

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

原 正寛 加藤 聰彦 伊藤 秀一

携帯電話などを用いた大規模なモバイルインターネットの基本プロトコルとして、モバイル IP プロトコルが採用されつつある。ここでは、無線リンクを介して MN を収容する機能は FA により実現され、HA はモバイルインターネットバックボーンの中で、MN の移動管理のみを行う構成になっている。このため大規模なモバイルインターネットにおいては、MN へのトラヒックを FA であてにフォワーディングするという HA でのフォワーディング処理のオーバーヘッドが大きな課題になると考えられる。本稿では、この問題を解決するために、MN が移動先で発呼する場合は、移動先の FA に IP アドレスの割り当てを要求し、さらにアドレスを割り当てられている間はその FA がホームエージェントの機能を果たす Mobile IP プロトコルを提案する。さらにそれによる HA のフォワーディング負荷の軽減についての評価結果を示す。

Mobile IP Protocol using FA Providing HA Functionality for MN-Initiated Traffic

Masahiro Hara, Toshihiko Kato and Shuichi Itoh

Mobile IP is being widely used as the fundamental protocol of mobile internet. In mobile internet, MN communicates through one of FAs which provides wireless communication, and therefore, IP datagrams destined to MN are always forwarded by its HA. So the overhead of forwarding in HA is a serious problem in large scale mobile internet. In this paper, we propose a new Mobile IP protocol in which FA works as HA for MN initiating a call. That is, the FA called HFA assigns an IP address to the MN and forwards IP datagrams to the assigned IP addresses when the MN has moved to another network while communicating using the IP address. While the MN keeps communication under the HFA, no forwarding overhead is required for HA and HFA. This paper describes the detailed design and the results of evaluation of our approach.

1. はじめに

携帯電話などを用いた大規模なモバイルインターネットの基本プロトコルとして、モバイ

電気通信大学 大学院 情報システム学研究所
University of Electro-Communications

ル IP プロトコル[1]が採用されつつある[2]。モバイル IP では、他のネットワークに移動した移動端末(MN: Mobile Node)は、移動先の FA (Foreign Agent)を介して自身の HA (Home Agent)に移動登録を行う。その移動情報に基づ

いて、MN へのトラフィックは、HA から FA に対して IP トンネリングを用いてフォワーディングされる。実際のモバイルインターネットにおいては、無線リンクを介して MN を収容する機能は FA により実現され、HA はモバイルインターネットバックボーンの中で、MN の移動管理のみを行う構成になっている[2]。このため MN は常にいずれかの FA に所属することとなり、通常のモバイル IP で想定されているような、ホームネットワークに接続されている状況は発生しない。すなわち、MN へのトラフィックは常に HA により移動先の FA にフォワーディングされることになる。また、実際のモバイルインターネットでは、ユーザ管理を容易にするために HA を広く分散させないと考えられる。すなわち、HA の数は、FA や加入する MN の数に比べると少ないと予想される。

このため、大規模なモバイルインターネットにおいては、MN へのトラフィックを FA へにフォワーディングするという HA でのフォワーディング処理のオーバーヘッドが大きな課題になると考えられる。

このような問題を解決するために、Mobile IP では、MN とそれがアクセスするノード (CN: Correspondent Node) との間で、ホームネットワークを介さずに直接データをやり取りする経路最適化手順[3]が定められている。特に Mobile IPv6 ではこの手順が必須とされている。しかし、現在広く用いられている Mobile IPv4 では、経路最適化を行うために一般のサーバプログラムに追加の手順を実装する必要があり、広く利用されるには至っていない。

そもそも Mobile IP が保証する IP アドレスの可動性は、MN が着呼する場合にのみ必須である。すなわち MN が新たに着呼する場合はホームアドレスを用いて、HA 経由で移動先に転送させる必要がある。一方、MN が新たに発呼する場合は、端末がその時点で所属するネットワークのアドレスを動的にもらえば十分である。移動先で与えられたアドレスを MN のホームアドレスとして使用するというアプロー

チは、IETF の Homeless Mobile IP [4]で検討されている。これは HA を用いずにそのつど割り当てられた気付けアドレスをその端末のアドレスとして使おうとするものである。しかしこの方法では、通信中にネットワークを移動した場合は、TCP コネクションの通信中に IP アドレスが変更されることに対応する必要があり、現実的でない。

そこで筆者らは、移動先のネットワークで MN が発呼する際には、そのネットワークにおいて一時的なホームアドレスを割り当て、さらにその通信中は、そのネットワークをホームネットワークとするという方法を提案している[5,6]。本稿ではその詳細設計と、HA によるフォワーディングオーバーヘッドを尺度とした評価結果について示す。以下、第 2 章では、提案する方式の設計方針を、3 章ではプロトコルの詳細設計を示す。さらに 4 章では提案する方式の評価を行い、5 章で結論を述べる。

2. 設計方針

プロトコルの設計にあたり、以下の方針を立てた。

- (1) 携帯電話などを用いた大規模なモバイルインターネットを想定する。前述のように、HA の数は MN や FA に比べると少ない。例えば、ネットワークの規模として、HA は 100 台、FA は 1 万台、MN が 1 千万台のオーダーのもの

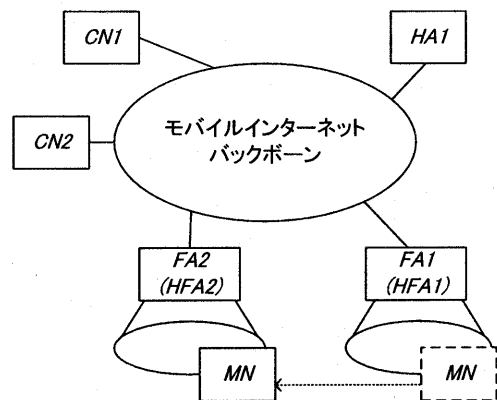


図1 ネットワーク構成

を想定する。また図1に示すように、MNの移動先のネットワークには、無線インタフェースを介して通信するFAのみが存在し、HAはモバイルバックボーンの中の要素として用意されている。

(2) MNが移動先のネットワークにおいて通信を始める場合、そのネットワークのFAに対して、発呼用のIPアドレスを要求し、そのMNをそのネットワークに属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FA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機能を持つFAを、Home FA (HFA)と呼ぶ。図1に示すように、各ネットワークのすべてのFAはHFA機能を有するものとする。

(3) モバイルインターネットにおいては、MNの管理をHAが行い、またFAとHAは相互に認証しあうのが通常であると考えられる。逆にいうと、FAがMNに対する認証を行うことは想定できない。すなわち、MNが移動先ネットワークのHFAに登録しIPアドレスを入手しようとした場合、HFAがそのMNを認証するための共通秘密鍵を事前に持っていることは想定できない。このため、HFAがMNを認証するために、MNとHFAの間で一時的な共通秘密鍵を用意することとする。この秘密鍵の割り当ては、そのMNを管理するHAを経由して行う。HAに一時的なMN-HFA共通秘密鍵を要求する処理を行うメッセージをHFA Registration Requestと呼び、これによりHFAでのMNの登録、発呼用IPアドレス要求割り当て、秘密鍵の割り当てを行う。HFAは、MNが発呼用IPアドレスを用いて通信する間、そのMNの登録を保持する。

(4) MNが発呼用IPアドレスを割り当てたHFAのネットワークにおいて通信を行う間は、ホームネットワークに存在することになり、HAおよびHFAによるフォワーディングは行われなない。ただし、HFAがMNの登録情報を維持するため、HFA Registration Requestを定期的に発行する手順を追加する。

(5) MNが発呼用IPアドレスを用いて通信を行っている間に他のネットワークへ移動した場合は、本来のHAと、発呼用IPアドレスを割り当てたHFAに対しても登録を行う。これらの登録はRegistration Request、Registration Replyを用いて行う。

3. プロトコルの詳細設計

本プロトコルを用いるネットワークにおいては、前述のようにMHに対応するHAが管理し、HAとHFAとは互いに認証しあうことを前提とする。すなわち、MNと対応するHAとの間でMH-HA共通秘密鍵を有し、さらにすべてのHAとHFAは、各ペアに対してHFA-HA共通秘密鍵を有する。

ホームエージェントHAに属する移動端末MNが、HFAのHFA1のネットワークに移動し通信相手(CN: Correspondent Node)CNIに対して発呼を行い、その通信中にHFA2のネットワークに移動した場合を想定する。ただしここでのCN固定ホストを想定する。その通信シーケンスを図2に示す。

まずMNがHFA1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、HFA1を介してHAへRegistration Requestを送信し、そのReplyを受け取る。

次にMNがCNIに対してTCPによる通信を行おうとしたとする。これはMNが発呼する通信であるため、前述のようにHFA1あてにHFA Registration Requestを送信する。このメッセージのフォーマットを図3に示す。このメッセージは通常のRegistration Requestと同様の形式を有し、Typeの値を17とし、先頭のフラグとしてRフラグのみが設定されている。Rフラグが1にセットされると、このメッセージが新たな登録を要求していることを示す。Home AddressにはMNのももとのホームアドレス(以下HoAとする)が、Home AgentにはHAのアドレスが、Care-of AddressはHFA1によりAgent Advertisementで通知された気付けアド

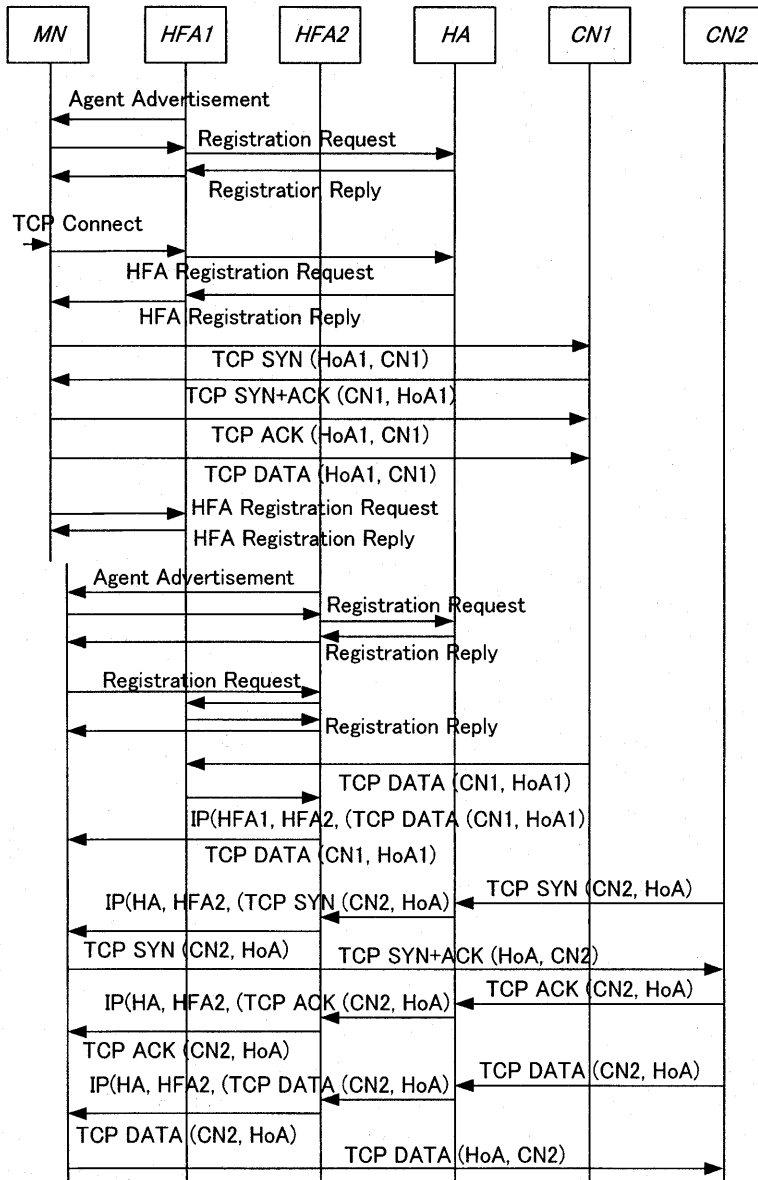


図 2 シーケンス例

レスが、それぞれ設定される。さらに、Type の値が 32 である Mobile-Home Authentication Extension が含まれる。

HFA1 はこのメッセージを受信すると、MN に対するレジスタリストに、HFA Registration

Request を受信したことで、要求された Lifetime、Identification などを記録する。

続いて HFA1 は HA に対して HFA Registration Request を送信する。そのフォーマットを図 4 に示す。MN からのメッセージとの相違点は、

Foreign-Home Authentication Extension が付加されたことのみである。

HA はこのメッセージを受信すると、MN と HFAI の認証を行った後、両者のための共通秘密鍵 (MN-HFA Shared Key) を生成する。ここで、HA は鍵の情報を生成するのみで、その後の管理は一切行わない。

次に HA は HFAI に対して HFA Registration Reply を返す。そのフォーマットを図 5 に示す。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。これらはそれぞれ、MN Key Extension と HFA Key Extension と呼び、64 と 66 の Type を割り当てている。

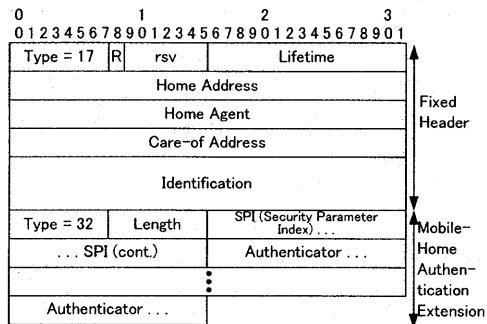


図 3 MN から HFA への HFA Registration Request のフォーマット

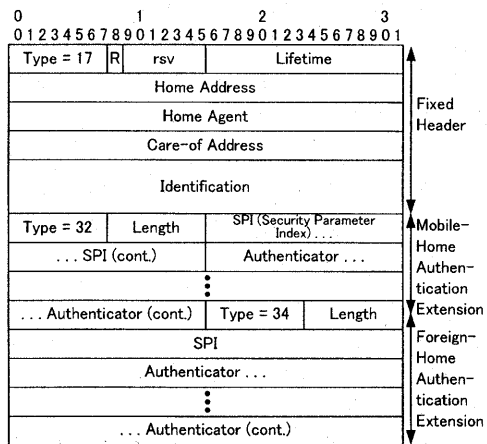


図 4 HFA から HA への HFA Registration Request のフォーマット

これらの 2 つの情報を含むことにより、HFAI 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。また HFA

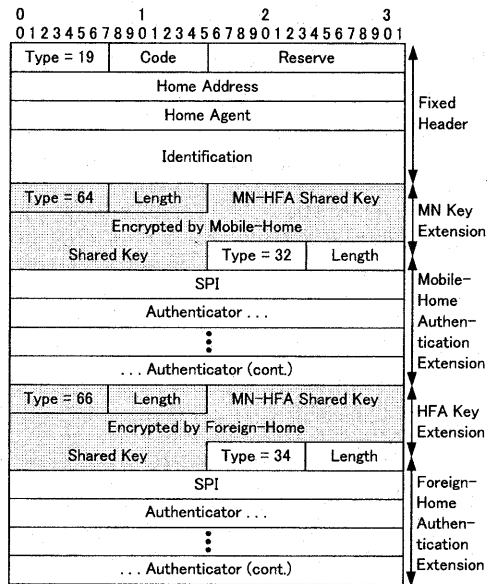


図 5 HA から HFAI への HFA Registration Reply のフォーマット

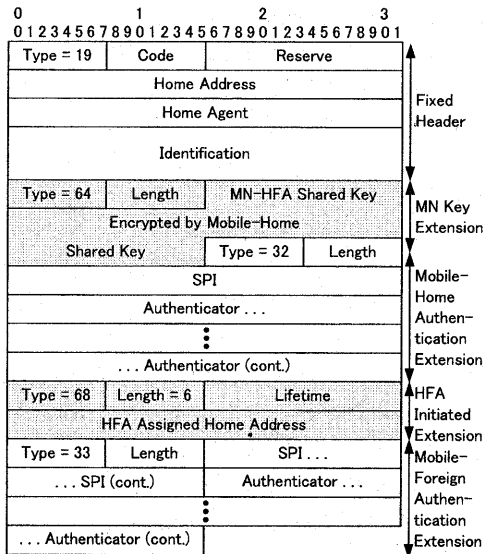


図 6 HFAI から MN への HFA Registration Reply のフォーマット

へ転送する鍵情報は *HFA1* おいてメッセージから取り除くため、*MN* を認証する Mobile-Home Authentication Extension の外側に置かれる。なお、Lifetime に相当するフィールドは予約フィールドとなっている。これは、*HA* においては HFA Registration Request の生存時間については管理したいためである。

HFA1 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（以降 *HoA1* とする）、最終的な登録の生存時間を定める。この段階で *HFA1* は *MN* を自身のネットワークに属する端末であると解釈する。このためモビリティバインディングリストに、*MN* に対応するエントリを作成し、これらの情報を記録する。

この後 *HFA1* は *MN* に対して HFA Registration Reply を転送する。そのフォーマットを図 6 に示す。このメッセージでは、自身が付与した発呼用 IP アドレス、最終的に決定された生存時間を HFA Initiated Extension (Type は 68 とした) に含んでいる。さらに、*HA* から与えられた *MN*-HFA 秘密鍵により生成した Mobile-Foreign Authentication Extension を追加する。

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 *HFA1* 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。

以上のような手順で得た発呼用 IP アドレス *HoA1* を用いて、*CN1* との間で TCP 通信を行う。その際 *HA* および *HFA1* は、前述のように *HA* のフォワーディング機能を提供する必要はない。ただし、*HFA1* に対して定期的に HFA Registration Request を送信する。この場合は図 3 のフォーマットにおいて、R フラグが 0 となり、Mobile-Home Authentication Extension の代わりに Mobile-Foreign Authentication Extension が挿入される。*HFA1* はそのような Request を受信すると、認証後、*MN* に対応するモビリティバインディングリストのエントリの生存時

間を更新し、HFA Registration Reply を返す。Reply メッセージは、Extension として、Mobile-Foreign Authentication Extension のみを含む。

その通信中に *MN* が *HFA2* のネットワークに移動すると、それを *HFA2* からの Agent Advertisement で検出する。すると、*HA* に対して通常の Registration Request を送信し、同時に、発呼用 IP アドレスを割り当てた *HFA1* へも Registration Request を送信する。このメッセージの認証情報は先に *HA* から与えられた *MN*-HFA 共通秘密鍵を用いて作成される。

HFA1 はこのメッセージを受信しその認証が完了すると、モビリティバインディングリストのエントリに新たな気付けアドレスなどの情報を追加し移動を管理する。ここで注意すべき点は、*MN* の移動により、ビジタリストからは、対応するエントリはなくなるが、*HoA1* を用いて引き続き通信を行っているため、モビリティバインディングリストにはエントリが存在し続ける。その結果、*CN1* からの IP パケットは、*HFA1* で取り込まれ、カプセル化されて *HFA2* へ転送され最終的に *MN* に送られる。

MN が通信を終了して、*HFA1* に対して Registration Request による登録を行わなくなると、*HFA1* は *MN* に対応するモビリティバインディングリストを開放し、その IP アドレスおよび *MN*-HFA 共通秘密鍵は使用されなくなる。

また、その他の *CNCN2* が *MN* に対して通信を開始した場合は、*CN2* は *MN* のもとのホームアドレスである *HoA* を用いて IP パケットを送出する。この場合は、図 2 に示すように、*HA* を介して通常のモバイル IP の手順のように通信が行われる。

4. 性能評価

前節で述べた方式の評価を行うために、以下のような仮定を設ける。

- モバイルインターネットには、*HA* が 100 台、*HFA* が 10,000 台、*MN* が 10,000,000 台存在し、ネットワークに均等に分布して

いるとする。

- 各MNはCNとCkbpsの双方向の通信を、1日にT秒間行うとする。このとき、MNが通信を行っている確率は、 $T/(24 \times 3600)$ となる。以下では、数値例として、 $C=384\text{Kbps}$ 、 $T=10 \times 60$ 秒を用いる。
- MNの通信はMN→CNの方向はFA経由で直接行われるものとし、CN→MNの方向のデータ通信は、HAによるトンネリングが行われるものとする。

4. 1 HAでのフォワーディングオーバーヘッドの評価

従来のMobile IPではすべてのトラフィックがHAを経由する。HAでのトラフィックの処理量は以下ようになる。

$$\frac{C \times T \times \text{MNの台数}}{\text{HAの台数} \times 24 \times 3600} \\ = \frac{384 \times 10^3 \times 10 \times 60 \times 10^7}{100 \times 24 \times 3600} \\ \approx 3 \times 10^8 (\text{bps})$$

すなわち、HAあたりのフォワーディング速度は300Mbps程度となる。これは発生するトラフィックが24時間の内に均等に分布するとの仮定であるため、最煩時はその3倍程度とすると、約1Gbpsのフォワーディング処理が必要となる。HAの処理はIPカプセル化によるフォワーディング処理であるため、通常のIPフォワーディングのようにハードウェア化されているわけではなく、最大1Gbpsという負荷は大きいと考えることができる。

一方、本方式を適用すると、同様なネットワーク規模で以下ようになる。MNが行う通信の内、2/3がMNからの発呼で、残りの1/3が着呼であると仮定する。すると、提案する方式では、着呼した通信のみがHAを経由するため、HA経由のトラフィックは1/3となり、フォワーディングの処理量は、上記の条件で、平均的に100Mbps、最煩時で300Mbpsとなる。これにより、HAでの処理負荷が大きく提言したことになる。

また、残りのMNのトラフィックは、各MN

が所属するネットワークにおいてHFAから発呼アドレスを割り当てられて行われる。MNがそのネットワークに存在して通信を行う限り、HAにもHFAにも処理の負担をかけないことは前述のとおりである。MNがさらに別のネットワークに移動しながら通信を行った場合のみに、HFAでのフォワーディングのオーバーヘッドが生ずる。発呼したMNがその通信を続けながら移動する確率はそれほど大きくないと予想される。ここでその確率を1/10とすると、各HFAにおけるHAとしてのフォワーディング処理のオーバーヘッドは以下のとおりとなる。

$$\frac{\text{HAで扱わないトラフィック量} \times \text{HAの台数}}{\text{HFAの台数}}$$

× 移動した割合

$$= \frac{(3-1) \times 10^8 \times 100}{10000} \times 0.1 \\ = 2 \times 10^5 (\text{bps})$$

すなわち、HFAあたりの追加のフォワーディング処理は20Kbps程度となり、最煩時でもその3倍の60Kbpsで、十分小さい処理量であると考えられる。

以上のように、本方式では従来のMobile IPに比べてHAのフォワーディングのオーバーヘッドを大きく低減することができると考えられる。

4. 2 HFAで用意すべきアドレス数の評価

提案した方式では、HFAが、発呼するMNに対して、動的にIPアドレスを割り当てる。そのアドレスは、MNが通信を行っている間利用される。このため本方式の評価においては、各HFAで必要とするIPアドレスの量を推定することも重要である。1つのHFAで同時に用意すべきIPアドレスの数は以下ようになる。

$$\frac{\text{MNの数} \times \text{MNが発呼の通信を行う確率}}{\text{HFAの数}}$$

ここで、MNが発呼の通信を行う確率は、1つのMNが通信を行う確率は $T/(24 \times 3600)$ であり、さらに移動先で発呼する割合はその2/3であるため、必要なIPアドレスは以下ようになる。

$$\frac{10^7 \times \frac{2}{3} \times \frac{10 \times 60}{24 \times 3600}}{10^4} \approx 5$$

すなわち平均5つとなる。最煩時に3倍のトラヒックを想定しても15となり、これは現実的に十分少ない値である。また安全側をとって10倍のマージンをとるとしても、必要なIPアドレスの数は50から150であり、これも実現可能な値であるといえる。すなわち、本方式において移動先のHFAで必要なIPアドレスの数については、実現上問題ない範囲であると考えることができる。

5. おわりに

本稿では、大規模モバイルインターネットにおいて、HAによるIPカプセル化・フォワーディングの処理オーバーヘッドを提言することを目的として、発呼に対しては移動先のネットワークのHAからIPアドレスを入手しそのHAをホームとして通信を行うという方法を提案した。具体的には、移動先のネットワークにはFAのみが存在すると想定し、MNの発呼に対しては、FAがIPアドレスを動的に割り当て、さらにそのFAが移動した場合にHAとして動作させるという方法を用いている。MNが移動先のネットワークで移動せずに通信する限り、他のモバイルエージェントのフォワーディング処理なしに、通信が可能となりHAの負荷の低減が可能となる。またFAとMNの間で認証を行うために、FAがMNを認証するための秘密鍵を前もって有することなしで、MNのホームエージェントから一時的な秘密鍵を入手する手順を実現している。さらに、大規模なモバイルインターネットを想定した評価を行い、本方式が従来方式に比べて、HAのフォワーディング処理を減らすことができることを確認した。また、HFAがMNに割り当てべきIPアドレスの個数を評価し、現実的に実現できる範囲であることも示した。

参考文献

[1]: C. Perkins, Ed., "IP Mobility Support for

IPv4," RFC3220, Jan. 2002.

[2]: 3rd Generation Partnership Project 2, "Wireless IP Architecture Based on IETF Protocols," 3GPP2 P.R0001, Ver.1.0.0, Jul. 2000.

[3]: G. Montenegro, Ed., "Reverse Tunneling for Mobile IP," RFC 3024, Jan. 2001.

[4]: P. Nikander, et al., "Homeless Mobile IPv6," work in progress, available at <draft-nikander-mobileip-homelessv6-01.txt>, Feb. 2001.

[5]: 加藤, 伊藤, "発着呼の区別により動的にHAを選択する Mobile IP 手順に関する検討," FIT2002, M-28, Sep. 2002.

[6]: 原, 加藤, 伊藤, "発呼トラヒックのためのHA機能をFAに持たせるモバイルIPプロトコルの設計," 情処第65回全大, 2H-6, Mar. 2003.