

SIP との協調により経路最適化ピアツーピア通信を実現する Mobile IPv6 通信方式の提案

村井 信彰 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

モバイルネットワークの基本プロトコルとして、IPv6 アドレスに対応するとともに、経路最適化などの考慮がなされた Mobile IPv6 が注目されている。しかし Mobile IPv6 の経路最適化では通信開始時の制御メッセージ転送がオーバーヘッドとなっており、特に移動端末同士が通信するピアツーピア通信ではその問題が顕著になる。そこで本稿では、ピアツーピア通信のセッションを管理する SIP と協調し、移動先で入手する気付アドレスをホームアドレスとして用いて通信を行うことで経路最適化ピアツーピア通信を実現する Mobile IPv6 通信方式を提案する。

Proposal of Mobile IPv6 Scheme Allowing Route Optimized Peer to Peer Communication in Cooperation with SIP

Nobuaki Murai Toshihiko Kato Shuichi Itoh

Graduate School of Information Systems, University of Electro-Communications

Recently, Mobile IPv6 that uses IPv6 addresses and supports the route optimization inherently is considered as one of the basic protocols for mobile networks. However, the route optimization of Mobile IPv6 introduces a large overhead of forwarding control messages. The problem becomes serious in the peer to peer communication in which mobile nodes communicate with each other. To solve such a problem, this paper proposes a new Mobile IPv6 scheme that realizes route optimized peer to peer communication in cooperation with SIP. In this scheme, MN uses the care-of address given in the foreign network as the home address, and SIP uses the care-of address as an IP address to start communication with.

1. はじめに

モバイルネットワークの普及に伴い、Mobile IP がその基本プロトコルとして注目されている。IETF では、IPv6 アドレスに対応するとともに、経路最適化やインGRESSフィルタリングを行うバックボーンルータへの対処などを考慮した Mobile IPv6 を標準化している[1]。

Mobile IPv6 により経路最適化通信を行うためには、モバイルノード(MN) は通信開始時に通信相手(CN: Correspondent Node)に対して Return Routability 手順を実行してセッション鍵を生成し、その上で気付アドレスとホームアドレスの対応を登録する必要がある。

これに対して筆者らは、MN が発呼を行う際に気付アドレス (CoA) をソースアドレスとして使用し、さらにそのアドレスに対してはアクセスルータをホームエージェント (HA) として動作させる Mobile IPv6 通信方式を提案している[2]。この方式では、MN が通信を

開始したアクセスルータの下にある限りは Mobile IP の手順を用いず発呼して通信を開始することが可能で、MN が移動した場合には移動元のアクセスルータが HA として動作し、移動先へのパケットの転送を行う。しかしこの方法では、MN が着呼して通信する場合は、パケットの送信先アドレスが MN のホームアドレス (HoA)宛に送信されるために、本来の HA を介して MN に届くことになる。よってこの方式は、MN 同士が通信するピアツーピア通信においては、経路が冗長となってしまう。

一方、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) [3]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。したがって通常の Mobile IPv6 を用いた場合は、SIP によるシグナリングの後で、

双方の MN が Return Routability 手順と登録を行う必要がある。これに対し、先の提案方式を SIP と組み合わせることにより、着呼でも MN の CoA を用いて通信が可能になり、制御メッセージの数を減少させることができると考えられる。

本稿では、先に提案した Mobile IPv6 通信方式を SIP と協調させ動作させることで、MN 同士のピアツーピア通信の経路の最適化を効率的に実現する方式を提案する。本稿の構成は以下の通りである。まず第 2 章で、Mobile IPv6 ネットワーク上で SIP を用いたピアツーピア通信を行う手順を示す。次に第 3 章で、筆者らが先に提案した気付アドレスに対する可動性を提供する Mobile IPv6 通信方式について概説する。そして第 4 章で、SIP と協調し経路最適化ピアツーピア通信を実現する Mobile IPv6 通信方式を示す。

2. Mobile IPv6 と SIP を用いたピアツーピア通信

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 を用いて認識される。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、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。このプロキシサーバでの転送の際にレジストラに登録され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、この内 OK レスポンスが、通信相手がセッションを受け入れたことを示し、その OK に対する ACK がセッション開始側から送られ、セッションが確立する。INVITE リクエストおよび OK レスポンスは、Contact フィールドに端末の IP アドレスを含むことが可能で、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、プロキシを経由することなく端末間で直接転送することが可能となる。

Mobile IPv6 ネットワーク上で SIP を用い、移動端末同士がピアツーピア通信を行う手順を考える。それぞれ HA1 と HA2 に属する移動端末 MN1 と MN2 が、外部のネットワークに移動した状況で、MN1 が MN2 に対してピアツーピア通信を行う場合の通信のシーケンスを図 1 に示す。なおこの例では、HA ごとに SIP ドメインを導入し、SIP のプロキシサーバと HA は同一システム内に実現されている状況を想定する。

まず MN1 と MN2 の両者が自身の HA に Binding Update を送信して、移動先での気付アドレス（それぞれ CoA1, CoA2）と自身のホームアドレス（それぞれ HoA1, HoA2）の対応をバインディングキャッシュに登録し、Binding Acknowledgment を得る。

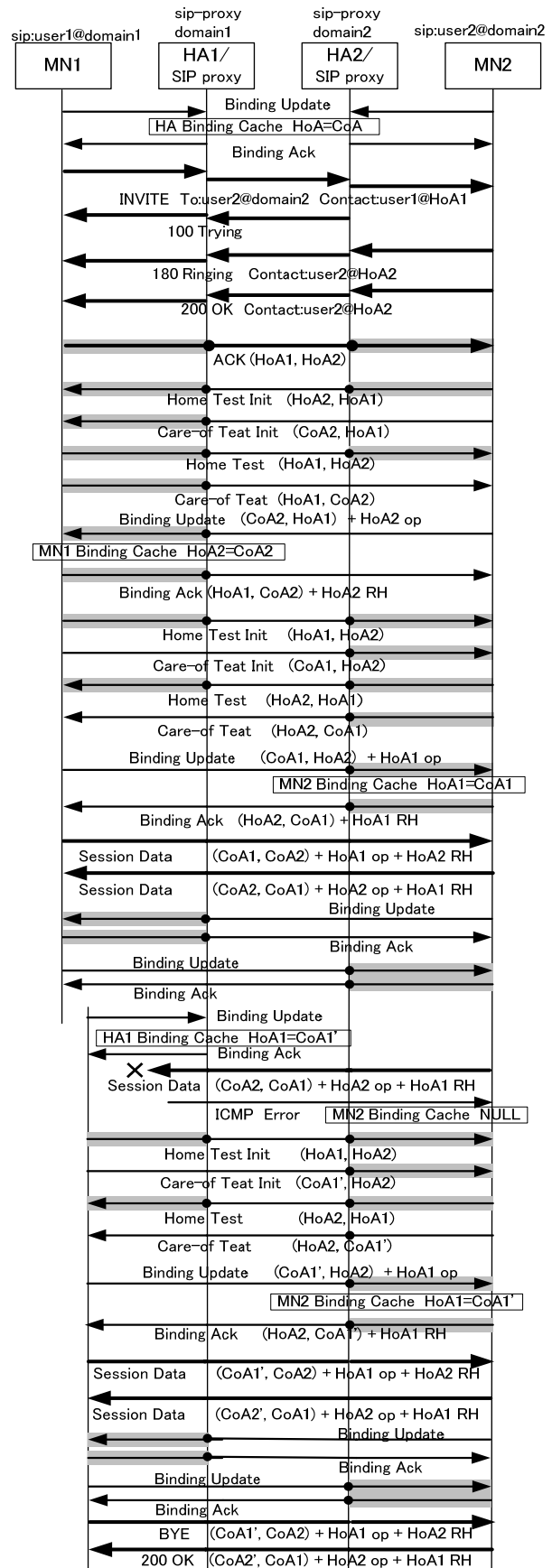


図 1 通信シーケンス例

次に、MN1 は MN2 とのセッションを確立するために、SIP の INVITE リクエストを SIP プロキシを兼ねる HA1 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>”, 受信者が発信者と直接通信するアドレスを示す Contact フィールド“Contact:<Sip:user1@HoA1>”が含まれる。このメッセージは、HA1 内のプロキシサーバが宛先ドメインのプロキシサーバを選定することで、HA2 に転送される。HA2 内のプロキシサーバは To フィールドの SIP URI から対応する IP アドレス HoA2 を検索し、HA2 がバインディングキャッシュエントリを参照することで HoA2 に対応する気付アドレス CoA2 宛てにメッセージを転送する。HoA2 はタイプ 2 ルーチングヘッダを用いて指定される。

MN2 はこの INVITE リクエストを受信すると、ユーザの呼び出し中に 180 Ringing レスポンスを、ユーザが応答すると 200 OK レスポンスをそれぞれ返送する。これらは Contact フィールド “Contact:<Sip:user2@HoA2>”を含み、リクエストが経由してきた2つの SIP プロキシを辿って MN1 まで到達する。

200 OK レスポンスを受け取った MN1 は、それに従ってセッションを確立するために、Contact フィールドから得たアドレス HoA2 宛てに ACK を返す。この ACK は、MN1 が自身の気付アドレスを登録した相手宛ではないため、Mobile IPv6 の動作に従い、双方向トンネリングで送信されることになる。すなわち、MN1 のホームアドレス HoA1 を送信元、MN2 のホームアドレス HoA2 を宛先とするパケットを、MN1 の気付アドレス CoA1 を送信元、HA1 のアドレスを宛先とするヘッダで IP カプセル化した形で MN1 から送信される。

パケットは HA1 でカプセル化を解除されて HoA2 宛てに転送されるが、HA2 がプロキシ・ネイバディスカバリを用いてこれを横取りし、カプセル化して CoA2 宛てに転送する。

MN2 は ACK を通達したパケットがカプセル化されており、かつカプセル内外のアドレスの整合が取れていることから、このパケットの受信に応じて HoA1 に対して Return Routability 手順を開始する。MN2 はまず、送信元 CoA2/宛先:HoA1 の Care-of Test Init と、送信元:HoA2/宛先:HoA1 の Home Test Init を送信する。Care-of Test Init は直接 HoA 1 に、また Home Test Init は HA2 を介して HoA1 に送られる。これらは HA1 にプロキシ・ネイバディスカバリを用いて横取りされ、MN1 にカプセル化して転送される。MN1 は2つの Init メッセージに応じて MN2 宛てに直接 Care-of Test, HA2 を介して Home Test を送信する(MN1→HA1 間はカプセル化され、送信元は HoA1 となる)。以上により Return Routability 手順は完成し、MN2 は両テストメッセージに含まれる鍵情報からバインディング鍵を形成する。

MN2 はこのバインディング鍵による署名を添えて HoA1 宛てに Binding Update を送信する。このメッセ

ージの送信元は CoA2 となり、ホームアドレスオプションヘッダに HoA2 が格納される。メッセージは HA1 によりカプセル化され MN1 に転送され、MN1 は MN2 のバインディングキャッシュエントリを作成した後、Binding Update に応えて、タイプ 2 ルーチングヘッダに HoA2 を格納する Binding Acknowledgment を返す。

MN1 は受信した Binding Update がカプセル化されており、かつカプセル内外の送信元、宛先アドレスの整合が取れていることから、Return Routability 手順を開始する。このとき、受信したメッセージにホームアドレスオプションが用いられていることから、Return Routability 手順は送信元である CoA2 ではなく、ホームアドレスオプションに格納されているアドレス HoA2 に対して実行される。以降は先ほどまでの手順が逆方向に繰り返され、双方が互いのバインディングキャッシュエントリを得ることになる。

この結果両端末間で、ホームアドレスオプションに自身のホームアドレス、タイプ 2 ルーチングヘッダに相手のホームアドレスを格納することで、送信元を自身の気付アドレス、宛先を相手の気付アドレスとするパケットを直接送信できるようになり、セッションデータを相手端末に直接、最適経路でやり取りできるようになる。

この通信中に MN1 が他のリンクに移動したとする。MN1 は新たな移動先での気付アドレス CoA1' を生成、HA1 に Binding Update を送信して CoA1' を登録し、Binding Acknowledgment を受け取る。次に、MN1 は自身の Binding Update リストにあるノードのために Return Routability 手順を開始する。その結果、MN2 の保持する MN1 に関するバインディングキャッシュエントリも CoA1' で上書きされることになり、経路最適化通信が再開される。

なお、登録が完了しない間に MN2 から MN1 へのデータ送信があると、MN2 は継続的な ICMP 宛先到達不能メッセージを受け取り MN1 に関するバインディングキャッシュエントリを削除して双方向トンネリングによる送信に切り替える場合がある。この場合も登録が完了し次第、経路最適化通信に戻る。

最後に、通信の終了が判断されると、一方から BYE リクエストが送られ、それに答えて他方が 200 OK レスポンスを返し、SIP のセッションが開放される。

3. CoA に対する可動性を提供する Mobile IPv6

次に、筆者らが提案した気付アドレスに対する可動性を提供する Mobile IPv6 通信方式について概説する。

図2に示すようなネットワーク構成を想定する。MN が移動先のネットワークで通信を始める場合、そのネットワークのアクセッスルータ(AR)に対して、MN をそのネットワークに存在する端末として登録する。また MN が通信中に移動した場合は、この AR が MN のホームエージェントとして移動管理を行う。このような HA

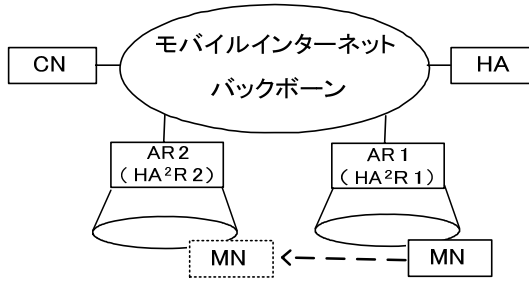


図2 ネットワーク構成

機能をもつARをHA²Rと呼ぶ。通信シーケンスの例を図3に示す。

本方式は、大規模携帯電話ネットワークのように、HA、アクセスルータ、無線基地局などを1つの管理主体が管理運用するネットワークを想定している。このため、MNの認証においては、HA²RとHAは互いに秘密鍵を有するが、MNとHA²Rは事前に認証情報を持たない。よって、MNは通信を開始する時点で、HA²Rに対してMNの認証を要求する必要がある。この要求とHA²Rへの登録を同時に行うために用いるメッセージをMN Authentication Requestと呼称する。MN Authentication RequestはBinding Updateに類似した形式の、新たなType値を持つモビリティヘッダを用いたメッセージになっており、モビリティオプションに気付アドレス、HAのアドレス、認証情報などの情報を格納する。

MN Authentication RequestはまずMNからHA²Rに送信され、受信したHA²RはLifetime、Sequence #等を記録した後、HA²R-HA間の認証情報をIPsecの認証ヘッダを用いて付加し、HAへ転送する。

MN Authentication Requestを受信したHAは、MNとHA²Rを認証し、HAとHA²Rのための一時的な秘密鍵をMN Authentication Replyにより配送する。MN Authentication ReplyもBinding Acknowledgmentに類似した形式の、新たなType値を持つモビリティヘッダを用いたメッセージになっており、モビリティオプションに気付アドレス、HAのアドレス、認証情報などの情報を格納する。こうしてMNとHA²Rが互いに認証できるようになる。

認証終了後、MNは気付アドレスをソースアドレスとして用いて通信を開始する。その際、HA²RがHAとして動作するため、MNは通常のBinding Updateを用いて有効期限の更新を行う。

MNがこの通信中に他のネットワークに移動した場合は、新たな気付アドレスを生成し、HAと、ソースアドレスとして使用していた元の気付アドレスを割り当てたHA²Rの双方に対して、Binding Updateを送信し移動を登録する。その場合HA²Rに対してはMN Authentication Replyで割り当てられた秘密鍵を用いてメッセージを暗号化する。この状態でCNからMNへの送信が起こると、パケットは元の気付アドレス宛に送られてくるが、HA²Rがプロキシ近隣探索を用いてそれ

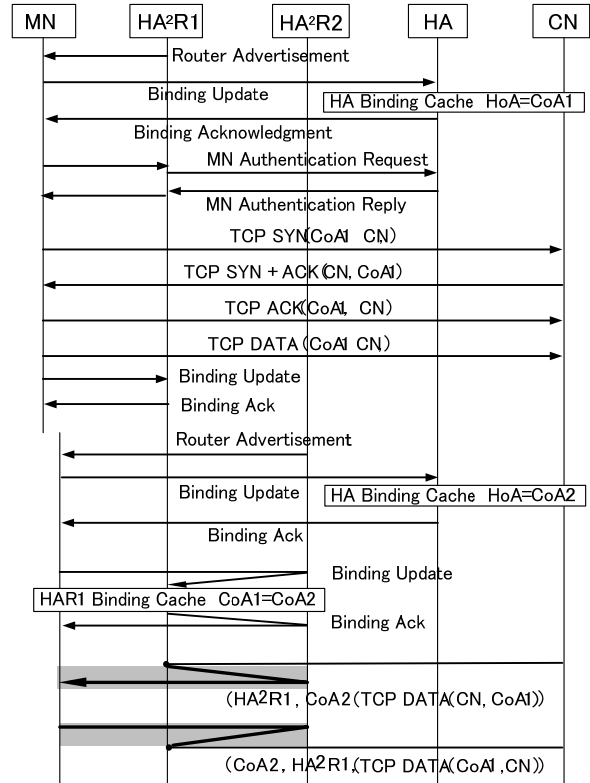


図3 通信シーケンス例

を横取りし、MNにカプセル化して転送する。また、MNからCNへも、HA²Rを介してカプセル化することで、ソースアドレスを移動前の気付アドレスのまま送信することができる。このようにして、移動後も通信を継続することが可能となる。

MNが通信を終了し、HA²Rに対してBinding Updateによる登録の更新を行わなくなると、HA²RはMNに対応するバインディングキャッシュを開放し、MN-HA²R間の秘密鍵は使用されなくなる。

4. SIP と組み合わせたピアツーピア通信方式

3章で述べた方式をSIPと協調して用いることにより、モバイル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効率的に実現することができる。

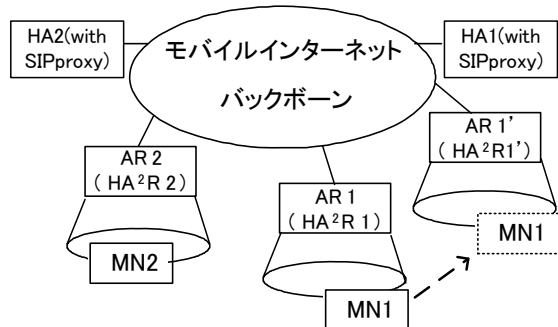


図4 ネットワーク構成

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HA²R1とHA²R2の下に移動した状態で、MN1がMN2に対して通信を開始し、その通信中にMN1がHA²R1からHA²R1'に移動した場合を想定する。この通信シーケンス例を図5に示す。なおこの例でも2章と同様、HAごとにSIPドメインを導入し、SIPのプロキシサーバはHA内に実現している状況を想定する。

まずMN1、MN2の両者が自身のHAにBinding Updateを送信して、移動先での気付アドレス（それぞれCoA1、CoA2）と自身のホームアドレス（それぞれHoA1、HoA2）の対応をバインディングキャッシュに登録し、Binding Acknowledgmentを得る。

次に、MN1、MN2はそれぞれの移動先のHA²R1、HA²R2に認証を要求するMN Authentication Requestを送信する。メッセージはそれぞれのHAに転送され、HAによりMN-HA²R間の秘密鍵が生成され、MN Authentication Replyにより両者に配送されると同時に、MNがHA²Rのネットワーク下の端末であることの登録がなされる。またMN1とMN2はSIPのレジストラに、現在の気付アドレスであるCoA1とCoA2をそれぞれ登録するものとする。

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プロキシを兼ねるHA1に送信する。この際、リクエストのToフィールドは“To:<Sip:user2@domain2>”，またContactフィールドは“Contact:<Sip:user1@CoA1>”となる。

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SIPURIから、対応するMNのホームアドレスを検索し、INVITEリクエストをMN2に転送する。

MN2はユーザの呼び出し中に180 Ringingレスポンス、ユーザが応答すると200 OKレスポンスを返送する。MN2もまた、HA²R2による認証が完了し発呼に気付アドレスを用いるようになっていたため、レスポンスのContactフィールドは“Contact:<Sip:user2@CoA2>”となり、リクエストが経由してきた2つのSIPプロキシを辿ってMN1まで到達する。200 OKレスポンスを受け取ったMN1が、それに応じてACKを返すことでセッションが確立される。

以降は、HAによるフォワーディングなどを必要としない適切な経路で、互いの気付アドレス宛にMN間で直接セッションデータがやりとりされる。通信中においては、通常のBinding Updateを用い、登録の有効期限が更新される。

この通信中に、MN1がHA²R1'に移動したと想定する。MN1は移動を検出し、あらたな気付アドレスCoA1'を得ると、Binding Updateを送信し、HA1とHA²R1に登録する。

その後、MN2からのセッションデータはCoA1宛てに送信されてくるが、HA²R1がこれをプロキシ・ネイ

バディスカバリで捕らえ、CoA1'宛てにカプセル化され、MN1に到達する。また、MN1から送られるセッションデータも、ソースアドレスはCoA1のままHA²R1宛てのパケットでカプセル化されてMN1から送信され、HA²R1によりカプセル化を解除され転送されてMN2に到達する。このようにして、SIPのセッションを保ったままの端末の移動が実現する。なお、この移動後の経路は完全に最適な経路ではないが、HA²R1とHA²R1'は一般的に隣り合うアクセスルータであるため、経路の冗長さの影響は最低限に抑えられると考えられる。

最後に、通信の終了が判断されると、一方からBYEリクエストが送られ、それに答えて他方が200 OKレスポンスを返し、SIPのセッションが開放される。

5. おわりに

本稿では、Mobile IPv6ネットワーク上で、MN同士が効率的に最適な経路でピアツーピア通信を行う方式を提案した。具体的には、発呼の際にはMNが移動した際に入手する気付アドレスを用いて通信し、その通信中の移動には、気付アドレスを割り当てたアクセスルータにHA機能を実現することで対応するというMobile IPv6の通信方式を、ピアツーピア通信のセッションを管理するSIPと協調させて動作させている。これにより、通常のMobile IPv6通信においてSIPを用いた場合に比べ、セッション開始時に必要なメッセージ交換を削減し、通信中に移動してもセッションデータの送受信をスムーズに再開する方法を実現した。本方式により、モバイルネットワークにおいて移動端末同士が効率的にピアツーピア通信を行うことが可能になると考えられる。

文 献

- [1] D. Johnson, et al., “Mobility Support in IPv6,” RFC 3775, Jun. 2004.
- [2] 加藤他, “気付アドレスに対する可動性を提供する Mobile IPv6 通信方式の設計,” 信学技報, NS2005-69, July. 2005.
- [3] J. Rosenberg, et al., “SIP: Session Initiation Protocol,” RFC 3261, Jun. 2002.

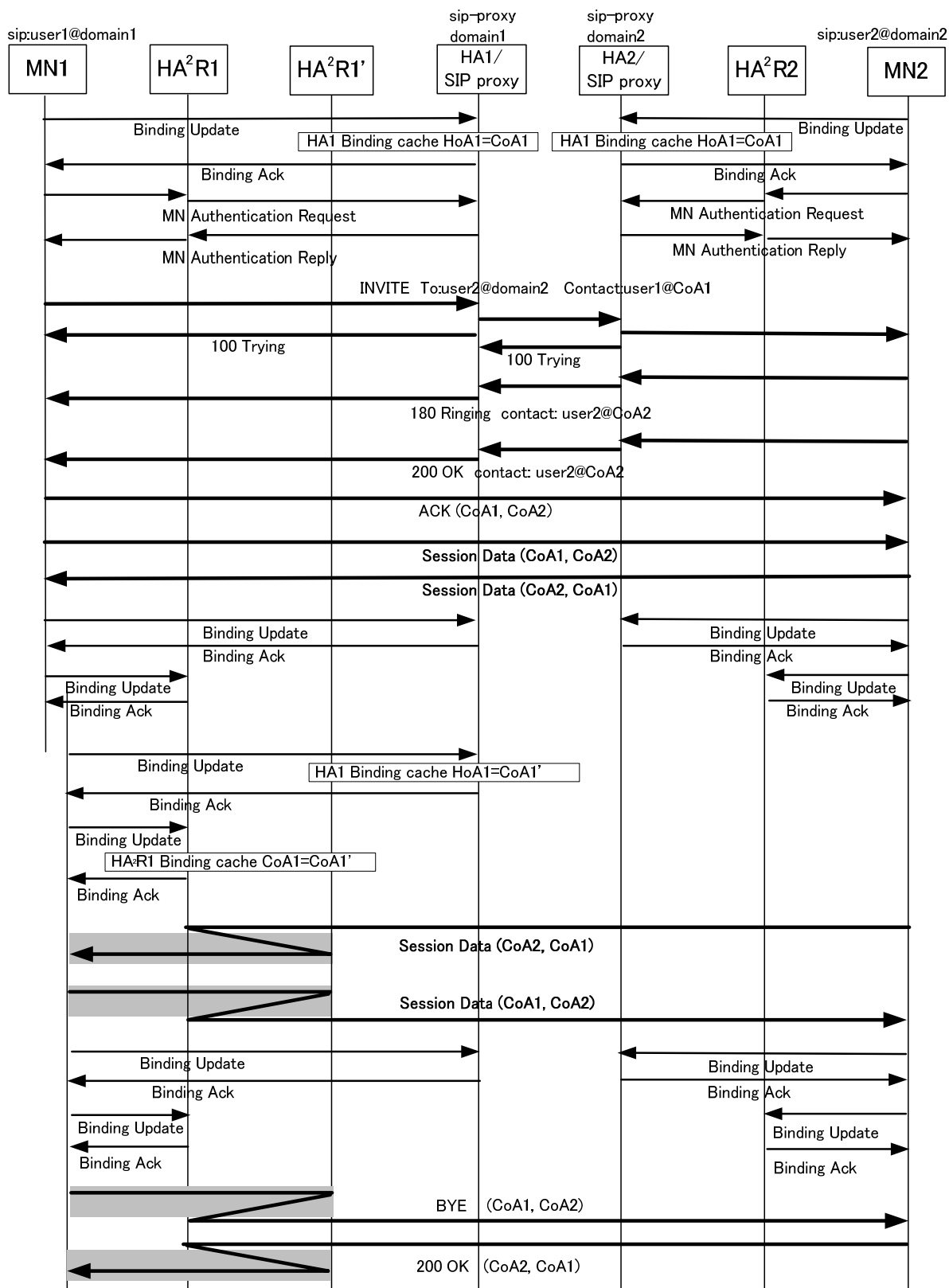


図5 通信シーケンス例