

平成27年度 修士論文

和文題目

**NTMobileにおける
仮想IPアドレス管理手法の提案と評価**

英文題目

**Proposal of Management Method of Virtual IP
Addresses
in NTMobile and its Evaluation**

情報工学専攻 渡邊研究室
(学籍番号: 143430004)

加古 将規

提出日: 平成28年1月28日

名城大学大学院理工学研究科

概要

モバイルネットワークの普及によって、自由に通信を開始できる通信接続性とネットワークを切り替えても通信を継続できる移動透過性が求められている。IPv4 ネットワークでは、グローバル IP アドレスの枯渇が深刻な問題となっており、NAT 配下にプライベートアドレスのネットワークを構築し、IP アドレスを節約するのが一般的となっている。しかし、グローバルネットワーク側からプライベートネットワークに対して通信を開始することができないという通信接続性の課題が生じている。また、通信中にネットワークを切り替えると IP アドレスが変化してしまい、通信を継続することができない。筆者は移動透過性と通信接続性を同時に実現する技術として、NTMobile (Network Traversal with Mobility) を提案している。NTMobile では、NTMobile の機能を実装した端末 (NTM 端末) に対して一意な仮想 IPv4 アドレスを割り当てるが、仮想 IPv4 アドレスとして利用できるアドレス帯域が小さいという課題があった。

そこで、本論文では Path ID と呼ぶ NTMobile 独自の通信識別子を用いて通信を識別し、仮想 IPv4 アドレスから通信識別子の役割を取り除く。加えて、NTM 端末が Path ID を用いて仮想 IPv4 アドレスを管理し、通信中は Path ID に基づき仮想 IPv4 アドレスを変換しながら通信することで、NTMobile の仮想 IP アドレスに係る課題を解決する。

目次

第 1 章	はじめに	1
第 2 章	既存研究	4
第 3 章	NTMobile	6
3.1	端末起動時と通信開始時の動作	7
3.2	トンネル通信時の動作	7
3.3	仮想 IP アドレスの管理に係わる課題	8
第 4 章	提案手法	9
4.1	通信シーケンス	9
4.1.1	端末起動時	9
4.1.2	通信開始時	10
4.1.3	トンネル通信時	10
4.2	通信相手が一般端末間の場合	11
4.2.1	通信開始時	11
4.2.2	トンネル通信時	12
第 5 章	実装	14
5.1	NTMobile デーモン	14
5.2	NTMobile カーネルモジュール	14
第 6 章	評価	15
6.1	性能測定	15
6.2	従来手法との比較	16
第 7 章	まとめ	18

第1章 はじめに

今日、通信環境の整備と通信技術、通信機器の発展により、現在のネットワークすなわち TCP/IP を利用した通信の様々な課題が明らかになってきた。TCP/IP によるネットワークは、当初 IPv4 アドレスを通信識別子とした通信として開発され、その IPv4 アドレスの枯渇が懸念されるようになると、IPv6 アドレスが開発された。また、IPv6 アドレスの導入と同時期にプライベートアドレスが導入され、NAT (Network Address Translation) 配下にプライベートアドレスによるネットワークを構築し、IP アドレスを節約する動きが一般的となった。NAT の導入には、外部ネットワークからアクセスできないという NAT 越え問題が存在したが、外部ネットワークから組織ネットワークが隠蔽される点が注目され、NAT によるプライベートアドレスの利用は瞬く間に普及した。IPv6 アドレスは IPv4 アドレスと互換性が無く、導入の敷居も高かったため、プライベートアドレスほど普及せず取り残される形となった。IPv4 アドレスはプライベートアドレスの導入によって延命したものの、インターネットの需要が爆発的に増加している昨今いよいよグローバル IP アドレスの枯渇が目前となっている。JPNIC によると、2011 年 2 月をもってインターネット上で利用されるアドレス資源をグローバルに管理する IANA(Internet Assigned Numbers Authority) から新規に割り振りできる IPv4 アドレスが枯渇し、同年の 4 月に JPNIC によるグローバル IP アドレスの割り当てが終了している [7]。そのため、IPv6 アドレスは必要に応じて徐々に導入され始めている。しかし、前述の通り IPv4 と IPv6 には互換性がなく、異なるネットワーク間では直接通信を行うことができない。以上の経緯から、現在のネットワークには以下のような課題が存在する。

- (1) NAT 越え問題
- (2) IPv4/IPv6 ネットワーク間の直接通信ができない

NAT 越え問題を解決する技術として、STUN (Session Traversal Utilities for NATs) [8,9], TURN (Traversal Using Relay around NAT) [10, 11], ICE (Interactive Connectivity Establishment) [12, 13] などが提案されている。また、IPv4/v6 相互通信技術として、トンネリング、デュアルスタック、トランスレータ技術があるとされ、トンネリング技術として 6to4 [14], ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) [15], トランスレータ技術として NAT-PT 方式 [16], TCP Relay 方式 [17] が標準化されている。

さらに、スマートフォンを始めとした高機能な携帯端末を利用するユーザが近年急増し、様々な用途・場面でインターネットが利用されている。このような環境では無線通信においても常に高品質の通信環境を利用できることが望ましい。しかし、現在の TCP/IP ネットワークではネットワークを切り替えた際に通信を継続することができない。通信中のネットワーク切り替えは移動透過性技術を利用することで実現することができる。

移動透過性技術は、当初ユーザの移動による IP アドレスの変化を想定して検討・開発が行われていた [18–24] が、近年は携帯電話網の普及により、同キャリアから提供される LTE などの通信規格を利用する限りユーザが移動しても端末の IP アドレスが変化しない。そのため、ユーザが意識・負担に感じることはほとんどなく、移動透過性技術が大きな話題になることはなかった。しかし、携帯電話網から Wi-Fi などの異なる

ネットワークへ切り替えた際には、IP アドレスが変化してしまうため、依然として通信継続の課題は残ったままである。

スマートフォンを利用するユーザが爆発的に増加している昨今、通信によるトラフィック増加が携帯電話網の許容量を超え、通信障害が発生することも珍しくなくなっている。通信業界ではこのような通信障害を抑制するため、一時的に公共無線などのネットワークに接続先を切り替え、トラフィックを分散させるオフロード技術の導入も進められている。しかし、ネットワークの切り替えに伴う一時的な通信断絶がユーザには負担となっている。また、スマートフォンを所持するユーザは、通信量節約のため移動時以外では組織 Wi-Fi や公共無線を積極的に利用するなど動きも見られ、ネットワークを切り替える場面も多く見られるようになった。頻繁にネットワーク切り替えが行われる昨今の無線事情を考えると、自由にネットワークを切り替え可能にする移動透過性技術が再び必要となってくる。

(3) 移動透過性技術の必要性

移動透過性技術に関して現在までに多くの研究 [18–24] が行われており、Mobile IPv4 [18] を拡張し、NAT 越えを実現する Mobile IP Traversal of NAT Devices [19] は、(1) の課題と (3) の要求を、Mobile IPv6 [21] を拡張し、デュアルスタック対応を実現する Dual Stack Mobile IPv6 [22] は、(2) の課題と (3) の要求を同時に満たすことができる。また、Mobile IP Traversal of NAT Devices [19] に Dual Stack Mobile IPv4 [20] を組み合わせることで (1)、(2) の課題と (3) の要求を同時に満たすことが可能と考えられるが、Mobile IPv4 には下記のような課題が存在する。Mobile IPv4 は移動透過性を実現するため、パケットの中継サーバを設置する必要があり、通信中は常に中継サーバを経由するため通信経路の冗長化が発生する。加えて、NAT 越え問題に対応する際には、移動端末 1 台に対して 1 つのグローバル IP アドレスを割り当てる必要があり、IP アドレス枯渇が叫ばれる昨今では致命的な課題となる。

現在、Web アプリケーションは前述したこれらのネットワークの課題を前提にしているため、そのほとんどがクライアント/サーバ型モデルとなっている。クライアント/サーバ型モデルでは、サーバがダウンするのを防ぐためにサーバの負荷分散やサーバの稼動状態を監視し、サーバがダウンした際には早急に復旧させる必要がある。また、個人情報を扱うサーバでは情報漏洩の危険性などをはらんでいる。特にクライアント/サーバ型モデルを利用するアプリケーションは、サーバ管理者の存在が不可欠であるため、この第三者をユーザが信用する必要がある。また、ユーザ間の直接通信ができないことを前提とした現モデルの在り方はアプリケーションの自由度を著しく損なっていると言える。ネットワークの課題を解決することは、クライアント/サーバ型モデルの一本柱であったアプリケーションの在り方を大きく変え、サービスの幅を広げることにつながると思われる。

著者は、上記 (1) から (3) で述べた課題および要求をすべて同時に実現する技術として、NTMobile (Network Traversal with Mobility) [1–6] を提案している。NTMobile は、既存ネットワークへの改造が不要であり、NAT 配下の端末に対しても通信接続性と移動透過性を実現することができるネットワークアーキテクチャとして設計している。また、NTMobile は、IPv4/v6 相互通信技術としてトンネリング技術を採用しており、IPv4 プライベートネットワーク、IPv4 グローバルネットワーク、IPv6 ネットワークのどのようなネットワークに端末が接続されていても、通信接続性を実現できる。移動透過性実現の手法として、NTMobile の機能を実装した端末 (NTM 端末) に対して、端末の位置に依存しない仮想 IP アドレスを割り当てる。NTM 端末のアプリケーションは仮想 IP アドレスを通信相手の IP アドレスと認識し通信を行う。アプリケーションが作成した仮想 IP アドレスに基づくパケットはネットワークへ出る際に端末のもつ実際の IP アドレス

(実 IP アドレス) でカプセル化し、通信相手に送信する。仮想 IP アドレスは実ネットワークのアドレス体系の違いやネットワーク切り替えによるアドレス変化に影響されないため、アプリケーションが仮想 IP アドレスを利用して通信を行う限り、ユーザはネットワークの切り替えを意識することなく通信を継続することができる。NTMobile の仮想 IP アドレスは、実 IP アドレスと重複することを防ぐために実ネットワークで利用されないアドレス帯域から生成し、端末に割り当てる。しかし、IPv4 ネットワークにおいて仮想 IP アドレスとして利用できる帯域が小さく、結果的に NTMobile を利用できる端末が少なくなってしまう課題があった。これは、NTMobile を実用化する上で避けては通れない課題であった。

本論文では、自端末の仮想 IPv4 アドレスと通信相手の仮想 IPv4 アドレスを端末内部で自律的に生成する手法を提案する。端末内部で生成された仮想 IPv4 アドレスは NTMobile の通信を一意に識別する通信識別子 Path ID と関連付ける。通信中は、Path ID をキーとして通信相手の仮想 IPv4 アドレスの検索を行い、パケット内の仮想 IPv4 アドレスを端末が管理する仮想 IPv4 アドレスへと変換する。以上の手法により、IPv4 における仮想 IP アドレスに係わる制約を除去することができる。

以下、2 章で既存研究、3 章で NTMobile の概要と仮想 IP アドレスの管理について説明する。そして、4 章で提案手法の動作、5 章で提案手法の実装、6 章で提案手法の評価について述べ、7 章でまとめる。

第2章 既存研究

本章では、IPv4 ネットワークにおいて NAT 越えと移動透過性を実現する Mobile IP Traversal of NAT Devices [19] の概要とその課題について述べる。

Mobile IP Traversal of NAT Devices では、Mobile IP Traversal of NAT Devices を実装した移動端末 MN (Mobile Node) とホームネットワーク上に存在し、MN の IP アドレスの管理および MN 宛のパケットを代理受信して転送を行う HA (Home Agent) によって構成される。また、MN は HA から割り当てられ、以降アプリケーションが通信識別子として利用する IP アドレス HoA (Home Address) と訪問先のネットワークで割り当てられ、HA が MN にパケットを中継する際に利用する IP アドレス CoA (Care of Address) の 2 種類の IP アドレスを用いて通信を行う。

図 1 に訪問先ネットワークに NAT が存在する場合の MN と CN 通信の様子を示す。MN がホームネットワーク上に存在する場合、MN は移動端末としての特別な処理を行わず、HoA を用いて通信相手である CN (Correspondent Node) と通常の通信を行う。MN が訪問先ネットワークに移動した場合、MN は HoA と CoA の登録を行うために HA に登録要求メッセージを送信する。MN からの登録要求メッセージを受信した HA は、メッセージ内に含まれる CoA とメッセージの IPv4 ヘッダに含まれる宛先 IP アドレスの比較を行う。2 つの IP アドレスが異なる場合、HA は MN が NAT 配下に移動したと判断し、HA と MN 間に UDP トンネルを構築する。その後、MN の HoA から送信されるすべてのパケットは CoA でカプセル化され、UDP トンネルを通じて HA に送信される。MN からパケットを受信した HA は、パケットをデカプセル化した後に CN へ転送する。CN から MN へ送信されるパケットは、一時的に HA に転送され、UDP トンネルを通じて MN に送信される。以上の手法により、Mobile IP Traversal of NAT Devices は NAT 越えと移動透過性を実現している。

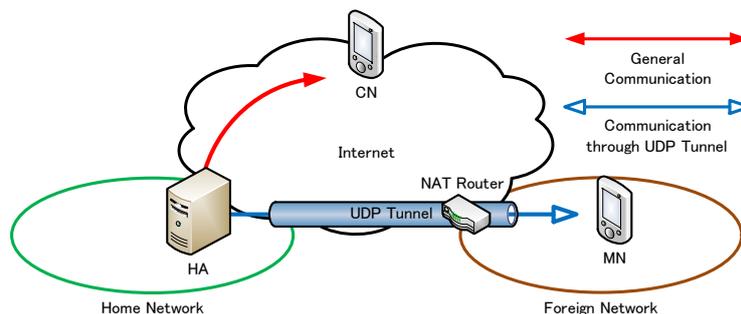


図 1 Mobile IP Traversal of NAT Devices における NAT が存在する環境での通信

Mobile IP Traversal of NAT Devices では、MN が NAT 配下で通信接続性および移動透過性を確保するために、HA をグローバルネットワーク上に設置する必要がある。その際、移動端末の利用する HoA は HA と同じ帯域の IP アドレスを用いる必要があるため、移動端末 1 台に対して必ず 1 つのグローバル IP アドレス

が必要となる。現 IPv4 ネットワークにおいて NAT の存在はもはや必要不可欠であり、NAT 対応のために多くのグローバル IP アドレスが必要となる。しかし、IPv4 ネットワークのグローバル IP アドレスは現在枯渇の危機にあり、2011 年の 4 月をもって JPNIC によるグローバル IP アドレスの割り当てが終了している [7]。そのため、移動端末が必ずグローバル IP アドレスを必要とする Mobile IP Traversal of NAT Devices は、現 IPv4 ネットワークの課題に逆行する致命的な課題を持つ。加えて、Mobile IP Traversal of NAT Devices の通信は常に HA による中継を必要とするため、通信経路が冗長化するという課題がある。

第3章 NTMobile

図2にNTMobileの概要を示す。NTMobileは、NTMobileを実装したNTM端末、通信経路を指示するDC (Direction Coordinator)、エンドエンドでの通信が行えない場合にパケットの中継を行うRS (Relay Server)によって構成される。DCおよび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。

NTMobileは、NTM端末に対して位置に依存しない仮想IPアドレスを割り当て、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う。DCはDNSサーバの機能を持ち、NTM端末の通信開始時に通信相手の名前解決を行った後、名前解決で得た情報を元に最適な通信経路の指示を行う。また、DCがNAT配下の端末に対して定期的にKeep Aliveを行うことにより端末との通信経路を確保し、NATが導入されたプライベートネットワークにおいても通信接続性を実現する。仮想IPアドレスは端末の移動により変化しないため、通信中に端末がネットワークを切り替えた場合でも、アプリケーションや通信相手に対してIPアドレスの変化を隠蔽し、移動透過性を実現する。アプリケーションによって生成された仮想IPアドレスに基づくパケットは、端末の実IPアドレスでカプセル化を行い、通信相手に送信される。端末どうしが直接通信を行えない場合は、RS経由の通信を行うが、その場合であっても複数のRSの中から1つを選択し、冗長経路の少ない経路を生成できる。

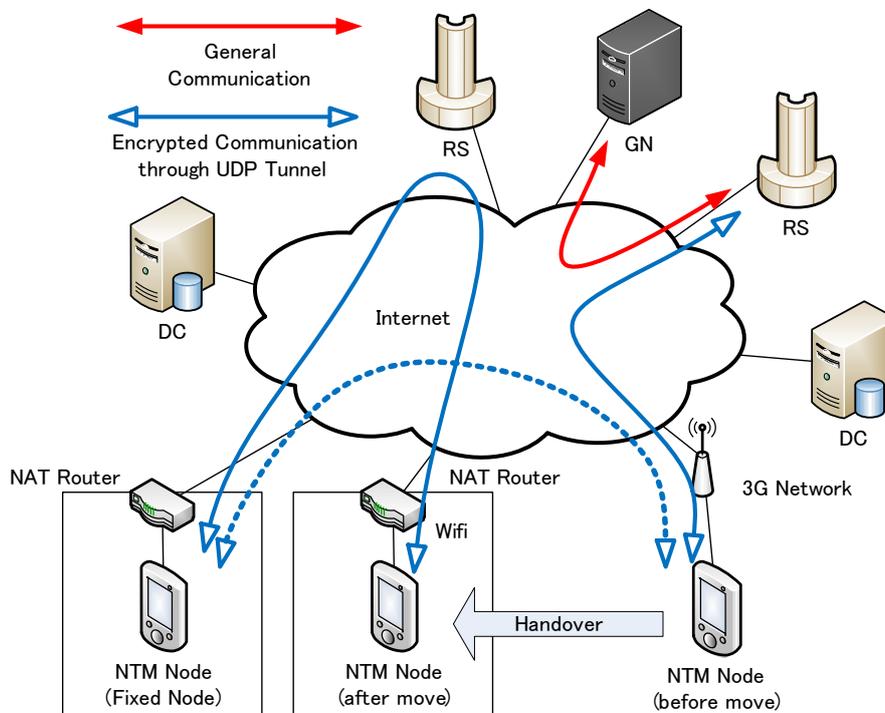


図2 NTMobileの概要

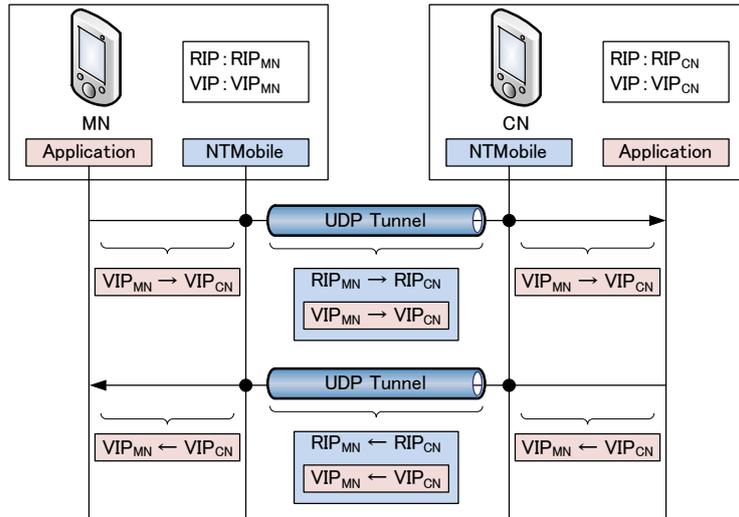


図3 トンネル通信時の動作

3.1 端末起動時と通信開始時の動作

以降の説明では、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) として説明する。また、NTM 端末 N の実 IPv4 アドレスを RIP_N 、仮想 IPv4 アドレスを VIP_N とし、NTM 端末 N を管理する DC を DC_N とする。NTM 端末 N1 と NTM 端末 N2 がトンネル通信時に用いる Path ID を $Path ID_{N1-N2}$ とする。Path ID は通信開始時に DC が NTM 端末、RS に対して配布する情報であり、NTMobile の通信を一意に識別するための通信識別子である。

端末起動時に MN は自身を管理する DC_{MN} に対して、 RIP_{MN} を含む端末情報の登録を行う。 DC_{MN} は MN の端末情報をデータベースに登録した後、MN に対して VIP_{MN} を配布する。

通信開始時に MN は DC_{MN} に対して、CN の名前解決およびトンネル構築の指示を依頼する。 DC_{MN} は、DNS サーバの仕組みを利用し、 DC_{CN} の探索を行い、 DC_{CN} から CN の端末情報を取得する。その後、 DC_{MN} は MN および CN の端末情報を元に適切なトンネル経路を判断し、MN と CN に対してトンネル構築の指示を行う。MN と CN は DC_{MN} の指示に従い、トンネルを構築する。

3.2 トンネル通信時の動作

図3にトンネル通信時の動作を示す。MN のアプリケーションは仮想 IP アドレスを用いてパケット (送信元: VIP_{MN} 、宛先: VIP_{CN}) を生成する。その後、仮想 IP アドレスに基づくパケットは NTMobile の機能により実 IP アドレス (送信元: RIP_{MN} 、 RIP_{CN}) でカプセル化され CN へ送信される。MN からのパケットを受け取った CN は、NTMobile の機能によりパケットのデカプセル化を行い、仮想 IP アドレスに基づくパケットを取り出す。その後、CN のアプリケーションに仮想 IP アドレスに基づくパケットを送ることにより通信を行う。

この手法により、MN や CN がネットワークを切り替えて実 IP アドレスが変化した場合でもアプリケーションが認識している仮想 IP アドレスは変化しないため、通信を継続することができる。

3.3 仮想 IP アドレスの管理に係わる課題

NTMobile では、仮想 IPv4 アドレスとして、IANA (Internet Assigned Numbers Authority) で規定された「198.18.0.0/15」 [25] のアドレス帯域を利用している。このアドレス帯域はネットワーク性能試験用に確保された帯域であるため、実ネットワークの IP アドレスとして利用されないことが保証されている。この帯域を、DC 同士が相互に管理し、全ての NTM 端末の仮想アドレスが重複しないように割り当てている。しかし、このアドレス帯域中の IP アドレスはわずか 13 万個しかなく、NTMobile を実用化した際、アクティブに利用できる NTM 端末数が 13 万台と限られてしまう課題が存在した。スマートフォンを始めとした通信機器の普及率が年々増加している昨今 [26] では、この課題が NTMobile の実用性・拡張性を大きく損なうため、この制約を除去することが NTMobile 最大の課題となっている。

第4章 提案手法

本章において、仮想 IPv4 アドレスに係わる制約を一切除去する手法を述べる。従来の NTMobile では仮想 IP アドレスを通信識別子として利用している。そのため、アドレス帯域が小さい仮想 IPv4 アドレスにおいては、NTMobile の端末数を制限してしまう。提案手法では、仮想 IP アドレスから通信識別子の役割を取り除き、Path ID と呼ぶ通信識別子を用いて NTMobile の通信を一意に識別する。通信中は NTM 端末が Path ID に基づいた仮想 IP アドレスの変換を行うことにより通信を実現する。上記の手法により、NTMobile 上の通信を Path ID のみで識別できるようになり、端末内で自由に仮想 IPv4 アドレスを利用することが可能となる。また、従来の NTMobile では DC から仮想 IPv4 アドレスの割り当てを行っていたが、提案手法ではそれを行わず、NTM 端末がそれぞれ自律的に仮想 IPv4 アドレスを管理する点が異なる。

4.1 通信シーケンス

4.1.1 端末起動時

図 4 に NTM 端末が自端末用の仮想 IP アドレスを生成する動作を示す。MN は端末起動時に、DC_{MN} に対して Registrtion Request を送信し、RIP4_{MN} を含む端末情報を DC_{MN} に登録する。DC_{MN} は MN の端末情報を登録した後、MN に登録完了の応答として Registrtion Response を送信する。MN は DC_{MN} から Registration Response を受信した際に、仮想 IPv4 アドレス空間から仮想 IPv4 アドレスを自律的に生成し、自端末の IP アドレスとしてアプリケーションに認識させる。

以前の NTMobile では、DC が仮想 IPv4 アドレスを管理していた。本提案手法を適用することで、DC による仮想 IPv4 アドレスの管理が不要となり、サーバ群の負荷低減にもつながる。

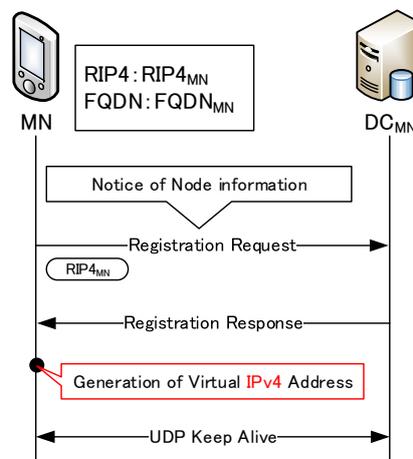


図 4 端末起動時の仮想 IP アドレス生成動作

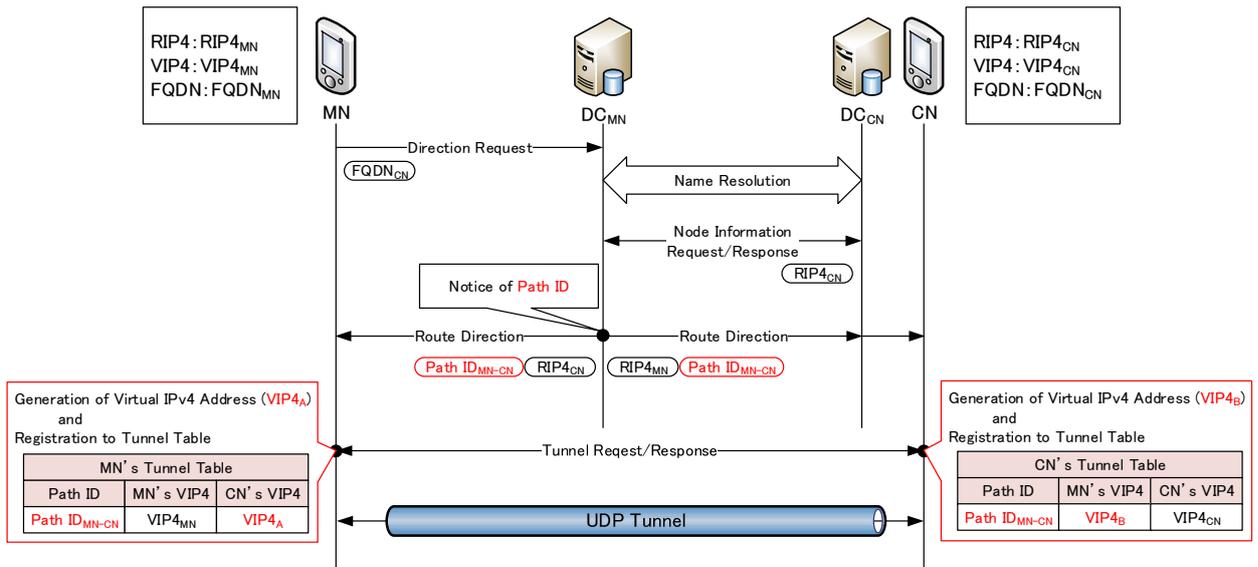


図 5 NTM 端末間通信における通信開始時の動作

4.1.2 通信開始時

図 5 に提案手法による NTM 端末間の通信開始時の動作を示す。MN はアプリケーションから DNS 問い合わせをフックすると DC_{MN} に対して Direction Request を送信し、CN の名前解決およびトンネル構築の指示を依頼する。DC_{MN} は名前解決のシーケンス中に CN の NS レコードを用いて DC_{CN} を探索し、TXT レコードを用いて DC_{CN} が一般の DNS サーバでないことを判断する。その後、DC_{MN} は Node Information Request / Response にて CN の端末情報を取得する。CN の端末情報を取得した DC_{MN} は Route Direction に Path ID_{MN-CN} を含む通信経路の指示を載せて MN および CN に送信する。DC_{MN} から Route Direction を受信した MN と CN は、Tunnel Request / Response によりトンネルを構築する。その際、MN は端末内部で一意的となる CN 用の仮想 IPv4 アドレス VIP4_A を自律的に生成する。VIP4_A を生成した MN は、VIP4_A を Path ID_{MN-CN} と関連付けて、トンネル通信の情報を記録するトンネルテーブルに登録する。その後、MN は DNS メッセージ内の通信相手の IP アドレスを VIP4_A に変更し、DNS 応答としてアプリケーションに渡す。同様に、CN では MN 用の仮想 IPv4 アドレスとして VIP4_B を自律的に生成し、CN のトンネルテーブルに登録する。

4.1.3 トンネル通信時

図 6 に NTM 端末間のトンネル通信によるアドレスの遷移を示す。MN のアプリケーションは、自身の仮想 IPv4 アドレスを VIP4_{MN}、CN の仮想 IPv4 アドレスを VIP4_A として認識している。また、CN のアプリケーションは、自身の仮想 IPv4 アドレスを VIP4_{CN}、MN の仮想 IPv4 アドレスを VIP4_B として認識している。

MN のアプリケーションは CN へパケットを送信する際、仮想 IP アドレスが記載された仮想 IP パケット（送信元：VIP4_{MN}、宛先：VIP4_A）を生成する。MN は宛先アドレスである VIP4_A をキーとしてトンネルテーブルを検索し、該当したエントリにしたがって仮想 IP パケットを実 IP アドレス（送信元：RIP4_{MN}、宛先：RIP4_{CN}）でカプセル化する。このとき、カプセル化するパケットには NTMobile の情報を記載した NTM ヘッダを付加する。NTM ヘッダには NTMobile の通信識別子である Path ID_{MN-CN} が含まれている。

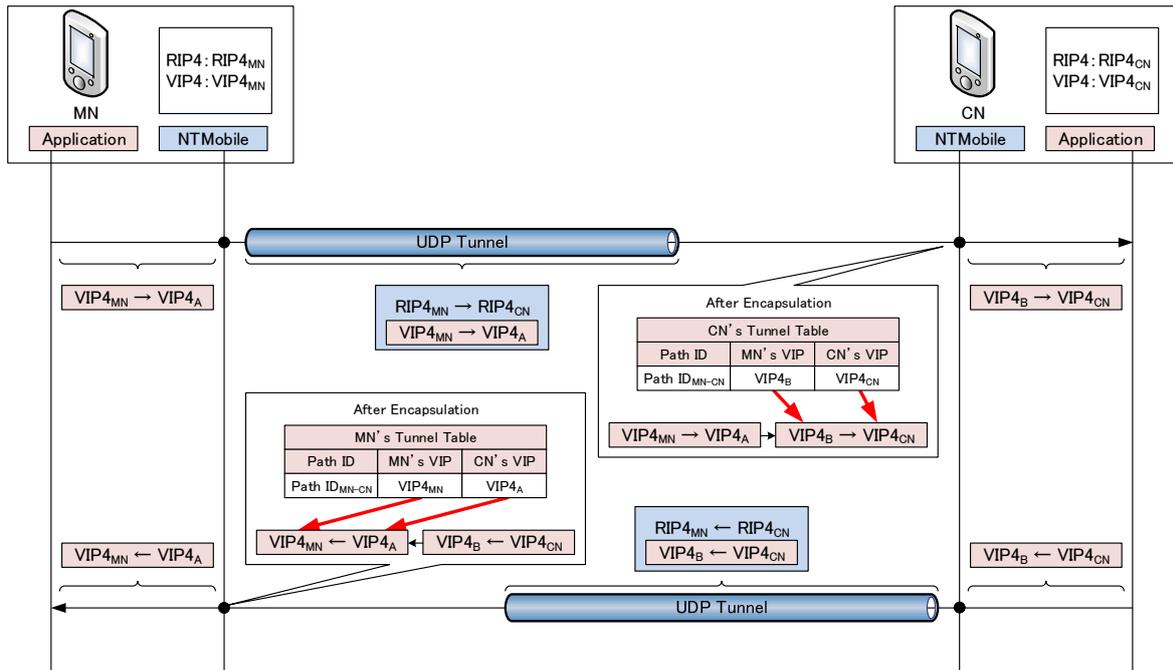


図 6 NTM 端末間通信におけるトンネル通信時のアドレス遷移

その後、MN はカプセル化されたパケットを CN へ送信する。CN はカプセル化パケットを受信すると、パケットのデカプセル化を行い仮想 IP パケットを抽出する。その後、CN はパケット内の Path ID_{MN-CN} を元に自身のトンネルテーブルを検索し、MN の仮想 IPv4 アドレス VIP4_B を取得する。CN は仮想 IP パケット内の送信元アドレスを VIP4_{MN} から VIP4_B へ、宛先アドレスを VIP4_A から VIP4_{CN} へ変換し、CN のアプリケーションへ渡す。

また、逆方向の通信においては、受信側である MN が仮想 IP パケット内の仮想 IPv4 アドレスを Path ID_{MN-CN} に基づく仮想 IPv4 アドレスに変換することで通信を行う。

4.2 通信相手が一般端末間の場合

NTMobile では NTM 端末と一般端末間の通信は RS-N を利用することで実現している [5]。提案手法を適用すると、現状の RS-N では通信が識別できず、一般端末への通信中継が行われなくなる。そのため、RS-N へ Path ID による NTMobile の通信を識別する機能を追加し、一般端末との通信を可能にする。

4.2.1 通信開始時

図 7 に提案手法による NTM 端末が一般端末と通信する際の通信開始時の動作を示す。この際、MN は 4.1.1 節により、DC_{MN} への端末登録処理およびアプリケーションへの仮想 IPv4 アドレスの割り当て処理が完了しているものとする。MN はアプリケーションから DNS 問い合わせをフックすると DC_{MN} に対して Direction Request を送信し、GN の名前解決およびトンネル構築の指示を依頼する。DC_{MN} は GN の NS レコードを用いて GN を管理する DNS サーバ_{GN} を探索する。DC_{MN} は探索により見つかった DNS サーバ_{GN} と TXT レコードを交換することにより GN が一般端末であると判断する。その後、GN の端末情報を取得した DC_{MN} は Relay Direction を RS-N へ送信し、一般端末へのパケット中継を依頼する。DC_{MN} は Route

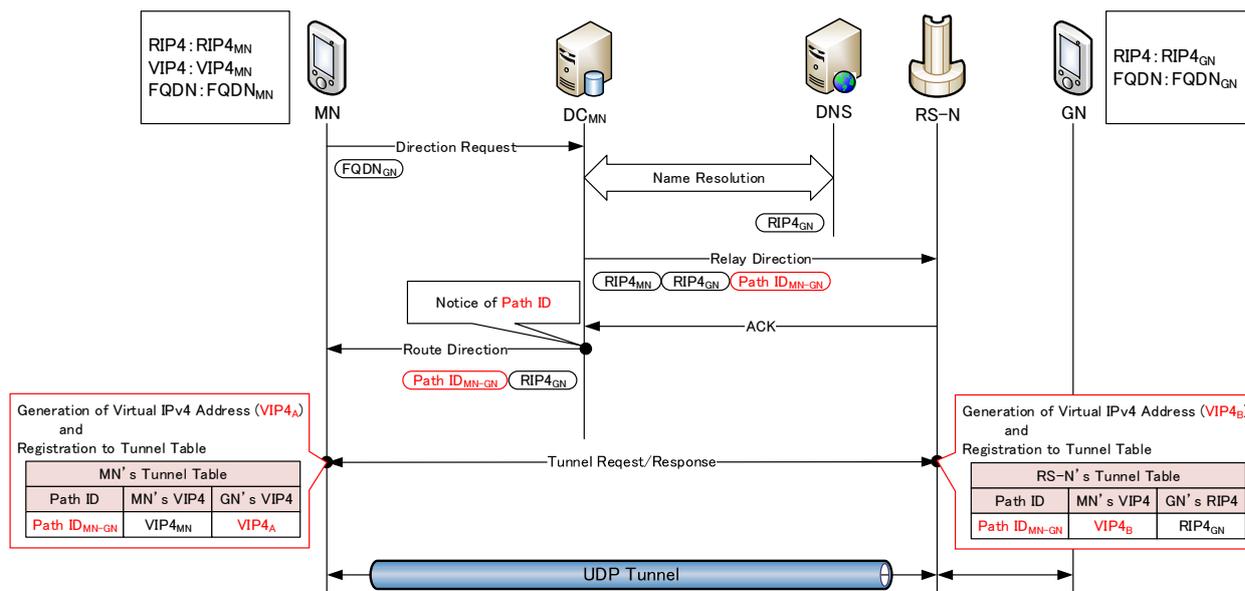


図 7 NTM 端末-一般端末間通信における通信開始時の動作

Direction に Path ID_{MN-GN} を含む通信経路の指示を載せて MN に送信する。DC_{MN} から Relay Direction を受信した RS-N と Route Direction を受信した MN は、Tunnel Request / Response によりトンネルを構築する。その際、MN は端末内部で一意的となる GN 用の仮想 IPv4 アドレス VIP_{4A} を自律的に生成する。VIP_{4A} を生成した MN は、VIP_{4A} を Path ID_{MN-GN} と関連付けて、トンネル通信の情報を記録するトンネルテーブルに登録する。その後、MN は DNS メッセージ内の通信相手の IP アドレスを VIP_{4A} に変更し、DNS 応答としてアプリケーションに渡す。同様に、RS-N では MN 用の仮想 IPv4 アドレスとして VIP_{4B} を自律的に生成し、Path ID_{MN-GN} と関連付けて RS-N のトンネルテーブルに登録する。

4.2.2 トンネル通信時

図 8 に NTM 端末と一般端末間のトンネル通信によるアドレスの遷移を示す。MN のアプリケーションは、自身の仮想 IPv4 アドレスを VIP_{4MN}、GN の仮想 IPv4 アドレスを VIP_{4A} として認識している。RS-N は、MN の仮想 IPv4 アドレスを VIP_{4B} として認識している。

MN のアプリケーションが GN へパケットを送信する際、仮想 IP アドレスを用いて仮想 IP パケット（送信元：VIP_{4MN}、宛先：VIP_{4A}）を生成する。MN は宛先アドレスである VIP_{4A} をキーとしてトンネルテーブルを検索し、該当したエントリにしたがって仮想 IP パケットを実 IP アドレス（送信元：RIP_{4MN}、宛先：RIP_{4RS}）でカプセル化する。このとき、カプセル化するパケットには NTM Mobile の情報を記載した NTM ヘッダを付加する。NTM ヘッダには NTM Mobile の通信識別子である Path ID_{MN-GN} が含まれている。MN はカプセル化されたパケットを RS-N へ送信する。RS-N はカプセル化パケットを受信すると、パケットのデカプセル化を行い仮想 IP パケットを抽出する。その後、RS-N はパケット内の Path ID_{MN-GN} を元に自身のトンネルテーブルを検索し、MN の仮想 IPv4 アドレス VIP_{4B} を取得する。RS-N は仮想 IP パケット内の送信元アドレスを VIP_{4MN} から VIP_{4B} へ、宛先アドレスを VIP_{4A} から RIP_{4GN} へ変換し、RS-N の Netfilter に渡す。Netfilter では NAT 処理を行い、パケット内の送信元アドレスを VIP_{4B} から RIP_{4RS} に変換した後、GN へパケットを送信する。

逆方向の通信の場合、RS-N は GN からパケット（送信元：RIP_{4GN}、宛先：RIP_{4RS}）を受信すると、NAT

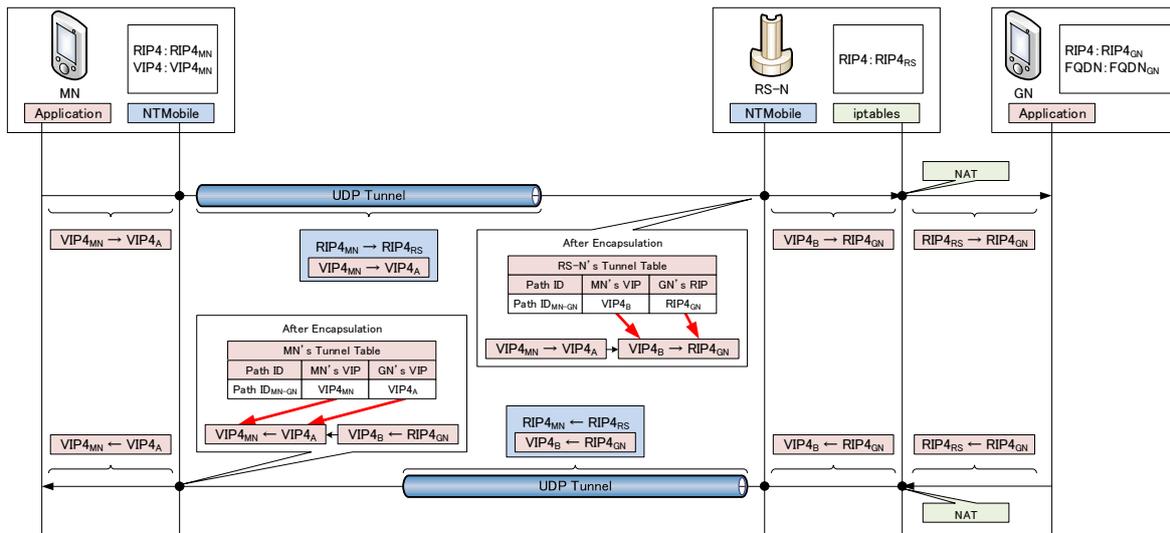


図 8 NTM 端末-一般端末間通信におけるトンネル通信時のアドレス遷移

処理を用いて GN から受信したパケット内の宛先アドレスを RIP4_{RS} から VIP4_B に変換する。その後、パケット内の VIP4_B と RIP4_{GN} を検索キーに RS-N 内のトンネルテーブルを検索する。該当したトンネルテーブルのエントリにしたがって、仮想 IP パケットを実 IP アドレス（送信元：RIP4_{RS}、宛先：RIP4_{MN}）でカプセル化し MN へパケットを送信する。RS-N からカプセル化されたパケットを受信した MN は、デカプセル化後に仮想 IP パケット内の仮想 IPv4 アドレスを Path ID_{MN-GN} に基づく仮想 IPv4 アドレスに変換することで通信を行う。

第5章 実装

NTMobile の基本動作は Linux において既に動作が検証されている。

図 9 に NTM 端末のモジュール構成を示す。NTMobile デーモンは DC への NTM 端末情報の登録と仮想 IP アドレスの取得、および DC の指示に従ったトンネル構築を行う。カーネルモジュールはパケットのカプセル化/デカプセル化および暗号化処理を行う。各モジュールに以下のような改造を行った。

5.1 NTMobile デーモン

NTM 端末の端末登録時に自端末の仮想インタフェースに仮想 IPv4 アドレスを設定する。通信開始時に通信相手用の仮想 IPv4 アドレスを端末内部で自律的に生成し、トンネルテーブルに登録する。またこの際、通信受信側（レスポнда）となる場合は、トンネル構築中に通信相手（イニシエータ）用の仮想 IPv4 アドレスを端末内部で自律的に生成し、トンネルテーブルに登録する。DNS 応答メッセージを用いて通信相手用の仮想 IPv4 アドレスを通知し、アプリケーションに仮想 IP アドレスを通信相手と認識させる。

5.2 NTMobile カーネルモジュール

NTMobile カーネルモジュールが受信パケットをフックし、デカプセル化を行った際に NTM ヘッダ内から Path ID を取得する。Path ID をキーとして、トンネルテーブルから通信相手用の仮想 IPv4 アドレスを取得する。その後、仮想 IP パケット内の仮想 IPv4 アドレスの送信元および宛先を端末内部で管理する仮想 IPv4 アドレスに変換する。

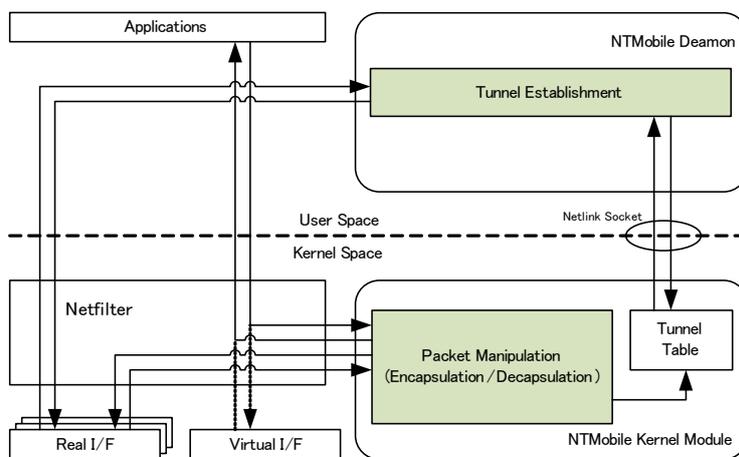


図 9 NTM 端末のモジュール構成

第6章 評価

本章では、5章のモジュールを実装したNTM端末による動作の性能評価を行う。また、提案手法とNTMobileの従来手法およびMobile IPv4によるアドレス資源の利用に関する比較・評価を行う。

6.1 性能測定

図10に試験ネットワークの構成を、表1に各装置の仕様を示す。NTM端末MNおよびCNはLinuxをインストールした実機PCに実装し、同一ネットワーク上に直接接続した。試験ネットワークでは、NATを導入していないが、本提案はNTMobileの内部処理に関わる実装のみであるため、検証は図10の構成で十分と判断した。MN、CN、DCはそれぞれ1000BASE-Tによる有線LANで接続している。

提案手法では、従来のトンネル通信に仮想IPパケットのアドレス変換処理が加わる。そのため、MNとCN間でiperf^{*1}を用いたTCP通信を行い、提案手法の動作検証およびトンネル通信中のスループット測定を行った。また、従来のNTMobileにおいても同様にスループットを測定し、提案手法によるスループットの測定結果と比較を行った。スループット測定には、10秒間のスループット測定をMN、CN間で10回繰り返し、その平均値を算出した。

表2にNTM端末間のトンネル通信によるスループットの測定結果を示す。従来手法に比べて提案手法のスループットは0.5%低い値となった。この結果より、提案手法の通信において、NTM端末の仮想IPv4アドレス変換処理がスループットの低下に大きな影響を及ぼすことがないことがわかった。

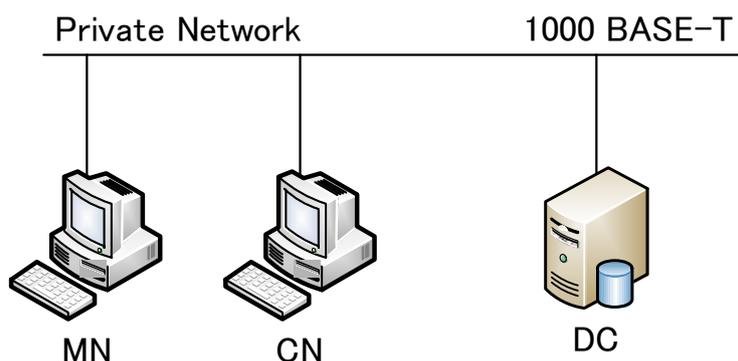


図10 ネットワーク構成

^{*1}<http://sourceforge.net/projects/iperf/>

表 1 NTM 端末の仕様

	MN	CN
Hardware	Thirdwave Prime	Thirdwave Prime
OS	Ubuntu 10.04	Ubuntu 10.04
Linux Kernel	2.6.32-21-generic	2.6.32-21-generic
CPU	Intel Core i7-860	Intel Core i7-930
Memory	3GB	3GB

表 2 トンネル通信時のスループット測定結果

	Conventional	Proposal
Throughput(Mbps)	402.5	400.4

6.2 従来手法との比較

移動透過性技術はネットワークの課題を解決するため、IP アドレスから位置識別子 (locator) と通信識別子 (identifier) を分離する形で提案・開発されている。表 3 に各手法における識別子の違いをまとめる。

表 3 識別子の比較

	Mobile IPv4	Conventional	Proposal
位置識別子	CoA	RIP	RIP
位置識別子の管理装置	DHCP	DHCP	DHCP
通信識別子	HoA	VIP	Path ID (一部 VIP)
通信識別子の管理装置	HA	DC	NTM 端末, RS-N

Mobile IPv4 では、移動端末が移動先のネットワークで割り当てられる IP アドレス CoA が位置識別子となり、NTMobile では、移動端末がそのネットワークで取得する実 IP アドレス RIP が位置識別子となる。手法毎に名称は異なるが、CoA と RIP は DHCP サーバから割り当てられる一般的な IP アドレスである。また、Mobile IPv4 の通信識別子は、ホームネットワーク上の HA から割り当てられる IP アドレス HoA であり、従来手法の NTMobile では DC から配布される仮想 IP アドレス VIP が通信識別子となる。提案手法においては、NTM 端末（一般端末との通信時は RS-N も同様）が Path ID を用いて通信を識別することで、NTMobile 上の VIP から通信識別子の役割を取り除いている。そのため、提案手法における通信識別子は Path ID となる。しかし、アプリケーション自体は VIP を用いて相手端末を認識しているため、一部 VIP も通信識別子としている。

表 4 に Mobile IPv4 および NTMobile の従来手法と提案手法におけるアドレス資源の利用を比較した表を示す。表 4 において、「G」はグローバル IPv4 アドレスとして利用可能な IP アドレス数^{*2}、「V」は仮想 IPv4

^{*2}現在、IANA による新規グローバル IPv4 アドレスの割り当ては終了しているため、利用できるグローバル IPv4 アドレス数を算出することはできない。そのためグローバル IPv4 アドレスは、すでに割り当てられた組織、研究機関等から提供されなにかぎり利用

アドレスとして利用可能な IP アドレス数^{*3}を示す。また、「普及可能な端末台数」は、その手法において移動端末として利用できる端末の最大値を表し、「1台あたりの同時接続台数」は、1台の移動端末が同時に通信を行うことが出来る最大の端末数を表している。

「普及可能な端末台数」に関して、Mobile IPv4 および NTMobile の従来手法では、通信識別子がそれぞれグローバル IPv4 アドレス、仮想 IPv4 アドレスであり、これらの IP アドレスがグローバルで一意になる必要がある。そのため、普及可能な端末数の上限はそれぞれの通信識別子の IP アドレスの上限に影響し、それぞれ G 台、 V 台が上限となる。提案手法では、仮想 IPv4 アドレスを移動端末自身が管理し、必ず仮想 IPv4 アドレスを自端末に割り当てることができるため、端末数の上限は仮想 IPv4 アドレス数に依存せず、無制限に利用することができる。その際、提案手法の通信識別子である Path ID は 128bit の領域を持つため、NTMobile の通信自体はグローバルで 2^{128} 本分までという制約が発生する。

「1台あたりの同時接続台数」に関して、Mobile IPv4 および NTMobile の従来手法では、通信識別子である IP アドレスがグローバルで一意になるため、自端末を除いた $G-1$ 台、 $V-1$ 台まで通信相手として認識することができる。提案方式においては、Path ID で通信を識別するものの、端末のアプリケーション自体は仮想 IPv4 アドレスで通信相手を認識するため、1台あたりの接続台数の上限は従来手法と同様に仮想 IPv4 アドレス数から自端末を除いた $V-1$ 台が上限となる。

Mobile IPv4 において IP アドレス枯渇が叫ばれている昨今、新規にグローバル IPv4 アドレスを確保することは難しく、移動透過性技術として広く普及することは困難である。また、従来の NTMobile においても、仮想 IPv4 アドレスの帯域が狭く、移動端末は最大でも 13 万台で打ち止めとなってしまうていた。提案手法においては、仮想 IPv4 アドレスから通信識別子としての役割を取り除き、Path ID を用いて通信を識別できるようになったため、ほぼ無限の規模まで移動端末を普及させることが可能となる。

表 4 従来手法との比較

	Mobile IPv4	Conventional	Proposal
普及可能な端末台数 (台)	G	V	∞
1台あたりの同時接続台数 (台)	$G-1$	$V-1$	$V-1$

することはできない。

^{*3}仮想 IPv4 アドレス帯域 (198.18.0.0/15) は 131,072 個の IP アドレス持つがネットワークアドレスおよびブロードキャストアドレスは除くため、 V の値は 131,070 個となる。

第7章 まとめ

本論文では、NTMobile の仮想 IPv4 アドレスの管理方法について提案を行った。NTMobile の IPv4 通信において、NTM 端末内部で仮想 IPv4 アドレスを自律的に生成する。Path ID で通信を識別し、通信パケットの仮想 IP アドレスを NTM 端末内部で自ら生成した仮想 IP アドレスに変換する手法を提案した。これにより、限られたアドレス帯域で NTMobile をほぼ無限の規模まで運用できるようになった。そして、Linux 上で提案手法の実装を行い、動作を検証した。従来の NTMobile と提案手法による NTMobile を用いて NTM 端末間のトンネル通信によるスループットを比較し、提案手法によるスループットの劣化がほとんどないことを確認した。

参考文献

- [1] 内藤克浩, 上酔尾一真, 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 年 1 月.
- [2] 鈴木秀和, 上酔尾一真, 水谷智大, 西尾拓也, 内藤克浩, 渡邊晃: NTMobile における通信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 年 1 月.
- [3] 上酔尾一真, 鈴木秀和, 内藤克浩, 渡邊晃: IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価, 情報処理学会論文誌, Vol.54, No.10, pp.2288 – 2299, 2013 年 10 月.
- [4] 納堂博史, 杉原史人, 鈴木秀和, 内藤克浩, 渡邊晃: NTMobile の実用化に向けた統合的枠組の検討, 情報処理学会研究報告モバイルコンピューティングとユビキタス通信研究会 (MBL), Vol.2015-MBL-77, No.20, pp.1 – 8, 2015 年 12 月.
- [5] 土井敏樹, 鈴木秀和, 内藤克浩, 渡邊晃: NTMobile におけるアドレス変換型リレーサーバの実装と動作検証, 情報処理学会研究報告モバイルコンピューティングとユビキタス通信 (MBL), Vol.2013-MBL-67, No.11, pp.1 – 6, 2013 年 9 月.
- [6] 上酔尾一真, 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 年 9 月.
- [7] JPNIC:IPv4 アドレスの在庫枯渇に関して,
<https://www.nic.ad.jp/ja/ip/ipv4pool/>.
- [8] J. Rosenberg, J. Weinberger, C. Huitema and R. Mahy.: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), RFC3489, IETF(2003).
- [9] J. Rosenberg, R. Mahy, P. Matthews and D. Wing. : Session Traversal Utilities for NAT (STUN), RFC5389, IETF(2008).
- [10] R. Mahy, P. Matthews and J. Rosenberg.: Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN), RFC5766, IETF(2010).
- [11] S. Perreault and J. Rosenberg.: Traversal Using Relays around NAT (TURN) Extensions for TCP Allocations, RFC6062, IETF(2010).
- [12] J. Rosenberg.: Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, RFC5245, IETF(2010).
- [13] M. Westerlund and C. Perkins.: IANA Registry for Interactive Connectivity Establishment (ICE) Options, RFC6336, IETF(2011).
- [14] B. Carpenter.: Connection of IPv6 Domains via IPv4 Clouds, RFC3056, IETF(2001).
- [15] F. Templin, T. Gleeson, M. Talwar and D. Thaler.: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), RFC4214, IETF(2005).
- [16] G. Tsirtsis and P. Srisuresh.: Network Address Translation - Protocol Translation (NAT-PT), RFC2766, IETF(2000).
- [17] J. Hagino and K. Yamamoto.: An IPv6-to-IPv4 Transport Relay Translator, RFC3142, IETF(2001).
- [18] C. Perkins. : IP Mobility Support for IPv4, Revised, RFC5944, IETF(2010).
- [19] H. Levkowitz and S. Vaarala.: Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC3519, IETF(2003).

- [20] G. Tsirtsis, V. Park and H. Soliman. : Dual-Stack Mobile IPv4, RFC5454, IETF(2009).
- [21] D. Johnson, C. Perkins and J. Arkko. : Mobility Support in IPv6, RFC3775, IETF(2004).
- [22] H. Soliman. : Mobile IPv6 Support for Dual Stack Hosts and Routers, RFC5555, IETF(2009).
- [23] M. Ishiyama, M. Kunishi, K. Uehara, H. Esaki and F. Teraoka.: LINA: A New Approach to Mobility Support in Wide Area Networks, IEICE Transactions on Communications, Vol. E84-B, No. 8, pp. 2076—2086 (2001).
- [24] 國司 光宣, 石山 政浩, 植原 啓介, 寺岡 文男 : 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 年 2 月.
- [25] S. Bradner.: Benchmarking Methodology for Network Interconnect Devices, RFC2544, IETF(1999).
- [26] 総務省:平成 25 年版 主な情報通信機器の普及状況 (世帯) ,
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc243110.html>.
- [27] G. Huston, A. Lord and P. Smith.: IPv6 Address Prefix Reserved for Documentation, RFC3849, IETF(2004).

研究業績

研究会・大会等

- (1) 加古将規, 鈴木秀和, 内藤克浩, 渡邊 晃 : NTMobile における仮想 IP アドレスの管理方法の提案と評価, マルチメディア, 分散, 協調とモバイル (DICOMO2014) シンポジウム論文集, Vol.2014, pp.1307 - 1312, 2014 年 7 月.
- (1) 加古将規, 鈴木秀和, 内藤克浩, 渡邊 晃 : NTMobile における仮想 IPv4 アドレスの管理方式の提案と実装, 情報処理学会研究報告モバイルコンピューティングとユビキタス通信 (MBL), Vol.2014-MBL-71, No.29, pp.1 - 6, 2014 年 5 月.
- (2) 加古将規, 上酔尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃 : NTMobile における仮想 IPv4 アドレス運用手法の提案と実装, 第 76 回情報処理学会全国大会講演論文集, Vol.2014, No.1, pp.347 - 348, 2014 年 3 月.
- (3) 加古将規, 上酔尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃 : NTMobile における仮想 IPv4 アドレス運用手法の提案, 平成 25 年度電気関係学会東海支部連合大会論文集, Vol.2013, No.P3-8, 2013 年 9 月.

受賞歴

- (1) 第 76 回情報処理学会全国大会・学生奨励賞受賞 (2014 年 3 月)
加古将規, 上酔尾一真, 鈴木秀和, 内藤克浩, 渡邊 晃 : NTMobile における仮想 IPv4 アドレス運用手法の提案と実装, 第 76 回情報処理学会全国大会講演論文集, Vol.2014, No.1, pp.347 - 348, 2014 年 3 月.

付録A 仮想IPv6アドレスのフォーマット

図 11 に仮想 IPv6 アドレスのフォーマットを示す。仮想 IPv6 アドレスは、IPv6 アドレスの上位 64bit をネットワーク部とし、下位 64bit をホスト部として定義する。ネットワーク部の上位 32bit は仮想 IP アドレス領域のネットワークプレフィックスと定義し、実ネットワークで利用されない「2001:db8::/32」[27]を用いる。このアドレス帯域は APNIC (Asia Pacific Network Information Centre) によって文書作成用に予約された帯域であり、実 IP アドレスとして利用されないことが保証されている。ネットワーク部の下位 32bit には、仮想 IPv6 アドレスを管理する DC のグローバル IPv4 アドレスを記述する。これにより、DC が異なれば仮想 IPv6 アドレスが重複しないことが保証される。ホスト部の 64bit には、DC 内で重複しないように生成した乱数を用いる。これらにより、重複しない仮想 IPv6 アドレスの管理が保証できる。また、DC 毎にアドレス管理が可能となるため、DC 間で仮想 IPv6 アドレスの重複チェックを行う必要がない。

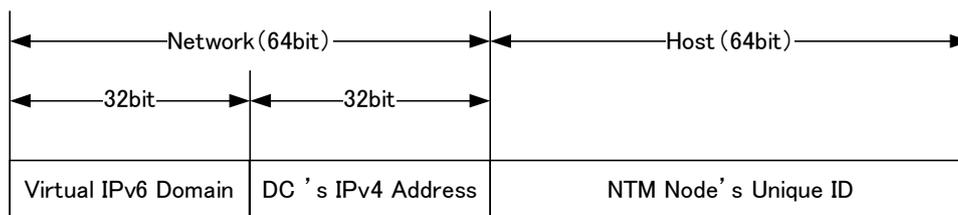


図 11 仮想 IPv6 アドレスのフォーマット