IPv6 における移動透過性の実現

舌間一宏[†]　寺岡文男[††]

本稿では，IPv6 において移動透過性を実現するための新たな手法を提案する．本稿で提案する手法は，IPv6 アドレスの上位 64 ビットをノードが接続しているサブネットを示す位置指示子 (Locator) として，下位 64 ビットをインターネット上でノード自体を識別するためのノード識別子 (Identifier) として用いることにより，IPv6 における移動透過性を実現する．

本稿で提案するアドレス構造は，上位層のプロトコルやアプリケーションにいくつかの変更が必要であるが，IPv6 アドレス中にノードの移動に対して不変なノード識別子を格納しているため，モーバイルコンピューティングに非常に適している．また，ヘッダサイズやセキュリティなどの点でこれまでに提案されている従来の手法よりも優れているという特徴を持つ．

Providing Host Migration Transparency in IPv6

Kazuhiro Shitama [†] and Fumio Teraoka[††]

This paper proposes a new approach for providing host migration transparency in IPv6. In the new approach, we divide IPv6 address into two 8 byte parts: the *Locator* and the *Identifier*. The Identifier is unique in Internet and specifies a node no matter where it is connected. The Locator is also unique in Internet and specifies the subnet to which the node is connected.

The new addressing architecture we propose may need some modifications of upper layer protocols and applications, but is suitable for mobile computing since it includes identifier which never changes even if node moves. Further our approach has more efficiency about header size and security for mobile node than existing approach.

1. はじめに

現在，次世代のインターネットプロトコルとして IPv6 (Internet Protocol version 6)[12) が注目を浴びている．各組織で IPv6 の実装が行われており，6Bone と呼ばれる世界的な IPv6 実験ネットワーク上で各実装の相互接続性の検証などが日々実施されている．

IPv6 の特徴は，アドレス空間の拡大，セキュリティ機能の強化，プラグ&プレイなどさまざまであるが，基本設計は IPv4 を踏襲している．たとえば，IPv6 アドレスは IPv4 アドレスと同様，インターネットに接続しているノード自体を識別するノード識別子 (**Identifier**) ではなく，インターネット上でノードのインターフェースの位置を示す位置指示子 (**Locator**) である．そのため IPv4 の場合と同様, 自分のノート PC を持ち運び別のサブネットに接続するたびに，IPv6 アドレスは変化してしまう．

DHCPv6 などを用いることにより，IPv6 アドレスの設定を自動化することは可能であるが，移動するたびに IPv6 アドレスが変化することに変わりない．したがって通信中の移動ノードが移動すると，通信相手のノードは移動したノードの新しい IPv6 アドレスを知らない限り，その移動ノードを認識できない．また，移動前に確立していた TCP コネクションも維持できない．この問題を解決するため，IPv6 においてノードの位置や移動にかかわらず通信を持続できる機能，つまり IPv6 における移動透過性を提供するための研究がこれまで行われてきた．

本稿では, IPv6 における移動透過性を実現するための新たな手法を提案する．本稿で新たに提案する手法は，これまでに提案されている手法と大きく異なり，IPv6 のアドレス構造自体をモーバイルコンピューティングの視点で見つめ直し, 結果として採用した新たな IPv6 アドレス構造を基に IPv6 における移動透過性を実現する．

[†] 慶應義塾大学大学院 理工学研究科 計算機科学専攻
Department of Computer Science, Graduate School of Science and Technology, Keio University
[††] (株) ソニーコンピュータサイエンス研究所
Sony Computer Science Laboratory Inc.

本稿の構成は次のとおりである．まず, これまでに提案された既存の手法について概説し，その問題点をいくつか示す．その後，本稿で新たに提案するアドレス構造について述べ，さらにそのアドレス構造を基にしたIPv6における移動透過性の実現手法を説明する．最後に，本稿で提案する手法の現時点での実装状況について簡単に報告する．

2. 既存の手法

本章では，IPv6における移動透過性を実現するための既存の手法として，IETF Mobile IPv6 9)10) と VIPonV6 2)3) の2つについて概説する．

2.1 IETF Mobile IPv6

IETF Mobile IPv6(以下，Mobile IPv6)は，現在IETFで開発が進められている, IPv6における移動透過性を実現するプロトコルである．

Mobile IPv6において移動ノードは移動によって変化しないホームアドレスと呼ばれるIPアドレスを持ち，このホームアドレスを利用して他のノードとの通信を行う．一方，移動ノードは接続したサブネット上でDHCPv6などを用い，気付アドレス(Care-of Address)と呼ばれる一時的なIPアドレスを取得する．気付アドレスは実際にパケットを移動ノードに送り届けるために使用する．

移動ノードは自分のホームアドレスと気付アドレスの対応付けをホームエージェントと呼ばれるルータに登録する．また，ホームエージェントは移動ノードのホームアドレスのための経路情報をアナウンスする．それにより，移動ノードのホームアドレス宛てのIPパケットは，まずホームエージェントに到着し，ホームエージェントがそのパケットをIP-in-IPのトンネリングを用いて気付アドレス宛てに送信する．なお，移動ノードから送信されるパケットはホームエージェントを経由することなく，通信相手のノードへ直接送信される.

このようにMobile IPv6は，基本的にはIETF Mobile IPv4(以下, Mobile IPv4) 9)11) と同じアプローチであり，ホームアドレスや気付アドレスを32ビットのIPv4アドレスから128ビットのIPv6アドレスに単純に置き換えることにより設計している．

Mobile IPv4では2つの大きな問題があった．1つは，移動ノード宛てに送信されたパケットがその移動ノードのホームエージェントを必ず経由しなければならないことである．もう1つは，移動ノードから送信されるパケットのヘッダ中の始点アドレスフィールドにそのノードの気付アドレスではなくホームアドレスを格納しているため，そのパケットがアドレス偽造パケット 8) になってしまうことである．しかし，Mobile IPv6では，前者の問題については，通信相手ノードに関するホームアドレスと気付アドレスを対応付けたキャッシュと経路制御ヘッダ 12) を用いることにより解決している．また後者の問題については，ホームアドレスオプションという終点オプションヘッダ(Destination Options Header) 12) を新たに用意し，ホームアドレスオプションにホームアドレスを格納しておき，IPv6ヘッダの始点アドレスフィールドには気付アドレスを格納することにより解決している(図1参照).

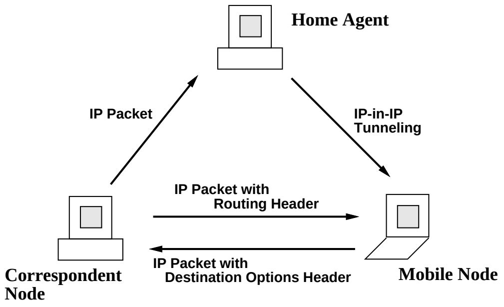


図1 IETF Mobile IPv6における通信経路

2.2 VIPonV6

VIPonV6は，我々が提案してきたVIP(Virtual Internet Protocol) 1) の機構を用いてIPv6における移動透過性を実現するプロトコルである．

VIPの基本概念は, ノード識別子と位置指示子の明確な分離である．VIPにおいて，TCP/UDP層よりも上位層では，ノードをVIPアドレスと呼ばれるノード識別子で認識する．さらにTCP/UDP層とIP層の間に新しく挿入したVIP層でVIPアドレスを，ノードのインターフェースの位置を示すIPアドレスにAMT(Addreess Mapping Table)によって対応付けする(図2参照). そしてIP層はこのIPアドレスに従ってパケットを配送する.

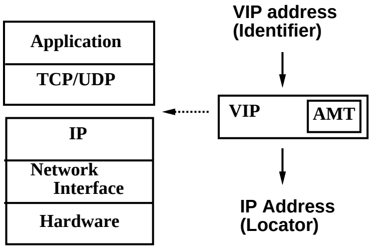


図2 VIPonV6におけるプロトコル階層

なお，移動ノードのVIPアドレスをIPアドレス

と考えた場合のサブネットを移動ノードのホームネットワークと呼び，ホームネットワークに接続しているルータをホームルータと呼ぶ．移動ノードが異なるサブネットに移動するたびに AMT アップデートメッセージと呼ばれる制御メッセージをホームルータへ送信することにより，ホームルータは必ずその移動ノードに関する最新の AMT エントリを保持することができる．通信相手に関する AMT エントリをもたないノードが移動ノードへ送信したパケットは，その移動ノードのホームルータに一度中継され，ホームルータがそのパケットを移動ノードへ転送する．

IPv4 における VIP には 4 つのバージョンがある．VIPv1 では移動透過性を実現し1)，VIPv2 ではノードの認証機能を加えた4)．さらに VIPv3 では安全なファイアウォール通過機構および移動サブネットのサポートを加え5)6)，VIPv4 では VIP パケットがアドレス偽造パケットとなってしまう問題を解決した7)．

VIPonV6 も，基本的には IPv4 における VIP と同じアプローチであり，ノード識別子 (VIP アドレス) や位置指示子 (IP アドレス) を表すアドレス空間を 32 ビットから 128 ビットに単純に置き換えることにより設計している．

3. 既存の手法の問題点

2章で述べたように，IPv6 における移動透過性を実現するための既存の手法は，基本的に IPv4 におけるアプローチをそのまま IPv6 に単純に応用した手法である．このため，比較的容易に実現可能であると考えられるが，一方で単純なアプローチであるためにいくつかの問題が生じる．本章では，既存の手法の問題点を示し，さらにこの問題の本質について検討する．

3.1 ヘッダサイズの増加

通信中の 2 ノードが移動や位置に関係なく互いを認識できるためには，やりとりされるパケットに 2 ノードのノード識別子情報を格納しておく必要がある．VIPonV6 では，始点ノード識別子オプションと終点ノード識別子オプションという 2 つの終点オプションヘッダを新たに用意し，各オプションにそれぞれ始点および終点のノード識別子を格納してパケットを送信している．オプションのサイズは共に 24 バイトで，終点オプションヘッダに必須の次ヘッダフィールド (1 バイト)，拡張ヘッダ長フィールド (1 バイト) を含め，オプションタイプフィールド (1 バイト)，オプション長フィールド (1 バイト)，タイムスタンプフィールド (4 バイト)，ノード識別子フィールド (16 バイト) で構成される．

したがって，VIPonV6 でやりとりされるパケット中のヘッダサイズは通常と比較して 48(24+24) バイト増加してしまう．拡張ヘッダを全く含まない IPv6 ヘッダのサイズは 40 バイトであるため，ヘッダサイズは 2 倍以上となる．このヘッダサイズの増加という問題は，ホームアドレスオプションや経路制御ヘッダを用いる Mobile IPv6 の場合でも同様に起こる．

3.2 IPsec の変更

IPsec15)の現時点の仕様では，2 ノード間の SA (Security Association) は 2 ノードの IP アドレスの組を用いて確立される．しかし，どちらかのノードが移動した場合，一方の IP アドレスが変化してしまうため，一度確立した SA を持続させることができない．つまり，ノードの移動ごとに SA を再確立する必要がある．

この問題を既存の手法で解決するためには，Mobile IPv6 のホームアドレスや VIPonV6 の VIP アドレスのような移動に対して不変なノード識別子を用いて SA を確立するように IPsec 自体を変更しなければならない．

3.3 問題点に関する考察

3.1節や 3.2節で示した問題点の本質は現在の IPv6 のアドレス構造自体にあると考えられる．1章でも述べたように，IPv6 アドレスはインターネット上でノードのインターフェースの位置を示すものであり，ノード自体を識別するためのノード識別子を含んでいない．そのため，IPv6 における移動透過性を実現するには既存の手法のように，移動に対して不変な 128 ビットのアドレスとしてホームアドレスや VIP アドレスを新たに導入せざるを得なかったといえる．この導入が結果としてヘッダサイズの増加や IPsec の変更の必要性を生じさせたと考えられる．

4. 移動指向 IPv6 アドレスの提案

本章では，3章で述べた既存の手法の問題点を踏まえ，ノードが移動することを前提として IPv6 のアドレス構造を再検討し，モーバイルコンピューティングに適した新たな IPv6 アドレス構造の提案を行う．

4.1 現在の IPv6 アドレス構造の概要

現在の IPv6 アドレス構造の仕様13)を図 3に示す．図 3のように，現在の IPv6 アドレス構造は上位 64 ビットと下位 64 ビットを分けて考えられている．上位 64 ビットは集約可能なネットワークプレフィックスであり，ノードが接続しているサブネットの位置を示している．これに対し，下位 64 ビットは上位 64 ビットで表されるネットワークプレフィックスをもつサブネット内でのインターフェース番号を示している．な

お，実際の経路制御ではIPv6アドレスの上位64ビットのみが使われ，下位64ビットはサブネット間の経路制御には利用されない．

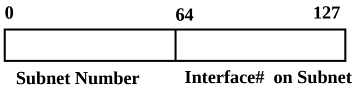


図3　IPv6アドレス構造の現在の仕様

ここで，IPv6アドレスの下位64ビットはノードが接続しているサブネットの方針により割り当てられたインターフェース番号を示しているにすぎないことに注意すべきである．たとえば，あるサブネットでは，単純に0から順番にインターフェース番号をノードに対して割り当てているかもしれないし，別のサブネットでは，ノードに挿しているEthernetカードのMACアドレスをそのままインターフェース番号として割り当てるかもしれない．

4.2　モーバイルコンピューティングに適したIPv6アドレス構造

3章で示した問題点の本質は，IPv6アドレスがノードの移動に対して不変なノード識別子を含んでいない点である．しかし，IPv6アドレス128ビット全体をノード識別子として用いると，逆にノードの位置に関する情報が完全に欠如していまうため，サブネット間の経路制御が実質不可能となってしまう．

そこで本稿では，4.1節で示したIPv6アドレスの現仕様において下位64ビットをインターネット上でノードを一意に識別するためのノード識別子として用いることを提案する．なお，IP層での経路制御機構と互換性を保つために，上位64ビットは従来通りノードの接続しているサブネットの位置を示すネットワークプレフィックスとする．本稿で採用するIPv6アドレス構造を移動指向 **(mobility-oriented)IPv6** アドレスと呼ぶ．なお，これまでノードの位置指示子とはIPv6アドレス128ビットで示されていたが，移動指向IPv6アドレスでは上位64ビットのみをノードの位置指示子と呼ぶことにした．なぜなら，サブネット間の経路制御で実際に用いられる位置情報は上位64ビット部分だからである．移動指向IPv6アドレス構造を図4に示す．

ここで，移動指向IPv6アドレスに格納されているノード識別子とは，ノード自体を識別するものであり，MACアドレスのようなNIC(Network Interface Card)のインターフェース識別子ではない．つまり，ノードに挿しているNICを入れ替えることでインターフェース識別子は変わってもノード識別子は不変である．

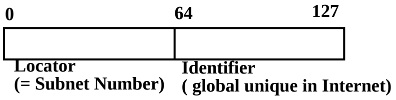


図4　移動指向IPv6アドレス構造

4.3　移動指向IPv6アドレスの特徴

移動指向IPv6アドレスは，現在のIPv6アドレス構造と異なり，IPv6アドレス内にノードの移動に対して不変なノード識別子を下位64ビットに格納しているため，モーバイルコンピューティングに適している．たとえば，移動透過性を実現するために既存の手法のように新たなアドレスを導入する必要はない．また，IPv6アドレス中に格納されたノード識別子を用いてIPsecのSAを確立することができるため，既存の手法の場合に比べてIPsecの変更箇所が少なくてすむと考えられる．

ある移動指向IPv6アドレスをもつノード宛てのパケットは，まず上位64ビットの位置指示子を用いて宛先ノードが接続しているサブネット上のルータまで転送される．パケットを受信したルータはNDP(Neighbor Discovery Protocol)を用いて, IPv6アドレスに対応する物理アドレスを解決し，最終的に宛先ノードへ転送される．

なお，IPv6アドレス中にノード識別子を導入した場合の一般的な分析はいくつか行われている17)18). 移動指向IPv6アドレスの有用性についても，こういった分析結果を参考に今後詳しく検討していく予定である．

5. IPv6における移動透過性の実現

本章では，4章で提案した移動指向IPv6アドレスを基に，IPv6における移動透過性を実現する手法について述べる．

5.1　基本方針

本稿で提案する手法の基本方針は以下2点である．

- IPv6アドレスとして, 移動指向IPv6アドレスを用いる
- 移動透過性を実現する基本概念として, 2.2節で述べたVIPの機構を用いる

TCP/UDP層より上位層では，移動指向IPv6アドレス(以下，特記しない限りIPアドレスとは移動指向IPv6アドレスを示す)下位64ビットのノード識別子を用いてノードを識別し，TCP/UDP層とIP層の間に挿入したVIP層のAMTでそのノード識別子に対応した位置指示子64ビットを結合することにより128

ビットの IP アドレスを生成する．本手法での AMT とは，ノードの現在の位置指示子とノード識別子を結合した IP アドレスのリストである．なお，VIP 層で宛先ノードに関する AMT エントリがない，つまり宛先ノードのノード識別子に対する現在の位置指示子が分からない場合は宛先ノードのホームネットワークのネットワークプレフィックスを位置指示子として宛先ノードのノード識別子と結合し IP アドレスを生成する．ホームネットワークのネットワークプレフィックスの取得方法は 6.3節で述べる．こうして生成された IP アドレスを基に IP 層はパケットの送信を行なう．パケット受信時は，VIP 層で IP アドレスから位置指示子が単純に除かれ，ノード識別子だけが上位層に渡される (図 5参照)．

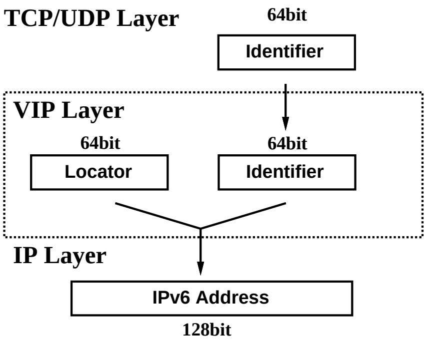


図 5　階層構造とノード識別子, 位置指示子,IPv6 アドレスの関係

5.2　移動ノードの動作

移動ノードは次の 3 つの動作を行う．

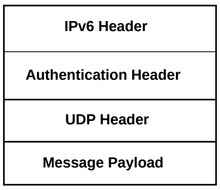
- 移動先サブネットでの位置指示子の獲得
- ホームルータや通信中のノードへの AMT アップデートメッセージの送信
- 通信中のノードからの AMT アップデートメッセージの受信

位置指示子の獲得

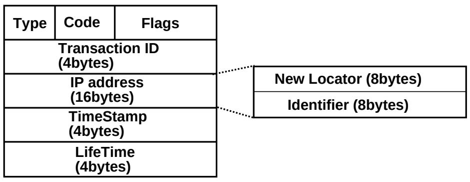
移動ノードはあるサブネットに接続すると，接続先のサブネット上のルータ通知 (router advertisement)[14] を受信し，ルータ通知に含まれるネットワークプレフィックスを移動ノードの位置指示子としてノード識別子と結合し，移動先での IP アドレスを生成する．このように，移動指向 IPv6 アドレスを使用すると，DHCPv6 などのステートフル自動設定は特に必要なく，移動先サブネット上で流れているルータ通知を受信するだけで移動先での IP アドレスを獲得することができる．

AMT アップデートメッセージの送信

移動先のサブネットで新たに IP アドレスを生成した移動ノードは，その移動ノードのホームルータおよび通信中のノードへ AMT アップデートメッセージを送信し，別のサブネットへ移動したことを報告する．なお，AMT アップデートメッセージは UDP を利用する．AMT アップデートメッセージのパケット構成を図 6 (a) に, メッセージペイロードを図 6 (b) にそれぞれ示す．



(a) パケット構成



(b) メッセージペイロード

図 6　AMT アップデートメッセージ

図 6 (a) で示されるように，AMT アップデートメッセージには，ホームルータや通信中の相手ノードに不正な AMT エントリが作成されることを回避するために， 拡張ヘッダの 1 つである認証ヘッダ[16]を必ず含まなければならない．また，図 6 (b) 中の IP アドレスフィールドに，移動ノードが取得した現在の位置指示子とノード識別子からなる IP アドレスを格納する．

さらに，移動ノードがホームルータから IP-in-IP のトンネリングで転送されたデータパケットを受信した場合にも，そのデータパケットを送信したノードがこの移動ノードに関する AMT エントリを保持していないと判断して，AMT アップデートメッセージを送信する．

AMT アップデートメッセージの受信

通信中のノードから AMT アップデートメッセージを受信したノードは, メッセージに含まれる認証ヘッダにより送信ノードと通信内容を認証した後，メッセージペイロードに格納されている IP アドレスを取り出し，そのノードが保持する AMT に登録する．

なお，ここで登録された AMT エントリは，通信中

のノードに関するものであるため，タイマを設定し，タイムアウト後はこの AMT エントリを削除する．

5.3　ホームルータの動作

ホームルータは次の 2 つの動作を行う．

- 移動ノードからの AMT アップデートメッセージの受信
- 移動先のノードへのパケットの転送

AMT アップデートメッセージの受信

移動ノードからの AMT アップデートメッセージを受信したホームルータは, メッセージに含まれる認証ヘッダにより送信ノードと通信内容を認証した後，メッセージペイロードに格納されている IP アドレスを取り出し，ホームルータが保持する AMT に登録する．

なお，ここで登録された AMT エントリは，そのホームルータが管理している移動ノードに関するものであるため，タイマを設定せず，AMT アップデートメッセージを再度受信するまで保持しておく．

移動先のノードへのパケットの転送

受信したパケットの宛先アドレスの下位 64 ビットが，そのホームルータの管理している移動ノードのノード識別子である場合は，まず保持している AMT エントリを参照し移動先のノードの IP アドレスを知る．そして，ホームルータは受信したパケットに，移動先のノードの IP アドレスを宛先アドレスとした新しい IPv6 ヘッダを付加し，移動先のノードへパケットを転送する (図 7参照)．この転送方法を IP-in-IP のトンネリングという．トンネリングを用いる理由は，受信したパケットの終点アドレスフィールドを直接書き換えて移動先のノードへ転送すると，転送したパケットが結果としてアドレス偽造パケット8) だと判断されてしまい，途中のルータで廃棄される可能性があるからである．

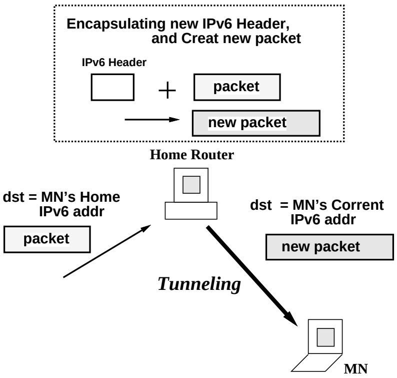


図 7　ホームルータによるパケットの転送

5.4　通信の具体例

本手法を導入したノード間でやりとりされるパケットの通信経路を図 8に示す．図 8において，ルータ HR は移動ノード MN のホームルータである．ここでは，ノード CN が MN にパケットを送信する手順について説明する．

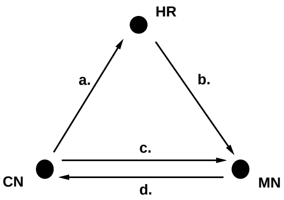


図 8　通信の具体例

(1) CN は保持している AMT に MN に関するエントリがあるかどうかチェックする．AMT エントリがある場合は (4) へ．ない場合は (2) へ．

(2) MN に関する AMT エントリがない場合，CN は MN のホームネットワークを示す位置指示子と MN のノード識別子を結合して IP アドレスを生成し，パケットを送信する (図 8中の a.). 次に (3) へ．

(3) (2) で CN が送信したパケットを HR が受信すると，受信したパケットの宛先アドレスの下位 64 ビットが MN のノード識別子であることを知る．HR は MN に関する AMT エントリから移動先の IP アドレスを知り，トンネリングを用いて，受信パケットを送信する (図 8中の b.). 次に (5) へ．

(4) MN に関する AMT エントリがある場合，CN は MN の移動先のサブネットを示す位置指示子と MN のノード識別子を結合して IP アドレスを生成し，MN へ直接パケットを送信する (図 8中の c.). 次に (5) へ．

(5) MN はパケットを受信すると，その受信パケットが HR によるトンネリングによるものかどうかチェックする．トンネリングによる場合は (6) へ．そうではない場合は (7) へ．

(6) 受信パケットがトンネリングによる場合，CN が MN に関する AMT エントリを保持していないと判断し，CN に AMT アップデートメッセージを送信する (図 8中の d.). 次に (8) へ．

(7) 受信パケットがトンネリングによるものでない場合，CN が MN に関する AMT エントリを保持していると判断し，MN は何もせずパケット

のやりとりを続行する．

(8) MNが送信したAMTアップデートメッセージをCNが受信すると，CNはメッセージの認証を行い，認証に成功するとCNが保持しているAMTにMNに関するエントリを追加する．今後，MN宛てのパケットはMNへ直接送信する．

6. 考察

本章では，5章で示した手法について考察を行う．

6.1 既存の手法との性能比較

ここでは，既存の手法と本手法の性能をいくつかの点において定性的に比較する．

- データパケット送受信の処理
  VIPonV6ではデータパケットを送信するたびに，始点ノード識別子オプションと終点ノード識別子オプションを用意し，始点および終点のノード識別子を各オプションに格納しなければならない．また，データパケットを受信する場合にも，始点ノード識別子オプションと終点ノード識別子オプションから始点および終点のノード識別子を抽出しなければならない．Mobile IPv6の場合も, ホームアドレスオプションや経路制御ヘッダに対して同様の処理が必要となる．
  これに対し，本手法ではIPアドレス自体がノードのノード識別子を含んでいるため，既存の手法のような処理は必要ない．
- キャッシュの記憶容量
  通信相手ノードとの通信経路の最適化を図るために，VIPonV6では通信相手ノードのVIPアドレスとIPアドレスの対応づけを，またMobile IPv6ではホームアドレスと気付アドレスの対応づけをそれぞれキャッシュとして保持している．そのキャッシュを保持しておくために必要な記憶容量は，1つのアドレス長が16バイトであるため，エントリ数をnとすると$32n$バイトとなる．
  それに対し，本手法では通信相手ノードの現在の位置指示子とノード識別子を結合したIPアドレスのみをキャッシュとして保持していればよい．したがって，必要な記憶容量は$16n$バイトでよいため，既存の手法と比較して半分の記憶容量で十分である．

以上のように，データパケットの送受信にかかる処理やキャッシュのために必要な記憶容量といった基本的な性能項目において，本稿で提案した手法は既存の手法よりも優れていることがわかる．

6.2 ノード識別子とインターフェース識別子

移動指向IPv6アドレスの下位64ビットやVIPonV6のVIPアドレスは，ノードに挿しているNICを識別するインターフェース識別子ではなく，ノード自体を識別するノード識別子である. そのため，このノード識別子を用いる本手法では，ノードが移動した場合だけでなく，ノードに挿しているNICを交換した場合でも，そのノードに対して透過的な通信が可能となる．

それに対し，Mobile IPv6ではホームアドレスをインターフェース識別子としか考えていないため，厳密な意味でノード識別子ではない．したがって，ノードに挿しているNICを交換してしまうとインターフェース識別子が変わってしまうため，そのノードに対して透過的な通信ができなくなる．

モーバイルコンピューティング環境では，ノードに挿しているNICの交換といった作業は頻繁に起こると考えられるため，本手法やVIPonV6で提供する機能は今後重要となるといえる．

6.3 DNSとの協調

本手法により，VIP層より上位層のプロトコルやアプリケーションはノード識別子を用いることでノードの移動を気にすることなく通信の持続が可能となる．しかし，64ビットで表されるノード識別子は，非常に覚えにくく扱いにくい．さらに，VIP層において，通信相手のノード識別子に対するAMTエントリがない場合，通信相手の位置指示子を知ることができないためIPアドレスを生成できず，通信不能となってしまう．この2点を解決するため， DNSを利用することを現在検討中である．ノードの移動に対して不変な**ID(IDentifier)**と**HL(Home Locator)**という2つのレコードをDNSに新たに登録する．IDレコードは，ノードのホスト名に対するノード識別子64ビットを格納し，ノードへのホスト名によるアクセスを可能にする．HLレコードは, そのホスト名をもつノードのホームネットワークを示すネットワークプレフィックス64ビットを格納し，VIP層において通信相手のノード識別子に対するAMTエントリがない場合に，その通信相手のホームルータへパケットを送信するために用いる．

6.4 上位層の変更と互換性の問題

4章で述べたように，移動指向IPv6アドレスは現仕様のIPv6アドレスと経路制御において互換性を保つように設計しているため，IP層に変更を加える必要はない．つまり，移動指向IPv6アドレスを用いるノードと現仕様のIPv6アドレスを用いるノード間の経路制御は従来通り可能である．

しかし，TCPやUDPおよび上位アプリケーションでは，IPアドレス全体ではなくIPアドレス下位64ビットのノード識別子でノードを識別するように変更を加える必要がある．

さらに，インターネット上の全てのノードが本手法を導入すれば問題ないが，本手法を導入したノードと導入していないノードがTCPのコネクションを確立する場合，本手法を導入したノードはTCPコネクションを(始点IPアドレスの下位64ビット, 終点IPアドレスの下位64ビット, 始点ポート番号，終点ポート番号)で識別するのに対し，本手法を導入しないノードは(始点IPアドレス128ビット, 終点IPアドレス128ビット, 始点ポート番号, 終点ポート番号)で認識するため，正しくTCPコネクションを確立できない場合がある．

この互換性に関する問題であるが，我々の最終目的は，ただ単にIPv6における移動透過性を実現することではなく，モーバイルコンピューティングに適したアドレス構造を提案し，移動を前提としたネットワークアーキテクチャを構築することである．したがって，上位層のプロトコルにおける互換性は現在考慮しない．

7. おわりに

本稿では, IPv6における移動透過性を実現するための新たな手法を提案した．本稿で新たに提案した手法は，これまでに提案されている手法と大きく異なり，IPv6のアドレス構造自体をモーバイルコンピューティングの視点で再検討し，その結果としてノードの移動に対して不変なノード識別子を含んだ移動指向IPv6アドレスを提案した．さらに移動指向IPv6アドレスを基に移動透過性を実現する手法を説明した．

現在，本稿で提案した手法を ***v6*VIP** と名付け，FreeBSD2.2.5上に実装中である．IPv6カーネルは，WIDEプロジェクトで開発中のhydrangeaを用いている．今後は，実装を完了し，次回の論文で詳しい実装方法や評価結果に関する検討を行なう予定である．

参考文献

1) F. Teraoka, K. Uehara, H. Sunahara, J. Murai, *VIP: A protocol providing host mobility*, CACM, vol.37, no.8, pp.67-75, August 1994

2) F. Teraoka, K. Uehara, *Mobility Support in IPv6 based on the VIP mechanism*, Proc. INET'95, June 1995

3) F. Teraoka *Mobility Support with Authentic Firewall Traversal in IPv6*, IEICE TRANS. COMMUN., vol. E80-B, no.8, August 1997

4) 植原 啓介, 寺岡文男, 砂原秀樹, 移動ノード用通信プロトコル*VIP*における認証機構, 日本ソフトウェア科学会 第11回大会論文集, 1994年10月

5) 寺岡文男, *VIPv3*における安全なファイアウォール通過機構, 情報処理学会 モーバイルコンピューティング研究グループ研究会 報告集, 1996年7月

6) 石井公夫, 寺岡文男, 村井純, 移動するネットワークのための透過的な通信機構の設計, 情報処理学会 マルチメディア通信と分散処理研究会 報告集, 1995年10月

7) 舌間一宏, 寺岡文男, *VIPv4*の設計と実装, 日本ソフトウェア科学会第14回大会 論文集, 1997年9月

8) Computer Emergency Response Team (CERT), *IP Spoofing Attacks and Hijacked Terminal Connections*, CA-95:01, January 1995

9) J. D. Solomon, *Mobile IP, The Internet Unplugged*, Prentice Hall, 1998

10) C. Perkins, J. David, *Mobility Support in IPv6*, MOBICOM'96, November 1996

11) C. Perkins, *IP Mobility Support*, RFC2002, IETF, October 1996

12) S. Deering, R. Hinden, *Internet Protocol, version 6 (IPv6) specification*, RFC1883, IETF, December 1995

13) R. Hinden, M. O'Dell, S. Deering, *An IPv6 Aggregatable Global Unicast Address Format*, Internet Draft, work in progress, March 1998

14) S. Thomson, T. Narten, *IPv6 Stateless Address Autoconfiguration*, RFC1971, IETF, August 1996

15) R. Atkinson, *Security Architecture for the Internet Protocol*, RFC1825, IETF, August 1995

16) R. Atkinson, *IP Authentication Header*, RFC1826, IETF, August 1995

17) M. O'Dell, *GSE - An Alternate Addressing Architecture for IPv6*, Internet Draft, work in progress, February 1997

18) M. Crawford, A. Mankin, T. Narten, J. W. Stewart III, L. Zhang, *Separating Identifiers and Locators in Addresses: An Analysis of the GSE Proposal for IPv6*, Internet Draft, work in progress, March 1998