Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

IPv6 ネットワークにおける NTMobile の検討

上酔尾　一真[†1]　鈴木　秀和[†1]
内藤　克浩[†2]　渡邊　晃[†1]

著者らは仮想 IP アドレスとトンネリング技術を用いて，IPv4/IPv6 混在環境で移動透過性を実現する NTMobile（Network traversal with Mobility）を提案している．NTMobile は NAT 配下に存在する NTMobile 端末に対してコネクションを確立することができる．NTMobile は現在までに IPv4 ネットワークにおいて実装を行ってきた．現在，IPv4 アドレスの枯渇により IPv6 への移行が進められているため，NTMobile も IPv6 への適用が必要である．IPv4 と IPv6 はアドレス構造が異なるため，従来の NTMobile の仕様をそのまま適用することはできない．また，従来の仕様では NAT 越えを考慮したトンネル構築動作を行っているため，IPv6 ネットワークにおいては冗長な手順が含まれている．本稿では，IPv6 ネットワークにおける NTMobile の仕様について検討を行う．トンネル構築動作を最適化することにより，通信開始時およびハンドオーバ時の遅延を削減する．

Researches on NTMobile in IPv6 Network

Kazuma Kamienoo,[†1] Hidekazu Suzuki,[†1]
Katsuhiro Naito[†2] and Akira Watanabe[†1]

We have proposed NTMobile (Network traversal with Mobility) that can provide mobility with virtual IP address and tunnel technology in IPv4/IPv6 coexistence environment. In the NTMobile, the node can establish a connection to the correspondent node that supports NTMobile located behind the NAT router. NTMobile has been implemented for IPv4 network. In recent years, IPv6 transration has progressively started due to IPv4 address exhaustion, therefore we have to apply NTMobile to IPv6 network. The specification of existing NTMobile cannot be applied to IPv6 environment because of the difference between IPv4 and IPv6 address structures. Additionally the tunnel establishment procedure of existing NTMobile is designed with NAT traversal, therefore the specifications have redundant procedures on IPv6 network. In this paper, we describe specifications of NTMobile in IPv6 network. Delay overgeads at the beginning of communication and in handover can be reduced by optimizing the tunnel establishment procedure.

1. はじめに

近年，スマートフォンやタブレットなどの携帯端末の普及に伴い，移動しながら通信を行いたいという要求が高まっている．しかし，インターネットで使用されている TCP/IP では，通信端末の IP アドレスとポート番号を用いて通信を管理しているため，携帯端末の移動に伴い IP アドレスが変化した場合，通信を継続することができない．このような問題を解決するための技術を移動透過性技術と呼ぶ．現在までに多くの移動透過性技術が提案されてきたが，その多くは IPv4 ネットワークまたは IPv6 ネットワークのみの環境を想定している[1)]．現在，IPv4 アドレスの枯渇により，IPv6 への移行が進められている．しかし，IPv4 と IPv6 には互換性がないため，完全に IPv6 へ移行するには時間が必要となる．そのため，当分の間は IPv4 と IPv6 が混在した環境が続くと考えられる．今後の IP ネットワークの状況を想定すると，IPv4 と IPv6 の混在環境において移動透過性を実現する必要があると考えられる．

著者らは移動透過性を IPv4/IPv6 混在環境で実現する技術として，NTMobile（Network Traversal with Mobility）を提案している[2)–4)]．NTMobile では，エンド端末に仮想 IP アドレスを割り当て，アプリケーションが仮想 IP アドレスを用いて通信を行うことにより，端末の移動に伴う実 IP アドレスの変化を隠蔽する．また，NAT の有無に応じて最適な経路でトンネルを構築し，アプリケーションが生成したパケットを転送する．NTMobile は現在までに IPv4 ネットワークにおいて実装および評価がなされており，基本的な動作はそのまま IPv6 ネットワークに適用することが可能である．

本稿では，IPv4 と IPv6 の混在環境への対応を見据え，NTMobile を IPv6 ネットワークに適用した場合の仕様を検討する．従来の NTMobile は NAT を考慮したトンネル構築手順となっているため，NAT の必要性が薄い IPv6 ネットワークにおいてはいくつかの不要な処理が含まれている．そこで，NTMobile を IPv6 ネットワークに適用させるにあたり，トンネル構築動作の最適化を行う．

以下，2 章で従来の IPv4 ネットワークにおける NTMobile について概説し，3 章で IPv6

†1 名城大学 理工学部
Faculty of Science and Technology, Meijo University
†2 三重大学大学院工学研究科
Graduate School of Engineering, Mie University

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

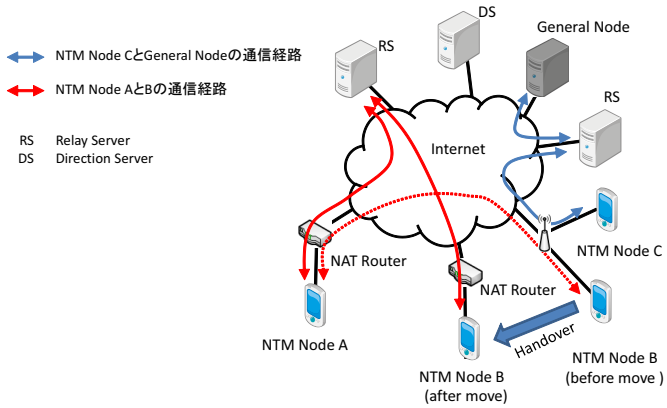

図 1 NTMobile の概要
Fig. 1 Overview of NTMobile.

ネットワークにおける NTMobile の仕様について述べる．4 章で関連技術を取り上げ，5 章でまとめる．

2. IPv4 ネットワークにおける NTMobile

2.1 概　　要

NTMobile で想定するネットワークを**図 1** に示す．NTMobile のシステムは，DS（Direction Server），RS（Relay Server），NTMobile に対応した端末（以下 NTM 端末）によって構成されている．DS は仮想 IP アドレスの割り当て管理や，NTM 端末に対して各種処理の指示を出す装置である．DS は管理する仮想 IP アドレスに重複が起きないように割り当てを行う．各 DS には予め異なる仮想 IP アドレスの帯域が割り当てられており，DS が管理する仮想 IP アドレスが他の DS と重複しないようになっている．そのため，DS へのアドレス帯域の割り当てのみで，簡易な仮想 IP アドレスの管理を行うことができる．また，DS は Dynamic DNS の機能を包含しており，NTM 端末の A レコードや NTMobile 専用のレコード（以下 NTM レコード）を登録することにより，NTM 端末のネットワーク位置情報を管理する．NTM レコードには NTM 端末の FQDN$^{\star 1}$，実 IP アドレス，仮想 IP アドレス，NAT の外側の実 IP アドレス$^{\star 2}$，NTM レコードが登録されている DS の実 IP アドレスが格納されている．

RS は，異なる NAT 配下に存在する NTM 端末で通信を行う場合の中継を行う．RS による通信中継は通信開始時だけでなく，NTM Node B のように移動後に通信ペアが共に NAT 配下に位置するようになる場合にも行う．また，NTM Node C のように NTMobile 非対応の一般端末と通信を行う場合にも RS を中継する．一般端末は RS と通信を行うことになるため，NTM 端末は通信中に移動することが可能になる．

NTM 端末は，移動先のネットワークから割り当てられる実 IP アドレスと，移動によって変化しない仮想 IP アドレスの 2 つのアドレスを保持している．NTM 端末が使用しているアプリケーションは，仮想 IP アドレスを用いてコネクションを確立することにより，NTM 端末の移動に伴い実 IP アドレスが変化しても，通信を継続することができる．なお，仮想 IP アドレスに基づくアプリケーションパケットは，NTM 端末間に構築される UDP トンネルによって転送される．

DS と各端末は信頼関係があることを前提としており，NTMobile で使用されるメッセージは各端末間で共有している暗号鍵を用いて暗号化される．また，NTM 端末間や NTM 端末と RS の間で行われるトンネル通信は，トンネル構築時に DS によって配布される共通鍵を用いて暗号化される．

2.2 動作シーケンス

以後の説明では，通信開始側の NTM 端末を MN（Mobile Node），通信相手側の NTM 端末を CN（Correspondent Node），通信相手側の NTMobile 非対応端末を GN（General Node）とする．また，MN の Node ID を NID_{MN}，実 IP アドレスを RIP_{MN}，仮想 IP アドレスを VIP_{MN} とし，位置情報を管理している DS を DS_{MN} とする．Node ID は端末を一意に識別することができる識別子である．

2.2.1 位置情報の登録

MN はネットワーク接続時および移動時に，実 IP アドレスなどの位置情報を DS_{MN} に登録する[4]．このとき，DS_{MN} の実 IP アドレスが分からない場合には，MN は自身の NTM レコードを問い合わせることにより，DS_{MN} の実 IP アドレスを取得する．MN は DS_{MN} の実 IP アドレスを取得した後，位置情報を登録するために DS_{MN} へ Registration Request を送信する．Registration Request には MN の位置情報として NID_{MN}，RIP_{MN}，MN

⋆1 Fully Qualified Domain Name
⋆2 NTM 端末が NAT 配下に存在する場合のみ

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

の FQDN が含まれている．DS_{MN} は MN から送信された Registration Request を受信すると，MN の NTM レコードおよび A レコードを更新する．なお，Registration Request の IP ヘッダーに格納されている送信元 IP アドレスが RIP_{MN} と異なる場合には，MN が NAT 配下に存在すると判断し，NAT の外側の実 IP アドレスとして送信元 IP アドレスを登録する．

2.2.2 名前解決

NTMobile では，通信開始時にアプリケーションが行う DNS による名前解決を検出した際にトンネル構築を行う[2)]．

MN は DNS リゾルバにより CN の A レコードの問い合わせを行い，DNS サーバからの応答をカーネル内で一時待避してから，CN の NTM レコードの問い合わせを行う．CN の NTM レコード取得後，MN は 2.2.3 項で説明するトンネル構築動作に移る．

MN が GN に対して通信を開始する場合は，NTM レコードを取得することができないが，GN の A レコードの情報のみを用いてトンネル構築へ移る．なお，カプセル化を行うためには仮想 IP アドレスが必要となるため，トンネル構築時に DS から GN に対して仮想 IP アドレスが割り当てられる．

トンネル構築後，MN はカーネルに待避していた DNS サーバからの応答に含まれる CN の実 IP アドレスを仮想 IP アドレスに書き換え，DNS リゾルバに渡す．以上により，MN のアプリケーションは通信相手の IP アドレスとして仮想 IP アドレスを認識することになる．

2.2.3 トンネル構築

グローバルネットワークに存在する MN が，プライベートネットワークに存在する CN との間にトンネルを構築するまでの様子を**図 2** に示す．MN はトンネルを構築するために，DS_{MN} に対して Direction Request を送信する．Direction Request には MN と CN の NTM レコードの情報が格納されており，DS_{MN} はこの情報から MN と CN の位置を判断し，両者へトンネル構築の指示を出す．DS_{MN} は CN のみがプライベートネットワークに存在することを認識すると，DS_{CN} 経由で CN へ Route Direction を送信し，MN へ Tunnel Request を送信するよう指示する．ここで，DS_{CN} と CN の間には常に制御メッセージ用の経路が確保されているため，DS_{CN} は NAT の外側から CN に対して通信を開始することができる．また，MN には CN から送信される Tunnel Request を受信するよう指示する．Route Direction には，Path ID，通信相手の実 IP アドレスと仮想 IP アドレス，トンネルの構築先の実 IP アドレス，エンド端末間通信の暗号化に用いる共通鍵などが格納されている．なお，Path ID は通信を一意に識別することができる識別子である．NAT の内側の端

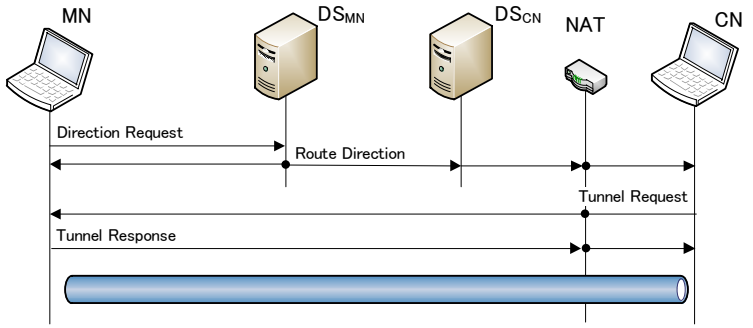

図 2 トンネル構築手順
Fig. 2 Tunnel establishment sequence.

末である CN から MN に対して Tunnel Request を送信することにより，MN と CN の間に NAT を跨ったトンネルを構築することができる．

MN と CN が異なるプライベートネットワークに存在する場合は，両ノードが送信する Tunnel Request は通信相手側の NAT により破棄されてしまうため，エンドツーエンドでトンネルを構築することができない．そこで，DS_{MN} は MN と CN に対して，RS に Tunnel Request を送信するよう指示する．また，DS_{MN} は Relay Direction を RS に送信し，MN と CN の通信を中継するよう指示する．これにより，MN と CN は RS との間にトンネルを構築する．

通信相手が GN である場合はエンドツーエンドでトンネルを構築することができないため，上述した動作と同様の手順により MN と RS の間にトンネルを構築する．

NTM 端末はカーネル空間にトンネルテーブルを保持しており，トンネル構築完了時に構築したトンネルの情報をトンネルテーブルに登録する．トンネル通信を行う際には，トンネルテーブルの当該エントリに従ってカプセル化およびデカプセル化を行う．また，カプセル化およびデカプセル化処理を行う際には，当該エントリに登録されている共通鍵を用いて暗号化および復号処理を行う．RS はカーネル空間にパケットの転送を行うための情報を格納したリレーテーブルを保持している．

2.2.4 トンネル通信

各端末間で構築されたトンネルには Path ID がつけられており，カプセル化時には Path ID が格納された NTM ヘッダが付加される．

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

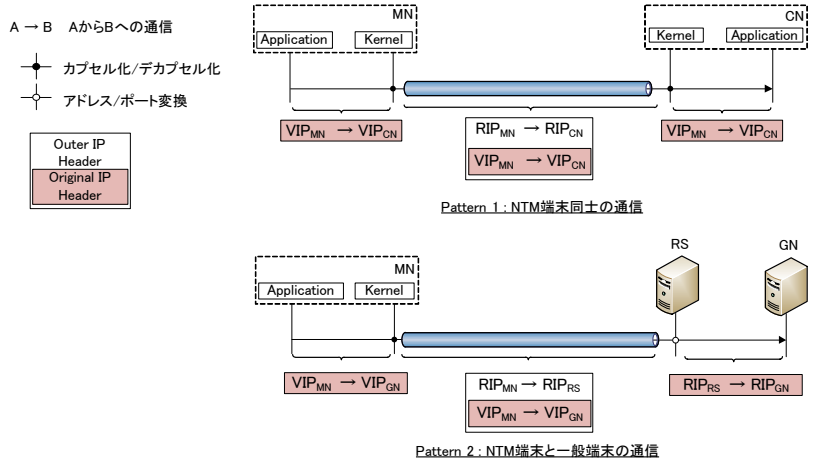

図 3 パケットのアドレス遷移
Fig. 3 Address transition of Packet.

図 3 に通信時のアドレス遷移の様子を示す．図 3 の Pattern 1 では NTM 端末同士で通信を行っているため，エンド端末間でトンネルが構築されている．アプリケーションレベルでは仮想 IP アドレスを用いてコネクションが確立されているため，アプリケーションパケットの IP ヘッダには仮想 IP アドレスが格納されている．パケット送信時，MN は宛先の仮想 IP アドレスをキーにトンネルテーブルを検索し，当該エントリに従ってカプセル化および暗号化を行い，CN へ送信する．CN はカプセル化されたパケットを受信すると，NTM ヘッダに格納された Path ID をキーにトンネルテーブルを検索する．その後，CN は当該エントリに従ってデカプセル化および復号処理を行い，抽出したアプリケーションパケットを上位アプリケーションへ渡す．

図 3 の Pattern 2 では NTM 端末と NTMobile 非対応の端末が通信を行っているため，MN と RS の間にトンネルが構築されている．MN と RS の間の通信は，上述したようにトンネルを用いた通信を行う．RS は MN から受信したパケットをデカプセル化および復号処理を行った後，リレーテーブルに従って宛先 IP アドレスを RIP_{GN} に変換する．また，送信元 IP アドレスとポート番号を RIP_{RS} と未使用のポート番号に変換し，GN へ転送する．以上の処理により，GN は通信相手が RS であると認識する．なお，RS は GN からの応答を受信すると，送信時と逆の変換を行い，リレーテーブルに従ってカプセル化および暗号化した後，MN へ転送する．

図 3 の Pattern 1 において，通信経路上に NAT が存在する場合には NAT を跨ったトンネル通信を行うことになる．この場合，MN が送信したパケットの外側 IP ヘッダと UDP ヘッダが NAT によってアドレス/ポート変換が行われるため，アプリケーションパケットの IP ヘッダや UDP ヘッダは送信時のまま維持される．CN は受信したパケットに格納された Path ID を元にデカプセル化および復号処理を行い，抽出したアプリケーションパケットを上位アプリケーションに渡す．以上により，MN と CN のアプリケーションは NAT に影響されることなく通信を行うことができる．

2.2.5 NTM 端末の移動

NTM 端末が他のネットワークへ移動して新たな IP アドレス取得した場合，その IP アドレスを DS に登録し，通信開始時と同様の手順でトンネルを再構築する[3)]．この時，NTM 端末のアプリケーションは仮想 IP アドレスを使用しているため，実 IP アドレスが変化してもアプリケーションに対して移動を隠蔽することができ，アプリケーション間のコネクションが切断されることはない．また，GN と通信を行っている場合，GN は RS を通信相手であると認識しているため，NTM 端末の実 IP アドレスが変化しても，GN に対して移動を隠蔽することができる．

3. IPv6 ネットワークにおける NTMobile

NTMobile の基本的な動作は，IPv6 ネットワークにそのまま適用することができる．しかし，IPv4 アドレスと IPv6 アドレスは互換性のないアドレス構造となっているため，各種メッセージのフォーマットを拡張する必要がある．また，従来の NTMobile は NAT を考慮したトンネル構築手順となっているため，IPv6 ネットワークにおいてはいくつかの不要な処理が含まれている．そこで，NTMobile を IPv6 ネットワークに適用するにあたり，トンネル構築動作の最適化を行う．

本稿ではすべての端末が IPv6 ネットワークに存在し，MN と CN は IPv6 対応のアプリケーションを使用することを想定する．

3.1 アドレス構造の違いによる追加・修正事項

IPv4 と IPv6 ではアドレス構造が異なるため，各メッセージに格納されているアドレス部分を IPv6 アドレス向けに拡張する．また，IPv6 ネットワークでは，NAT が存在しないため各種メッセージから NAT に関する情報を削除する．

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

アプリケーションは仮想 IP アドレスを使用するため，新たに仮想 IPv6 アドレスを定義する．仮想 IPv6 アドレスは，新たに定義する仮想ネットワークプレフィックスと仮想 IPv4 アドレスを元に生成する．仮想 IPv4 アドレスを元に生成することにより，仮想 IPv6 アドレスを一意に生成することができる．また，仮想 IPv6 アドレスは仮想 IPv4 アドレスと同様に，DS が割り当てを行う．

NTM 端末は自身の位置情報として，AAAA レコードと IPv6 に対応させた NTM レコード（以後 NTMv6 レコード）を DS に登録する．NTMv6 レコードには NTM 端末の FQDN と Node ID，実 IP アドレス，仮想 IPv6 アドレス，NTMv6 レコードが登録されている DS の実 IP アドレスを格納する．

3.2 動作シーケンス

以下，MN の IPv6 の実 IP アドレスを $RIP6_{MN}$，仮想 IPv6 アドレスを $VIP6_{MN}$ とし，MN と CN 間の通信で用いる Path ID を PID_{MN-CN}，トンネル通信の暗号化・復号に用いる共通鍵を K_{MN-CN} とする．

NTM 端末は従来の NTMobile と同様の手順で位置登録処理を完了しており，DS に実 IP アドレスなどの位置情報が登録されているものとする．

3.2.1 名前解決

IPv4 ネットワークにおける NTMobile では，A レコードの問い合わせを検出した場合にトンネル構築を行っていた．IPv6 ネットワークにおいては，AAAA レコードの問い合わせを検出した場合にトンネル構築を行う．

MN が CN に対して通信を開始する場合，MN は DNS リゾルバにより CN の AAAA レコードの問い合わせを行い，DNS サーバからの応答を NTM デーモンに一時待避してから，CN の NTMv6 レコードの問い合わせを行う．CN の NTMv6 レコードの取得後，3.2.3 項で説明するトンネル構築動作に移る．この時，通信相手が GN である場合には NTMv6 レコードを取得することができないが，GN の AAAA レコードの情報のみを用いてトンネル構築へ移る．なお，GN の仮想 IPv6 アドレスは，トンネル構築時に DS から割り当てられる．

トンネル構築完了後，NTM デーモンに待避していた CN の AAAA レコードの実 IP アドレスを仮想 IPv6 アドレスに書き換えることにより，アプリケーションに通信相手の IP アドレスとして仮想 IPv6 アドレスを認識させることができる．このように，名前解決処理の基本的な考えは従来の NTMobile を踏襲している．

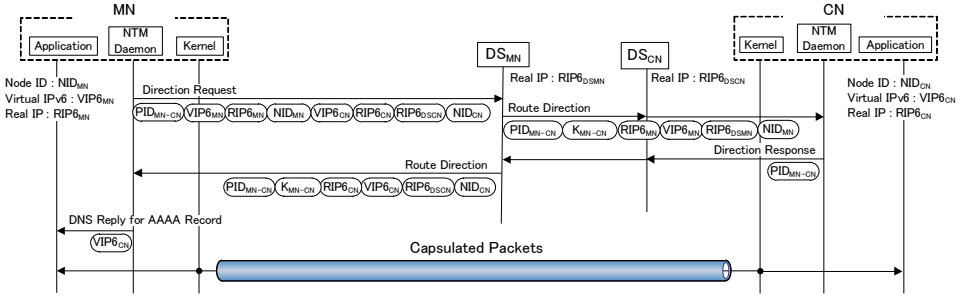

図 4 NTM 端末間のトンネル構築手順
Fig. 4 Tunnel establishment procedure between NTM nodes.

3.2.2 トンネル構築

MN と CN の間に UDP トンネルが構築されるまでの様子を**図 4** に示す．MN は NTMv6 レコードにより CN の情報を取得した後，トンネルを構築するために DS_{MN} へ Direction Request を送信する．なお，Direction Request には MN と CN の NTMv6 レコードの情報が格納されている．DS_{MN} は MN と CN へ Route Direction を送信し，エンド端末間でトンネルを構築するよう指示する．ここで，IPv4 ネットワークでは，この後の Tunnel Request によりエンド端末間でトンネルを構築しているが，IPv6 ネットワークではこの処理を省略する．このとき，CN に Route Direction が到達しなかった場合に確認を取ることができない．また，CN に Route Direction が到達する前に，MN がトンネルを用いた通信を開始することが考えられる．そのため，DS_{MN} は CN へ Route Direction を送信し，CN から新たに定義する Direction Response が返ってきてから，MN へ Route Direction を送信する．CN と MN は Route Direction の情報からトンネルテーブルを生成する．以上により，CN と MN の間にトンネルが構築されるため，以後はエンドツーエンドのトンネル通信が開始される．なお，MN と CN 間で行われるトンネル通信は Route Direction に格納された共通鍵 K_{MN-CN} を用いて暗号化される．

MN が GN と通信を行う場合のトンネル構築動作を**図 5** に示す．MN は GN の AAAA レコードを取得後，トンネルを構築するために Direction Request を DS_{MN} へ送信する．このとき，通信相手が NTM 端末の場合と異なり，Direction Request には MN の NTMv6 レコードの情報と GN の実 IP アドレスのみが記載される．DS_{MN} は Direction Request を受信すると，その内容から GN が NTMobile 非対応の端末であることを判断し，GN の仮想

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

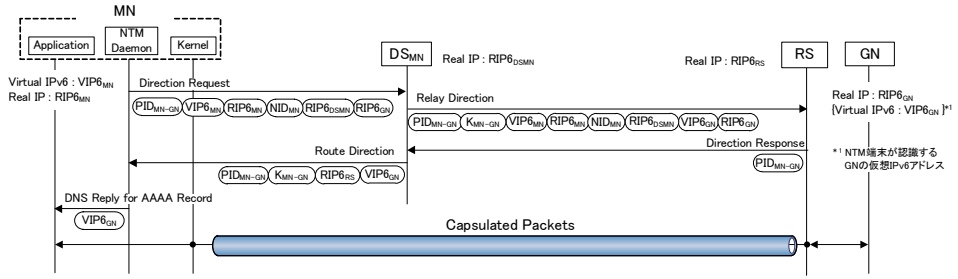

図 5 NTM 端末と RS 間におけるトンネル構築手順
Fig. 5 Tunnel establishment procedure between NTM node and RS.

IPv6 アドレスとして $VIP6_{GN}$ を生成する．その後，DS_{MN} は RS に Relay Direction を送信し，MN と GN の通信を中継するように指示する．Relay Direction には MN と GN の情報や Path ID など，通信の中継に必要な情報が格納されており，これを受信した RS は MN と RS の間に構築するトンネルの情報および，$VIP6_{GN}$ 宛のパケットを $RIP6_{GN}$ へ転送するための転送情報をリレーテーブルに登録する．その後，DS_{MN} に Direction Response を返す．DS_{MN} は Direction Response を受信すると，Route Direciton を MN へ送信する．このとき，Route Direction には GN の仮想 IPv6 アドレスとして $VIP6_{GN}$ が格納されている．MN は Route Direction の情報からトンネルテーブルを生成する．以上により MN と RS の間にトンネルが構築され，MN は GN との通信を開始する．なお，MN と RS が行うトンネル通信は，Route Direction および Relay Direction に格納された共通鍵 K_{MN-GN} を用いて暗号化される．

3.2.3 トンネル通信および移動時の動作

従来の NTMobile と同様に，アプリケーションレベルでは仮想 IP アドレスを用いてコネクションが確立されているため，アプリケーションパケットの IP ヘッダには仮想 IPv6 アドレスが格納されている．MN は CN に対してトンネル通信を開始する場合，宛先の仮想 IPv6 アドレスをキーにトンネルテーブルを検索し，当該エントリに従ってカプセル化および暗号化した後，CN へ送信する．CN は受信したパケットに格納された Path ID をキーにトンネルテーブルを検索し，当該エントリに従ってデカプセル化・復号処理を行い，抽出したパケットを上位アプリケーションへ渡す．

通信相手が GN である場合，従来の NTMobile と同様に RS は MN から受信したパケットをデカプセル化および復号処理を行い，アドレス/ポート変換を行った後，GN へ転送する．また，RS は GN からの応答を受信すると，送信時と逆の変換を行った後，リレーテーブルに従ってカプセル化および暗号化し，MN へ転送する．

NTM 端末が移動した場合には新たな位置情報を DS に登録した後，通信開始時と同様の処理を行い，トンネルを再構築する．アプリケーションは仮想 IPv6 アドレスを用いてコネクションを確立しているため，移動に伴う実 IP アドレスの変化を隠蔽することができる．

3.3 考　　察

NTMobile はトンネリング技術と仮想 IP アドレスを用いることにより，IPv6 ネットワークにおいても移動透過性を実現することが可能である．また，IPv6 ネットワークにおいては，NTM 端末が通信を行う場合には常にエンドツーエンドの通信が可能となる．

従来の NTMobile では NAT 配下の端末とコネクションを確立するために，Tunnel Request と Tunnel Response を使用していたが，IPv6 ネットワークには NAT が存在しないため，Tunnel Request と Tunnel Response を省略した．これにより，トンネル構築時に必要となるメッセージが少なくなるため，トンネル構築におけるオーバヘッドを削減することができる．また，これに伴い，通信開始時およびハンドオーバ時に生じる遅延を削減することができると考えられる．なお，本稿で提案したトンネル構築手法は，NTM 端末がグローバルネットワークに存在する場合に適用可能であるため，IPv4 ネットワークにおいても状況に応じて同様の手法を用いることができる．

4. 関 連 技 術

IPv6 ネットワークにおいて移動透過性を実現する技術として，MIPv6（Mobile IPv6）[5]，LIN6（Location Independent Networking for IPv6）[6),7]，MAT（Mobile IP with Address Translation）[8]，Mobile PPCv6（Mobile Peer-to-Peer Communication）[9] などが提案されている．

MIPv6 では，移動端末に HoA（Home Address）と CoA（Care of Address）の二つのアドレスを割り当てる．HoA は移動端末のホームネットワークに到達する IP アドレスであり，CoA は移動端末の訪問先ネットワークから割り当てられる IP アドレスである．移動端末のホームネットワークには HA（Home Agent）が設置されており，移動端末の代わりに HoA 宛のパケットを受信し，移動端末の CoA 宛に転送する．HA を用いることにより，MIPv6 非対応の端末から通信を開始した場合であっても，MIPv6 対応端末の移動透過性を実現することができる．しかし，基本的に HA を経由した通信となるため，経路が冗長な

Vol.2011-MBL-59 No.9
Vol.2011-CDS-2 No.9
2011/9/5

るといった問題点がある．また，通信相手が MIPv6 に対応している場合には，経路最適化を行うことによりエンドツーエンドの通信が可能となるが，通信開始時には必ず HA を経由した通信が必要となる．それに対して，NTMobile は NTM 端末同士で通信を行う場合，通信開始時から最適な経路で通信を行うことが可能である．しかし，NTMobile 非対応の端末から通信を開始する場合，RS 経由ではなく直接 NTM 端末に対して通信を開始してしまうため，この場合には NTM 端末の移動透過性を実現することができない．

LIN6 は，LINA（Location Independent Network Architecture）における縮退アドレスモデルに基づいた移動透過技術である．LIN6 では，IP アドレスを位置指示子とノード識別子の二つの空間に分離し，アプリケーションレベルでは固定の位置指示子を用いることにより，端末の移動に伴う位置指示子の変化を隠蔽する．LIN6 はエンド端末において位置指示子の変換を行うことにより，エンドツーエンドで移動透過性を実現することができる．また，カプセル化によるオーバヘッドが生じないため，高いスループットが期待できる．しかし，一つの IP アドレスを二つの空間に分離するため，アドレスの利用効率が低くなってしまう．

MAT と Mobile PPCv6 は端末内部でアドレス変換を行うことにより，エンドツーエンドで移動透過性を実現する．MAT ではノード識別子を表す HoA（Home Address）と位置指示子を表す MoA（Mobile Address）の二つのアドレスを移動端末に割り当て，アプリケーションは HoA を用いた通信を行い，ノード間の通信では MoA を使用する．ネットワーク層において HoA と MoA を変換することにより，端末の移動に伴う IP アドレスの変化をアプリケーションに対して隠蔽することができる．Mobile PPCv6 では，アプリケーションに対して常に通信開始時に使用していた IP アドレスを認識させておき，パケット送信時に現在端末が取得している IP アドレスに変換する．アドレス変換を行うことにより，端末の移動に伴う IP アドレスの変化をアプリケーションに対して隠蔽することができる．MAT や Mobile PPCv6 はエンドツーエンドで通信を行うことができ，また，カプセル化を行わないため高いスループットが期待できる．

MAT や Mobile PPCv6 はエンド端末でアドレスの変換処理を行うため，移動透過性を実現するためには通信相手も MAT や Mobile PPCv6 に対応している必要がある．それに対して，NTMobile では RS を用いることにより，通信相手が NTMobile 非対応の端末であっても NTM 端末の移動透過性を実現することができる．また，NTMobile はカプセル化を行うため，LIN6 や MAT，Mobile PPCv6 よりもスループットが低くなると考えられる．しかし，NTMobile ではカーネル空間でカプセル化処理を行うことにより，カプセル化処理に伴うスループットの低下を抑制しているため，一般的なカプセル化処理を行う方式よりも高いスループットが期待できる[3]．

5. ま と め

本稿では，IPv4/IPv6 混在環境において移動透過性を実現する NTMobile を IPv6 に適用させた場合の検討を行った．NTMobile は IPv6 ネットワークにおいても，通信相手によらず NTM 端末の移動透過性を実現することができ，NTM 端末同士であれば常に最適な経路で通信を行うことが可能であることを示した．また，トンネル構築手順を最適化することにより，通信開始時および移動時に生じる遅延を削減することが期待できる．

NTMobile は IPv4 ネットワークにおいて，アドレス空間を跨がった移動透過性を実現できることが証明されており，IPv4 と IPv6 の混在環境においても移動透過性を実現することが可能である．今後は，NTMobile を IPv4 と IPv6 の混在環境に適用させた場合や，NTMobile 非対応の端末から通信を開始した場合に，NTM 端末の移動透過性を実現するための検討を行う予定である．

参 考 文 献

1) Le, D., Fu, X. and Hogrefe, D.: A Review of Mobility Support Paradigms for the Internet, *IEEE Communications Surveys*, Vol.8, No.1, pp.38–51 (2006).
2) 鈴木秀和，水谷智大，西尾拓也，内藤克浩，渡邊　晃 : NTMobile における相互接続性の確立手法と実装，DICOMO2011 論文集，pp.1339–1348 (2011).
3) 内藤克浩，西尾拓也，水谷智大，鈴木秀和，渡邊　晃，森香津夫，小林英雄 : NTMobile における移動透過性の実現と実装，DICOMO2011 論文集，pp.1349–1359 (2011).
4) 西尾拓也，内藤克浩，水谷智大，鈴木秀和，渡邊　晃，森香津夫，小林英雄 : NTMobile における端末アドレスの移動管理と実装，DICOMO2011 論文集，pp.1139–1145 (2011).
5) Johnson, D., Perkins, C. and Arkko, J.: Mobilit Support in IPv6, *RFC 3775,IETF* (2004).
6) Masahiro, I., Mitsunobu, K., Keisuke, U., Hiroshi, E. and Fumio, T.: LINA:A New Approach to Mobility Support in Wide Area Networks, *IEICE TRANS. COMMUN*, Vol.E84-B, No.8, pp.2076–2086 (2001).
7) 光宣國司，政浩石山，啓介植原，文男寺岡 : 移動体通信プロトコル LIN6 の性能評価，情報処理学会論文誌，Vol.43, No.2, pp.398–407 (2002).
8) 相原玲二，藤田貴大，前田香織，野村嘉大 : アドレス変換方式による移動透過インターネットアーキテクチャ，情報処理学会論文誌，Vol.43, No.12, pp.3899–3897 (2002).
9) 寺澤圭史，鈴木秀和，渡邊　晃 : IPv6 における Mobile PPC の実現と評価，情報処理学会研究報告，Vol.2010-MBL-52, No.5, pp.1–8 (2010).