS、GWとの暗号化メッセージのやりとりに使われます。端末は新しいロケータをHNRに、ロケータ更新メッセージを送ることによって登録します。こうしてこの端末は他の端末と通信する準備ができました。

●セッション初期化機能

端末1が端末2と通信したいとき、端末1は端末2の端末名しか知らないため、端末1は端末2のID、ロケータ、公開鍵をLNSに問い合わせます。LNSはDNR、HNRから情報を入手して端末2のID、ロケータ、公開鍵を受け取り端末1に送ります。こうして端末1は端末2に対して制御パケットを交換し始め、セキュリティコンテキスト (セッションキーなど) を確立し、両方のGWのIDテーブルにID・ロケータのマッピングを保存します。GWはIDテーブルからID・ロケータのマッピングを使うことによってパケットのヘッダの中のネットワークプロトコルやロケータの変換を行います。

●移動通信機能

(a) 移動端末 (たとえば端末1) は 移動して新エッジネットワークにアクセスして新しいロケータを得て、(b) 旧GWにある端末1のロケータ情報を新しいロケータに更新し、移行中にも旧GWが新しいGWにパケットが転送されるようにし、(c) 端末2とそのGWの情報を更新し、新しい位置にいる端末1にパケットを転送できるようにする、(d) 端末1のHNRレコードを更新し、(e) 旧エッジネットワークから切断する、という手順で信号をやりとりします。HIMALISアーキテクチャでは、ネットワークアクセスやセッション初期化のプロセスで確立されたセキュリティコンテキストを移動管理機能の安全確保にも使用できます。

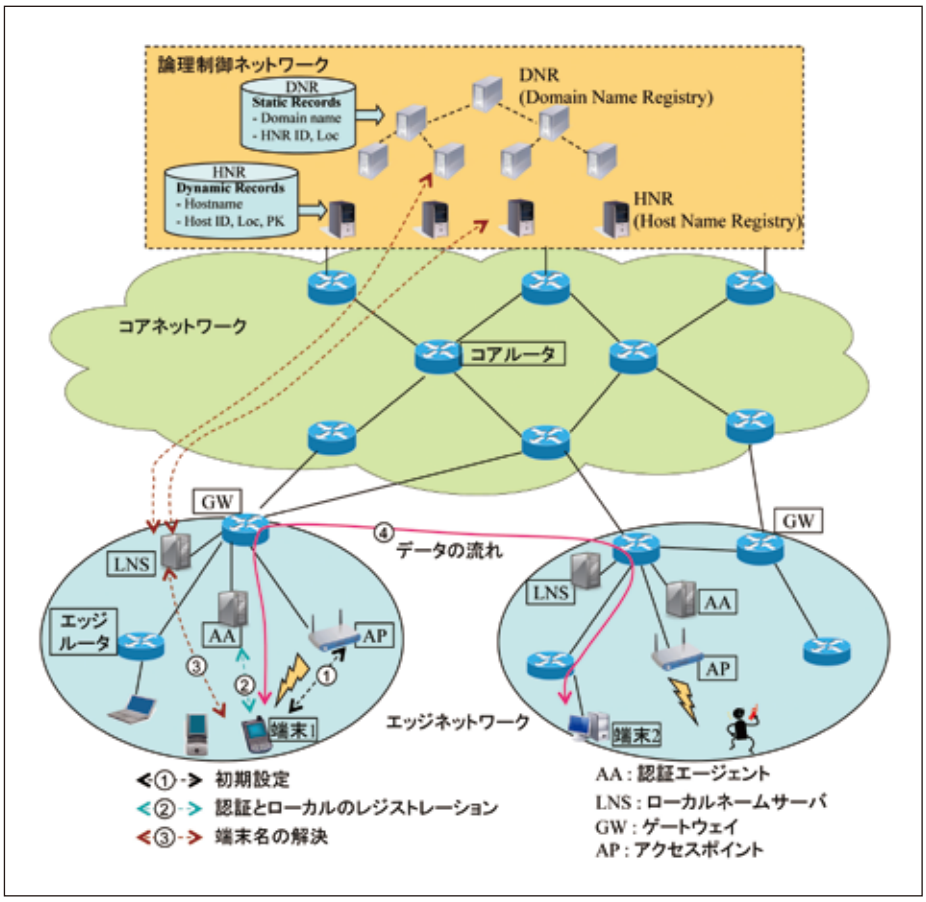

図2●HIMALISアーキテクチャの構成要素

実装の様子

HIMALISアーキテクチャに基づくID・ロケータ分離の技術はNICTにおける新世代ネットワークの研究の重要な要素です。私たちはHIMALISアーキテクチャを、ローカルなテストベッドネットワーク上で実装してきました。DNRとHNRの機能はPlanetLab (約1,000ノードから成る地球規模のオーバーレイテストベッドネットワーク) のノードにも実装されています。広範囲にわたる実証実験を行い、このアーキテクチャが継続的に改良されていくようにしています。HIMALISの実装システムについては、6月のInterop Tokyo 2012で新しい機能を追加してご覧いただく予定です。