情報処理学会論文誌 Vol.54 No.1 1–13 (Jan. 2013)

推薦論文

NTMobileにおける通信接続性の確立手法と実装

鈴木 秀和[1,a)] 上醉尾 一真[1] 水谷 智大[1,†1] 西尾 拓也[2] 内藤 克浩[2] 渡邊 晃[1]

受付日 2012年4月5日, 採録日 2012年10月15日

概要：モバイルインターネット環境の普及に伴い，ユーザが通信中に様々なネットワークへ移動することが考えられる．本論文では，IPv4 ネットワークにおけるグローバルアドレスやプライベートアドレスの違いに関わりなく，ノードの通信接続性の確立と移動透過性を同時に実現する NTMobile（Network Traversal with Mobility）を提案する．NTMobile ではノード間にトンネルを構築した上で仮想 IP アドレスを用いたコネクションを確立する．本論文ではアドレス空間が異なる IPv4 ネットワークにおいて NTM ノード間の通信接続性を確立する手法を示す．提案方式を Linux に実装することにより，NAT 配下のノードに対して低オーバヘッドでコネクションを確立できることを確認した．

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，仮想 IP アドレス，トンネル

Design and Implementation of Establishment Method of Connectivity on NTMobile

Suzuki Hidekazu[1,a)] Kamienoo Kazuma[1] Mizutani Tomohiro[1,†1] Nishio Takuya[2]
Naito Katsuhiro[2] Watanabe Akira[1]

Received: April 5, 2012, Accepted: October 15, 2012

Abstract: With the spread of mobile Internet environment, it is thought that users are going to move to various networks during communication. In this paper, we propose a network architecture called “Network Traversal with Mobility” (NTMobile) that can achieve both connectivity and mobility of nodes in IPv4 networks regardless of global addresses and private addresses. An NTMobile node creates a tunnel with a correspondent node, and establishes a connection with their virtual IP addresses through the tunnel. This paper describes the establishment method of the connectivity between NTMobile nodes in IPv4 networks having different address spaces. We have implemented the proposed method on Linux, and confirmed that the node can establish a connection with the correspondent node located behind the NAT router with low latency.

Keywords: mobile network architecture, mobility, NAT traversal, virtual IP address, tunnel

1. はじめに

近年，スマートフォンやタブレットなど高性能な携帯端末が急激に普及しつつある．これらの移動端末は無線 LAN だけでなく，3G や WiMAX，LTE（Long Term Evolution）などの無線ブロードバンドサービスといった複数の手段によりインターネットに接続することが可能である．そのため，利用者の位置や無線ネットワークの状況に応じて最適な通信品質を選択するために，通信メディアを切り替えて通信を行う場面が一般的になりつつある．このように異なる無線システムを切り替える動作を垂直ハンドオーバと呼ぶが，無線システムを切り替えると同時に移動端末が接続するネットワークも変化するため，移動端末の IP アドレスが変化してしまう．インターネットで使用されている TCP/IP は IP アドレスを用いて通信端末間のコネクショ

[1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 468–8502, 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
[†1] 現在，株式会社システムコーディネイト
Presently with System Coordinate Co., Ltd.
[a)] hsuzuki@meijo-u.ac.jp

ンを管理しているため，ネットワークの移動が発生するとコネクションが切断されてしまう．この問題を解決する技術を移動透過性技術と呼び，多くの実現手法が提案されている [1].

一方，現在の IP ネットワークの状況に着目すると，IPv4 アドレスの枯渇がいよいよ目前に迫ってきており，IPv6 への移行が徐々に進みつつある．しかし，IPv6 は IPv4 との下位互換性がない独立したプロトコルとして定義されているため，現在の IPv4 ネットワークを即座に IPv6 ネットワークへ移行することができない．そのため当分の間，IPv4 ネットワークと IPv6 ネットワークが混在した環境が続くものと想定されている．また，IPv4 ネットワークではグローバル IP アドレスの数が十分にないため，NAT（Network Address Translation）によりプライベートネットワークを構築して運用が行われている．このような異なるアドレス空間/アドレス体系が混在する環境において移動透過性を実現するためには，通信開始時や移動時における端末間の接続性を確実に確立する必要がある．

本論文では，IPv4 ネットワークを対象とした移動透過性技術における端末間の通信接続性に焦点を当てて議論を進める．IPv4 を対象とした移動透過性技術には，Mobile IPv4 [2], MATv4 [3], Mobile PPCv4 [4] などがある．IPv4 ネットワークではグローバルネットワークとプライベートネットワークをまたがって移動することが考えられ，このような移動では移動前と移動後の通信経路のどちらかに NAT が介在することになる．移動透過性技術では移動ノード（MN; Mobile Node）の IP アドレスの変化を管理する装置を用意し，MN はハンドオーバ時に IP アドレスの変化を管理装置に通知する必要がある．ここで，MN と管理装置の間に NAT が存在すると，通知する IP アドレスと実際の通信で用いられる IP アドレスが一致せず，移動前後の IP アドレスの関係を正しく管理できないという課題が生じる．この問題を解決するために，Mobile IPv4 では移動通知を UDP によりカプセル化したり，NAT に独自の機能を追加する等の対策がある [5], [6], [7]．しかし，管理装置（HA; Home Agent）を常に経由した冗長な通信となってしまったり，MN が特殊な NAT ルータの配下でしか移動透過性を実現できないなどの課題がある．MATv4 は MN と通信相手ノード（CN; Correspondent Node）および管理装置の間の通信経路上に NAT が存在しないことを前提としている．これは NAT 配下のノードへの到達性を確保する手段を持ち合わせていないためであり，結果として NAT をまたがった移動はできない．

Mobile PPCv4 は著者らが提案している移動透過性技術であり，アドレスの変化を MN と CN 間で直接交換することにより，特別なアドレス管理装置を必要としない方式である．Mobile PPCv4 では Hole Punching を応用した手法や，NAT 越えを実現する NAT-f（NAT-free protocol）[8] を組み合わせた方式を提案してきた [9], [10]．しかし，近年の NAT ルータに標準的に搭載され始めている SPI（Stateful Packet Inspection）と呼ぶフィルタリング技術により，移動後の TCP パケットが破棄されてしまったり，NAT-f を実装した特別な NAT ルータが設置されていなければ接続性を確保できないなどの課題がある．

これらの課題を解決するために，本論文では NAT に一切の機能を追加することなく，かつ移動先ネットワークを限定しない移動透過性技術として NTMobile（Network Traversal with Mobility）を提案する．NTMobile では，エンドノードに仮想 IP アドレスを割り当てることにより，移動時の IP アドレスの変化を隠蔽し，IP 層より上位層ではアドレス空間に依存しない仮想的なコネクションを確立する．このコネクションを実ネットワーク上で確立するために，通信開始時にエンドノード間で UDP トンネルを構築する．通信開始ノードは DNS による名前解決時に通信相手ノードに接続するために必要なアドレス情報を収集し，NAT の有無に応じて最適経路を実現できるトンネルを構築する．これにより，エンドノード間の通信経路上に NAT が存在しても，アドレス空間に影響されない相互接続を実現する．なお，ノードが移動した際には通信開始時と同じトンネル構築手順を行うことにより，トンネル経路の再構築と移動透過性を同時に実現することができる．そのため本論文では通信開始時と移動時に行うトンネル構築方法と実装について詳述する．

以下，2 章で提案方式の概要，3 章で通信接続性の確立手法，4 章で実装方法とプロトタイプシステムの動作結果，およびその性能評価を示す．5 章で関連技術を取り上げ，6 章でまとめる．

2. NTMobile の概要

NTMobile は次の要求を満たすことができるネットワークアーキテクチャである．

通信接続性の実現： 通信相手 NTM ノード [*1]がグローバルネットワークだけでなく，プライベートネットワークに存在していても，通信を開始することができる．

移動透過性の実現： NTM ノードは通信中に別のグローバルネットワークおよびプライベートネットワークにハンドオーバできる．

図 1 に NTMobile の概要を示す．NTM ノードの他にシステムを構成する装置として，NTM ノードのアドレス情報を管理する Direction Coordinator（DC），異なる NAT 配下のプライベートネットワークに存在する NTM ノード間の通信を中継する Relay Server（RS）を設置する．NTM ノードはパケットロスのないシームレスハンドオーバを実現するために，無線 LAN や 3G，WiMAX など複数の

[*1] NTMobile 実装したノードを NTM ノードと呼ぶ.

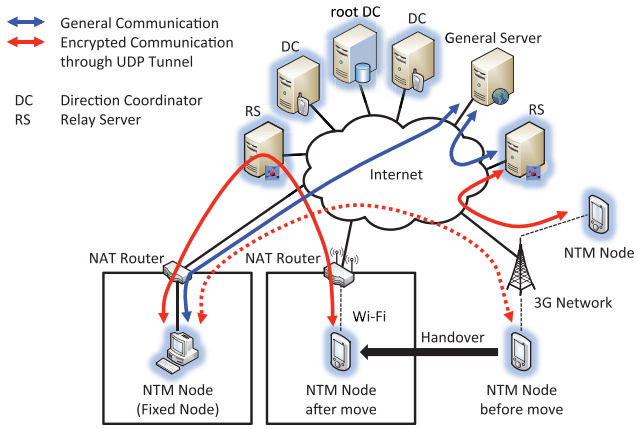


図 1 NTMobile の概要
Fig. 1 Overview of NTMobile system.

無線通信技術を実装しているものと想定する．プライベートネットワークを構成する NAT は，SPI などのフィルタリング機能を実装している一般的な NAT ルータであり，NTMobile に関わる特別な機能は一切持たない．

すべての NTM ノードはネットワーク接続時に DC に対してアドレス登録処理を行う．アドレス登録処理では，NTM ノードの実 IP アドレス，ノード ID，FQDN に加えて，NTM ノードがプライベートネットワークに存在する場合は NAT のグローバル IP アドレスが登録される．この時，NTM ノードは DC から仮想 IP アドレスが割り当てられ，NTM ノード間の通信に利用する．NTM ノードは通信開始時に相手 NTM ノードとの間に UDP トンネルを構築し，仮想 IP アドレスを用いてコネクションを確立する．UDP トンネルを用いることにより，NTM ノード間の通信経路上に SPI に対応した NAT が存在しても確実にコネクションの確立を実現することができる．また，仮想 IP アドレスを用いることにより，移動に伴う NTM ノードの実 IP アドレスの変化を隠蔽して移動透過性を実現する．さらに NTM ノード間の通信はエンドエンドで暗号化され，盗聴の防止や改ざんの検出が可能である．

NTMobile では，できる限りエンドツーエンド通信が行えるように，通信ペアとなる NTM ノードが存在するネットワークに応じて，DC から NTM ノードに最適なトンネル構築を指示する．この指示は通信開始時だけでなく，NTM ノードが様々なネットワークへ移動した時にも行われる．どちらか一方の NTM ノードがグローバルネットワークに存在すれば，他方は NAT 配下のプライベートネットワークにいても，RS を中継しない最適経路による通信を実現できる．なお，RS による中継通信が行われるのは，2 台の NTM ノードが異なるプライベートネットワークに存在する場合と，通信相手が NTMobile に対応しない一般ノードの場合だけである．後者の場合は，RS が NTM ノードの代理で通信を行うため，一般ノードは通信相手を RS と認識する．そのため，一般の通信相手ノードに対して NTM ノードのアドレスは隠蔽されるため，NTM ノードは移動しても通信を継続することができる．

NTM ノードは移動を前提としているが，例えばデスクトップ PC のように移動することがないノードの場合は移動のサポートに係わる機能を除いたモードとしても動作できる．このような NTM ノードは NAT 配下のプライベートネットワークに存在していても，外部の NTM ノードからの接続性を確立することができる．また，移動しない NTM ノードが一般ノードと通信する場合は，仮想 IP アドレスを用いず，RS を中継しない通常のエンドツーエンド通信を行う．

DC は Dynamic DNS 機能を有しており，NTM ノードのアドレス管理や暗号鍵の生成，配布も行う．この他に，NTM ノードに割り当てる仮想 IP アドレスプールの保持や，NTM ノードに対してトンネル構築指示を行う役割を担っている．各 DC が管理する仮想 IP アドレスプールが重複しないよう，root DC と呼ぶ親 DC を導入し，root DC の管理者が各 DC へ仮想サブネットスコープの管理を委譲することを想定している．これにより，NTM ノードに割り当てられる仮想 IP アドレスは重複がないことが保証される [11]．DC と RS は全てのノードがアクセス可能なグローバルネットワーク上に設置する．また，ネットワークの規模に応じて複数台設置することにより，DC や RS に発生する処理負荷を分散することができる．

3. 通信接続性の確立手法

本章では，NTMobile における NTM ノード間のコネクション確立手順について詳述する．NTMobile では通信を行うペアが本方式に対応していれば，双方とも移動が可能であるが，以後の説明では通信開始側 NTM ノードを MN，通信相手側ノードを CN として説明する．なお，用語の定義として，MN と CN を区別しない場合は NTM ノードと表記し，本論文で用いる記号は付録 A.1 に示す．

3.1 前提条件

NTM ノードはネットワーク接続時に Registration Request/Response によるアドレス登録処理 [11] を完了しており，DC_N には NTM ノード N のアドレス情報が NTMobile 専用レコード（NTM レコード）として登録されているものとする．ここで，アドレス情報とはノード ID NID_N，実 IP アドレス RIP_N，仮想 IP アドレス VIP_N，NAT のグローバル IP アドレス RIP_{NAT_N}[*2]，および DC_N の IP アドレス RIP_{DC_N} である．ノード ID とは NTM ノードを一意に識別する値であり，UUID（Universally Unique

[*2] NTM ノードがプライベートネットワークに存在している場合，DC_N は受信した Registration Request の送信元 IP アドレスから取得する．なお，NTM ノードがグローバルネットワークに存在する場合は，自身のグローバル IP アドレス RIP_N となる．

表 1 NTMobile で想定する通信パターンとトンネル経路
Table 1 Communication patterns and its tunnel route in NTMobile.

Pattern	Location of Initiator's NTM Node	Location of Correspondent Node	Tunnel Route
1	Global	Global (NTM node)	End-to-End
2	Private	Global (NTM node)	End-to-End
3	Global	Private (NTM node)	End-to-End
4	Private1	Private2 (NTM node)	via RS
5	Private2	Private2 (NTM node)	End-to-End/via RS
6	Anywhere (Mobile Node)	Global (General node)	via RS
7	Anywhere (Fixed Node)	Global (General node)	End-to-End (No Tunnel)

Identifier) [12] を採用している．NTM ノードのホスト名を新規に登録する際に，DC が NTM ノードの FQDN をもとに SHA-1 を用いて生成する．UUID は一元管理をすることなく，128bit の一意な値を生成することができる．NTM ノードが使用する仮想 IP アドレス VIP_N は DC_N により割り当てられ，重複がないものとする．

なお，DC_N と NTM ノード N 間，各 DC 間および各 DC と RS 間には信頼関係があるものと仮定する．また，NTM ノード N がプライベートネットワークに存在する場合は，DC_N に対して Keep Alive を実行して NTMobile における制御チャネルを維持する．

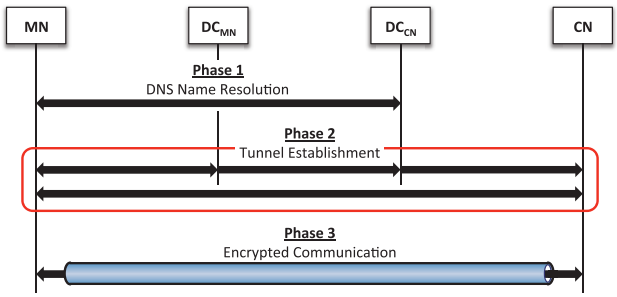


図 2 NTMobile シーケンス
Fig. 2 NTMobile sequence.

3.2 通信シーケンス

NTM ノードが通信を開始するまでの手順は**図 2** に示す名前解決，トンネル構築，暗号化通信の 3 つのフェーズで構成される．IPv4 環境における NTMobile アーキテクチャでは**表 1** に示す通信パターンを想定しており，NTM ノードが存在しているネットワークのアドレス空間の違いに応じて，最適な通信経路が確立できるようにトンネル確立フェーズのシーケンスが変化する．基本的な考え方として，通信ペアとなる NTM ノードのうち，どちらか一方がグローバルネットワークに接続している場合は，エンドエンドでトンネルを構築する．両 NTM ノードともプライベートネットワークに存在したり，通信相手が一般ノードの場合は RS を中継したトンネルを構築する．

本論文では，NTMobile 対応の MN・CN の一方または両方が NAT 配下のプライベートネットワークに存在している 3 つのパターン（Pattern 2〜4）の場合を中心に取り上げて，通信シーケンスを示す．

3.2.1 名前解決フェーズ

MN のアプリケーションは CN の IP アドレス RIP_{CN} を取得するために，DNS による CN の名前解決を行う．DC_{CN} は RIP_{CN} が登録されている A レコードを MN へ応答する．MN は RIP_{CN} が記載された DNS クエリ応答を DNS リゾルバへ渡す前に，一時待避してから DC_{CN} へ NTM レコードの問合せを行う．CN が NTM ノードであれば，MN は DC_{CN} から NTM レコードを入手でき，CN に関するアドレス情報（NID_{CN}，RIP_{CN}，VIP_{CN}，$RIP_{NAT_{CN}}$[*3]，$RIP_{DC_{CN}}$）を取得する．次に，MN は 3.2.2 項に示すトンネル構築フェーズを実行し，完了後に待避していた DNS クエリ応答メッセージに記載されている RIP_{CN} を仮想 IP アドレス VIP_{CN} に書き換えてから，DNS リゾルバへ渡す．これにより，MN の上位アプリケーションは CN のアドレスを VIP_{CN} と認識することになる．

NTM レコードの応答が得られない場合，MN は RS とトンネルを構築するためにトンネル構築フェーズを実行する．このとき，DC が CN が一般ノードであると認識すると，DC がプールしている仮想 IP アドレスを一時的に CN に対応付けて MN へ通知する．MN はトンネル構築完了後，DNS クエリ応答に記載されている RIP_{CN} を，DC から通知された CN の仮想 IP アドレス VIP_{CN} に書き換えてから DNS リゾルバへ渡す（Pattern 6）．なお，MN が移動をサポートしない NTM ノードの場合は，トンネル構築処理や DNS クエリ応答の書き換えを行わず，RIP_{CN} をそのまま DNS リゾルバへ渡す（Pattern 7）．

3.2.2 トンネル構築フェーズ

MN は DC_{MN} へ Direction Request メッセージを送信する．このメッセージには MN 自身のアドレス情報[*4]と

[*3] CN がプライベートネットワークに存在している場合．グローバルネットワークの場合は，RIP_{CN} となる．
[*4] アドレス登録処理時にキャッシュした MN に関する NTM レコードの情報．

NTM レコードにより入手した CN のアドレス情報，および CN との間に構築するトンネルの識別子（Path ID）PID_{MN-CN} が記載されている．ここで，Path ID は NTM ノードが疑似乱数で生成した UUID であり，一意性が保証されている．DC_{MN} は受信した MN と CN のアドレス情報から，表 1 のどの通信パターンに当てはまるかを判断し，各パターンに応じたトンネル構築手順を決定する．その後，Route Direction メッセージにより各 NTM ノードにトンネル構築動作の指示と，DC_{MN} が生成した共通鍵 CK_{MN-CN} の配布を行う．

図 3 に 3 つの通信パターンを例にトンネル構築手順を示す．これらのパターンでは NAT の配下に存在する NTM ノードに対して Route Direction を送信する必要がある．プライベートネットワークに存在する NTM ノード N は定期的に DC_N に対して Keep Alive を実行しているため，NAT_N には NTM ノード N 宛の制御メッセージを受け入れるためのポートが常に維持されている．そのため，DC_N は NAT_N に開けられているポート番号に向けて Route Direction を送信することにより，NTM ノード N に対して動作指示を行うことができる．NTM ノードに対する指示は下記の通りである．

Private-to-Global (Pattern 2)： NTM ノード間で直接トンネルを構築するが，MN はプライベートネットワークに存在するため，以後のシーケンスは MN 側から開始する必要がある．そのため，DC_{MN} は Route Direction により，CN に対して MN からの Tunnel Request メッセージを受信するよう DC_{CN} 経由で指示する．一方，MN に対しては CN へ Tunnel Request を送信するよう指示する．

Global-to-Private (Pattern 3)： Pattern 2 と同様に MN と CN 間のエンドエンドでトンネルを構築する．このとき，CN はプライベートネットワークに存在するため，以後のシーケンスは CN 側から開始する必要がある．そのため，DC_{MN} は Route Direction により，MN には CN からの Tunnel Request を受信するよう指示する．一方，CN には DC_{CN} を経由して，MN へ Tunnel Request を送信するよう指示する．

Private-to-Private (Pattern 4)： MN と CN が別々のプライベートネットワークに存在するため，Relay Server との間にトンネルを構築する．このとき，以後のシーケンスは MN，CN 両側から開始する必要がある．そのため，DC_{MN} は Relay Direction メッセージにより，RS に対して MN と CN からの Tunnel Request を受信するよう指示する．RS から Relay Response を受信後，さらに Route Direction により，MN と CN 双方に対して RS へ Tunnel Request を送信するよう指示すると共に，共通鍵 CK_{MN-CN} を配布する．以上の処理により，MN と CN は RS との間で共通鍵を共有することができる．

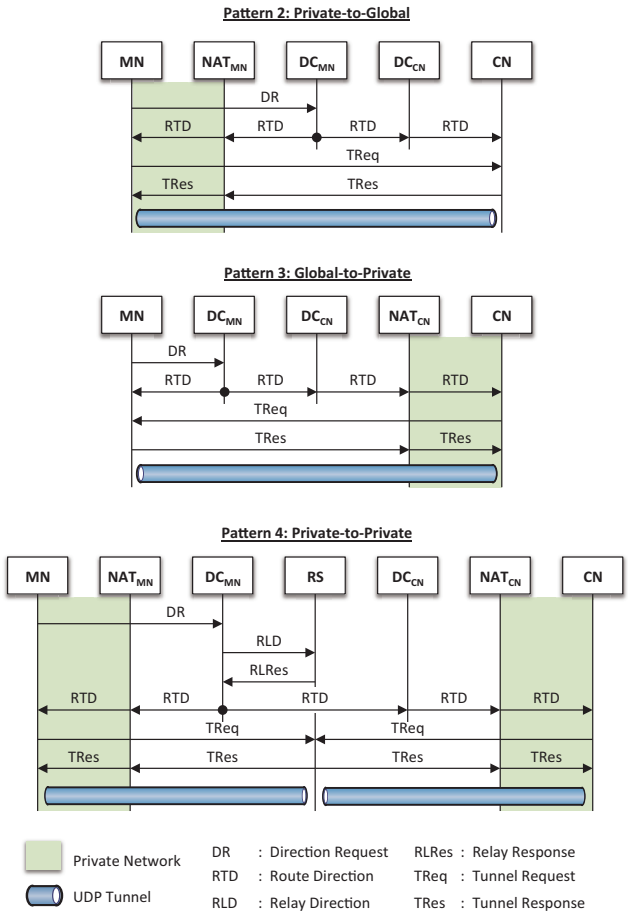


図 3 トンネル構築手順
Fig. 3 Tunnel establishment procedure.

以後，DC からの指示に応じて該当ノード間で Tunnel Request/Response メッセージの交換を行い，NTM ノードはトンネルテーブルを，RS はリレーテーブルを作成する．Tunnel Response を受信した MN はトンネル構築フェーズを終了し，待避していた DNS クエリ応答に対して 3.2.1 項で述べた書き換え処理などを行う．

なお，Pattern 1 の場合は Pattern 2 と全く同じ手順でトンネル構築処理が行われる．MN と CN が両方ともプライベートネットワークに存在する場合，両ノードのアドレス情報の中にプライベートネットワークを構成する NAT の外側 IP アドレス RIP_{NAT} が含まれている．DC はこの IP アドレスを比較することにより，Pattern 4 および Pattern 5 を区別することができる．Pattern 5 は同一 NAT 配下に MN と CN が存在するため，Pattern 1 と同じ手順でトンネル構築処理が行われる．Pattern 6 は CN が一般ノードである点が上記とは異なり，Pattern 4 のうち MN，DC_{MN}，RS 間のシーケンスのみが実行され，MN と RS の間にトンネルが構築される [13].

3.2.3 暗号化通信フェーズ

MN は宛先が仮想 IP アドレスのパケットを送信する際，

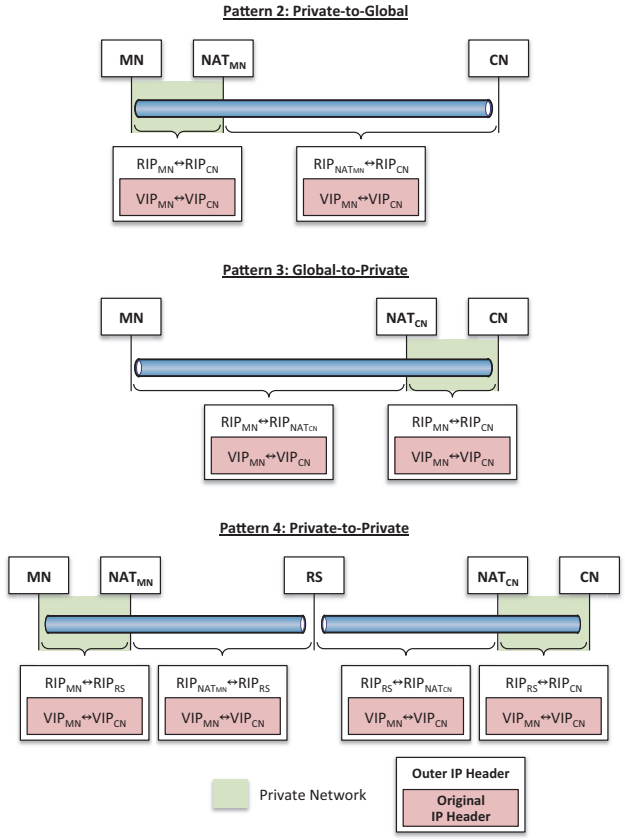


図 4 IP パケットのアドレス遷移
Fig. 4 Address trantisions of IP packet.

IP 層に生成されたトンネルテーブルに従って，元の IP パケットを UDP でカプセル化し，暗号化処理の後にトンネル構築対象ノードへ送信する．このとき，**図 4** に示すように，元の IP ヘッダは送信元を VIP_{MN}，宛先を VIP_{CN} としたままで，新たに付け加えられる IP ヘッダはトンネルの両端の実 IP アドレスとなる．従って，NTM ノード間の通信経路上に NAT が存在する場合は，外側の IP ヘッダおよび UDP ヘッダが NAT によりアドレス変換され，カプセル化されたオリジナルの IP パケットは仮想 IP アドレスのまま維持される．RS を中継する場合はリレーテーブルに従って，外側の IP ヘッダと UDP ヘッダの IP アドレス・ポート番号を変換して転送する．トンネルの出口に当たる CN は，受信したパケットを復号，デカプセル化してから上位アプリケーションへ渡す．

以上の処理により，NTM ノードが存在するネットワークに応じた最適なトンネル経路が構築され，仮想 IP アドレスによる通信接続性を確立することができる．なお，同一 NTM ノード間であれば，構築された 1 つのトンネルで複数のコネクションをまとめて転送することができる．

3.3 移動時の対応

NTM ノードが移動して実 IP アドレスが変化した場合，通信開始時とまったく同じトンネル構築フェーズを実行してトンネルの再構築を行う [14]．これは移動先ネットワークのアドレス空間に応じて，エンドエンドまたは RS 経由のトンネルに切り替える必要があるためである．トンネルの再構築処理が完了しても，NTM ノードの上位アプリケーションは常に仮想 IP アドレスに基づいたコネクションを確立しているため，実 IP アドレスの変化に影響されることはなく，通信継続性を満たすことができる．また，トンネルの再構築と並行して，DC に登録されている NTM ノードのアドレス情報を更新することにより，移動後の NTM ノードに対する到達性を満たす．すなわち，NTMobile は通信接続性を確立するしくみをそのまま移動透過性の実現手法として応用しており，その結果，NTM ノードは通信中に様々なアドレス空間のネットワークへ移動しても通信を継続することができる．

3.4 メッセージフォーマット

図 5 に NTMobile におけるトンネル構築に関わる制御メッセージフォーマットを示す．制御メッセージは UDP プロトコルを利用し，NTM ヘッダと各制御メッセージペイロードで構成される．NTM ヘッダには以下のフィールドが定義されている．

Version： 制御メッセージのバージョン．
Message Type： 制御メッセージの種類．
Flags： 制御メッセージの状態．
Count： 制御メッセージに記載されている通信相手側アドレス情報の数．
Transaction ID： トンネル構築トランザクションを示す識別子．トリガとなった DNS クエリのトランザクション ID が格納される．
Sequence No.： シーケンス番号．初期値は乱数で，以降はインクリメントされる．
Message Length： ヘッダ以降のメッセージ長．
Reserved： 予約フィールド．
Sender's Node ID/Path ID： 制御メッセージの場合は送信者のノード ID，トンネル通信時は Path ID が記載される．

DC や NTM ノード間は信頼関係があることを前提としているため，Direction Request，Route Direction，Relay Direction/Response はすべて事前に共有済みの暗号鍵を用いて暗号化および MAC（Message Authentication Code）の付与が行われる．Tunnel Request/Response およびトンネル通信の暗号化と認証には，トンネル構築フェーズで配布された共通鍵を利用する．

各ノードは NTM ヘッダに記載されている送信元ノード ID をキーにして，復号や MAC の検証に用いる暗号鍵を決定する．カプセル化パケットではノード ID の代わりに，構築されたトンネル経路を示す Path ID が NTM ヘッダに記載されており，トンネルテーブルおよびリレーテーブル

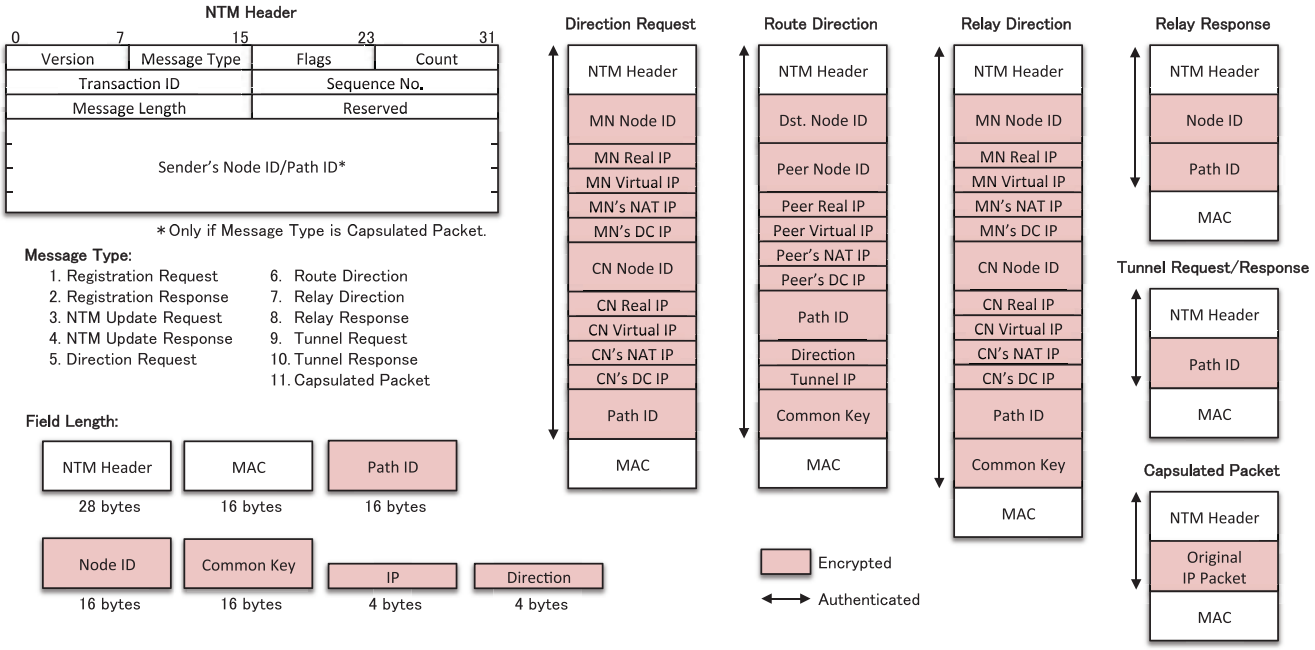


図 5 メッセージフォーマット
Fig. 5 Message formats.

の検索時のキーとして利用する．

4. 実装と評価

NTMobile は Android OS を搭載した携帯端末での利用を想定しているため，本論文では Linux での実装方法について述べる[*5]．

4.1 NTM ノード

図 6 に NTM ノードのモジュール構成を示す．NTM ノード側にはユーザスペースで動作する (A)NTM デーモンと，カーネルで動作する (B) パケット操作モジュール，(C) トンネルテーブルおよび (D) 仮想インタフェースを実装する．

NTM デーモンは Netfilter[*6] を利用して DNS クエリの応答をフックする (i)．クエリ応答を解析して A レコードの結果を取得していたら，そのレコードを保持している DC へ NTM レコードの問合せを行う (ii)．その後，トンネル構築フェーズの終了時に，Netlink ソケットを通じてカーネルに実装されているトンネルテーブルにエントリを登録する (iii)．

通常のアプリケーションが送信する IP パケットの宛先は仮想 IP アドレスとなっているため，仮想インタフェースに向けてカーネルへ渡される (iv)．仮想インタフェースに渡される IP パケットは Netfilter によりパケット操作モジュールに渡され (v)，カプセル化，暗号化などの処理が行われ後，実インタフェースから送信される (vi)．受信時は逆の手順により復号，デカプセル化された後，アプリケーションへデータが渡される．

一般にカプセル化を行うための仮想インタフェースとして，TUN/TAP デバイス[*7] がある．この仮想インタフェースは OpenVPN をはじめとする多くの VPN ソフトウェアで採用されており，TUN/TAP デバイスに渡されたパケットデータを一度ユーザ空間へ戻してから暗号化を行い，再度ソケットを通じて送信することによりカプセル化を実現している [15]．そのため，カーネル空間とユーザ空間の間でメモリコピーが 2 回発生するため，スループットが低下するという課題がある．これに対して，NTMobile ではパケットのカプセル化処理をすべてカーネル内で完結するように設計しており，冗長のないパケットフローと高スループットを実現できる．

4.2 Direction Coordinator と Relay Server

図 7 に DC と RS のモジュール構成を示す．DC と RS には，上述した NTM ノードのモジュールの一部を実装する．DC は NTM ノードのアドレス情報を動的に登録するために，(E)Dynamic DNS サーバを稼働させる．この DNS サーバには NTM レコードを扱えるよう，`bind`[*8] に機能を追加して実現している．NTM ノードおよび RS との制御メッセージ交換は (A)NTM デーモンが行う．

RS は DC および NTM ノードとの制御メッセージ交換

[*5] Android とは，米 Google 社がモバイル向けプラットフォームとして発表したオープンソースの OS である．カーネルとして Linux を採用しているため，今回実装したモジュールを Android へ移植することが可能である．
[*6] `http://www.netfilter.org/`
[*7] `http://vtun.sourceforge.net/tun/`
[*8] `http://www.isc.org/software/bind`

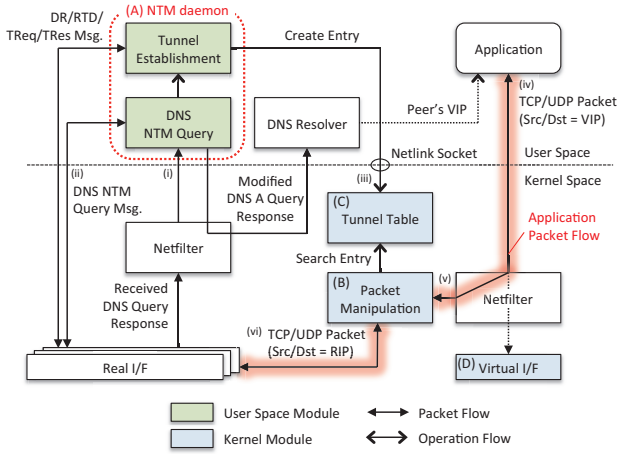


図 6 モジュール構成（NTM ノード側）
Fig. 6 Module configuration (NTM node).

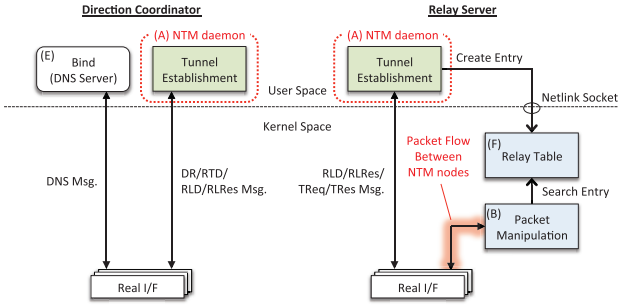
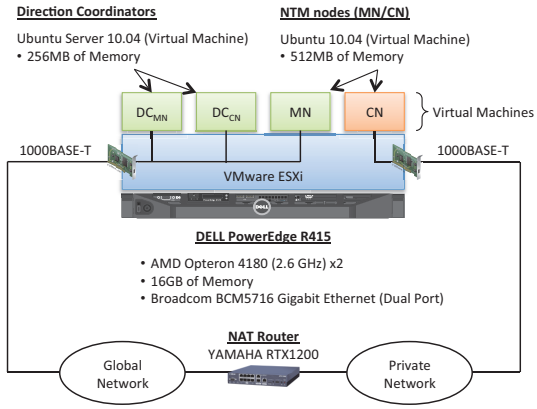


図 7 モジュール構成（左：DC 側，右：RS 側）
Fig. 7 Module configuration (Left: Direction Coordinator, Right: Relay Server).

を行う (A)NTM デーモンに加えて，カーネルモジュールとして (F) リレーテーブルと (B) パケット操作モジュールを実装する．なお，RS は受信したカプセル化パケットの転送処理が主な役割であるため，仮想インタフェースは実装しなくてもよい．

4.3 動作検証と性能評価

提案方式による通信接続性の確立を検証するために，プロトタイプシステムを実装した．**図 8** に試験ネットワーク構成と各装置の仕様を示す．1 台の実機サーバにインストールした VMware ESXi 4.1 を利用して，NTM ノードおよび DC を仮想マシンとして構築した．今回は表 1 の Pattern 3 の動作検証と通信開始時に発生するトンネル構築時間を測定するために，MN と 2 台の DC にグローバル IP アドレスを，CN にプライベート IP アドレスを割り当て，CN を NAT ルータの LAN 側に，その他を NAT ルータの WAN 側に接続した．各装置の仕様および平均 RTT は図中の通りである．また，MN のプライマリ DNS サーバは DC_{CN} とした．このような構成において MN から CN の FQDN 宛へ ping を実行し，このときのパケットフローを Wireshark を用いて MN 側で観測した．なお，制御



	MN ~ DC_{MN}	MN ~ DC_{CN}	DC_{MN} ~ DC_{CN}	CN ~ DC_{CN}	CN ~ MN
RTT [ms]	0.24	0.24	0.28	0.79	0.77

図 8 試験ネットワーク構成
Fig. 8 Test network configuration.

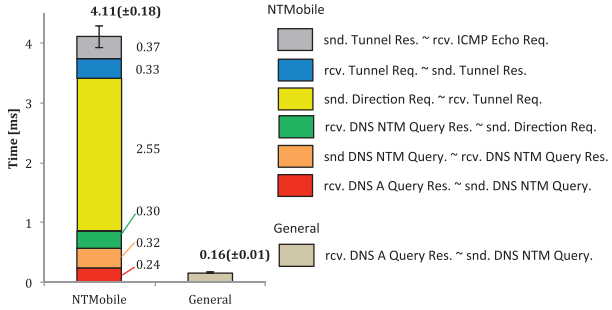


図 9 Pattern 3 における通信開始時のトンネル構築時間の結果
Fig. 9 The Result of initial time caused by the tunnel establishment in Pattern 3.

メッセージの暗号化および認証アルゴリズムは AES-CFB, HMAC-MD5 とし，各装置には制御メッセージを暗号化するための共通鍵（鍵長 128bit）を事前に設定した．

図 9 に通信開始時におけるトンネル構築時間を示す．測定回数 10 回の平均値であり，図中のエラーバーは 95%の信頼区間を表す．DNS クエリ応答を受信してから最初の ICMP パケットを送信するまでに要した時間は，一般ノードの場合は 0.16 ms，NTM ノードの場合は 4.11 ms であった．トンネル構築時間の内訳に着目すると，名前解決フェーズの NTM レコードの問合せが 0.32 ms であり，これは NTM ノードに実装したプログラムの処理負荷に当たる．NTM レコードの応答受信からトンネル構築フェーズの Direction Request 送信までに 0.30 ms を要しており，これは DNS 応答メッセージの解析，制御メッセージの生成，暗号化および MAC 生成処理が含まれる．Pattern 3 では MN が Direction Request を送信すると，CN 側から送信される Tunnel Request を受信する．この時間が 2.55 ms であったが，この間に Route Direction が DC_{MN} から DC_{CN}，CN の順に転送されており，各装置でメッセージの復号・検証

および暗号化・MAC 生成などの処理が行われている．MN が Tunnel Response を返答してから ICMP パケットを送信するまでに 0.37 ms かかっており，トンネルテーブルの作成，DNS 応答メッセージ内の IP アドレスを仮想 IP アドレスに書き換える処理などを行っている．

今回は仮想マシンを用いた環境での測定結果であるため，実環境では各装置間の伝送遅延が上記結果に加わることになる．ここで，MN と DC_{MN} の位置を日本，CN と DC_{CN} の位置を米国と仮定すると，DC 間および MN と CN 間の伝送遅延が大きくなる．Pattern 3 の場合，トンネル構築フェーズで日米間を 1.5 往復するため，約 150 ms のエンドツーエンド遅延が発生すると推測される．

例えば，NAT 越えを実現するための技術として ICE（Interactive Connectivity Establishment） [16] がある．ICE は SIP（Session Initiation Protocol）で NAT 越えをするための技術で，通信開始時に STUN（Session Traversal Utilities for NAT） [17] や TURN（Traversal Using Relays around NAT） [18] を反復的に実行し，エンドノードが互いに接続可能な IP アドレスとポート番号を発見・交換する．文献 [19] によると，ICE によるコネクション確立に約 2〜10 秒必要であることが示されている．スマートフォンでの利用を想定すると，Web ブラウジングやビデオチャットなどのアプリケーションが考えられる．文献 [20] によると，ユーザが Web ブラウジングにおいて許容できる待ち時間は 2 秒程度と報告されている．また，ビデオチャットなどでは通信開始時に数秒間バッファリングを行うことが一般的である．従って，提案方式のトンネル構築時間は，通常の通信開始時に発生する待機時間と比較して十分短く，ユーザがその遅延を意識することはないと考えられる．

4.4 定性評価と残された課題

4.4.1 仮想 IP アドレスの数量制限

仮想 IP アドレスは NTMobile の枠組みの中で一意であり，かつ実ネットワークで用いられる IP アドレスと衝突しないこと，さらに移動しても変化しないことが前提となる．ただし，仮想 IP アドレス宛のパケットは実際のネットワーク上で直接ルーティングされることはないため，クラス E を利用することを想定している．DC が管理する仮想ネットワークアドレスを 16bit とした場合，設置可能な DC は 4,096 台，各 DC が管理する仮想 IP アドレスは 65,534 個となる [*9]．従って，NTMobile のシステム全体では，約 2 億 7,000 万個の仮想 IP アドレスを利用することができる．

ただし，NTMobile はスマートフォンへの適用を想定しているため，この場合は IPv4 アドレスだけでは不足すると考えられる．本論文では詳述しないが，NTMobile は IPv6 ネットワークへの対応も検討している [21]．IPv6 に対応した場合，仮想 IP アドレスは IPv4 だけでなく，IPv6 アドレスも配布することを想定している．全ての NTM ノードは IPv6 アドレスを持つことにより，アプリケーションが IPv6 対応であれば仮想 IPv6 アドレスによる通信を行うため，この場合は仮想 IPv4 アドレスが不要となる．今後，仮想 IP アドレスを IPv6 に統合するなど，仮想 IPv4 アドレスの不足を補う検討が必要である．

4.4.2 DC 間および DC と RS 間の信頼関係

DC や RS の台数が小規模で，これらサーバ群の管理者が同一であれば，事前共有鍵方式により信頼関係を構築することができるが，ネットワークの規模が拡大すると，任意の DC 間および DC と任意の RS 間で共通鍵を共有することが困難となる．そこで，DC と RS に公開鍵証明書を発行し，これを用いた相互認証方式を検討している．root DC が証明書を発行する役割を担っており，これにより任意の DC 間および DC と RS 間の信頼関係を構築することができる．

4.4.3 DC と RS に発生する負荷

DC の主な処理は，通信開始時および移動時のトンネル構築指示およびプライベートネットワークに存在する NTM ノードからの Keep Alive 処理である．トンネル構築指示は，NTM ノードがある通信相手に初めて通信を開始する際に発生することを考慮すると，DC1 台あたりで管理する NTM ノードが増加しても大きな負荷は発生しないと考えられる．Keep Alive は NAT マッピング情報のタイムアウト時間より短い間隔で行う必要があるが，ベンダや設定の違いにより異なっている．Mobile IP における NAT 越え手法では，UDP トンネルを維持するために Keep Alive のデフォルト間隔は 110 秒と定義されている [5]．NTMobile における Keep Alive の送信間隔もこれに準ずることとしている．Keep Alive メッセージは，IP ヘッダ，UDP ヘッダ，NTM ヘッダから構成され，メッセージサイズは 56byte である．4.4.1 項で示したように，1 台の DC が管理する NTM ノード数を最大 65,534 台とすると，Keep Alive メッセージのトラヒックは約 260Kbps となる [*10]．従って，相当数の NTM ノードを収容したとしても，DC が Keep Alive メッセージのトラヒックで障害を起こすことはないと考えられる．

RS は NTM ノードのトラヒックを中継する装置であるため，RS が利用可能なネットワーク帯域をどれくらいの

[*9] クラス E は 240.0.0.0/4 の範囲で実験用として定義されているため，実際のネットワークでは使われることはない．定義可能な仮想サブネットワークは 16bit から上位 4bit を除いた 12bit 分，すなわち $2^{12} = 4,096$ 個となる．ホストアドレス部は残り 16bit であるため，ブロードキャストアドレスを除いた $2^{16} - 2 = 65,534$ 台分の仮想 IP アドレスを 1 つの仮想サブネットワークに設定できる．

[*10] $(56 \times 8)[bit] \times 65,534 \div 110[sec] \fallingdotseq 260[Kbps]$．この値はデータリンク層のヘッダやフレーム間隔などを考慮していないラフな見積もりである．

セッション数で共有するかにより，RS が処理可能な NTM ノード数が決まる．例えば NTM ノード間で IP 電話アプリケーションの利用を想定すると，音声コーデックに G.711 を採用した場合，上りと下り共に約 100Kbps の帯域が必要となる．RS が利用可能な帯域を 1Gbps と仮定すると，1 台の RS では最大 5,000 台の NTM ノードを同時に処理可能と見積もることができる．

ただし，実際には DC や RS の性能により処理可能な NTM ノード数が変わるため，今後は DC や RS における負荷評価を行う必要がある．

4.4.4 DNS による名前解決

NTM ノードは，通信開始時に DNS の仕組みを利用して通信相手 NTM ノードのアドレス情報を取得する．この時，A レコードと NTM レコードの問合せを行うため，NTM ノードと DNS サーバ間で 2 往復の DNS クエリが実行される．現在の仕様では逐次的に問合せを行っているが，これを同時に行うことによりクエリ時間の短縮が可能である．

今回のプロトタイプ実装では Linux を採用しており，DNS リゾルバは DNS クエリの内容をキャッシュしない．そのため，DNS クエリは毎回行われるため，NTM ノードは常に最新の通信相手のアドレス情報を取得することができる．ただし，Linux 以外のプラットフォームでの利用を考慮する場合は，DNS リゾルバのキャッシュ機能を無効にしたり，または，A レコードおよび NTM レコードの TTL を短く設定してキャッシュが長時間残らないような運用を検討する必要がある．

4.4.5 ハンドオーバ

3.3 節で述べたように，NTM ノードが移動した際にはトンネル構築フェーズのみ行うため，名前解決フェーズに要していた時間を短縮することができる．ただし，実際には基地局の切り替えなどの L2 ハンドオーバや，移動先ネットワークにおける DHCP による IP アドレスの取得，およびアドレス重複チェック処理の時間が発生する．

文献 [22] にて，Android スマートフォンに NTMobile を実装し，ハンドオーバ評価を行った結果，ハンドオーバに要する時間は 1 秒程度であった．その内訳は L2 ハンドオーバおよび IP アドレスの取得が 0.95 秒，トンネル再構築が 0.04 秒であり，NTMobile 以外の処理が大半を占めていることを確認している．この問題は移動透過性を実現する全ての技術に共通する課題であり，例えば移動先ネットワークにハンドオーバした際に高速に IP アドレスを取得する手法 [23] や，複数の無線インタフェースを効率よく切り替えることによりアドレス取得に関わる処理の影響を受けない手法 [24] などが提案されている．NTM ノードがスマートフォンであると想定すると，後者のような手法で対策が可能であるため，十分実ネットワークで運用できると判断できる．

4.4.6 IPv6 のサポート

4.4.1 項で述べた通り，NTMobile は IPv4 だけでなく IPv6 が混在した環境での利用を検討している．NTM ノードを IPv4/IPv6 デュアルスタックに対応させることにより，IPv6 ネットワークにも接続可能である．本論文で示した制御メッセージの IPv4 アドレス部分を IPv4/IPv6 の両アドレスへ拡張し，IPv6 アドレス情報を含む NTM レコードを定義することにより，Pattern 1 と同じシグナリング手順で IPv6 のトンネルを構築できる，また，IPv4/IPv6 デュアルスタックネットワークに RS を設置することにより，IPv4 と IPv6 の橋渡しを行うことができる．NTM ノード間では Pattern 4 と同じ考え方により仮想 IP アドレスによるコネクションを確立するが，接続しているネットワークのアドレス体系に応じて，上記 RS との間にトンネルを構築して転送する．これにより，IPv4 と IPv6 が混在した環境においても NTM ノードへの通信接続性および移動透過性を実現することができる．

5. 関連技術

異なるアドレス空間をシームレスに接続するアーキテクチャとして，SIPS（Seamless IP Sublayer）が提案されている [25]．SIPS は IP 層とトランスポート層の間に IP 層の副層を定義して既存の IP 層を拡張している．この副層においてラベルスイッチング技術により，ヘッダ変換，ホストの特定，パケットのルーティングなどを行うことにより，異なるアドレス空間での通信を実現している．SIPS ではエンドノードの IP 層拡張の他，各アドレス空間の境界に SIPS 対応ルータを配置する必要があるため，例えば IPv4 ネットワークでは NAT ルータの位置に該当する．そのため，本論文で議論している異なるアドレス空間に存在するノード間の通信接続性の実現には適用できるものの，SIPS 対応ルータが設置されていないネットワーク，すなわち一般の NAT ルータ配下に移動した場合は相互接続することができない．また，移動透過性については考慮されていない．

IPv4 ネットワークで移動透過性を実現する代表技術として，Mobile IPv4 がある．Mobile IPv4 では，MN は移動しても変化しない HoA（Home Address）を用いて通信を行う．そのため，訪問先ネットワークへ移動すると MN から CN へ送信するパケットの送信元と訪問先ネットワークのアドレスが異なるため，イングレスフィルタリングにより途中のルータで破棄されてしまい，通信接続性を実現することができない．この課題の対策としてリバーストンネルが定義されたが [6]，常に HA を経由した通信となるため，スループットの低下や遅延の増加が発生する．また，全てのトラヒックが HA に集中するため，HA が単一点障害となりシステムがダウンするリスクが高いなどの課題がある．Mobile IPv4 では，Mobile IPv6 で定義されたよう

な経路最適化や HA の二重化機能は定義されていない．

IETF では Mobile IPv4 の他に HIP（Host Identity Protocol）と呼ぶ次世代モバイルプロトコルが標準化されている [26]．HIP は IP 層とトランスポート層に Host Identity 層を追加し，ID と Locator を分離して使い分ける．上位層ではノード識別子 HI（Host Identifier），下位層では IP アドレスを使用することにより，上位層に IP アドレスの変化を隠蔽して移動透過性を実現している．HIP は IPv4 ネットワークと IPv6 ネットワークをまたがった移動に対応しており，IPv4 における NAT 越えを実現するために ICE を用いた拡張仕様が定義されている [27]．そのため，ハンドオーバ時に ICE に基づくシグナリングを行うことを考慮すると，オーバヘッドが高いと想定される．

これまでに挙げた移動透過性技術はネットワーク層で実現する技術であったが，アプリケーション層で実現する技術もある．代表的な技術として SIP を用いた方式が多く，例えば All-SIP mobility では従来の UDP セッションだけでなく TCP コネクションの維持も可能な技術である [28], [29]．この技術はエンドノードが仮想 IP アドレスと UDP トンネルを用いて移動透過性を実現している点が提案方式と類似している．UDP カプセル化処理はアプリケーション層に実装された SMC（Session and Mobility Controller）モジュールが行うため，仮想インタフェースに渡された IP パケットを一度アプリケーション層へ戻す必要がある．一方，提案方式はカプセル化処理はカーネルモジュールで行うため，All-SIP mobility に対してスループット性能の優位性がある．

提案技術と類似したアプローチにより NAT をまたがった移動透過性を実現する技術として，UPMT（Universal Per-Application Mobility management using Tunnels）が提案されている [30], [31]．UPMT はアプリケーション層の移動透過技術で，NAT 配下に存在するノードはインターネット上に設置した AN（Anchor Node）に対してトンネルを構築し，AN は受信パケットをデカプセル化した後，NAT によるアドレス変換を行って通信相手ノードへ転送する．しかし，通信相手ノードがグローバルネットワークに存在していても常に AN を中継したデータ転送となるため，提案方式と比較すると経路が冗長であること，また AN に負荷が集中するなどの課題がある．なお，UPMT においても ICE を用いてエンドツーエンド通信を行う拡張仕様があるが，前述の通りシグナリングのオーバヘッドが高いと考えられる．

6. まとめ

本論文では，移動先ネットワークの制約がない移動透過性技術として NTMobile を提案した．提案方式は DC を導入することにより，エンドノードが存在するネットワークに応じた最適なトンネル通信経路を確立できることを示した．仮想 IP アドレスによる実 IP アドレスの変化を隠蔽しているため，移動後にトンネルの再構築をおこなうことにより，NAT をまたがった移動透過性を実現できる．提案方式のプロトタイプシステムを Linux に実装したところ，NAT 配下のノードに対して低オーバヘッドでコネクションを確立できることを確認した．

今後はハンドオーバ時の詳細な評価結果および IPv4/IPv6 混在ネットワークに対応した仕様について報告する．また，DC および RS の負荷評価，サーバ間の信頼関係の構築，シグナリングのさらなる高速化などの課題に取り組む必要がある．

謝辞 カーネルモジュールの実装に御協力頂いた東京システムハウス株式会社の関係各位に深謝する．

参考文献

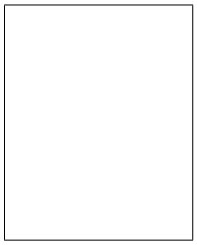
[1] Le, D., Fu, X. and Hogrefe, D.: A Review of Mobility Support Paradigms for the Internet, *IEEE Communications Surveys & Tutorials*, Vol. 8, No. 1, pp. 38–51 (2006).
[2] Perkins, C.: IP Mobility Support for IPv4, Revised, RFC 5944, IETF (2010).
[3] 関 顕生，岩田裕貴，森廣勇人，前田香織，近堂 徹，岸場清悟，西村浩二，相原玲二：IPv4 拡張し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).
[4] 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).
[5] Levkowetz, H. and Vaarala, S.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519, IETF (2003).
[6] Montenegro, G.: Reverse Tunneling for Mobile IP, revised, RFC 3024, IETF (2001).
[7] 井戸上彰，久保 健，横田英俊：プライベートアドレスを使用するモバイルネットワーク間のローミング手順とその実装，情報処理学会論文誌，Vol. 44, No. 12, pp. 2958–2967 (2003).
[8] 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).
[9] Suzuki, H. and Watanabe, A.: Design of NAT Traversal for Mobile PPC Applying Hole Punching Technology, *Proc. of IEEE TENCON2008* (2008).
[10] 鈴木秀和，渡邊 晃：プライベートネットワーク内のノードを通信相手とした移動透過性の実現方式，電子情報通信学会論文誌 (B)，Vol. J92-B, No. 1, pp. 109–121 (2009).
[11] 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，Vol. 2011, pp. 1139–1145 (2011).
[12] Leach, P., Mealling, M. and Salz, R.: A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122, IETF (2005).
[13] 土井敏樹，鈴木秀和，内藤克浩，渡邊 晃：NTMobile における RS の検討，DICOMO2012 論文集，Vol. 2012, pp. 1162–1168 (2012).
[14] 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，Vol. 2011, pp. 1349–1359

(2011).
[15] Khanvilkar, S. and Khokhar, A.: Virtual Private Networks: An Overview with Performance Evaluation, *IEEE Communications Magazine*, Vol. 42, No. 10, pp. 146–154 (2004).
[16] Rosenberg, J.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC 5245, IETF (2010).
[17] Rosenberg, J., Mahy, R., Matthews, P. and Wing, D.: Session Traversal Utilities for NAT (STUN), RFC 5389, IETF (2008).
[18] Mahy, R., Matthews, P. and Rosenberg, J.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), RFC 5766, IETF (2010).
[19] Maenpaa, J., Andersson, V., Camarillo, G. and Keranen, A.: Impact of Network Address Translator Traversal on Delays in Peer-to-Peer Session Initiation Protocol, *Proc. of IEEE GLOBECOM2010* (2010).
[20] Yang, H. and Faris, N.: September 14, 2009 - Akamai Reveals 2 Seconds as the New Threshold of Acceptability for eCommerce Web Page Response Times, (online), available from ⟨http://www.akamai.com/html/about/press/releases/2009/press_091409.html⟩ (2009).
[21] 上醉尾一真，鈴木秀和，内藤克浩，渡邊 晃：IPv6 ネットワークにおける NTMobile の検討，情報処理学会研究報告，Vol. 2011-MBL-59, No. 9, pp. 1–7 (2011).
[22] 上醉尾一真，鈴木秀和，内藤克浩，渡邊 晃：NTMobile の Android 端末への実装と評価，情報処理学会研究報告，Vol. 2012-MBL-62, No. 19, pp. 1–8 (2012).
[23] Zúquete, A. and Frade, C.: Pre-Allocation of DHCP Leases: A Cross-Layer Approach, *Proc. of 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2011*, pp. 1–5 (2011).
[24] Abdelatif, M. A., Kalebaila, G. K. and Chan, H. A.: A Cross-Layer Mobility Management Framework based on IEEE802.21, *Proc. of IEEE PIMRC 2007*, pp. 1–6 (2007).
[25] 角野宏光，内田良隆，石川憲洋，峰野博史，水野忠則：異なるアドレス空間をシームレスに接続する IP 層拡張の提案と実装，電子情報通信学会論文誌 (B)，Vol. J93-B, No. 10, pp. 1397–1407 (2010).
[26] Moskowitz, R. and Nikander, P.: Host Identity Protocol (HIP) Architecture, RFC 4423, IETF (2006).
[27] Komu, M., Henderson, T., Tschofenig, H., Melen, J. and Keranen, A.: Basic Host Identity Protocol (HIP) Extensions for Traversal of Network Address Translators, RFC 5770, IETF (2010).
[28] Seta, N., Miyajima, H., Zhang, L., Hayashi, H. and Fujii, T.: All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment, *Proc. of IEEE VTC2007-Spring*, pp. 1121–1126 (2007).
[29] Miyajima, H., Zhang, L., Hayashi, H. and Fujii, T.: An Implementation of Enhanced All-SIP Mobility, *Proc. of IEEE PIMRC2008* (2008).
[30] Bonola, M., Salsano, S. and Polidoro, A.: UPMT: Universal Per-Application Mobility Management Using Tunnels, *Proc. of IEEE GLOBECOM2009* (2009).
[31] Bonola, M. and Salsano, S.: S-UPMT: a secure Vertical Handover solution based on IP in UDP tunneling and IPsec, *GTTI Riunione Annuale 2010*, (online), available from ⟨http://www.gtti.it/GTTI10/papers/gtti10_submission_29.pdf⟩ (2010).

付　　録

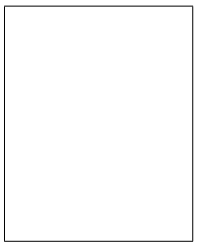
A.1 記号の定義

- RIP_N; ノード N の実 IP アドレス
- VIP_N; ノード N の仮想 IP アドレス
- NID_N; ノード N の識別子
- PID_{N1-N2}; ノード $N1$ とノード $N2$ 間で構築するトンネルの識別子（Path ID）
- CK_{N1-N2}; ノード $N1$ とノード $N2$ の共通鍵
- $IP_{N1} \leftrightarrow IP_{N2}$; ノード $N1$ の IP アドレスとノード $N2$ の IP アドレス間のコネクション



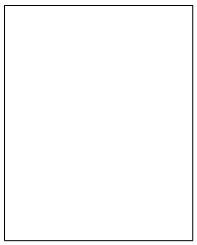
鈴木 秀和　（正会員）

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．



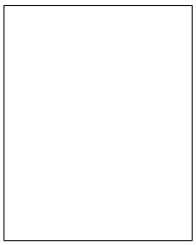
上醉尾 一真　（学生会員）

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．



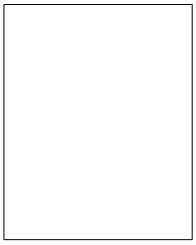
水谷 智大

2009 年名城大学理工学部情報工学科卒業．2011 年同大学大学院理工学研究科情報工学専攻修了．同年株式会社システムコーディネイト入社．西日本事業部名古屋事業所所属．修士（工学）．



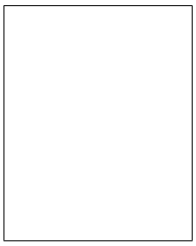
西尾 拓也

2011 年三重大学工学部電気電子工学科卒業．現在，同大学大学院工学研究科電気電子工学専攻在学中．電子情報通信学会会員．



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．博士（工学）．電子情報通信学会，IEEE 各会員．