

プライベート IP アドレスを用いたモバイル IP ネットワークにおける経路最適化ピアツーピア通信の実現

加藤 聰彦 伊藤 秀一

電気通信大学 大学院情報システム学研究科

近年 Mobile IPv4 を用いたモバイルインターネットの構築が行われているが、移動端末の増加に伴い IP アドレスの不足が懸念される。これに対し Mobile IPv4 では逆方向トンネリングの使用を前提として、HA ごとに独立にプライベート IP アドレスを移動端末に割り当てる方法を導入している。これは固定網のプライベート IP アドレスの利用と同等であり、外部のホストの通信するためには、HA において NAT 機能を実施する必要がある。このため、この方法でアドレス不足は解決できるものの、移動端末間のピアツーピア通信を行うことが不可能となる。これに対しては、VoIP など用いられている SIP を Mobile IP と協調させることにより解決することができる。しかし単に SIP と Mobile IP を用いただけでは、移動端末間の通信に相互の HA を経由する必要があり、経路最適化が実現できない。このような背景の下で、筆者らは動的に発呼用 IP アドレスを割り当てる Mobile IP と SIP を用いて、HA ごとのプライベートホームアドレスの利用と経路最適化されたピアツーピア通信を両立する方式を検討している。本稿ではその方式について述べる。

Route Optimized Peer-to-Peer Communication over Mobile IP Network with Private IP Addresses

Toshihiko Kato Shuich Itoh

University of Electro-Communications

Recently, Mobile IPv4 is being used widely as the fundamental protocol for mobile internet. But, resulting from the increase of mobile terminals, the IP address starvation becomes a serious problem. Mobile IPv4 includes the procedure that an HA can independently assign private IP addresses to MNs it manages, based on the assumption to use the reverse tunneling. However, this procedure requires NAT functionality at HAs and it is impossible to make a call to an MN with private home address. This problem is solved by combining SIP with Mobile IPv4, by making HAs work as SIP proxies. Now, a new problem that, in this scheme, MN to MN communication is realized through MN-FA-HA-HA-FA-MN path and that the route optimization is not realized. We are proposing a new Mobile IPv4 that an FA assigns an IP address to an MN when it initiates a new call and the FA works as a home agent for assigned IP address. In this paper, we describes a detailed procedure which realizes the route optimized peer-to-peer communication using private IP home address, SIP and our new Mobile IP procedure.

1. はじめに

近年モバイルインターネットが広く普及しているが、Mobile IP [1]がその基本プロトコルとして使用されている[2]。しかし IPv4 アドレスを用いた Mobile IP では IP アドレス数の不足が課題となる。このため、プライベート IP アドレスの使用が検討されており、逆方向トンネリング[3]を用いた Mobile IP 手順をベースとして、ホームエージェント (HA) 単位に独立に、

移動端末(MN)のホームアドレスとして、プライベート IP アドレスを割り当てる方法が定められている[3]。これにより 1 つの HA の配下の MN の間だけでユニークなプライベート IP アドレスを割り当てるだけですみ、MN の増加によるアドレス数の不足に対応することができる。

しかしこの方法では、異なる HA に属する MN または一般のホストに対して通信を行う

場合は、HA において、MN のプライベート IP アドレスをグローバルな IP アドレスに変換する NAT (Network Address Translator) 機能[4]を実現する必要があり、このため、MN への着呼を行うことができない。すなわち、HA 単位のプライベート IP アドレス割り当てを導入した場合は、MN 間での VoIP などのピアツーピア通信を行うために、直接通信相手の IP アドレスを指定できないことになる。

これに対し、ピアツーピア通信のセッションを管理するために、SIP (Session Initiation Protocol) [5]が使用されている。SIP では、通信相手の論理名(SIP URI)を用いて、IP アドレスを明示的に指定することなしに通信を開始することを可能としている。そこで、SIP と組み合わせることにより、プライベート IP アドレスを用いた Mobile IP において、MN 間でのピアツーピア通信が可能となると考えられる。

しかし、この方式では、MN 間のピアツーピア通信において、必ず双方の HA を経由することになる。これにより転送される IP パケットは、一方の MN の移動先の FA から対応する HA へ転送され、さらに相手の MN に対応する HA 経由で、相手の移動先の FA へ転送され、最終的に MN に受信される。すなわち、FA→HA→HA→FA という経路をとることになり、最適な経路 (FA→FA) に比べると 2 ホップが冗長となる。

筆者らは、これまでに MN が発呼を行う場合は、移動先の FA から IP アドレスを動的に割り当てられ、その FA をホームエージェントとして動作させることにより、IP の可動性を保証するとともに、自然な経路最適化と、HA でのフォワーディングオーバーヘッド削減を実現する Mobile IP 通信方式の提案を行っている [7,8]。この方式と、SIP を用いたプライベート IP アドレスベースの Mobile IP とを組み合わせることにより、前述の MN 間のピアツーピア通信の経路冗長化の問題点を解決することができると思われる。そこで本稿では、その通信手順について述べる。

本稿の構成は以下のとおりである。まず 2 節で、HA 単位のプライベート IP アドレスを割り当てる Mobile IP の概要を示す。次に 3 節で

そのような Mobile IP ネットワークに SIP を導入することによりピアツーピア通信を実現する方式について概説する。続いて 4 節において、筆者らが提案する発呼に対する HA 機能を FA に持たせる Mobile IP 手順について述べる。さらに 5 節において、プライベート IP アドレスにより Mobile IP ネットワークの経路最適化ピアツーピア通信の実現方法を提案する。

2. プライベート IP アドレスによる Mobile IP

文献[3]の示すプライベート IP アドレスによる Mobile IP 手順の概要を図 1 に示す。この図では、HA1 に属する MN1 と HA2 に属する MN2 とが同一のプライベート IP アドレス HoA をホームアドレスとして有し、フォーリンエージェント (FA) FAa の下に移動しかつ同じ通信相手 (Correspondent Node: CN) CN と通信を行っている状況を示している。HA1 および HA2 は FAa を介して、それぞれ HA1 および HA2 に登録する。その結果、HA1 および HA2 は、モビリティバインディングリストに、各 MN のホームアドレス HoA と、移動先の気付けアドレス (CoA) である FAa を保持する。また、FAa は、ジタリストに MN1 および MN2 のホームアドレス HoA、対応する HA のアドレス HA1 または HA2、各 MN の MAC アドレス MAC1 または MAC2 を保持する。

MN が CN と通信する場合は、以下のようになる。

・MN と FA の間はプライベート IP アドレスを用いた通信となる。一方 FA は、MN が送信した IP パケットを受信すると、ジタリストに保持された MAC アドレスから MN1 か MN2

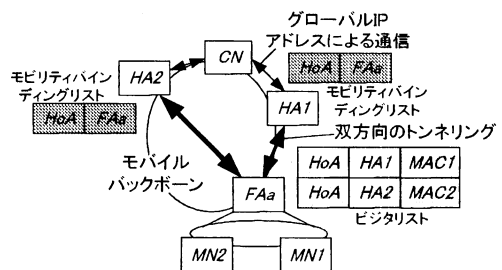


図1 プライベート IP アドレスによる Mobile IP 手順

かを区別し、対応する HA に対してカプセル化して転送する（逆方向トンネリング）。すなわちモバイルバックボーン内を転送される IP パケットは、FAa から HA1 または HA2 宛となり、これにより MN のプライベート IP アドレスが処理されることはない。

・ HA から MN に IP パケットが転送される場合は、通常のトンネリングで HA1 または HA2 から FAa に転送され、MN のプライベート IP アドレスはモバイルバックボーン内では現れない。また、FAa はジグザグのホームアドレス(HoA)と HA のアドレス(HA1 または HA2) から MN を区別し、カプセル化をはずした IP パケットを対応する MAC アドレス宛に直接送信する。

・ HA と CN の間の IP パケットの転送においては、HA において NAT の処理が行われ、MN1 または MN2 のホームアドレス HoA は、HA1 または HA2 の持つグローバル IP アドレスに変換されて CN 宛に送られる。このため CN では MN1 と MN2 をそのグローバル IP アドレスで区別することになる。

3. SIP を用いたピアツーピア通信方式

SIP は VoIP のようなピアツーピア通信のセッションの開始・完了を管理するためのプロトコルである。SIP を用いる端末は“sip:user@domain”の形式を持つ SIP URI を用いて識別される。またドメインごとにプロキシサーバおよびレジストラと呼ばれるサーバが用意される。

各端末は、事前に自身の SIP URI や IP アドレスをレジストラに登録しておく。通信を開始する端末は、通信相手の SIP URI を指定した INVITE リクエストを、自身のドメインのプロキシサーバに対して送信する。このメッセージは、通信相手のドメインのプロキシサーバ経由で通信相手に転送される。相手ドメインのプロキシサーバが端末に転送する場合にレジストラに登録した情報が利用される。

INVITE リクエストには Trying、Ringing、OK などのレスポンスが用意されており、OK レスポンスが、最終的に通信相手がセッションを受け入れたことを示し、OK レスポンスがセッシ

ョン開始側から ACK により確認された時点でセッションが確立される。また、INVITE リクエストおよび OK レスポンスは、端末の IP アドレスを Contact フィールドに含むことが可能で、これにより、その後のセッションデータや SIP メッセージは、プロキシ経由なしで直接端末間で転送することが可能となる。ただし、INVITE リクエストに Record-Route フィールドにプロキシサーバの IP アドレスまたはホスト名を指定することにより、その後の SIP メッセージを指定したプロキシサーバを経由させることができる。またセッションを終了する場合には、一方が BYE を他方が OK レスポンスを送信する。

プライベート IP アドレスを用いるモバイル IP に、SIP を適用するために、次のアプローチを採用する。

- ・ HA ごとに SIP ドメインを導入し、SIP のプロキシサーバを HA 内に実現する。SIP URI については、MN に割り当てられた NAI (Network Access Identifier) を流用するまたは明示的に導入することとする。前者の場合はレジストラを導入することはしない。また NAT 機能を HA に導入する。
 - ・ HA に存在するプロキシサーバは、自分自身の管理する MN から、他のドメインに属する MN との通信を開始する INVITE リクエストを受信すると、そのセッションで使用するグローバル IP アドレスを確保する。また、他のプロキシサーバから自分の管理する MN 宛の INVITE リクエストを受信すると、その MN のためのグローバル IP アドレスを確保する。これらのアドレスはそのセッションが終了するまで保持される。
 - ・ HA に存在する NAT は 2 節で示した方式に従って、中継する IP パケットにおいて、プライベート IP アドレスとグローバル IP アドレスの付け替えを行う。
 - ・ プロキシサーバはその後 SIP メッセージを転送する際に、メッセージ内の MN の IP アドレスに対して、プライベート IP アドレスとグローバル IP アドレスの変換を行う。
- それぞれ HA1 または HA2 に属する MN1 ま

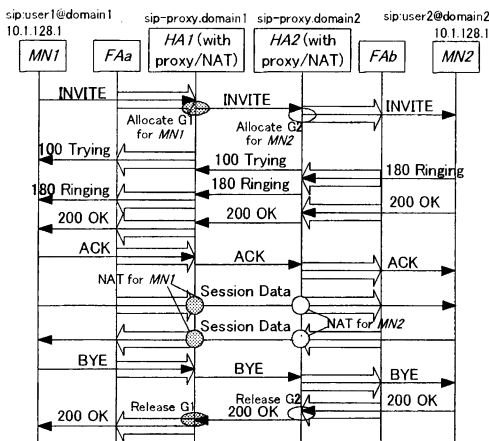


図2 SIPによる通信シーケンス例

たは MN2 が、FAa または FAb に移動した状況で、MN1 が MN2 に対してピアツーピア通信を行う場合の通信シーケンスを図 2 に示す。ここで MN1 と MN2 は同一のプライベート IP アドレスを付与されているとする。

まず MN1 が INVITE リクエストを HA1 に存在するプロキシサーバに送信する。このメッセージには、宛先を示す To フィールド“To: <sip:user2@domain2>”、発信者側と直接通信するためのアドレスを示す Contact フィールド“Contact: <sip:user1@10.1.128.1>”が含まれる。このメッセージは FAa によりカプセル化され HA1 まで転送され、プロキシサーバに渡される。この際、HA1 内の NAT は MN1 に対してグローバル IP アドレス G1 を割り当てる。

次に、HA1 のプロキシサーバは、宛先の SIP URI から宛先ドメインのプロキシサーバを選定し、INVITE リクエストを転送する。その際、Contact フィールドと、中継ノードを示す Via フィールドの received パラメータの MN1 のプライベート IP アドレスを G1 で置き換える。さらにセッションを通して SIP メッセージを処理するために、Record-Route フィールド“Record-Route: <sip:sip-proxy.domain1; lr>”を追加する。また MN1 に対して INVITE を処理中であることを示す 100 Trying レスポンスを送信する。これは FAa までカプセル化されて転送される。

HA2 のプロキシサーバは、この INVITE リクエストを受信すると、To フィールドから宛先

の MN2 のホームアドレスを検索し、グローバル IP アドレス G2 を割り当て、INVITE リクエストを MN2 に転送する。その際、HA1 と同様に Record-Route フィールドを追加する。さらに 100 Trying レスポンスを HA1 に送信する。

MN2 は INVITE リクエストを受信すると、呼び出し中であることを示す 180 Ringing と、受信者が応答しセッションが確立されたことを示す 200 OK レスポンスを返送する。これらのレスポンス中には、Contact フィールドと Via フィールドの received パラメータに MN2 のプライベート IP アドレスである 10.1.128.1 が含まれる。これらのレスポンスは、INVITE リクエストの Via フィールドを逆にたどって転送される。

まず、これらを受信する HA2 のプロキシサーバでは、上記の MN2 のプライベート IP アドレスをグローバル IP アドレス G2 に変更して、HA1 のプロキシサーバに転送する。HA1 では MN1 に割り当てたグローバル IP アドレス G1 (Via フィールドに含まれる)をプライベート IP アドレスに戻して、MN1 に転送する。

次に、OK レスポンスの受信を確認する ACK が MN1 から送信される。Record-Route フィールドで 2 つのプロキシが指定されているため、このメッセージも同様な経路で転送され、それぞれプライベートとグローバルの IP アドレスの置き換えが行われる。

その後、セッションデータが転送されるが、この転送は双方向のトンネリングの経路を用いて行われ、それぞれの HA で NAT の処理がなされる。

セッション終了時において、図に示すように確保されたグローバル IP アドレスが解放される。

4. 発呼 IP アドレスを動的に割り当てる Mobile IP

(1) MN がネットワークを移動した後に発呼を行う際は、現在の移動したネットワーク上の FA から発呼用の IP アドレスを入手し、移動先のネットワークを自身のホームであるとする。このアドレスにより MN と CN の間で HA を介さない通信が可能となる。また MN がさらに

ネットワークを移動する場合には発呼用の IP アドレスを割り振った FA がホームエージェントとして機能し、フォワーディングを行う。この HA の機能を持った FA を Home FA (HFA) と呼ぶ。

(2) HFA に HA の機能を持たせるためには、HFA と MN との間で互いに認証しあう必要がある。しかし不特定の FA に移動する MN に対して、HFA が事前に秘密鍵を持つことは想定できない。そのため HA が HFA と MN のための一時的共通秘密鍵を生成・配布することとする。

(3) MN が HFA と HA に対して発呼用 IP アドレスの割り当てを要求するために、HFA Registration メッセージと呼ばれる新しいメッセージを導入する。HFA Registration メッセージは、ある HFA のネットワークにその MN が存在することを通知するためにも用いる。MN がさらにネットワークを移動した際には Registration メッセージを用いて本来の HA と発呼用のアドレスを割り当てた HFA の双方に対して登録を行う。

(4) 本方式では MN が本来のホームアドレスを含めて複数のホームアドレスを持ち、セッション毎に異なる IP アドレスを使用して通信する場合がある。各セッションの開始及び終了は個別のプロセスが管理するため、ホームアドレス対応付けはアプリケーションレイヤで行うこととする。

ホームエージェント HA に属する移動端末 MN が、HFA である HFA の下のネットワークに移動し通信相手の CN に対して発呼を行った場合の通信シーケンスを図 3 に示す。

まず MN が HFA からの Agent Advertisement を受信し移動を検出すると、通常モバイル IP の手順に従って、HFA を介して HA へ Registration Request を送信し、その Reply を受け取る。

次に MN が CN に対して TCP による通信を行おうとする時点で、HFA へ HFA Registration Request を送信する。このメッセージを受信すると、HFA は MN のために MN 登録情報のエントリを確保し、ホームアドレス、要求された登録の生存時間などを登録する。続いて HFA は、HA へ HFA Registration Request を送信する。この HFA から HA へのメ

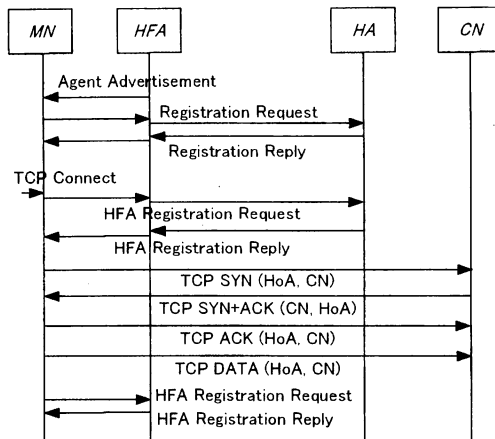


図 3 動的な IP アドレス割り当ての通信シーケンス例

ッセージは、MN からのものに HF と HA の認証情報が付加されたものである。

HA はこのメッセージを受信すると、送信した MN と HFA の認証を行った後、両者のための共通秘密鍵を生成する。次に HA は HFA に対して HFA Registration Reply を返す。このメッセージは生成された MN-HFA 共通秘密鍵を、MN-HA 共通秘密鍵と HFA-HA 共通秘密鍵で暗号化したものが含まれる。これらの 2 つの情報を含むことにより、HFA と MN のそれぞれに対して、生成された鍵の情報を安全に転送することができる。

HFA はこのメッセージを受信すると、HA の認証を行った後 MN-HFA 共通秘密鍵を入手する。さらに、MN のための発呼用 IP アドレスを生成し、最終的な登録の生存時間を定め、これらの情報を MN 登録情報のエントリに書き込む。その後 HFA は MN に対して HFA Registration Reply を転送する。HFA では自分自身のため MN-HFA 共通秘密鍵の情報と認証用情報の代わりに、自身が付与した発呼用 IP アドレスと最終的に決定された生存時間を付加する。さらに HA から与えられた秘密鍵を用いて生成した MN と HFA の認証情報を付与する。

この HFA Registration Reply を MN が受信すると HA に対する認証を行い、MN-HFA 共通秘密鍵を取り出す。さらにそれを用いて HFA を認証した後に、発呼用 IP アドレスと登録の生存時間を取得する。

その後 MN は入手した発呼用 IP アドレス (HoA1 とする) で CN と通信する。この通信はホームネットワークに接続された状況での通信であるため、HA および HFA によるフォワーディングは行われない。また MN は、HFA で管理された登録情報を保持するために、定期的に HFA Registration Request と Reply を HFA との間で交換する。

5. HFA を用いた経路最適化ピアツーピア通信方式

3 節および 4 節に述べた 2 つの方式を用いることにより、プライベート IP アドレスを HA ごとに MN に割り当てるモバイル IP ネットワークにおいて、経路を最適化したピアツーピア通信を実現することができる。

図 4 に示すようなネットワーク構成において、HA1 に属する MN1 と HA2 に属する MN2 が、それぞれ HFAa と HFAb の下に移動した状況で、MN1 が MN2 に対して通信を開始し、その通信中に MN1 が HFAa から HFAc に移動した場合を想定する。

その通信手順の詳細は以下のとおりになる (図 4 参照)。まず、MN1 と MN2 (ホームアドレスであるプライベート IP アドレスを P1、P2 とする) は、それぞれの HFA の下で Agent Advertisement を受信すると移動を検知し、気付けアドレス (それぞれ CoAa、CoAb とする) を HA に登録する。

次に MN1 が MN2 に対してピアツーピア通信を行う。MN1 は HFAa に対して発呼アドレスの割り当てを要求する HFA Registration Request を送信する。HFAa はそのメッセージを HA1 に転送し MN1 の認証を行うとともに、MN1 との間の共通秘密鍵を入手する。さらに、MN1 のための発呼アドレスを割り当てる。その際発呼アドレスは HFA1 が所有するグローバル IP アドレス (Ga) を割り当てるものとする。

続いて MN1 は MN2 との間のセッションを確立するために、SIP の INVITE リクエストを、SIP プロキシをかねる HA1 に転送する。その際の IP ヘッダのソースアドレスは割り当てられた発呼用 IP アドレス Ga を使用し、また MN2 の SIP URI と Ga を用いた MN1 の Contact フィ

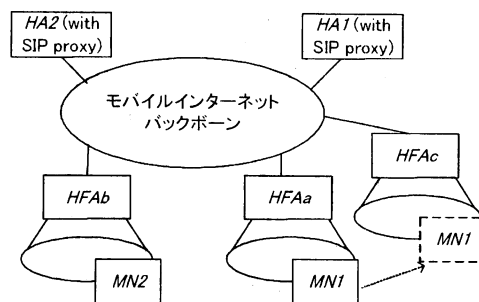


図4 想定するネットワーク構成

ールドなどを含んでいる。

HA1 はその INVITE リクエストを MN2 のドメインの SIP プロキシである HA2 に転送する。HA2 は To フィールドの SIP URI から対応する MN のホームアドレス (この場合は P2) を検索し、P2 宛てに INVITE リクエストを転送する。このメッセージは HFAb までカプセル化されて転送される。

MN2 はこの INVITE リクエストを受信すると、グローバルな通信が行われると判断し、HFAb に対して発呼用 IP アドレスを要求する HFA Registration Request を送信する。HFAb はこのメッセージを MN2 に対応する HA である HA2 に送信し MN2 の認証と共通秘密鍵の入手を行った後、MN2 に対してグローバルな発呼用 IP アドレス (Gb とする) を割り当て、HFA Registration Reply で通知する。

MN2 はその後、ユーザを呼び出し中である 180 Ringing レスポンスと、ユーザが応答したことを示す 200 OK レスポンスを返送する。これらのメッセージの IP ヘッダのソースアドレスは、新たに割り当てられた Gb であり、MN2 に対する Contact フィールドも Gb を明示する。

これらのメッセージが 2 つの SIP プロキシを経由して転送され、MN1 はそれに対して ACK メッセージを送信し、セッションが確立される。本手順では 3 節に述べた手順と異なり、グローバル IP アドレスは HFA により割り当てられ、その解放は通信が終了した時点で MN と HFA の間で行うことができる。このため、SIP プロキシはセッション確立後の SIP メッセージを監視する必要がない。従って、INVITE リクエストおよびその後のレスポンスには

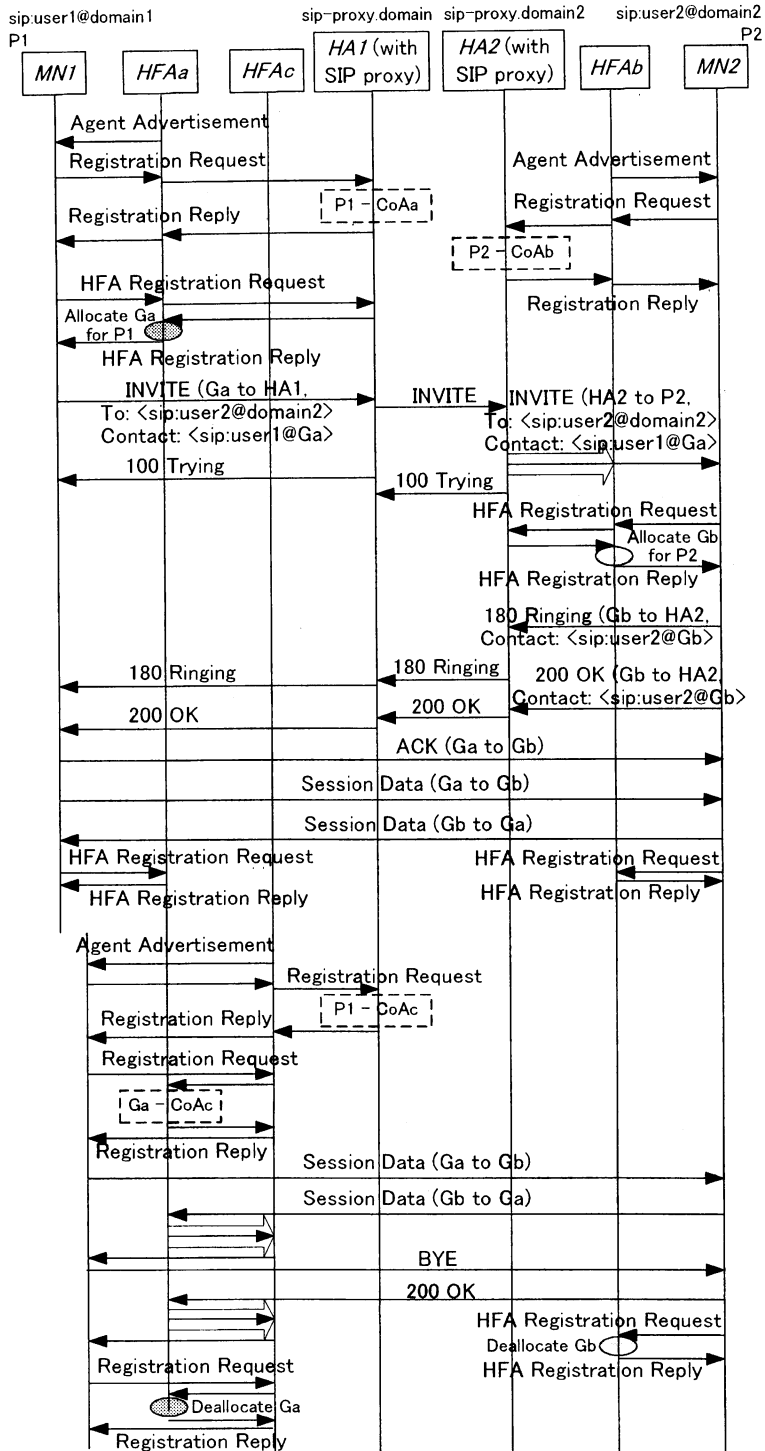


図5 提案する方式のシーケンス例

Record-Route フィールドは含まれず、ACK メッセージも *MN1* と *MN2* の間で直接転送される。

その後のセッションデータの転送は、グローバル IP アドレス *Ga* と *Gb* の間で行われ、*HA* および *HFA* によるフォワーディングを受けない最適な経路による転送が実現される。通信中においては、*MN1* と *MN2* は発呼用 IP アドレスの登録を更新するために、4 節で述べたように定期的に *HFA* Registration Request を対応する *HFA* に送信する。

次に、*MN1* が通信中に *HFAc* の下に移動したと想定する。*MN1* は *HFAc* からの Agent Advertisement により移動を検知し、*HFAc* 経由で、Registration Request を対応する *HA* である *HA1* に送信する。*MN1* は *HFAa* により割り当てられた発呼用 IP アドレス *Ga* を持っているため、*HFAa* に対しても Registration Request を送信する。これにより *HA1* および *HFAa* におけるホームアドレスと気付けアドレス (CoAc とする) の対応付けが変更される。

その後、*MN2* から転送されるセッションデータは *Ga* に対応する *HA* である *HFAa* により取り込まれ、移動先の *HFAc* までカプセル化され、最終的に *MN1* に配送される。

最後に *MN1* が通信の終了を判断すると、SIP の BYE メッセージを送信し、*MN2* からそれに対する 200 OK レスポンスが転送された時点でセッションが終了する。その後、*MN1* および *MN2* はこのセッションに利用したグローバル IP アドレスを解放する。

MN1 は現在 *HFAc* の下に移動しているため、*HFAc* 経由で *HFAa* に対して Lifetime を 0 に設定した Registration Request を送信し、ホームアドレス *Ga* に対する移動登録を抹消する。この時点で *HFAa* は *Ga* の利用者が存在しなくなったため、*Ga* の割り当てを解放する。

一方 *MN2* は、発呼用 IP アドレス *Gb* を割り当てた *HFA* のネットワークに存在するため、Lifetime を 0 に設定した *HFA* Registration Request を *HFAb* に送信する。これにより、*HFAb* は *Gb* の利用者が存在しなくなったため、*Gb* の割り当てを解放する。

6. おわりに

本稿では、動的に発呼アドレスを割り当てるモバイル IP 通信方式を用いた、*HA* 単位のプライベート IP アドレススペースのモバイル IP ネットワークにおける経路最適化ピアツーピア通信の実現方式について述べた。この方式により、*MN* のホームアドレスを、*HA* ごとに独立にプライベート IP アドレスを用いて割り当てることが可能となり、Mobile IPv4 におけるホームアドレスの不足の問題を解決できるとともに、*MN* 間のピアツーピア通信において、*MN* が移動している *FA* (*HFA*) を直接結ぶ経路を用いた通信を実現することが可能となった。

参考文献

- [1]: C. Perkins, Ed., "IP Mobility Support for IPv4," RFC 3344, Aug. 2002.
- [2]: 3rd Generation Partnership Project 2, "Wireless IP Architecture Based on IETF Protocols," 3GPP2 P.R0001, Jul. 2000.
- [3]: G. Montenegro, Ed., "Reverse Tunneling for Mobile IP," RFC 3024, Jan. 2001.
- [4]: K. Egevang, et al., "The IP Network Address Translator (NAT)," RFC 1631, May 1994.
- [5]: J. Rosenberg, et al., "SIP: Session Initiation Protocol," RFC 3261, Jun. 2002.
- [6]: 加藤他, "プライベート IP アドレスによるモバイル IP と SIP を用いたピアツーピア通信手法," 情処第 66 回全大 発表予定, Mar. 2004.
- [7]: 原他, "発呼トラヒックに対する HA 機能を FA に持たせるモバイル IP プロトコル," 情処 研究報告, 2003-MBL-25, Jul. 2003.
- [8]: 加藤他, "MN からの発呼トラヒックに対する HA 機能を FA に持たせる Mobile IP 通信方式," 信学論 D 掲載予定, May 2004.