情報処理学会論文誌 Vol.54 No.10 2288–2299 (Oct. 2013)

推薦論文

IPv4/IPv6混在環境で移動透過性を実現するNTMobileの実装と評価

上醉尾 一真[1,a)] 鈴木 秀和[1] 内藤 克浩[2] 渡邊 晃[1]

受付日 2013年4月10日, 採録日 2013年6月14日

概要：IPv4 グローバルアドレスの枯渇にともない，今後は互換性のない IPv4 と IPv6 が混在したネットワークになることが想定される．著者らは NAT が導入された IPv4 ネットワークにおいて確実な接続性の確保と，移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）を提案してきた．本論文では NTMobile を IPv4 と IPv6 の混在環境に対応するよう拡張し，Android OS を搭載したスマートフォンへ実装して動作検証および性能評価を行った．動作検証の結果，IPv4 と IPv6 混在環境において NTMobile の機能を実現可能であることを確認した．また，NTMobile による処理遅延はわずかであるものの，ハンドオーバ時には IP アドレス取得処理に起因する通信断絶時間が発生することが分かった．

キーワード：モバイルネットワークアーキテクチャ，移動透過性，NAT 越え，IPv4/IPv6 混在環境，Android

Implementation and Evaluation of NTMobile to Achieve IP Mobility in IPv4 and IPv6 Networks

Kazuma Kamienoo[1,a)] Hidekazu Suzuki[1] Katsuhiro Naito[2] Akira Watanabe[1]

Received: April 10, 2013, Accepted: June 14, 2013

Abstract: With the exhaustion of IPv4 global addresses, it is expected that IPv4 and IPv6 networks will be gradually spreading hereafter. We have been proposing Network Traversal with Mobility (NTMobile) that can achieve connectivity and mobility at the same time in IPv4 networks that use NAT. In this paper, we have expanded the function of NTMobile for IPv4 and IPv6 networks, and implemented it in Android smartphones. As the result of our verification, NTMobile works as expected. It was also found that there is a period of communication interruption owing to the process of acquiring a new IP address at the time of handover, although the delay due to the process by NTMobile is quite small.

Keywords: mobile network architecture, mobility, NAT traversal, IPv4 and IPv6 networks, Android

1. はじめに

現在の IP ネットワークは IPv4 から IPv6 への過渡期にあり，IPv4 と IPv6 が共存した環境が広まりつつある．しかし，IPv4 と IPv6 には互換性がないため，これらのネットワーク間において相互に通信を行うことができない．一方，既存の IPv4 ネットワークでは NAT（Network Address Translation）を導入してプライベートネットワークを構築することが一般的であり，CGN（Carrier Grade NAT）のようにキャリアレベルでも NAT が導入され始めている [1]．NAT が導入された環境（以下 NAT 環境）においては，グローバルネットワーク側の端末からプライベートネットワーク側の端末に対する接続性を確保できない，NAT 越

[1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 462–8502, Japan
[2] 三重大学大学院工学研究科
Graduate School of Engineering, Mie University, Tsu, Mie 514–8507, Japan
[a)] 123430013@ccalumni.meijo-u.ac.jp

本論文の内容は 2012 年 7 月のマルチメディア，分散，協調とモバイル（DICOMO2012）シンポジウム 2012 にて報告され，モバイルコンピューティングとユビキタス通信研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

え問題とよぶ課題があり，エンドツーエンドの接続性というインターネット本来の理念を損なう要因となっている．これまで NAT 越え問題を解決する様々な技術が提案されてきたが，シグナリングオーバヘッドの増大，NAT やプライマリ DNS（Domain Name System）サーバなどの特定の装置に改造が必要になる，経路が冗長になるなどの課題がある [2], [3], [4]．今後の IP ネットワークを想定すると，NAT 環境や IPv4 と IPv6 が混在した環境においても，確実に接続性を確保する技術が必要である．

また，スマートフォンやタブレットなどの高性能な携帯端末の普及や無線通信技術の発展により，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．スマートフォンには 3G や Wi-Fi，WiMAX など複数の無線インタフェースが搭載されており，必要に応じてインタフェースを切り替えて通信を行うことができる．しかし，IP ネットワークでは通信端末のインタフェースに割り当てられた IP アドレスを用いて通信を管理しているため，インタフェースやネットワークの切替えにともない IP アドレスが変化すると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技術を移動透過性技術と呼び，現在までに様々な移動透過性技術が提案されている [5], [6], [7], [8], [9], [10]．既存の移動透過性技術の多くは IPv6 ネットワークを想定しており，IPv4 ネットワークへの適用が検討されている技術であっても，NAT 環境においては移動や通信が制限されることや，経路が冗長になるという課題がある．

IPv4/IPv6 混在環境において移動透過性と NAT 越えを実現する技術として，DSMIPv6（Dual Stack Mobile IPv6）が IETF（Internet Engineering Task Force）で標準化されている [11]．DSMIPv6 では，ホームネットワークに設置した HA（Home Agent）が通信を中継することにより，IPv4/IPv6 ネットワーク間の通信や NAT 越えを実現している．しかし，DSMIPv6 では，IPv4 ネットワークにおいてつねに HA を経由した冗長経路となることや，HA の分散設置ができないことなどが課題となっている．

著者らは，NAT が導入された IPv4 ネットワークにおいて確実な接続性を確保し，移動透過性を実現する NTMobile（Network Traversal with Mobility）を提案してきた [12], [13], [14]．NTMobile は NAT 越えの技術を兼ね備えており，NAT に改造を加えることなく NAT 配下の移動端末（以後 NTM 端末）に対する接続性を確保することができる．NTMobile では NTM 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 アドレスに基づいた通信を行うことにより，端末の移動にともなう実 IP アドレスの変化を隠蔽し，アプリケーション間の通信を継続する．また，通信経路上の 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．NTM 端末間に構築されるトンネルは，特定の状況を除きエンドツーエンドで構築されるため，経路が冗長になりにくい．

NTMobile は IPv6 ネットワークへの適用を想定しており，IPv4 と IPv6 が混在した環境においても IPv4 ネットワークと同様に確実な接続性と移動透過性を実現することができる．本論文では NTMobile を IPv4 と IPv6 の混在環境に対応するよう拡張し，Android OS [*1] を搭載したスマートフォンへ実装することにより，実環境において動作検証および性能評価を行った．

以下，2 章で関連研究の課題について述べ，3 章で IPv4 環境における従来の NTMobile，4 章で IPv4 と IPv6 の混在環境に対応するよう拡張した NTMobile について概説する．5 章で実装および性能評価について述べ，6 章でまとめる．

2. 関連研究

本章では，IPv4 と IPv6 の混在環境において移動透過性を実現する，DSMIPv6 の概要と課題について述べる．DSMIPv6 は，IPv6 ネットワークにおいて移動透過性を実現する Mobile IPv6 [7] を IPv4/IPv6 混在環境へ適用するために拡張した技術である．DSMIPv6 では移動端末に対して，ホームネットワークで取得する HoA（Home Address）と訪問先ネットワークから取得する CoA（Care of Address）の 2 種類のアドレスを割り当て，アプリケーションが HoA を用いた通信を行うことにより，移動端末の移動にともなう CoA の変化を隠蔽する．

図 1 に DSMIPv6 の概要を示す．移動端末 MN（Mobile Node）はホームネットワークに設置した HA との間にトンネルを構築し，HA を経由して通信相手 CN（Correspondent Node）と通信を行う．ホームネットワークはデュアルスタックネットワークとして構築されており，HA が IPv4 ネットワークと IPv6 ネットワーク間の橋渡しをする．MN のアプリケーションが生成したパケットはトンネルを用いて HA へ送信され，HA によりデカプセル化されたあと，CN へ送信される．これにより，CN は通信相手の IP アドレスとして HoA を認識することになり，MN のアプリ

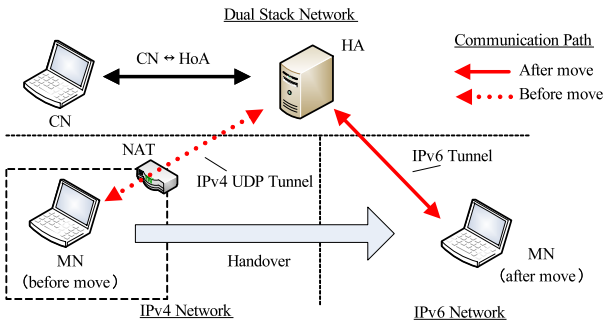

図 1 DSMIPv6 の概要
Fig. 1 Overview of DSMIPv6.

[*1] 米 Google 社が発表した Linux をベースとした携帯端末向けの OS.

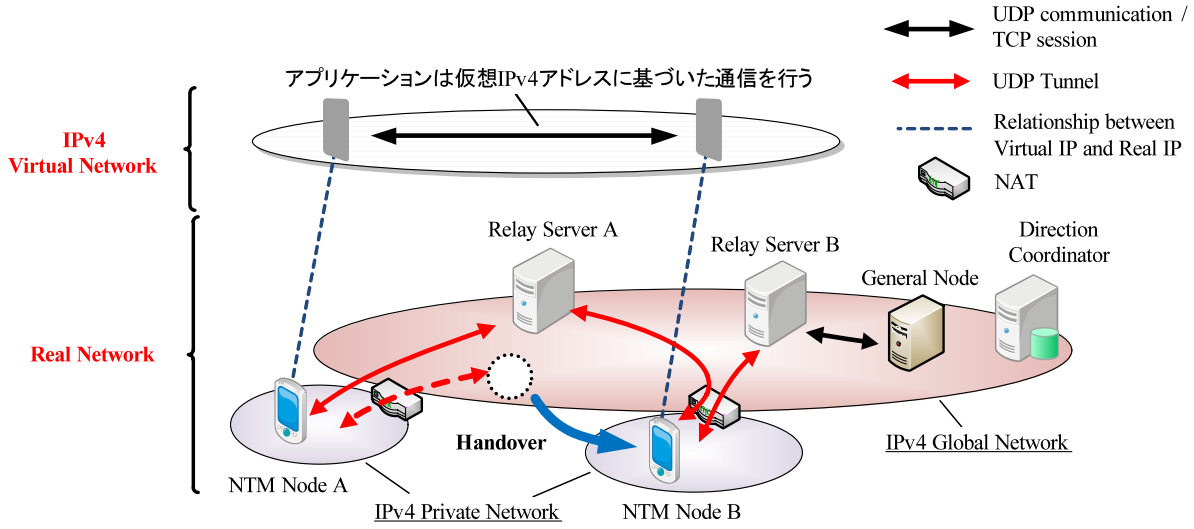

図 2 IPv4 環境における NTMobile の概要
Fig. 2 Overview of NTMobile in IPv4 network.

ケーションと CN 間には HoA に基づいたコネクションが確立される．HoA は移動により変化しないため，通信中に MN が移動をしても，アプリケーションや CN に対して移動を隠蔽し，通信を継続することができる．また，IPv4 の HoA を用いることにより，IPv6 ネットワーク上にて IPv4 アプリケーションを使用することができる．

Mobile IPv6 には，MN と CN 間でエンドツーエンド通信を行うために経路最適化機能が定義されている．しかし，この機能は IPv6 特有のヘッダオプションを使用しており，また，NAT 環境を想定していないため，通信端末が IPv4 ネットワークに位置する場合や IPv4 アプリケーションを使用している場合には適用することができない．そのため，DSMIPv6 では MN が IPv4 ネットワークに接続している場合，つねに HA を介した冗長な経路で通信を行うか，訪問先のネットワークに特殊な NAT を設置する必要がある [15]．

Mobile IPv6 では HA への負荷分散や経路の冗長性を抑制するために，Global HA to HA Protocol とよぶ技術が議論されている [16]．この技術では，複数の HA をホームネットワーク外に分散設置し，HA 同士がオーバレイネットワークを構築する．MN の通信を中継する際には，経路的に近い HA が中継装置として選ばれる．これにより，HA の多重化を可能とし，経路の冗長性を抑制することができる．しかし，この機能は DSMIPv6 や IPv4 ネットワークへの適用は議論されていないため，DSMIPv6 によるシステムでは HA を分散設置することができず，また，冗長経路が発生しやすいという課題がある．

3. IPv4 環境における NTMobile

本章では IPv4 環境における NTMobile の概要について述べる．NTMobile では，NTM 端末に実際のネットワークに依存しない仮想 IPv4 アドレスを割り当て，アプリケーションは仮想 IPv4 アドレスに基づいた通信を行う．これにより，アプリケーションはネットワークの切替えや通信経路上の NAT に影響されることなく，自由に通信を行うことができる．なお，仮想 IPv4 アドレスに基づくパケットは，NTM 端末間に構築される UDP トンネルによって送信される．このトンネルは特定の状況を除きエンドツーエンドで構築されるため，通信端末はつねに最適な経路でトンネル通信を行うことができる．

NTMobile のネットワーク構成を**図 2** に示す．NTMobile は DC（Direction Coordinator），NTM 端末，RS（Relay Server）によって構成される．DC や RS はグローバルネットワークに設置し，ネットワークの規模に応じて複数台設置することができる．

- DC（Direction Coordinator）
  DC は仮想 IPv4 アドレスの割当て管理や，NTM 端末に対してトンネル構築などの指示を出す装置である．NTM 端末に割り当てられる仮想 IPv4 アドレスは一意なアドレスであり，各 DC は自身に割り当てられたアドレス空間から重複が起きないよう割当てを行う．また，DC は Dynamic DNS の機能を包含しており，NTM 端末の A レコードに加えて，NTMobile 専用レコード（以下 NTM レコード）を登録することにより，NTM 端末のアドレス情報を管理する．NTM レコードには NTM 端末の FQDN（Fully Qualified Domain Name），実 IPv4 アドレス，仮想 IPv4 アドレス，NAT の外側の実 IPv4 アドレス，自身のアドレス情報を管理する DC の実 IPv4 アドレスなどが記載されている．
- NTM 端末
  NTM 端末は移動先のネットワークから割り当てられる実 IPv4 アドレスと，DC から割り当てられる仮想

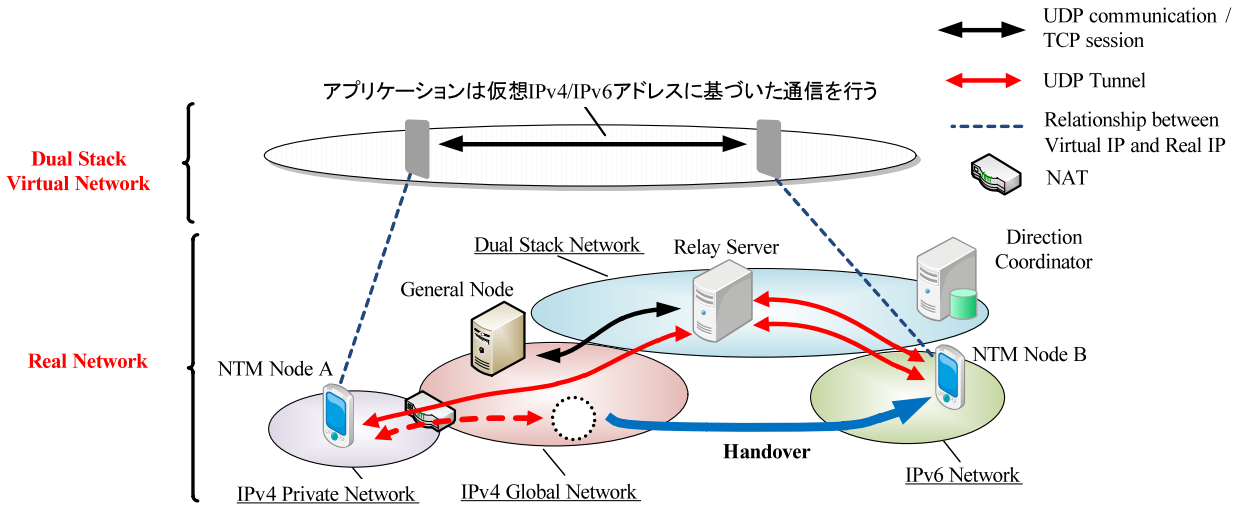

図 3 IPv4/IPv6 混在環境における NTMobile の概要
Fig. 3 Overview of NTMobile in IPv4 and IPv6 networks.

IPv4 アドレスの 2 種類のアドレスを保持している．仮想 IPv4 アドレスはネットワークに依存しない IPv4 アドレスであり，NTM 端末が接続先のネットワークを切り替えても変化しない．アプリケーションが仮想 IPv4 アドレスに基づいた通信を行うことにより，通信中にネットワークを切り替えても，アプリケーションの通信を継続することができる．なお，仮想 IPv4 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 トンネルによって送信される．図 2 における NTM 端末 A と移動前の NTM 端末 B のように，どちらか一方の端末がグローバルネットワークに接続している場合には，エンドツーエンドでトンネルが構築される．

- RS（Relay Server）
  RS は，図 2 における NTM 端末 A と移動後の NTM 端末 B のように通信端末が異なる NAT 配下に位置する場合や，一般端末のような NTMobile 非対応端末と通信を行う場合に通信を中継する装置である．RS はインターネット上に分散設置することが可能であり，中継負荷や経路の冗長性を考慮してトンネル構築時に最適な RS を選択することができる．

DC 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および MAC（Message Authentication Code）が付加される．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 DC より配布される共通鍵を用いて暗号化および MAC が付加される．

4. IPv4/IPv6 混在環境における NTMobile

IPv4 環境を想定した従来の NTMobile の基本的な仕組みは，IPv4 と IPv6 の混在環境へ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，NTM レコード，仮想 IP アドレス，およびネットワーク構成などを拡張する必要がある．本章では IPv4 と IPv6 の混在環境に対応するよう拡張した NTMobile について述べる．

4.1 アドレス構造の違いによる変更事項

IPv4 と IPv6 の混在環境における NTMobile のネットワーク構成を図 3 に示す．DC および RS は，IPv4 ネットワークと IPv6 ネットワークのどちらからでもアクセスできるよう，デュアルスタックネットワークに設置する．NTM 端末には，仮想 IPv4 アドレスと新たに定義した仮想 IPv6 アドレスをつねに割り当てる．NTM 端末のアプリケーションは仮想 IPv4 アドレスまたは仮想 IPv6 アドレスのどちらかに基づいた通信を行うことにより，ネットワークの切替えや接続しているネットワークの違いに影響されることなく，通信を行うことができる．

また，NTM 端末の IPv6 のアドレス情報を管理するために，新たに NTMv6 レコードを定義する．NTMv6 レコードには，NTM 端末の FQDN，実 IPv6 アドレス，仮想 IPv6 アドレス，自身のアドレス情報を管理する DC の実 IPv6 アドレスなどが記載されている．DC は A レコードおよび IPv4 アドレスを記載した従来の NTM レコード（以後 NTMv4 レコード）に加え，AAAA レコードおよび NTMv6 レコードを登録することにより，NTM 端末のアドレス情報を管理する．

図 3 における NTM 端末 A と移動後の NTM 端末 B のように，通信端末が異なるアドレス構造のネットワークに接続している場合には，プロトコルの違いから直接通信を行うことができない．そのため，NTM 端末 A と NTM 端末 B は，デュアルスタックネットワークに設置した RS との間にトンネルを構築し，RS を経由したトンネル通信を

行う．

以後の説明では，通信開始側の NTM 端末を MN，通信相手側の NTM 端末を CN とし，IPv4/IPv6 混在環境において，MN と CN が IPv4 のアプリケーションによる通信を行う際の動作を例に記述する．また，端末 X の実 IPv4 アドレスを $RIP4_X$，仮想 IPv4 アドレスを $VIP4_X$，実 IPv6 アドレスを $RIP6_X$ とし，アドレス情報を管理している DC を DC_X とする．MN と CN の通信時に用いる Path ID を PID_{MN-CN}，暗号化および認証に用いる共通鍵を CK_{MN-CN} とする．Path ID は NTM 端末間の通信を一意に識別するための識別子である．

4.2 アドレス情報の登録

NTM 端末は端末起動時および接続先ネットワークの切替え時に，アドレス情報を各自の DC に登録する．MN は FQDN や $RIP4_{MN}$，$RIP6_{MN}$ など，NTMv4 レコードおよび NTMv6 レコードに登録する情報を記載した Registration Request を DC_{MN} へ送信する．DC_{MN} は Registration Request を受信すると，DNS サーバに登録されている MN のリソースレコードを更新し，MN へ応答を返す．IPv4 ネットワークにおいて，Registration Request の IP ヘッダに格納されている送信元 IPv4 アドレスが MN の実 IPv4 アドレスと異なる場合には，MN が NAT 配下に存在すると判断し，送信元 IP アドレスを NAT の外側の実 IPv4 アドレスとして MN の NTMv4 レコードに登録する．また，IPv6 ネットワークでは，インタフェースへ複数の IPv6 アドレスを設定することが可能であり，リンクローカルユニキャストアドレスのように，インターネット上で使用することができない IPv6 アドレスが端末へ割り当てられることがある．この場合には，インターネット上で通信可能なグローバルユニキャストアドレスのみを NTMv6 レコードへ登録する．

登録処理が完了した後，MN と DC_{MN} は定期的にメッセージを交換することにより，制御メッセージ用の通信経路を確保する（Keep Alive）．これにより，MN が NAT 配下に接続している場合であっても DC_{MN} はつねに MN へ制御メッセージを送信することができる．また，CN についても同様の処理を行い，DC_{CN} へアドレス情報を登録する．

4.3 トンネル構築処理

NTMobile では，NTM 端末が通信開始時に行う DNS による名前解決処理や，ハンドオーバによる実 IP アドレスの変化を検出した際にトンネル構築処理を実行し，通信相手との間にトンネル通信経路を確立する．MN は DNS による名前解決処理として A レコードの問合せを検出した場合には，CN の AAAA レコード，NTMv4 レコードおよび NTMv6 レコードを追加で問い合わせることにより，CN の仮想 IPv4 アドレスや DC_{CN} の IPv4 アドレスなどのアドレス情報を取得する．その後，DNS サーバからの A レコードの応答を一時待避し，取得したアドレス情報をもとにトンネル構築処理を実行する．

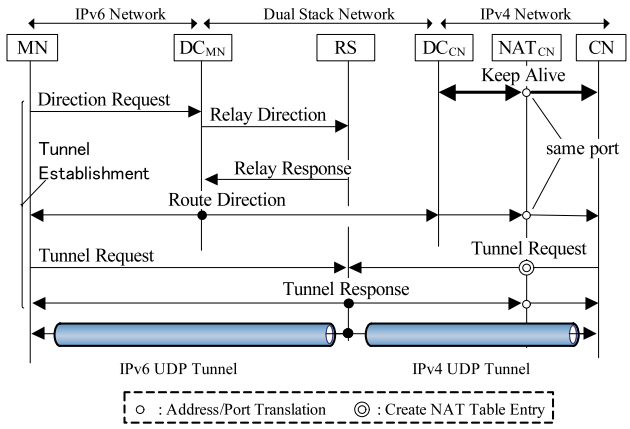

図 4 トンネル構築手順
Fig. 4 Tunnel establishment procedure.

図 4 に，IPv6 ネットワークに接続した MN が IPv4 プライベートネットワークに接続した CN との間にトンネル通信経路を確立するまでの様子を示す．各端末は以下の手順に従って，MN と CN 間にトンネル通信経路を確立する．

- 指示要求（Direction Request）
  MN は DC_{MN} へ Direction Request を送信し，CN と通信を行うためのトンネルの構築指示を要求する．Direction Request には，MN と CN の実 IP アドレスや仮想 IP アドレスなどの NTMv4/NTMv6 レコードに記載されたアドレス情報が含まれている．DC_{MN} はこの内容から通信端末の位置関係を認識し，トンネル通信時の経路を決定する．今回は IPv4 ネットワークと IPv6 ネットワーク間の通信であるため，RS を経由したトンネル通信経路となる．
- 中継指示（Relay Direction）
  DC_{MN} は，RS に対して MN と CN の通信を中継するよう指示を記載した Relay Direction を送信する．Relay Direction には PID_{MN-CN} および，MN と CN のアドレス情報が記載されており，これを受信した RS は DC_{MN} へ応答を返し，MN と CN から送信される Tunnel Request を待機する．
- 経路指示（Route Direction）
  RS からの応答を受信した DC_{MN} は，MN と CN へ Route Direciton を送信し，RS に対して Tunnel Request を送信するよう指示する．Route Direction には PID_{MN-CN}，通信相手のアドレス情報，トンネルの構築先の実 IP アドレス，およびトンネル通信時の暗号化に用いる共通鍵 CK_{MN-CN} などが記載されている．
- トンネル構築要求（Tunnel Request/Response）
  MN と CN は DC_{MN} の指示に従って RS へ Tunnel Re-

quest を送信する．NAT 配下に接続した CN から RS へ Tunnel Request を送信することにより，NAT_{CN} に CN と RS がトンネル通信を行うためのマッピング情報が生成され，CN と RS の間に NAT をまたがった IPv4 によるトンネルを構築することができる．また，MN が RS へ Tunnel Request を送信することにより，MN と RS 間には IPv6 によるトンネルが構築される．

NTM 端末は構築したトンネルの Path ID や通信相手の仮想 IP アドレス，トンネルの構築先の実 IP アドレス，暗号化に用いる共通鍵などをカーネル空間に保持しているトンネルテーブルへ登録する．また，RS はカーネル空間にリレーテーブルを保持しており，構築したトンネルの Path ID や転送先の実 IP アドレス，暗号化に用いる共通鍵などを登録する．

以上により，MN と CN がトンネル通信を行うための通信経路を確立することができる．A レコードの問合せをトリガーに処理を実行していた場合，MN は待避していた DNS サーバの応答に含まれる IP アドレスを $VIP4_{CN}$ に書き換え，DNS リゾルバへ渡す．これにより，MN のアプリケーションは CN の IPv4 アドレスとして $VIP4_{CN}$ を認識し，アプリケーション間では仮想 IPv4 アドレスに基づいた通信が開始される．

DNS リゾルバの実装によっては，A レコードの問合せが完了した後に AAAA レコードの問合せが実行される．この場合にはトンネル構築処理は行わず，構築済みのトンネル情報をもとに CN の仮想 IPv6 アドレスを記載した DNS 応答メッセージを生成し，DNS リゾルバへ渡す．これにより，アプリケーションは CN の IPv6 アドレスとして仮想 IPv6 アドレスを認識することになる．仮想 IPv6 アドレス宛のパケットが送信された場合には，A レコード問合せ時に構築されたトンネルにより送信する．

4.4 トンネル通信

IPv6 ネットワークに接続した MN から，IPv4 プライベートネットワークに接続した CN へトンネル通信を行う様子を**図 5** に示す．アプリケーションは，名前解決処理により取得した仮想 IPv4 アドレスまたは仮想 IPv6 アドレス宛に通信を開始する．この例ではアプリケーションが仮想 IPv4 アドレスに基づいた通信を行うため，アプリケーションが生成したパケットの送信元アドレスには $VIP4_{MN}$，宛先アドレスには $VIP4_{CN}$ が記載される．MN は宛先アドレスである $VIP4_{CN}$ をキーとしてトンネルテーブルを検索し，該当エントリに従ってカプセル化を行う．ここでは，実 IPv6 アドレス $RIP6_{RS}$ にてカプセル化したパケットを RS へ送信する．なお，カプセル化の際には IP ヘッダと UDP ヘッダ，Path ID などを記載した NTM ヘッダが付加され，共通鍵 CK_{MN-CN} により元パケットすべてが暗号化される．RS は，受信したパケットの NTM ヘッダに記載されている Path ID をキーとしてリレーテーブルを検索し，転送先の経路情報を取得する．RS は該当エントリに従って受信パケットをデカプセル化し，実 IPv4 アドレス $RIP4_{CN}$ にて再度カプセル化したあと，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 ヘッダに記載されている Path ID をキーにトンネルテーブルを検索し，該当エントリに従ってデカプセル化および復号処理を行う．その後，抽出したパケットを上位アプリケーションへ渡す．

以上により，IPv6 ネットワークに接続した MN と IPv4 ネットワークに接続した CN 間にて通信を行うことができる．アプリケーションは仮想 IPv4 アドレスに基づいた通信を行うため，NTM 端末が接続しているネットワークの違いによる影響を受けない．通信経路上に NAT が存在している場合であっても，NAT によるアドレス/ポート変換はカプセル化パケットの外側 IP ヘッダと UDP ヘッダに対して行われるため，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．

4.5 ネットワーク切替え時の動作

MN の移動や無線インタフェースの切替えにより，接続先が異なるネットワークへ切り替わった場合には，4.3 節と同様の手順により CN との間にトンネルを再構築する．トンネル構築時には MN と CN の位置関係に応じて DC が

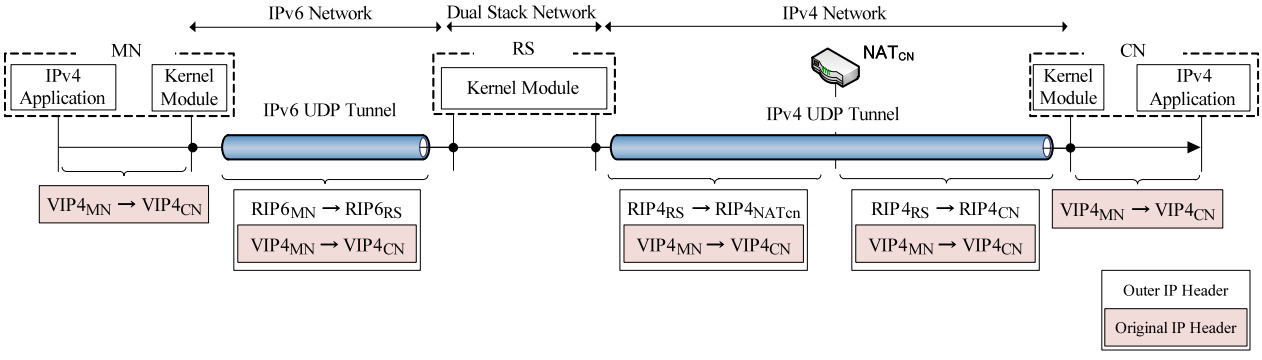

図 5 トンネル通信時のアドレス遷移
Fig. 5 Address transition in tunneling communication.

適切なトンネル通信経路を指示し，エンドツーエンドでトンネルを構築可能な場合には文献 [12] の手順によりトンネルを再構築する．このとき，CN のアドレス情報は取得済みであるため，名前解決処理を省略してトンネル構築のみを実行する．MN と CN のアプリケーションは仮想 IP アドレスに基づいた通信を行っているため，実 IP アドレスが変化してもその影響を受けることなく，通信を継続することができる．また，MN はトンネル通信経路の切替えと並行して 4.2 節で説明した登録処理を行い，DC_{MN} に登録したアドレス情報を更新する．つねに最新のアドレス情報を DC へ登録することにより，NTM 端末に対する到達性を確保する．

5. 実装・性能評価

5.1 実装

IPv4 環境における NTMobile はすでに Linux へ実装しており，有効性を確認済みである．本論文では，IPv4 と IPv6 が混在したネットワーク環境における動作検証および性能評価を行うため，各種プログラムを IPv4 と IPv6 の両方に対応するよう拡張した．

NTM 端末はカプセル化を行うカーネルモジュール，ネゴシエーションを行うデーモンプログラム（以後 NTM デーモン），および仮想インタフェースを実装することにより動作する．カーネルモジュールでは Netfilter によりパケットをフックし，カーネル空間においてカプセル化および暗号化を実行する．NTMobile ではカーネル空間でカプセル化処理を完結することにより，スループットの低下を抑制している [13]．

NTM デーモンは，DC へのアドレス情報の登録処理やトンネル構築処理を行う．IPv6 ネットワークへの移動時における IPv6 アドレス自動生成に要する時間は，ルータから送信される RA（Router Advertisement）の送信間隔による影響が大きいため，L2 ハンドオーバを検出した際に RA の送信を促す RS（Route Solicitation）を送信するよう NTM デーモンへ処理を追加した．なお，L2 ハンドオーバおよび IP アドレスの変化は，カーネル空間から送信されるリンク情報およびアドレス情報の変化通知を NTM デーモンが netlink ソケットにて受信することにより検出する．

RS は，トンネル通信の中継を行うカーネルモジュールとネゴシエーションを行うデーモンプログラムを実装することにより動作する．本論文では，新たにカーネルモジュールへ IPv4 ネットワークと IPv6 ネットワーク間のパケット転送機能を実装した．**図 6** に RS による IPv4/IPv6 ネットワーク間の転送処理を示す．RS は受信したパケットを Netfilter の `NF_INET_PRE_ROUTING` によってフックしてカーネルモジュールへ渡すことにより，転送処理を実行する．IPv6 ネットワークから IPv4 ネットワークへの転送を行う際には，受信した IPv6 パケットをデカプセル化し，

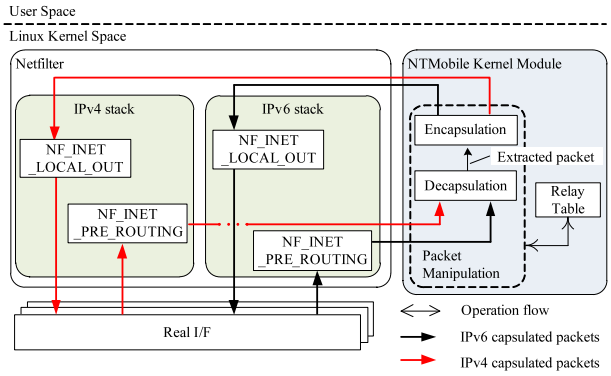

図 6 RS による IPv4/IPv6 ネットワーク間の転送処理
Fig. 6 Procedure of forwarding between IPv4 and IPv6 networks by RS.

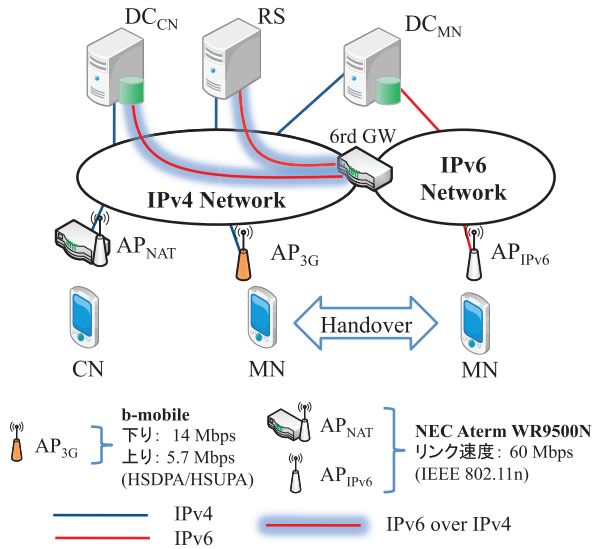

図 7 測定環境
Fig. 7 Evaluation environment.

抽出したパケットを実 IPv4 アドレスにて再度カプセル化したあと，IPv4 の `NF_INET_LOCAL_OUT` へ渡す．これにより，カプセル化パケットが実インタフェースから IPv4 ネットワークへ送信される．IPv4 ネットワークから IPv6 ネットワークへ転送する際にも，同様の手順により処理する．

5.2 実験環境

NTMobile を実装した Android 端末を用いて，IPv4/IPv6 混在環境における接続性の確立およびハンドオーバの動作検証と性能評価を行った．**図 7** および**表 1**，**表 2** にネットワーク構成と各装置の仕様を示す．MN と CN は市販の Android スマートフォンであり，NTMobile のカーネルモジュールを実装するために必要な Netfilter や Netlink などの機能を有効にして Linux カーネルを再構築した．また，通常の Android アプリケーションは Dalvik 仮想マシン上で動作するが，NTM デーモンはネイティブプログラム[*2]として実装した．DC および RS は VPS（Virtual

[*2] CPU が直接解釈可能な形式のバイナリプログラム．

表 1 DC および RS の装置仕様
Table 1 Device specifications of DC and RS.

	DC_{MN}	DC_{CN}, RS
Hardware	ServersMan@VPS（Entry プラン）	さくら VPS（1G プラン）
OS	CentOS 6.3 32 bit	CentOS 6.3 32 bit
Kernel	Linux 2.6.28	Linux 2.6.32
CPU	Intel Xeon L5630	Intel Xeon E5645
	仮想 8 コア 2.13 GHz	仮想 2 コア 2.4 GHz
Memory	1 GB	1 GB

表 2 MN および CN の装置仕様
Table 2 Device specifications of MN and CN.

	MN, CN
Hardware	Sumsung Galaxy Nexus (SC-03C)
OS	Android 4.0.2
Kernel	Linux 2.6.35
CPU	Texas Instruments OMAP4460 1.2 GHz
Memory	512 MB

Private Server）上に構築し，それぞれにグローバル IPv4 アドレスおよび IPv6 アドレスを割り当てた．なお，DC_{CN} および RS は 6rd（IPv6 rapid deployment）[*3] により IPv6 ネットワークへ接続した [17]．

アクセスポイント AP_{NAT} および AP_{IPv6} は市販のブロードバンドルータであり，AP_{NAT} の配下は IPv4 プライベートネットワークとして構築した．また，AP_{IPv6} はルータ機能を無効にして，一般的なアクセスポイントとして動作させた．なお，今回使用した Galaxy Nexus では，DHCP（Dynamic Host Configuration Protocol）による IPv4 アドレスの取得処理に失敗した際に AP から強制的に切断されてしまい，IPv6 ネットワークへ接続することができなかった．そのため，NTM 端末が AP_{IPv6} へ接続する際には，Wi-Fi インタフェースに IPv4 アドレスとして 0.0.0.0 を静的に設定した．MN と CN は各 AP へ IEEE 802.11n で接続し，暗号化および認証機能には WPA/WPA2-PSK（AES）を使用した．また，MN は Wi-Fi 無効時に HSPA 方式の 3G ネットワークへ接続する．

NTMobile のトンネル構築処理に使用する暗号化アルゴリズムとして AES-CFB，トンネル通信時には AES-CBC を設定し，認証アルゴリズムは HMAC-MD5，鍵長 128 bit とした．また，測定環境の特性を明確にするために，各端末間の RTT（Round-Trip Time）を測定した．RTT の測定には `ping` を使用し，1 秒間隔で 64 バイトのパケットを 100 回送受信した．**表 3** に測定した端末間の RTT を示す．

5.3 ネゴシエーションによるオーバヘッド

通信開始時に発生するオーバヘッドを明らかにするため

[*3] IPv4 トンネルを用いることにより，IPv4 ネットワークから IPv6 ネットワークへ接続する技術．

表 3 端末間の RTT
Table 3 RTT between the terminals.

	RTT [ms]		
	min	avg.	max
MN_{IPv4}–DC_{MN}	106.11	122.90	350.21
MN_{IPv4}–CN	114.01	143.16	621.25
MN_{IPv6}–DC_{MN}	13.09	23.01	200.78
MN_{IPv6}–RS	29.91	38.51	48.16
CN–DC_{CN}	14.59	21.31	49.81
CN–RS	28.87	39.38	106.78
DC_{MN}–DC_{CN}	11.91	14.12	38.43
DC_{MN}–RS	20.10	20.41	20.80

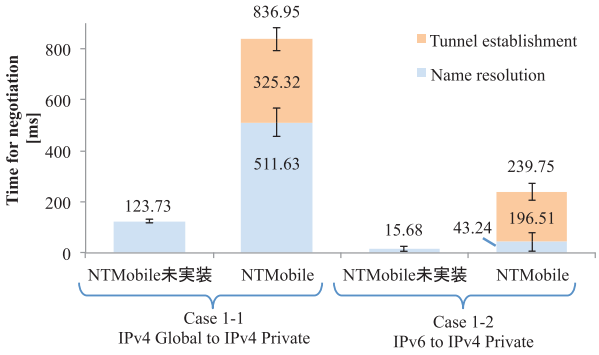

図 8 ネゴシエーションによるオーバヘッド時間
Fig. 8 Results of overhead time by negotiation.

に，MN と AP_{NAT} へ接続した CN の間にトンネル通信経路が確立されるまでに要する時間を測定した．測定は以下の 2 ケースにて，それぞれ NTMobile 未実装の場合と実装した場合について実施した．

Case 1-1 MN を 3G ネットワークへ接続
（IPv4 Global to IPv4 Private）

Case 1-2 MN を AP_{IPv6} へ接続
（IPv6 to IPv4 Private）

測定用に A レコードの問合せのみを行う Android 端末向けのネイティブプログラムを作成し，A レコードの問合せ前と問合せ結果取得後のタイムスタンプの差分から，通信開始時に発生するオーバヘッドを算出した．なお，NTMobie のネゴシエーション処理に要した時間を測定するために，NTM デーモンにイベントごとのタイムスタンプを出力するようプログラムを追加し，その差分から名前解決処理とトンネル構築処理に要した時間を算出した．

通信開始時に行うネゴシエーションによるオーバヘッドを 100 回測定した平均値を**図 8** に示す．なお，エラーバーは標準偏差を表す．NTMobile 未実装時の測定結果は通常の名前解決に要する時間であり，Case 1-1 では 123.73 ms，Case 1-2 では 15.68 ms で処理が完了した．ただし，この場合は CN に対する接続性を確保することができない．それに対して NTMobile 実装時は，名前解決処理に Case 1-1 では 511.63 ms，Case 1-2 では 43.24 ms を要した．これ

表 4 トンネル構築処理によるオーバヘッド時間の内訳
Table 4 Details of overhead time by tunnel establishment.

	Time [ms]	
	Case 1-1	Case 1-2
Direction Request ～Route Direction	193.47	68.46
Route Direction ～Tunnel Request/Response	120.55	125.92
Tunnel Request/Response ～DNS 応答メッセージの返答	11.30	2.13

は A レコードの問合せを行った後に，NTMv4 レコード，NTMv6 レコードおよび AAAA レコードを DNS サーバへ問い合わせるためである．

NTMobile 実装時にトンネル構築処理に要した時間は，Case 1-1 では 325.32 ms，Case 1-2 では 196.51 ms であった．トンネル構築処理に要した時間の内訳を**表 4** に示す．Case 1-1 では IPv4 グローバルネットワークと IPv4 プライベートネットワーク間の通信であるため，MN と CN は RS を経由せずに，エンドツーエンドでトンネルを構築した．一方，Case 1-2 では IPv4 ネットワークと IPv6 ネットワーク間の通信となるため，MN と CN は RS との間にトンネルを構築した．

MN が DC_{MN} へ Direction Request を送信し，DC_{MN} から Route Direction を受け取るまでに Case 1-1 では 193.47 ms，Case 1-2 では 68.46 ms を要した．この間に，DC_{MN} から DC_{CN} 経由で CN へ Route Direction が送信され，各装置でメッセージの暗号化・復号処理，および MAC の生成・検証処理が行われている．また，Case 1-2 では MN と CN が RS を経由したトンネル通信を行うため，DC_{MN} と RS 間で Relay Direction と Relay Response の送受信が行われている．

Case 1-1 では，MN は Route Direction を受信したあと，CN から送信される Tunnel Request を受信する．この時間が 120.55 ms であった．MN が Tunnel Response を CN へ返答してから，測定プログラムが処理を完了するまでに 11.30 ms を要した．この間に，トンネルテーブルの生成処理，仮想 IP アドレスを記載した DNS 応答メッセージの生成処理，および DNS リゾルバによる受信処理などを行っている．

Case 1-2 では，MN および CN は Route Direction を受信したあと，RS へ Tunnel Request を送信する．その後，RS から Tunnel Response を受信することにより，RS との間にトンネルを構築する．この時間が 125.92 ms であった．この間には，各装置でメッセージの暗号・復号処理，MAC の生成・検証処理，トンネルテーブルおよびリレーテーブルの生成などの処理が行われる．MN が Tunnel Response の受信処理を完了してから，測定プログラムが処理を完了するまでに 2.13 ms を要した．この間に DNS 応答メッセージの生成処理および DNS リゾルバによる受信処理が行われている．

IP を用いて携帯電話のマルチメディアサービスを実現する IMS（IP Multimedia Subsystem）では，端末間におけるセッション制御に SIP（Session Initiation Protocol）を用いている．文献 [18] によると，IMS は通信開始時に行うシグナリングに 2～3 秒程度を要するとされている．また，文献 [19] による調査では，モバイル環境を利用しているユーザの 8 割以上は，動画再生時に 10 秒程度の待ち時間を許容できるとされている．このような事例から判断すると，NTMobile による通信開始時のオーバヘッドは許容できる値であり，実用上は問題ないと考えられる．

5.4 通信断絶時間の測定

ハンドオーバ時には，L2 ハンドオーバや IP アドレスの取得処理に起因する通信断絶時間が発生する．これにともない，パケットロスが発生してアプリケーション間の通信に影響が及ぶ可能性がある．そこで，MN が CN との通信中に接続先のネットワークを切り替えることによって発生する通信断絶時間を測定した．CN はつねに AP_{NAT} へ接続しておき，MN の接続先のネットワークを次のように手動で切り替えた．

Case 2-1 3G ネットワーク経由での通信中に Wi-Fi を有効にし，接続先を AP_{IPv6} へ切り替える．

Case 2-2 AP_{IPv6} 経由での通信中に Wi-Fi を無効にし，接続先を 3G ネットワークへ切り替える．

MN と CN は iperf[*4] による TCP 通信を行い，TCP のシーケンス番号の変化および通信パケットから通信断絶時間を明らかにした．TCP シーケンス番号を観測するために，カプセル化を行う前に TCP シーケンス番号をカーネルメッセージへ出力するよう NTMobile のカーネルモジュールを修正した．また，パケットの送受信をキャプチャするために，MN と CN へ LAN アナライザアプリケーションである tcpdump をインストールした．なお，キャプチャしたデータの解析には Wireshark[*5] を使用した．

表 5 および**表 6** にハンドオーバにともなう通信断絶時間を 10 回測定した結果を示す．Case 2-1（IPv4 ネットワークから IPv6 ネットワークへのハンドオーバ）では平均で 7.46 秒間通信が断絶され，Wi-Fi を有効にしてから IPv6 アドレスを取得するまでに平均 4.01 秒を要した．**図 9** に Wi-Fi を有効にしてからトンネル構築処理が開始されるまでのシーケンスと処理時間の内訳を示す．MN は IPv6 アドレスを生成したあと，そのアドレスをターゲットとした NS（Neighbor Solicitation）を送信し，平均で 1.69 秒後にトンネル構築処理が開始された．これは，アドレス重複チェック DAD（Duplicated Address Detection）によるも

*4 http://sourceforge.net/projects/iperf/
*5 http://www.wireshark.org/

表 5 Case 2-1：IPv4 ネットワークから IPv6 ネットワークへのハンドオーバにともなう通信断絶時間の測定結果

Table 5 Case 2-1: Results of suspended time by handover from IPv4 network to IPv6 network.

	Time [sec]		
	min	avg.	max
無線 AP への接続処理	1.14	1.50	1.83
IPv6 アドレス取得処理	0.40	2.51	4.17
トンネル構築処理	0.34	0.42	0.67
TCP の再送待機	0.33	3.37	5.92
通信断絶時間	3.75	7.46	10.72

表 6 Case 2-2：IPv6 ネットワークから IPv4 ネットワークへのハンドオーバにともなう通信断絶時間の測定結果

Table 6 Case 2-2: Results of suspended time by handover from IPv6 network to IPv4 network.

	Time [sec]		
	min	avg.	max
3G ネットワークへの接続処理	5.28	5.45	5.69
トンネル構築処理	0.17	0.27	0.38
TCP の再送待機	2.02	3.86	5.28
通信断絶時間	7.74	9.58	10.92

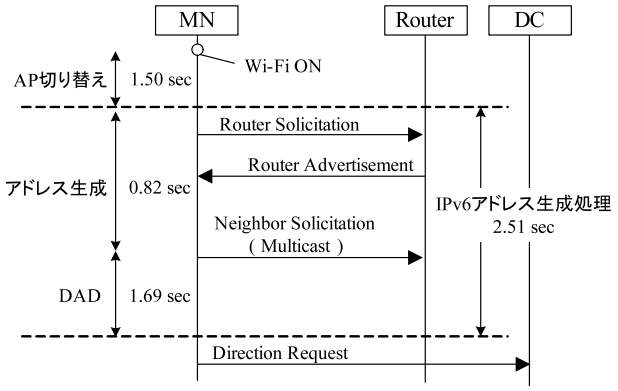

図 9 IPv6 におけるハンドオーバの処理

Fig. 9 Handover flow in IPv6.

のである [20]．MN で生成された IPv6 アドレスは，DAD による処理が完了するまでの間は使用することができない．この処理が完了した後，NTMobile によるトンネル構築処理が開始されたが，全体の 5%程度の時間で処理を完了した．

Case 2-2（IPv6 ネットワークから IPv4 ネットワークへのハンドオーバ）では Wi-Fi を無効にしてから平均 9.58 秒間，通信が断絶された．**図 10** に IPv6 ネットワークから IPv4 ネットワークへのハンドオーバによる TCP シーケンス番号の変化の様子を示す．Wi-Fi を無効にしてから IP アドレスを取得するまでに，TCP による再送が 4 回行われた．MN の Wi-Fi をオフにしてから 3G ネットワークへ接続し，IPv4 アドレスを取得するまでに平均 5.45 秒を要し，全体の 57%程度の時間を占めている．また，IP アドレス取得後に NTMobile によるトンネル再構築処理が実行され，平均で 0.27 秒を要したが，全体の 3%程度の時間で処理が完了した．トンネルの再構築完了後，すぐにはアプリケーションによる通信は再開されず，平均で 3.86 秒後にアプリケーションによる通信が再開された．これは，TCP の再送制御が機能したものと考えられる．

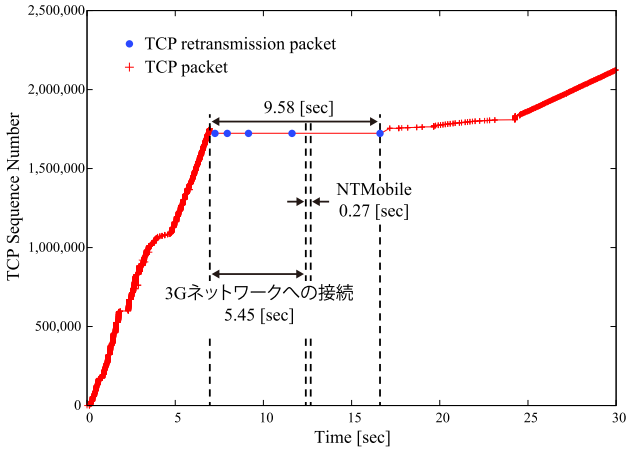

図 10 IPv6 ネットワークから IPv4 ネットワークへのハンドオーバによる TCP シーケンス番号の変化

Fig. 10 Changes of TCP sequence number by handover from IPv6 network to IPv4 network.

Wi-Fi を用いて IPv4 ネットワークへ接続する際には，DHCP により IPv4 アドレスを取得する．文献 [21] によると，DHCP にて IP アドレスを取得する際には，ネットワークに接続してから 1〜10 秒程度待機したあとに処理を開始すべきであるとされている．そのため，通信中に Wi-Fi により IPv4 ネットワークへハンドオーバした際には，アドレス取得処理に最大で 10 秒程度を要し，通信が 10 秒以上断絶するものと考えられる．

5.5 今後の検討課題

5.4 節に示した通信断絶時間の測定結果より，ハンドオーバ時に行う NTMobile による処理はわずかな時間で完了するが，無線インタフェースの切替えおよび IP アドレスの取得処理に 4.01〜5.45 秒を要し，通信断絶時間の半分以上を占めていることが分かった．リアルタイム性を要する音声通信や動画通信の利用を想定すると，通信断絶時間の削減が必要である．

IEEE 802.21 ではリンク情報を抽象化することにより，異なる無線システム間においてシームレスハンドオーバを実現することができる [22]．文献 [23] では，SIP-based Mobility と IEEE 802.21 を組み合わせることにより，ハンドオーバ時に発生する通信断絶時間を 4 秒から 20 ms まで短縮している．また，IEEE 802.11ai では，Wi-Fi による認証・接続にかかる時間を従来の 300 分の 1 まで短縮する高速認証技術が議論されている [24]．

IETF では DAD 処理を最適化する Optimistic DAD が

定義されており，生成直後のアドレスの状態を Optimistic とすることにより，生成した IPv6 アドレスを即座に使用可能にする [25]．これにより，DAD による待機時間をなくすことができる．

また，著者らは Wi-Fi や 3G などの異なる無線インタフェースを連携して利用することにより，通信断絶時間やパケットロスが発生しないシームレスハンドオーバ手法を提案している [26]．今後はこれらの手法を用いることにより，通信断絶時間を削減するための検討が必要である．

6. おわりに

本論文では，IPv4/IPv6 混在環境において相互接続を確保して，移動透過性を実現する NTMobile を Android 端末へ実装し，動作検証および性能評価を行った．動作検証により，NAT や IPv4/IPv6 ネットワークの違いに影響されることなく接続性を確保し，移動透過性を実現可能なことを確認した．今後は残された課題を解決するとともに，大規模環境における通信性能およびスケーラビリティの評価を行っていく予定である．

謝辞 本研究の一部は，総務省戦略的情報通信研究開発推進制度（SCOPE）の支援を受けて実施された．

参考文献

[1] Jiang, S., Guo, D. and Carpenter, B.: An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition, RFC 6264, IETF (2011).
[2] Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, IETF (2010).
[3] 鈴木秀和，宇佐見庄五，渡邊 晃：外部動的マッピングにより NAT 越え通信を実現する NAT-f の提案と実装，情報処理学会論文誌，Vol.48, No.12, pp.3949–3961 (2007).
[4] 宮崎 悠，鈴木秀和，渡邊 晃：端末の改造が不要な NAT 越え通信システム NTSS の提案と評価，情報処理学会論文誌，Vol.51, No.9, pp.1234–1241 (2010).
[5] 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).
[6] Perkins, C.: IP Mobility Support for IPv4, RFC 3220, IETF (2002).
[7] Johnson, D., Perkins, C. and Arkko, J.: Mobilit Support in IPv6, RFC 3775, IETF (2004).
[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] 関 顕生，岩田裕貴，森廣勇人，前田香織，近堂 徹，岸場清悟，西村浩二，相原玲二：IPv4 拡張した移動透過通信アーキテクチャ MAT の設計と性能評価，情報処理学会論文誌，Vol.52, No.3, pp.1323–1333 (2011).
[10] 竹内元規，鈴木秀和，渡邊 晃：エンドエンドで移動透過性を実現する Mobile PPC の提案と実装，情報処理学会論文誌，Vol.47, No.12, pp.3244–3257 (2006).
[11] Soliman, H.: Mobile IPv6 Support for Dual Stack Hosts and Routers, RFC 5555, IETF (2009).
[12] 鈴木秀和，上醉尾一真，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，情報処理学会論文誌，Vol.54, No.1, pp.367–379 (2013).
[13] 内藤克浩，上醉尾一真，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，情報処理学会論文誌，Vol.54, No.1, pp.380–393 (2013).
[14] 納堂博史，鈴木秀和，内藤克浩，渡邊 晃：NTMobile における自律的経路最適化の提案，情報処理学会論文誌，Vol.54, No.1, pp.394–403 (2013).
[15] Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
[16] Wakikawa, R., Kuntz, R., Zhu, Z. and Zhang, L.: Global HA to HA Protocol Specification, draft-wakikawa-mext-global-haha-spec-02, IETF (2011).
[17] Townsley, W. and Troan, O.: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) Protocol Specification, RFC 5969, IETF (2010).
[18] Munir, A. and Gordon-Ross, A.: SIP-Based IMS Signaling Analysis for WiMax-3G Interworking Architectures, *IEEE Trans. Mobile Computing*, Vol.9, No.5, pp.733–750 (2010).
[19] Krishnan, S.S. and Sitaraman, R.K.: Video stream quality impacts viewer behavior: Inferring causality using quasi-experimental designs, *Proc. 2012 ACM Conference on Internet Measurement*, pp.211–224, ACM (2012).
[20] Thomson, S. and Narten, T.: IPv6 Stateless Address Autoconfiguration, RFC 2462, IETF (1998).
[21] Droms, R.: Dynamic Host Configuration Protocol, RFC 2131, IETF (1997).
[22] IEEE 802.21: MEDIA INDEPENDENT HANDOVER SERVICES, available from ⟨http://www.ieee802.org/21/⟩.
[23] Dutta, A., Das, S., Famolari, D., Ohba, Y., Taniuchi, K., Kodama, T. and Schulzrinne, H.: Seamless Handover across Heterogeneous Networks – An IEEE 802.21 Centric Approach, *WPMC2005*, Vol.31, No.TM11-4, pp.VI-31–VI-35 (2005).
[24] IEEE 802.11ai (Fast Initial Link Set-up), available from ⟨http://www.ieee802.org/11/Reports/tgai_update.htm⟩.
[25] Moore, N.: Optimistic Duplicate Address Detection (DAD) for IPv6, RFC4429, IETF (2006).
[26] 福山陽祐，上醉尾一真，旭 健作，鈴木秀和，内藤克浩，渡邊 晃：Android 端末における Wi-Fi/3G 間のシームレスハンドオーバの提案と実装，情報処理学会研究報告，Vol.2012-MBL-65, No.27, pp.1–8 (2013).

推薦文

本研究は IPv4 や IPv6 が混在する環境での Nat Traversal の研究であり，現実的な問題に対処した有用性の高い論文といえる．また，実現のための機能要件もまとめられており，実用化が期待できる．よって，ここに研究会推薦論文として推薦する．

（モバイルコンピューティングとユビキタス通信研究会主査 竹下 敦）

上醉尾 一真 （学生会員）

2012 年名城大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科情報工学専攻在学中．モバイルネットワークに関する研究に従事．IEEE 会員．

鈴木 秀和 （正会員）

2004 年名城大学理工学部情報科学科卒業．2006 年同大学大学院理工学研究科情報科学専攻修了．2009 年同大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．2008 年日本学術振興会特別研究員．2010 年より名城大学理工学部助教．博士（工学）．ネットワークセキュリティ，モバイルネットワーク，ホームネットワーク等の研究に従事．電子情報通信学会，IEEE 各会員．

内藤 克浩 （正会員）

1999 年慶應義塾大学理工学部電気工学科卒業．2004 年名古屋大学大学院工学研究科情報工学専攻博士課程後期課程修了．同年，三重大学工学部電気電子工学科助手．2007 年同大学大学院工学研究科電気電子工学専攻助教．2011 年カリフォルニア大学ロサンゼルス校客員研究員．博士（工学）．無線ネットワーク，ネットワークモビリティの研究に従事．電子情報通信学会，IEEE 各会員．

渡邊 晃 （正会員）

1974 年慶應義塾大学工学部電気工学科卒業．1976 年同大学大学院工学研究科修士課程修了．同年三菱電機株式会社入社後，LAN システムの開発・設計に従事．1991 年同社情報技術総合研究所に移籍し，ルータ，ネットワークセキュリティ等の研究に従事．2002 年より名城大学理工学部教授．情報処理学会モバイルコンピューティングとユビキタス通信研究会主査．博士（工学）．電子情報通信学会，IEEE 各会員．