第XV部

移動体通信環境

第 15 部
移動体通信環境

第 1 章　はじめに

携帯端末の性能の向上と、移動通信機器の普及に伴い、移動先から携帯端末を利用したインターネットへのアクセス、いわゆるモバイルコンピューティングが活発に行われるようになってきた。また、インターネットへの接続点および接続方法のさらなる増加が見込まれ、加えて第三世代携帯電話のような高速かつ広域の無線通信のサービスも始まっていることから、車や電車などで移動しながらのネットワークへのアクセスといった、ネットワークの利用方法の多様化が考えられる。

Rover は、このようなネットワークを利用した移動計算機環境について研究するグループである。我々が研究の対象とする移動計算機は主にノート型 PC 等の十分な処理能力を持つ計算機であるが、PDA 等の比較的能力の低い計算機も視野に入れた議論を行っている。より具体的には、インターネット移動体通信機構 (LIN6, Mobile-IP) の開発、より高速なネットワーク間ハンドオフの手法、地理情報システムに関する議論、移動に伴う動的適応の枠組の開発などの活動が行われている。

本年度は、これまで Rover で議論してきた研究項目のうち、WIDE メンバーが積極的に開発した LIN6 プロトコルにおける後方互換性拡張方式および、ネットワークの移動方式について報告する。

第 2 章　移動体通信プロトコル LIN6 における後方互換性拡張の一方式

2.1 はじめに

現在提案されている移動透過性保証プロトコルの一つに Location Independent Networking for IPv6(LIN6)[71] がある。LIN6 は、LIN6ID と呼ばれる単一の ID 空間における識別子を利用して移動透過性保証を提供するプロトコルである。LIN6 は 現在 IETF で標準化が行われている Mobile IPv6[81] が持ついくつかの問題点を解決しているが、一方で LIN6 が実装されていない既存ノードとの通信の際には移動透過性が保証できないという問題があった。加えて、移動ノードの LIN6ID に関連する Domain Name System(DNS) サーバに対して、LIN6 で使用する新しいレコードを理解するように変更を加える必要があり、LIN6 の導入を難しくしていた。

本章では、LIN6 における位置管理エージェントである Mapping Agent(MA) の機能を拡張することにより、既存の LIN6 を理解しないノードとの通信においても移動透過性保証を提供可能にし、かつ、DNS サーバに対して変更を加えなくとも LIN6 を導入可能とする方式を提案する。

2.2 現在の LIN6 の通信方式の概略

本章では、LIN6 の通信方式について概観する。詳しい概念の説明については [71] を参照されたい。

LIN6 は、現在の移動透過性が困難となっている原因はネットワークアーキテクチャそのものにあると考え、ネットワークアーキテクチャの再考を行って得られた概念である LINA を基底に構築された IPv6 上の移動体プロトコルである。LIN6 では位置指示子とノード識別子という 2 つの情報を概念的に分離する。ネットワーク層より上位層では、ノード識別子を用いた位置に依存しないコネクションを確立し、ネットワーク層では、位置指示子を用いた経路制御を行うことにより移動透過性を保証する。

2.2.1 縮退アドレスモデル

LINA では**縮退アドレスモデル**と呼ばれるアドレスモデルを導入している。縮退アドレスモデルでは、ノード識別子を位置指示子の中に縮退させるという構造を取る。ノード識別子が縮退された位置指示子を**縮退アドレス**と呼ぶ。縮退アドレスモデルにより、概念的に識別子を扱う層 (識別副層) と位置指示子を扱う層 (配送副層) の 2 層に分離されたヘッダを 1 つのヘッダに統合することが可能となる。また、ネッ

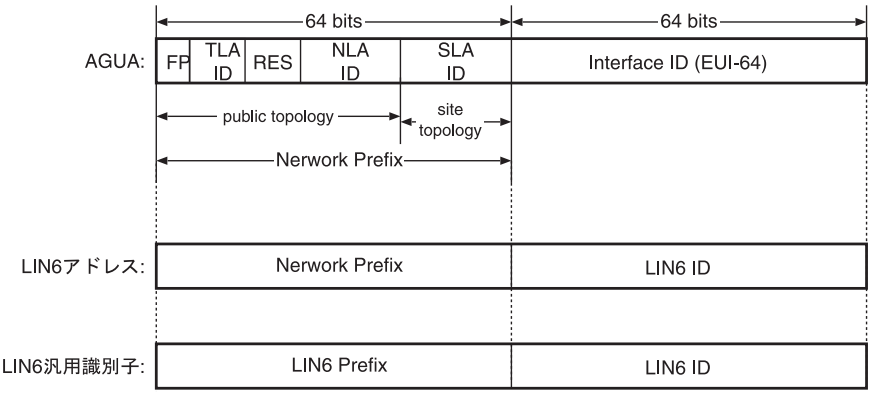

図 2.1. AGUA、LIN6 アドレスおよび LIN6 汎用識別子: 既存の IPv6 アドレスである AGUA では上位 64 bit はサブネットの位置を示し、下位 64 bit はインタフェース識別子である。LIN6 アドレスでは上位 64 bit は AGUA と同様にノードの現在位置のサブネットの位置を示すが、下位 64 bit はノード識別子である LIN6ID である。LIN6 汎用識別子は、上位 64 bit は位置に依存しない LIN6 プレフィクスである

トワーク層より上位層で用いられる識別子は汎用識別子と呼ばれる。汎用識別子は、**固有位置指示子**とノード識別子とを縮退したものである。固有位置指示子はあらかじめ定められた固定値であり、位置に依存しない。すなわち、移動により変化しない。また、縮退アドレスあるいは汎用識別子からノード識別子を得る操作を抽出と呼ぶ。

LIN6 では、この縮退アドレスモデルを以下のように実現している。まず、LIN6 では 64 bit のノード識別子を導入する。これを **LIN6ID** と呼ぶ。

現在、IPv6 の通信で主に使用されている Aggregatable Global Unicast Address(AGUA)[128] は、上位 64 bit がネットワークプレフィクス、下位 64 bit がインターフェース識別子という構造である (図 2.1(a))。LIN6 のアドレスモデルは、この構造を利用し、アドレス構造の 128 bit 全体を位置指示子とし、この位置指示子の下位 64 bit にノード識別子である LIN6ID を縮退させる。この 128 bit の位置指示子を **LIN6 アドレス**と呼ぶ (図 2.1(b))。

図 2.1 に示すように、LIN6 アドレスは従来の AGUA 形式と互換性を保ちながら、LINA における縮退アドレスと同様に位置指示子とノード識別子という分離された 2 つの情報を保持したアドレスとなる。

LIN6 での汎用識別子の導出は次のようになる。まず、LINA における固有位置指示子に対応する上位 64 bit の固定値を導入する。これを **LIN6 プレフィクス** と呼ぶ。そして、この固有プレフィクスに LIN6ID を縮退させる。この縮退されたアドレスが LIN6 における汎用識別子となり、これを **LIN6 汎用識別子**と呼ぶ (図 2.1(c))。

2.2.2 LIN6ID と LIN6 アドレスとの対応づけ

LIN6 では、移動ノードと通信する際に、LIN6ID とそのノードの現在の位置指示子である LIN6 アドレスとの対応関係を得る必要がある。この対応関係を **Mapping** と呼ぶ。LIN6 では、Mapping を管理する Mapping Agent(MA) と呼ばれるノードを導入する。ノードは移動した際には現在の位置指示子を MA に通知する。MA は LIN6ID と位置指示子の関係を保持し、通信ノードから要求があった場合、指定された LIN6ID 対する位置指示子を通知する役割を担う。あるノード A の Mapping を管理する MA を、ノード A の **Designated Mapping Agent** と表現する。あるノードの Designated MA は複数存在しても良い。

2.2.3 LIN6 アドレスと通常の IPv6 アドレスとの識別

LIN6 アドレスは、AGUA の形式と構造上同じであるため、アドレス構造だけでは与えられたアドレスが LIN6 アドレスかどうか識別することはできない。しかし LIN6 では、受信時にアドレスから汎用識別子に変換するかどうかを判断しなければならず、このため、アドレスからそれが LIN6 アドレスかどうか識別する機構が必要となる。

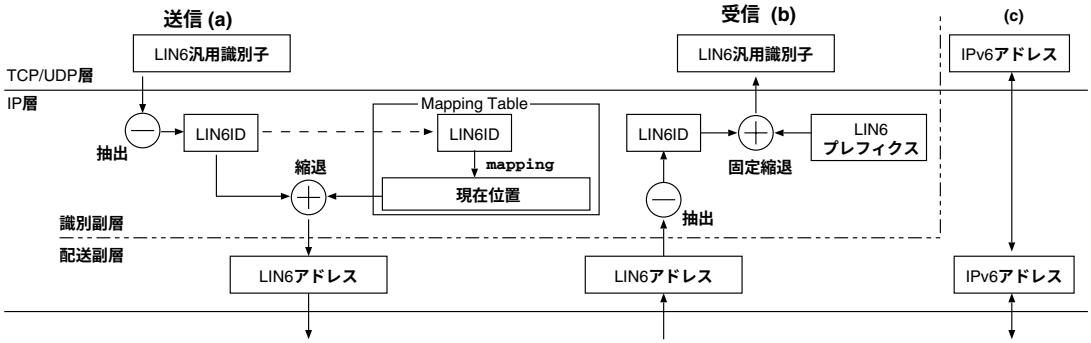

図 2.2. LIN6 における通信モデル: LIN6 汎用識別子は送信時にノード識別子を基に得られた現在の位置指示子から LIN6 アドレスに変換される。LIN6 アドレスは受信時に LIN6 汎用識別子に変換される。LIN6 汎用識別子は上位層における識別子として利用され、LIN6 アドレスはパケットの経路制御のために利用される。上位層から直接 IPv6 アドレスを指定された場合には変換操作はおこなわない。

通常、AGUA のインターフェイス ID 部は EUI-64[67] の構造に従っている。EUI-64 の構造は、IEEE から割当てられる先頭 24 bit の Organizationally Unique Identifier(OUI) と OUI の管理者が割り付ける 40 bit からなる。この構造を利用し、64 bit ノード識別子の先頭 24 bit には、LIN6 固有の OUI を付加することとする。これにより、アドレスから抽出したノード識別子がこの特定の OUI から始まるかどうかを確認することにより、LIN6 アドレスと通常の IPv6 アドレスを識別できる。

2.2.4 LIN6 の通信モデル

LIN6 の通信モデルを図 2.2 に示す。

送信時に上位層から LIN6 汎用識別子が指定された場合 (図 2.2(a))、まず識別副層で LIN6ID を抽出する。次に MA からこの LIN6ID に対する Mapping を取得して現在の位置指示子を導く。得られた位置指示子に LIN6ID を縮退させ、LIN6 アドレスに変換する。LIN6 アドレスは配送副層に渡され、送信パケットはそのアドレスを基に経路制御される。

受信時 (図 2.2(b)) にはデータリンク層からネットワーク層に渡されたパケットは、まず配送副層に到達する。このパケットから得られた LIN6 アドレスは識別副層に渡され LIN6ID が抽出される。そして LIN6 プレフィクスに LIN6ID を縮退させ LIN6 汎用識別子に変換する。得られた LIN6 汎用識別子は上位層に渡される。

アプリケーションから直接位置指示子を指定された場合 (図 2.2(c)) には、LIN6 のネットワーク層は従来のネットワーク層と同様の処理を行う。

2.2.5 Mapping Agent の発見

LIN6 では、あるノードの Designated MA の発見に DNS を用いる。LIN6 では、DNS のレコード群に新たに MA のアドレスを表す MA レコードを導入する。LIN6ID に対する MA レコードを DNS に問い合わせることにより、対象の LIN6ID を持つノードの Designated MA のアドレスを得ることができる。この問い合わせの際、DNS サーバには、LIN6ID を 4bit づつ逆順に並べた文字列に、lin6.net を連結した形式で問い合わせる。例えば、LIN6ID として 0001:4afe:dcba:9876 を持つノードの Designated MA のアドレスを得る場合には、6.7.8.9.a.b.c.d.e.f.a.4.1.0.0.0.lin6.net の MA のレコードを問い合わせれば良い。以後、この LIN6ID を逆順に並べたものを **rev(LIN6ID)** と表現する。すなわち、

rev(0001:4afe:dcba:9876) =
6.7.8.9.a.b.c.d.e.f.a.4.1.0.0.0

となる。

2.3 提案方式

2.3.1 Mapping Agent の拡張

従来方式では、MA はすべて通常のホストでも運用可能であったが、提案方式では MA を拡張し、MA は必ず LIN6 を理解するルータであることとする。MA は必ず一つ以上の仮想ネットワークを持つ。仮想ネットワークとは、ここでは物理的な存在を伴わない論理的に存在するネットワークを指す。また、この仮想ネットワークへの経路はインターネットに広告されているものとする。加えてすべての MA は、

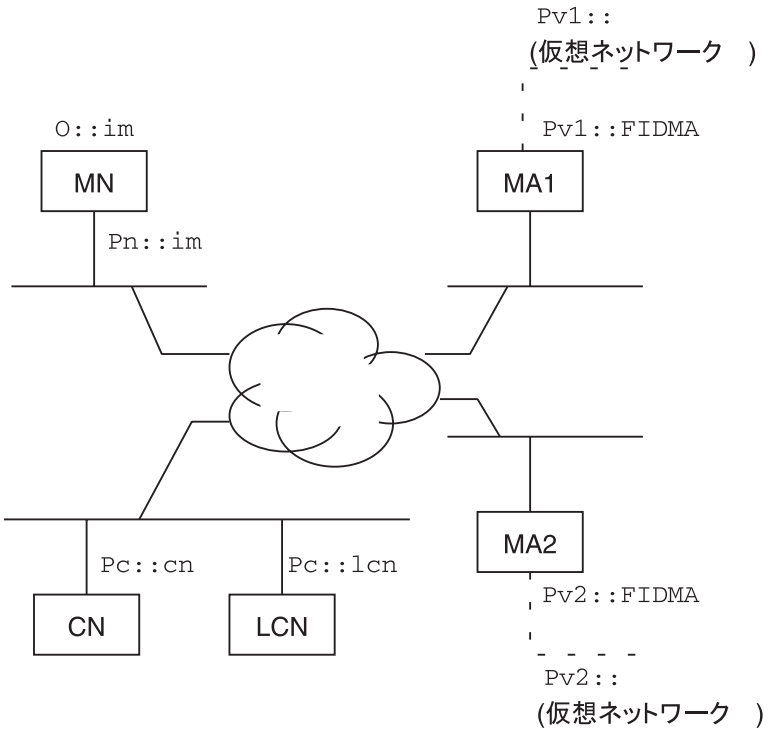

図 2.3.　提案方式におけるネットワーク例: MN, CN はそれぞれ LIN6 ノードであり、LCN は LIN6 を理解しない従来の IPv6 ノードである。MA1, MA2 はともに MN の Designated MA である。

仮想ネットワーク上のインターフェイス ID 部があらかじめ定められた固定値となるアドレスを自己のアドレスとして割り付ける。すべての LIN6 ノードはこの固定値をあらかじめ知っているものとする。以後、この固定値を **FIDMA** と表現する。例えば、ある MA が持つ仮想ネットワークのプレフィクスが Pv::である場合、Pv::FIDMA はその MA が持つアドレスである。

提案方式を図 2.3 を例に説明する。MN, CN は LIN6 を理解するノードであり、MN の LIN6ID を im とする。LCN は LIN6 を理解しない従来の IPv6 ノードである。Pn, Pc, Pv1, Pv2 はそれぞれネットワークプレフィクスを示す。O は LIN6 プレフィクスを表す。MA1, MA2 はそれぞれ MN の Designated MA である。

2.3.2 MA レコードを利用しない MA の発見方式

2.2.5 章で述べたように、従来方式では、ある移動ノードの Designated MA のアドレスを知るためには、LIN6 独自のレコードである MA レコードが必要である。すなわち、MA の位置を管理する DNS サーバには、この新しい MA レコードを理解できるように変更を加える必要があった。これは現在運用されているすべての DNS サーバが MA レコードを理解する必要があるということではなく、一部の DNS サーバのみの変更であるため導入の障壁としては低いといえるが、LIN6 の普及を阻害する一要因となりうることは否めない。

そのため我々は、あるノードの Designated MA のアドレスを既存の AAAA レコード [139] を利用して表現する方式を提案する。AAAA レコードは、現在 IPv6 アドレスを表現するために利用されているレコードである。

提案方式では、移動ノードの AAAA に対して、Designated MA の仮想ネットワークプレフィクスに、自分の LIN6ID を連結した結果を登録する。この例では、mn.lin6.net の AAAA レコードの値は、Pv1::im および Pv2::im となる。以後、移動ノードのこの仮想ネットワーク上のアドレスを後方互換アドレスと呼ぶ。同様に、従来 MA レコードを引くために利用していた rev(LIN6ID).lin6.net には PTR レコード [124] を設定し、そのノードの FQDN を定義しておく。PTR レコードは現在逆引き、すなわちアドレスから FQDN を取得するために利用される既存のレコードである。本例においては、rev(im).lin6.net の PTR レコードには、mn.lin6.net が定義される。

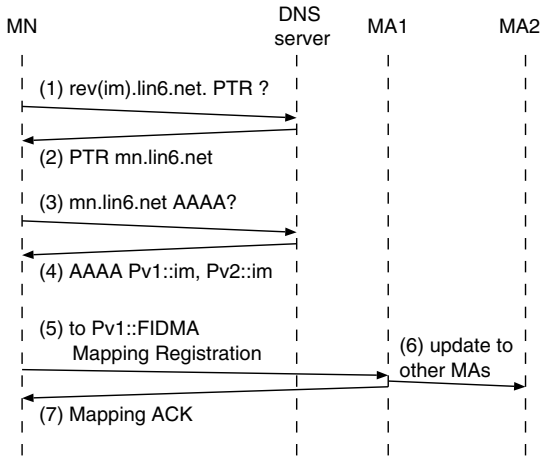

図 2.4. 提案方式における MN の登録処理: MN は自己の FQDN から後方互換アドレスを求め、そのネットワーク上の MA に登録要求を送信する。

これにより、あるノードが Designated MA のアドレスを取得する手順は次のようになる。

- rev(LIN6ID).lin6.net の PTR レコードを問い合わせ、対象ノードの FQDN を得る
- 対象ノードの FQDN に対応した AAAA を問い合わせる。
- 得られた IP アドレスのうち、下位 64 bit を FIDMA にすることによって MA のアドレスが得られる。

図 2.3 を例にすると、MN の Mapping の登録処理は図 2.4 のようになる。

- MN はまず自分の LIN6ID から FQDN を取得する (1, 2)。
- 次に、FQDN から AAAA を取得し、下位 64 bit を FIDMA に入れ換えることで MN の Designed MA のアドレスを得る (3, 4)。
- MN は得られたアドレスのうち、任意の一つを選び、その MA に対して登録要求を行う (5, 7)。
- MN から登録要求を受けた MA1 は、他の MA すなわち MA2 にこの登録要求を転送する (6)。

2.3.3 従来ノードとの通信手順

次に、従来ノードとの通信手順について述べる。従来ノードは、通信相手となる LIN6 ノードの FQDN から AAAA を引き、そこで示されたアドレスに対してパケットを送出する。すなわち、従来ノードが提案方式の LIN6 ノードにパケットを送信する場合には、すべての対象ノードのいずれかの designated MA の仮想ネットワークへと配送されることになる。提案方式では、この仮想ネットワークへと配送されるパケットを MN の現在位置にトンネリングによって配送を行うことによって移動透過性を提供する。

図 2.3 を例にすると、MN と従来ノードである LCN の通信手順は図 2.5 のようになる。

- LCN は MN の FQDN から AAAA レコードを使ってアドレスを解決する (1, 2)。
- LCN は得られたアドレスから任意の一つを選び、パケットを送信する (3)。
  ここでは MN は MA1 のアドレスを選択したとする。
- パケットは MA1 が持つ仮想ネットワークへと配送される。MA1 は、対象となるパケットの宛先が、自分が Mapping を持つノードへのパケットであるかを宛先アドレスの下位 64 bit を見て判断する。この例では MA1 は MN の Mapping を持つため、MN への IPv6-in-IPv6 のトンネリングを利用してパケットを配送する。MN は、後方互換アドレス宛のパケットを自分宛のパケットとして受信する。
- MN は、LCN に対する応答パケットを MA1 へトンネリングして送出する (5)。
- MA1 は、MN からトンネルされたパケットを decapsulation し、LCN へパケットを転送する。

この結果、MN が移動しても、LCN の上位層が通信相手である MN を認識するアドレスは MA1 が持つ後方互換アドレスであるため変化せず、また、MN へのパケットも MA1 が MN へのパケットを適切な現在位置へと転送するため、従来ノードとの通信に

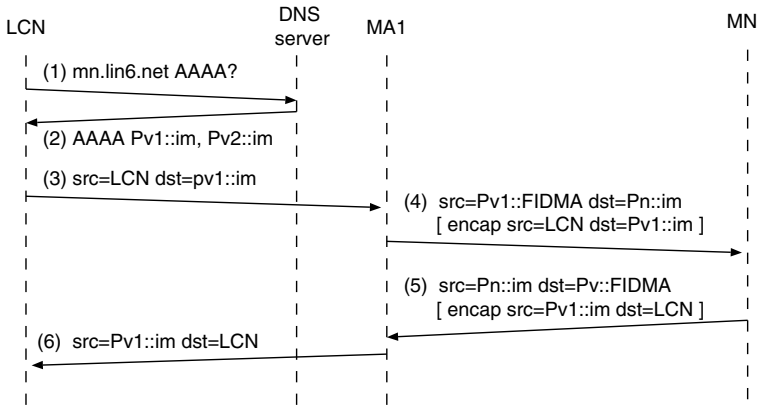

図 2.5. 提案方式における通常ノードとの通信手順: LCN は MN の後方互換アドレスに向けてパケットを送信する。MA はこのパケットを MN との IPv6-in-IPv6 のトンネルを利用して転送する。

おいても移動透過性が保証されることになる。

2.3.4 LIN6 ノード間の通信手順

提案方式では MA の発見方式を変更しているため、従来の LIN6 ノード間の通信手順は利用できない。提案方式では、リゾルバに変更を加えた手法を提案する。

一般的に、アプリケーションは FQDN によって通信相手を指定された場合、これを IPv6 アドレスに変換するために DNS に問い合わせを行う。この処理はアプリケーション非依存であるので、OS が提供する共通の関数群が利用されることが多い。この関数群はしばしば**リゾルバ**とよばれる。以後本章においてもこの処理を行う関数群をリゾルバと呼ぶ。

提案方式では、AAAA レコードを問い合わせた結果が、LIN6ID を含むアドレスであった場合、リゾルバでこのアドレスを LIN6 汎用識別子に変換してアプリケーションに渡すようにする。以下、提案方式における LIN6 ノード間の通信手順を、図 2.3 において CN が MN に発呼する例を用いて説明する。

- ユーザあるいはアプリケーションは FQDN 形式、すなわち mn.lin6.net で通信相手を指定する。
- アプリケーションはリゾルバに対して、mn.lin6.net を IPv6 アドレスに変換するように要求する。
- リゾルバは、与えられた FQDN から IPv6 アドレスへの変換を行うために DNS サーバに AAAA レコードを問い合わせる。この結果、Pv1::im および Pv2::im が得られる。
- リゾルバは、得られた IPv6 のアドレスが LIN6ID を含んでいるため、これを LIN6 汎用識別子に変換する。すなわち、この 2 つのアドレスは O::im に変換され、アプリケーションに渡される。
- アプリケーションは O::im に対して発呼を行う。
- O::im のマッピングを得るために、LIN6ID が im であるノードの Designated MA のアドレス、Pv1::FIDMA、Pv2::FIDMA を得る (2.3.2 章参照)。
- Pv1::FIDMA(あるいは Pv2::FIDMA) に対して Mapping の問い合わせを行う。

2.4 考察

2.4.1 移動ノードの設定の自律性について

まず移動ノードは、通常ノードと通信する際に自分の designated MA が管理する後方互換アドレスをソースアドレスとするため、それらのアドレスリストを保持する必要がある。これらは、自分の LIN6ID から、自分に割り当てられた FQDN を求め、その FQDN の AAAA レコードとして定義されている値が後方互換アドレスであるため、ユーザが静的に設定する必要はない。

また、複数の MA を利用する場合、トンネリング先も複数個存在することになる。MN は、各後方互換アドレスについて、トンネルのエンドポイントとして適切な MA を選択する必要がある。しかし、提案方式では、トンネルのエンドポイントは MA が持つ仮想ネットワーク上の既知のインターフェイス ID であるので、トンネルのエンドポイントは、トンネルするパケットの送出時に、ソースアドレスから決定可能である。このため、トンネルのエンドポイン

トための特別なテーブル等は必要とならない。

よって、本提案方式によってあらたにノード側で静的に設定する情報はなく、ノードの設定の自律性は高いといえる。

2.4.2 従来ノードとの通信時におけるソースアドレスの選択

LIN6 ノードがパケットを送出する際においてソースアドレスを選択する場合について考える。従来ノードとの通信は、基本的に後方互換アドレスを選択することになる。しかし、後方互換アドレスを選択する場合、すべての通信はその後方互換アドレスに対応する MA を経由する通信となるため、通信路のオーバヘッドが大きい。とくに短いトランザクションとなることが予想される通信においては、このオーバヘッドは好ましくない。例えば、DNS への問い合わせパケットなどがこのような通信に適合する。

この問題は、ソースアドレスの選択時に、ユーザなどが指定可能なフィルタを用いて、あるパケットが指定された条件に合致した場合には後方互換アドレスではなく現在移動ノードが利用可能な通常の IPv6 アドレスをを選択可能にするようなメカニズムによって回避可能である。

2.4.3 Designated MA の発見処理のオーバヘッド

従来方式において、Designated MA の発見は、ある LIN6ID id に対して、rev(id).lin6.net の MA レコードを問い合わせるだけで可能であった、すなわち DNS サーバへの問い合わせ回数は 1 回であった。一方、提案方式では、rev(id).lin6.net の PTR レコードを問い合わせ、その結果得られた FQDN に対して AAAA を問い合わせる、すなわち 2 度 DNS サーバへ問い合わせる必要があり、オーバヘッドが増加している。しかし、rev(id).lin6.net の PTR レコードを問い合わせた結果の FQDN は、高い確立でユーザあるいはアプリケーションが指定した通信相手の FQDN になると考えられる。そのため、この FQDN に対する問い合わせの結果は MA の発見の前にすでに行われており、ノードが問い合わせに利用する DNS サーバにキャッシュされている可能性が高く、オーバヘッドの増加はそれほど高くならないと考えれられる。

2.4.4 セキュリティ

提案方式においては、従来の LIN6 に加え、MA とのトンネリングが新たに加わっており、この通信のセキュリティが問題となる。提案方式では、MA が仮想ネットワーク上に持つ既知のアドレスを、LIN6 の stationary adress[93] とすることにより、移動ノードとのトンネリングに対しても LIN6 を利用し、移動透過性を得ることができる。このため、このトンネリングに対して IP security (IPsec)[136] を適用することが可能である。すなわち、MA と移動ノードとの間で利用される Security Association (SA) はノードの位置に関わらず一組の SA を継続的に利用可能である。よって、トンネリングのパケットは IPsec によってセキュリティを確保できる。

2.5 おわりに

本章では、移動等価性保証プロトコルである LIN6 を拡張し、既存の IPv6 ノードとの通信時においても移動等価性保証を提供できる LIN6 の機能拡張方式について議論した。提案方式は、MA に仮想的なネットワークを配置し、そのアドレスに移動ノードが存在するように見せることで MA へパケットを誘導し、そのパケットをトンネリングによって移動ノードにパケットを配送することで、既存のノードとの通信においても移動等価性保証を提供可能とした。同時に、MA レコードを利用せず AAAA レコードに MA の情報を埋め込むことによって、既存の DNS サーバを変更することなく LIN6 を使用することができるようになり、より LIN6 への移行が容易となった。

今後は本提案の実装を行い、実際の性能評価と運用実験を行い、提案方式が現実のインターネット上で動作することを証明していきたい。

第 3 章 ORC: Optimized Route Cache Management Protocol for Network Mobility

3.1 Introduction

Along with the advancement in wireless networking technologies, the mobile population of the Internet is expected to contain over a billion wireless devices, such as telephone handsets, in the

near future. Therefore this research deals only with IPv6 [136], because IPv6 has scale advantages such as huge address space and plug and play support. In addition, IPv6 is expected to promote wireless computing and is deployed rapidly due to IPv4 address insufficiency. Current research of mobility protocol called Mobile IPv6 is almost ready for a standardization at the Internet Engineering Task Force (IETF). Mobile IPv6 is designed to provide continuous accessibility to mobile nodes with mobility transparency on IPv6. Demands of network mobility arise from real situations such as PAN and network inside vehicles [59, 90, 58], but Mobile IPv6 does not provide solution in response to these demands. Network mobility provides mobility for a cluster of nodes (i.e. It can be treated as a network and is called mobile network [57]). A PAN built around one's body is a typical situation to apply network mobility. The continuous mobility of human will lead to movements of many nodes in the PAN. If all the nodes are forced to run Mobile IPv6 due to the movement of human body, the protocol overhead causes futile consumption of network and hardware resources. Instead, an elected node should become a gateway (called mobile router) to the Internet with computational ability and network performance. It is more efficient that the mobile router provides mobility to a mobile network in these situations.

This research proposes the Optimized Route Cache Management Protocol (ORC). ORC provides network mobility along with security and scalability to take approaches combining internet routing and Mobile IPv6. When a network changes its point of attachment due to its movement, the location of the mobile network is changed in the Internet. To suppress the topology change, ORC aims to scatter a route of a mobile network to portions of the Internet, i.e. either domains or Autonomous Systems (AS) where the mobile network communicates. Distribution of the route is achieved by extending binding update mechanism of Mobile IPv6. As a result, ORC reduces protocol signaling, disperses bottleneck of intermediate agent, and avoids single point of failure.

3.2 Problem Statement

When a mobile network moves around the Internet, it brings several issues due to the fact that the current protocols does not assume this situation. The issues are **network transparency**, **scalability and quickness**, **security**, and **route optimization**. **Network transparency** indicates that correspondent nodes (CNs) are unaware of a mobile network's movement during communication, and communications should not be affected by its movement. It is important to have **scalability and quickness** for mobile network's route propagation in the Internet, and for updating a route of a mobile network as soon as the mobile network changes its attached network. **Security** is an important feature for a mobile network to protect from attackers. It can be expected to hijack a mobile network by attackers and steal all packets to the mobile network. **Route optimization** brings better communication performance since a route path needs to be changed frequently along with network movements.

3.3 Optimized Route Management Protocol

ORC is designed to address all the issues described in section 3.2. It provides network transparency by assignment of unique unchanging prefix to a mobile network. Scalability is supported by running ORC on the existing internet routing mechanism, and quickness is achieved by taking Mobile IP functions to ORC. ORC also uses Mobile IPv6 mechanism for route optimization. Figure 3.1 shows the overview of ORC. In the figure 3.1, there are 4 ASs connected to each other by Border Gateway Protocol (BGP) [164]. Currently this is assumed to be typical internet routing topology.

3.3.1 Mobile Prefix

Mobile prefix is a prefix and is assigned to a

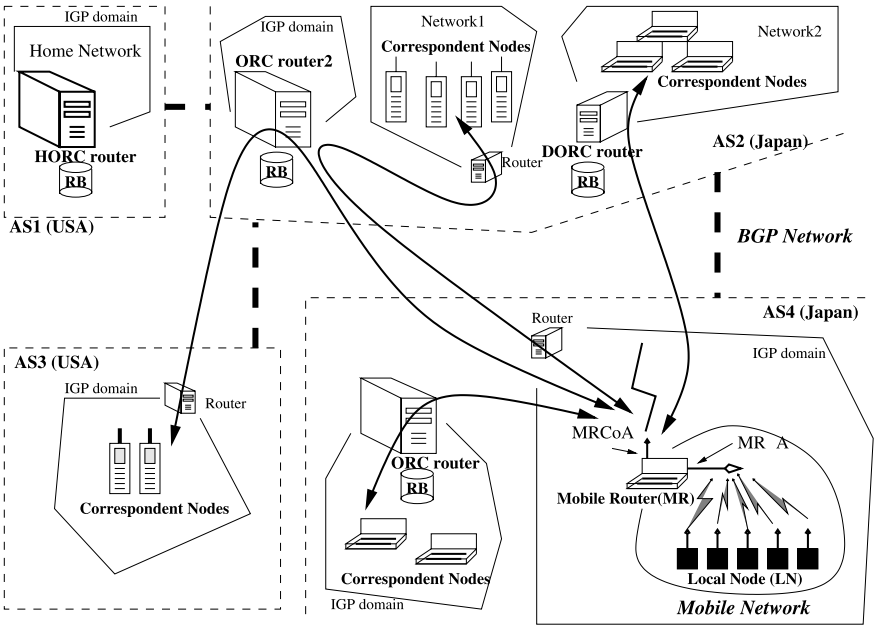

Fig. 3.1. Optimized Routing Cache Management Protocol

mobile network as an unchanging prefix. A mobile network has a home network where its prefix is securely delegated and defined. Operation of prefix delegation is not discussed in this research, but any protocol can be used.

3.3.2 Mobile Router

Mobile Router (MR) is the only router in the mobile network which has common functions to a router such as forwarding and routing packets, and handling ICMP error messages. Local Node (LN) is a node attached to the mobile network. The address assignment can be performed for LNs by existing protocols such as address autoconfiguration [140] and DHCPv6.

The MR has two network interfaces for connecting to the Internet and to the mobile network. Mobile Router Address (MR-A) is statically assigned to the interface connected to the mobile network (named ingress interface). The MR-A should be generated by a MR's host EUI-64 identifier and the mobile prefix of the MR. Mobile Router Care-of Address (MR-CoA) is an address which is dynamically assigned to the interface connected to the visited network (named egress interface). The MR-CoA is acquired by router advertisements [155] at the visited network.

Routing inside a mobile network can be managed by any existing protocols such as Mobile Adhoc Network (MANET) routing protocols [119, 162], OSPF6 [103] and RIPng [61]. But MR must not advertise inner routes to the Internet from the egress interface by any routing protocol. MR may distribute router advertisements of the mobile prefix with a new-defined mobility flag to the ingress interface for LNs' address auto-configuration. The mobility flag is used for nested mobility operations described in section 3.3.6, or for default route selection. Possibly, the flag could be ignored if LNs do not recognize it.

3.3.3 Binding Route

Binding Route (BR) is a special route of a mobile network along with the remaining lifetime. The BR has the similar structure to a Mobile IPv6's binding. The BR contains an association between the mobile prefix and the MR-CoA of the MR. Generally, a route entry is organized as follows: a destination is the mobile prefix and a next hop is the MR-CoA. The BR is cached in a routing table with the appropriate lifetime.

The BR is updated securely by the MR. The BR

should be processed and maintained by routers instead of end-nodes. It is expectable that hundreds of CNs in an IGP domain communicate with LNs over the MR of a mobile network. Sending hundreds of BRs to CNs on the IGP domain is obviously redundant operations to the MR and CNs. The MR efficiently notifies single BR to a router on the IGP domain across the Internet. The BR itself cannot be (re-)advertised with routing protocol as routing information to the Internet, because the BR does not belong to the route management range of the IGP network. Current routing protocol will not fall into disorder with the BR.

3.3.4 Optimized Route Cache Router

An ORC router is an anchor router of a mobile network and maintains a BR of the mobile network persistently. The ORC router can be configured anywhere in the Internet. Practically, the ORC routers should be put on expected networks where there exist CNs for the mobile network, because it is impossible to replace all routers on the Internet to ORC routers. Whenever a MR moves, ORC routers receive a BR notification from the MR and cache it in their routing table. The ORC router must authorize the mobile network to receive the BR as described in section 3.4.1. After creation of the BR, the ORC router intercepts packets destined to the mobile network, and tunnels them to the MR-CoA which is registered in the BR.

All ORC routers advertise a proxy route of the mobile prefix to capture packets destined to the mobile network by any IGP protocols. The proxy route can not be inter-exchanged by any Exterior Gateway Protocol (EGP) such as BGP. The proxy route is not a BR, but it contains the mobile prefix as a destination and the ORC router's address as the next hop. The proxy route will not be aggregated in ORC router's IGP domain. ORC router can reject receiving BR of any mobile network according to domain policies, because the advertisement of unaggregated route may swell routing entries on IGP routers. According to routing management policies of each AS, ORC routers should be approved to provide ORC services from their affiliated IGP domain.

When one of the nodes inside Network1 of AS2 communicates with the mobile network in the figure 3.1, packets destined to the mobile network are always routed to the ORC router2, because the ORC router2 advertises a proxy route to turn the route of the mobile network to itself in AS2. The ORC router2 intercepts packets and tunnels them to the MR attached in AS4. On the return path, the MR could send packets to the CN via the ORC router2 by the use of IP-in-IP Encapsulation [15] with the ORC router2's address. The MR may reply packets directly to the node by encapsulation, if the node can decapsulate these packets.

There are two special types of ORC routers which are Home ORC Router and Discovered ORC router.

Home ORC Router

One of the ORC routers called Home ORC router (H-ORC router) must be a router of the link on which a mobile prefix is defined. The H-ORC router assigns a prefix from its managed prefix ranges, and delegates it to the mobile network. The H-ORC router is well-known by the MR and always have a fresh BR of the mobile network. The H-ORC router intercepts packets on the link destined to the mobile prefix, and tunnels them to the registered MR-CoA, while the MR is away from home.

Discovered ORC Router

Discovered ORC router (D-ORC router) is an edge router of CNs' network, capable of dynamically becoming a ORC router. The D-ORC router must have a D-ORC anycast address which is generated by the D-ORC router's 64 bit prefix and an anycast identifier. The D-ORC router is dynamically discovered with "ORC Router Discovery and Reply" (UDP packets) to the D-ORC anycast address by a MR. The discovery is operated on demand whenever the MR starts communicating with the IGP network of the D-ORC router, or receives packets destined to the mobile network via one of the ORC routers. Discovery mecha-

nism is similar to the home agent discovery mechanism of Mobile IPv6 [81]. If no replies are received, the MR stop discovering D-ORC routers in the CN's network and receives packets via one of the ORC routers (or maybe via the H-ORC router). If the MR finds the D-ORC router2 of the Network2 by "ORC Router Reply", it starts sending a BR to the D-ORC router2 described in section 3.4.1. After creating the BR, the D-ORC router2 establishes a tunnel between the MR and itself, and takes on responsibility of routing packets destined to the MR according to the BR. The D-ORC router maintains the BR only while CNs are communicating with the mobile network.

3.3.5 Routing to Mobile Network

Route path depends on availability of ORC routers on the way to a H-ORC router from a CN. When packets destined to a mobile network arrive at one of the ORC routers, the receiving ORC router intercepts them, encapsulates them, and tunnels them to the mobile network's registered MR-CoA in a BR. Therefore, the route path to the mobile network is optimized by bypassing the H-ORC router, because the route path to the H-ORC router is different from the current topological position of the mobile network. There are mainly three network environments depending on configuration of ORC routers.

First, the network environment is where there are ORC router(s) on the CN's network regardless of ORC router's type. Packets from the CN will reach the nearest ORC router in the AS. The nearest ORC router is selected by IGP routing protocols which have the shortest path finder algorithm such as the Dijkstra algorithm [103]. Second, there is no ORC routers on the CN's network, but one of transit ASs on the way to the H-ORC router has ORC routers(s). The ORC router in the transit AS is selected by general internet routing, because it advertises proxy route of the mobile network to its AS. The last environment is where there is no ORC router on the way to the H-ORC router from the CN. In such environment, the H-ORC router is used, because it can intercept packets on the home network destined to the mobile network. In second and third environments, the MR can discover D-ORC routers and notify a BR to them.

Increasing the number of ORC routers caring the mobile network is an important factor to distribute route of the mobile network on the Internet depending on a number of networks which LNs are communicating with. Distributed BR also helps to avoid single point of failure. If the H-ORC router goes unavailable, CNs can communicate with a mobile network except for the third network environment. However, ORC is not always requested to have a lot of ORC routers, because updating its BR to all the ORC routers brings considerable overhead and prevents scalability and quickness of updating BRs.

3.3.6 Nested Mobility

Nested mobility is known as the state when a MR is itself attached to a mobile network in the hieratical fashion. When a mobile network attaches another mobile network, the MR of the upper mobile network becomes a parent-MR, and the MR underneath it becomes a sub-MR as defined in [57]. If the sub-MR could obtain a sub-MR-CoA by address auto-configuration, it detects that the upper router is the parent-MR from the mobility flag in parent-MR's router advertisements described in section 3.3.2. The sub-MR must then send a route of its own mobile prefix to the parent-MR by any routing protocol running inside the mobile network. The parent-MR should send its own BR to ORC routers of the sub-MR while the sub-MR operates notifying sub-MR's BR to them. If ORC routers have only a BR of the sub-MR, they encapsulate packets with the sub-MR-CoA. Therefore, packets routed to one of the parent-MR's ORC routers are encapsulated again, and are tunneled to the parent-MR. On the other hand, if ORC routers have BRs of both the parent-MR and the sub-MR, they encapsulate packets with the parent-MR-CoA according to recursive BR search described in section 3.4.2. The parent-

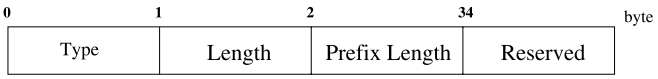

Fig. 3.2. Prefix Mobility Option

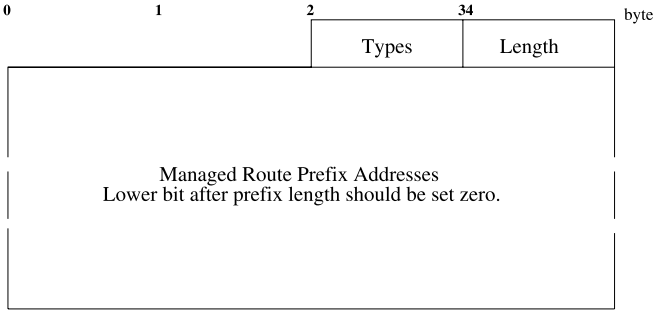

Fig. 3.3. Managed Prefix Mobility Option

MR decapsulate packets and route them to the sub-MR, since the parent-MR obtained the route of the sub-MR.

3.4 Processing Binding Route

3.4.1 Securely Notifying Binding Route

The processing for BR is designed to exploit binding processing of Mobile IPv6, because BR's relation of destination and next hop can be treated as binding's association of home address and care-of address. Messages and their options described in this section are mostly defined in [81].

Notification

When a MR attaches to a network, it obtains a MR-CoA at the visiting network. The MR sends a Binding Update (BU) to ORC routers with its MR-A and the MR-CoA, but it does not send BUs to end-nodes which does not have router functionality. BU packets must be organized with a BU message, a prefix mobility option defined in figure 3.2, and a home address destination option. The MR should add a binding authorization data mobility option and a nonce indices mobility option depending on security mechanism described in section 3.4.1.2. The MR contains its MR-A in the home address destination option. The mobile prefix length is contained in the prefix mobility option.

The binding ack flag must be set in the BU to receive a Binding Ack (BA) from recipient. A ORC router must return BA containing a list of managed prefixes of its IGP domain in a managed prefix mobility option. The managed prefix mobility option is defined in figure 3.3. If the BU is successfully processed by the ORC router, the MR establishes a tunnel to the ORC router as in [81]. The MR also records pair of the prefixes retrieved from the managed prefix mobility option and the ORC router's address as route entries in its routing table. These routes may be used to search a correspondent ORC router in a routing table when the MR sends packet to CNs described in section 3.4.2.

The ORC router creates a BR of a mobile network to associate a mobile prefix with a MR-CoA and insert it into its routing table. ORC router retrieves the mobile prefix from the MR-A in the home address destination option and the mobile prefix length in the prefix mobility option. MR-CoA is stored in the source address field of IPv6 header.

Security

ORC enables to manage routing information across AS boundaries. In other words, it is possible for a MR to alter routing table of opposite routers. Wrong BRs will cause opposite ASs to fall into confusion or to have black-hole of routing. ORC uses Mobile IPv6 security mechanism [81]

for protecting BUs of BR such as IPsec authentication header [126] and Return Routability (RR) scheme. Furthermore, recipient routers can apply their IGP domain or AS routing policies to handle each BR.

This section describes the extension of RR to ensure that correct BR will be notified to ORC routers. In Mobile IPv6, RR procedure plays two roles when authenticating a BU. One is to verify if binding between the home address and the care-of address is legit, another is to exchange keys for authorizing BU. In ORC, following extensions are required in addition to RR mechanism used in Mobile IPv6. First is between a MR and a H-ORC router, secure tunnel such as ESP [138] should be created using the MR-A in order to avoid malicious nodes to send BUs of BR to the H-ORC router. Another is on the H-ORC router, HoTI sent from the secured tunnel between the MR and the H-ORC router should be checked for its source address and prefix length. This is required since HoTI will be sent with the MR-A for the source address, and if the source address does not match the MR-A registered in H-ORC's binding or prefix length in the prefix sub-option does not match the H-ORC router should discard the HoTI. On the other hand, CoTI will be sent with the MR-CoA as its source address. Once the MR receives both HoT and CoT back from the ORC router, we can tell that MR exists in topologically correct position and also a router of the network with the MR-A's prefix. The MR can send BU of BR to the ORC router with keys exchanged in RR, if the ORC router can recompute the encryption, BU using RR completes in success.

IPsec operations are same as the operations of Mobile IPv6 except for a security association. The MR establishes a security association between the MR-A and the H-ORC router's address.

3.4.2 Management of Binding Route

Whenever a ORC router receives packets and query routing table as general router operations, it also searches BR caches for a destination address in an IPv6 header. The ORC router should select the prefix longest matched BR or route for the destination. When the ORC router finds the prefix longest matched BR for the destination, it must search BRs recursively for the next hope address of the BR and must select the last matched BR for the destination. This recursive operation is aimed to support nested mobility. Once the ORC router finds a BR instead of an IGP route for outgoing packets, it tunnels packets directly to the MR-CoA according to the BR by IP-in-IP encapsulation. For the opposite direction, the MR may encapsulate outgoing packets with the MR-CoA as an outer IPv6 source address to bypass ingress filtering of the visiting network. Therefore, CNs must support decapsulation of these packets. Alternatively, the MR may reverse tunnel packets to the ORC router at CN's IGP domain which is found with route of the ORC router's managed prefixes in MR's routing table. The MR obtains the managed prefixes by receiving a BA with a managed prefix mobility option. The ORC router then decapsulates packets and route them to a CN. The MR does not insert the home address option as general Mobile IPv6, since falsification of LNs packets on intermediate nodes like the MR should be avoided for security considerations. The Encapsulation of packets adds additional IPv6 header, and it does not change original packets.

3.5 Conclusion

This research proposes the Optimized Route Cache Management Protocol for mobile networks. ORC provides network transparency by assignment of an unique unchanging mobile prefix to a mobile network. A MR notifies a BR which is an association of a MR-CoA and a MR-A by BU mechanism of Mobile IPv6. Recipient caches the BR and manage it during BR's lifetime. In this protocol, the MR sends a BU to ORC routers instead of CNs. The BR is treated as route information for the mobile network. This prevents an explosive increase of BU processing overhead on

the MR, even when the number of CNs increases. ORC routers allow CNs to communicate with the mobile network without any modifications. ORC routers can route packets destined to the mobile network according to the BR. The route path is always optimized by bypassing MR's H-ORC router. As routers route packets according to route information on the Internet, ORC routers send packets to the mobile network in compliance with the BR. This architecture is so scalable with minimum impact to the Internet. BU containing the BR is protected by security mechanism such as IPsec and RR. RR provides authentication of the MR, authorization of the mobile prefix, confidentiality of the BR.

第 4 章　おわりに

本年度は、IPv6 における新しい移動透過保証プロトコルである LIN6 プロトコルの後方互換性拡張の一方式と、モバイルネットワークの実現方式について報告した。

Rover では、今後も定期的なミーティングを通して、移動計算機に適したファイルシステムや、移動透過性保証のためのプロトコルといったモバイルコンピューティングに関する議論を活発に行っていく予定である。なお、Rover のより詳細な活動については、`http://www.imobility.org/`を参照されたい。