Vol.2014-DPS-159 No.10
Vol.2014-MBL-71 No.10
2014/5/15

NTMobileにおける 仮想IPv4アドレスの管理方式の提案と実装

加古 将規[1,a)]　鈴木 秀和[2]　内藤 克浩[3]　渡邊 晃[2,b)]

概要：NAT（Network Address Translation）を導入したネットワークでは，インターネット側の端末から NAT 配下の端末に対して通信を開始できないという NAT 越え問題が存在し，IPv4 ネットワークの汎用性を損なう要因となっている．また，公共無線網の普及や携帯端末の発達により，移動しながら通信を行いたいという要求（移動透過性技術の要求）が増加している．我々は，NAT 越えと移動透過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，実 IP アドレスとして利用されないアドレス空間の中から一意な仮想 IPv4 アドレスを割り当てる必要がある．そのため，NTMobile の普及を想定した場合，十分な仮想 IPv4 アドレス数が確保できないという課題があった．そこで，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方式を提案する．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 Path ID と関連付ける．以上の手法により，NTMobile の仮想 IPv4 アドレスに関する課題を解決することができる．提案方式を実装した NTM 端末により動作検証および性能評価を行い，性能の劣化がほとんどなく実現できることを確認した．

1. はじめに

現在の IP ネットワークでは IPv4 アドレスの枯渇が問題となっており，短期的な解決策として NAT を導入し，NAT 配下のネットワークにプライベートネットワークを構築することが一般的となっている．しかし，NAT が導入された環境では，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して通信を開始できない NAT 越え問題という通信接続性の課題がある．IPv4 アドレス枯渇問題の長期的な解決策として IPv6 アドレスが検討されているが，IPv6 アドレスは IPv4 アドレスと互換性がないプロトコルとして定義されているため，即座に IPv6 ネットワークに移行することができない．そのためしばらくの間，IP ネットワークは IPv4 ネットワークと IPv6 ネットワークが混在した環境が続き，かつ IPv4 ネットワークには NAT がそのまま利用されるものと想定される．一方，公共無線網の普及や携帯端末の発達により，移動しながら通信を行いたいという要求が増加している．しかし，ネットワークの切り替えに伴い 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．そのため通信中に IP アドレスが変化しても通信を継続できる技術（移動透過性技術）が必要である．

本論文では，今後も重要な位置づけを占めることが想定される IPv4 ネットワークを中心に記述する．IPv4 ネットワークにおいて NAT 越えと移動透過性を同時に実現する技術として，Mobile IPv4[6] を NAT が存在する環境でも利用できるようにした Mobile IP Traversal of NAT Devices[7] がある．しかし，この技術では，NAT 配下の端末への通信接続性を確保するために HA（Home Agent）をグローバルアドレス空間に設置する必要がある．即ち，移動端末の HoA（Home Address）としてグローバル IP アドレスを割り振る必要があり，グローバル IP アドレスの枯渇に相反するという課題がある．また，Mobile IP Traversal of NAT Devices は常に中継装置である HA を経由した通信が行なわれるため，通信経路が冗長化するという課題がある．

そこで我々は NAT 越えと移動透過性を同時に実現する技術として，NTMobile（Network Traversal with Mobility）[1], [2], [3], [4], [5] を提案している．NTMobile では，NTMobile の機能を実装した端末に対して，端末の位置に依存しない仮想 IP アドレスを割り当てる．端末のアプリ

[1] 名城大学大学院理工学研究科
Graduate School of Science and Technology, Meijo University
[2] 名城大学理工学部
Faculty of Science and Technology, Meijo University
[3] 三重大学大学院工学研究科
Graduate School of Engineering, Mie University
[a)] masanori.kako@wata-lab.meijo-u.ac.jp
[b)] wtnbakr@meijo-u.ac.jp

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．仮想 IP アドレスに基づくパケットは実 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 NAT やネットワーク切り替えによるアドレス変換に影響されないため，アプリケーションは IPv4 ネットワークの制約を一切受けないという利点がある．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領域から生成し，端末に割り当てている．しかし，仮想 IPv4 アドレス領域として利用可能なアドレス領域が小さいため，NTMobile を大規模システムに適用できず，このままでは NTMobile の拡張性がないという課題があった．

この課題を解決するため，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方式を提案する．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 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，NTMobile の仮想 IPv4 アドレスに関する課題を解決することができる．提案方式を実装した NTM 端末により動作検証および性能評価を行い，性能の劣化がほとんどなく実現できることを確認した．

以下，2 章で既存技術，3 章で NTMobile の概要について説明する．そして，4 章で提案方式の動作，5 章で提案方式の実装，6 章で提案方式の評価について述べ，7 章でまとめる．

2. 既存技術

本章では，IPv4 ネットワークで NAT 越えと移動透過性を実現する Mobile IP Traversal of NAT Devices[7] の概要と課題について述べる．

Mobile IP Traversal of NAT Devices 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 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 から割り当てられる位置に依存しない IP アドレス HoA（Home Address）と訪問先のネットワークで利用する 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なわず，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

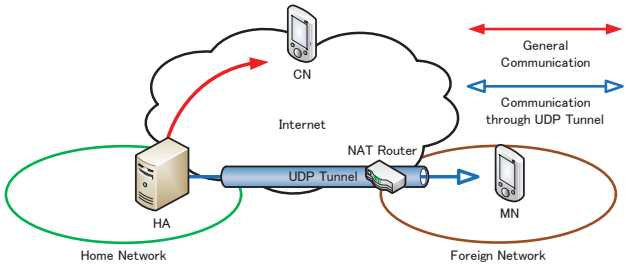

図 1 Mobile IP Traversal of NAT Devices における NAT が存在する環境での通信

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 トンネルと構築する．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．

Mobile IP Traversal of NAT Devices において，MN が通信接続性を確保するためには，HA をグローバルネットワーク上に設置する必要があり，移動端末の利用する HoA は必ずグローバル IP アドレスである必要がある．これは，IPv4 アドレス枯渇が問題となっている昨今では致命的な課題となる．また，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．

3. NTMobile

3.1 NTMobile の概要

図 2 に NTMobile の概要を示す．NTMobile は，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．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 越えに用いる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 CN に対して IP アドレスの変化

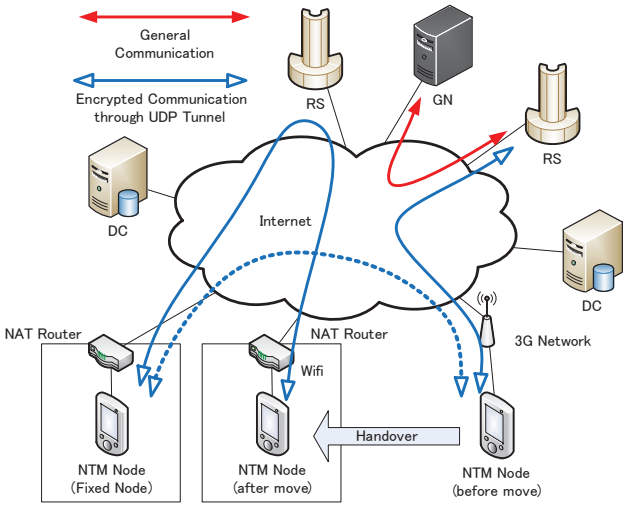

図 2 NTMobile の概要

を隠蔽し，移動透過性を実現する．仮想 IP アドレスに基づくパケットは，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．NTM 端末間の通信は DC の指示により常に最適な通信経路で通信を行うことができる．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．

3.2 端末起動時と通信開始時の動作

以下の説明では，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} 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．

3.3 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：

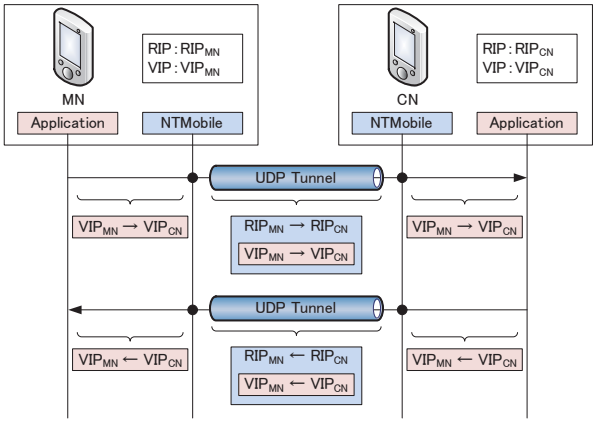

図 3 トンネル通信時の動作

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．

3.4 NTMobile の課題

NTMobile では，仮想 IPv4 アドレスが実 IPv4 アドレスと重複することを避けるため，仮想 IPv4 アドレスを実ネットワークで利用されないネットワーク（198.18.0.0/15）[10] から生成している．しかしこの領域では仮想 IPv4 アドレスを約 13 万個しか確保することができない．

そのため，NTMobile の大規模システムを想定した場合に NTM 端末に割り当てる仮想 IPv4 アドレスが足りず，NTMobile の拡張性を失うことが考えられる．この課題は NTMobile 最大の課題である．

4. 提案方式

NTM 端末が仮想 IPv4 アドレスを自律的に生成し，Path ID を用いて NTMobile の通信を一意に識別する手法について提案する．この手法を用いることにより，NTMobile のシステム全体で仮想 IPv4 アドレス領域を共有する必要がなくなり，限られた仮想 IPv4 アドレス領域を用いて大規模に NTMobile を運用することが可能となる．

4.1 端末起動時の動作

図 4 に NTM 端末起動時の動作を示す．MN は端末起動時に，DC_{MN} に対して NTM Registrtion Request を送信

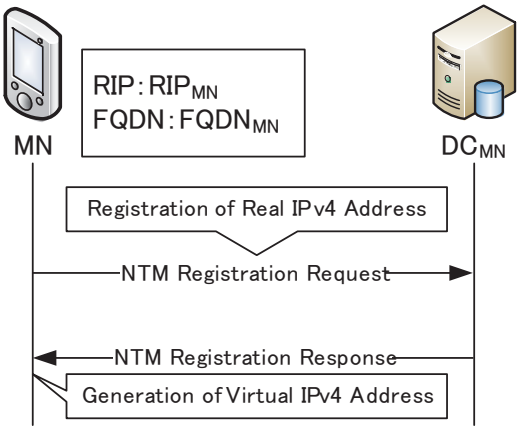

図 4 端末起動時の動作

し，RIP_{MN} 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 NTM Registrtion Response を送信する．MN は DC_{MN} から NTM Registration Response を受信した際に，静的な仮想 IPv4 アドレスを生成し，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．これまでの方式では，NTM Registrtion Response の中に DC が定めた MN の仮想 IPv4 アドレスを含めていた．提案方式では，この情報が不要となるため，DC が仮想 IPv4 アドレスの管理をする必要がなくなる．

4.2 通信開始時の動作

図 5 に MN と CN の通信開始時における動作を示す．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 NTM 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 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 NTM 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 NTM 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 NTM Route Direction を受信した MN は，端末内部で一意となる CN の仮想 IPv4 アドレスとして VIP_B を生成する．VIP_B を生成した MN は，VIP_B 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 VIP_B に変更し，DNS Response for A Record としてアプリケーションに渡す．また同様に，DC_{MN} の NTM Route Direction を DC_{CN} から受信した CN は，端末内部で一意となる MN の仮想 IPv4 アドレスとして VIP_X を生成し，自端末のトンネルテーブルに登録する．

4.3 トンネル通信時の動作

図 6 に，NTM 端末間において提案方式によるトンネル通信を行った場合の動作を示す．MN のアプリケーションは，自身の仮想 IPv4 アドレスを VIP_A，CN の仮想 IPv4 アドレスを VIP_B 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 VIP_Y，MN の仮想 IPv4 アドレスを VIP_X として認識している．

MN のアプリケーションが CN へパケットを送信する際，送信元アドレスに VIP_A，宛先アドレスに VIP_B が記載された仮想 IP パケットが生成される．仮想 IP パケットは実 IP アドレスでカプセル化された後，CN へ送信される．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 Path ID が含まれる．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 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_X を取得する．CN はパケット内の送信元アドレスを VIP_A から VIP_X へ，宛先アドレスを VIP_B から VIP_Y へ変換し，CN のアプリケーションへ渡す．

また，CN のアプリケーションが MN へパケットを送信する際は，MN が同様にデカプセル化時にパケット内の仮想 IPv4 アドレスを変換を行う．

5. 実装

図 7 に NTM 端末のモジュール構成を示す．NTMobile の基本動作は Linux において既に動作が検証されている．NTM 端末はユーザ空間の NTMobile デーモンと，カーネル空間の NTMobile カーネルモジュールにより動作する．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．提案方式は NTMobile デーモンと NTMobile カーネルモジュールを改造することにより動作する．各モジュールに以下のような改造を行った．

- NTMobile デーモン
  NTM 端末の端末起動時に自端末の仮想インタフェースに静的な仮想 IPv4 アドレスを設定する．また，通信開始時に通信相手の仮想 IPv4 アドレスを端末内部に設定し，トンネルテーブルに登録する．提案方式では，通信相手の仮想 IPv4 アドレスを NTM 端末が一意に生成するが，本実装では仮想 IPv4 アドレス生成処理が未実装であるため通信相手の仮想 IPv4 アドレスは静的に設定している．また，DNS 応答メッセージ内の仮想 IPv4 アドレスを NTM 端末が生成した仮想 IPv4 アドレスに変換する．
- NTMobile カーネルモジュール

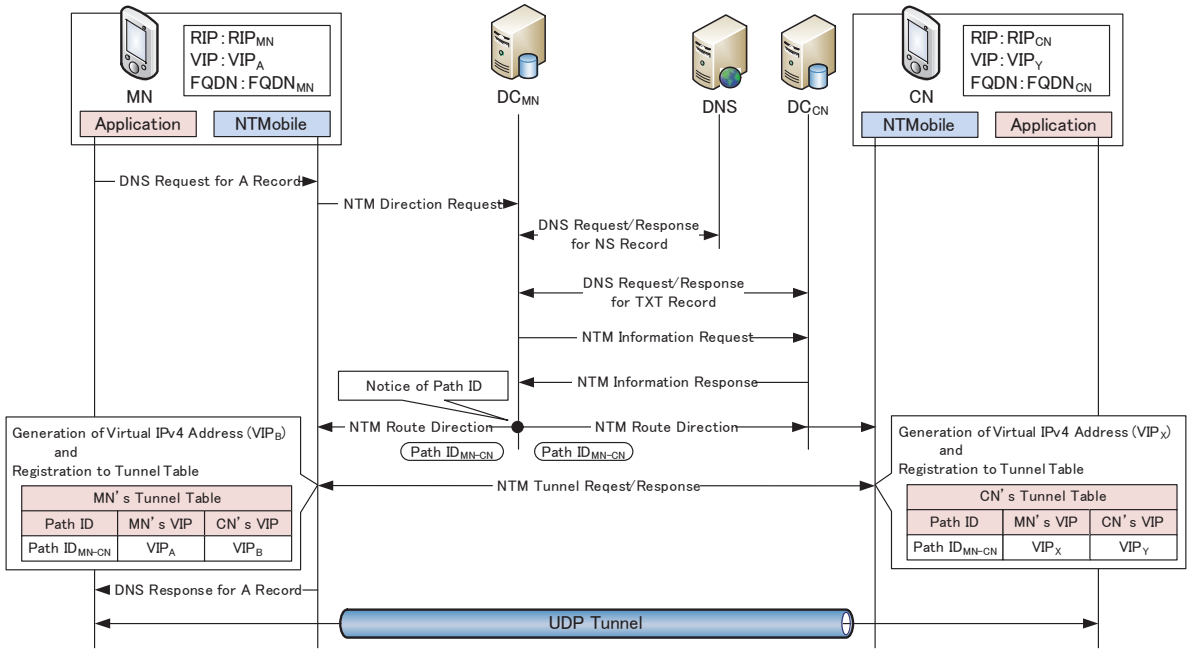

図 5 通信開始時の動作

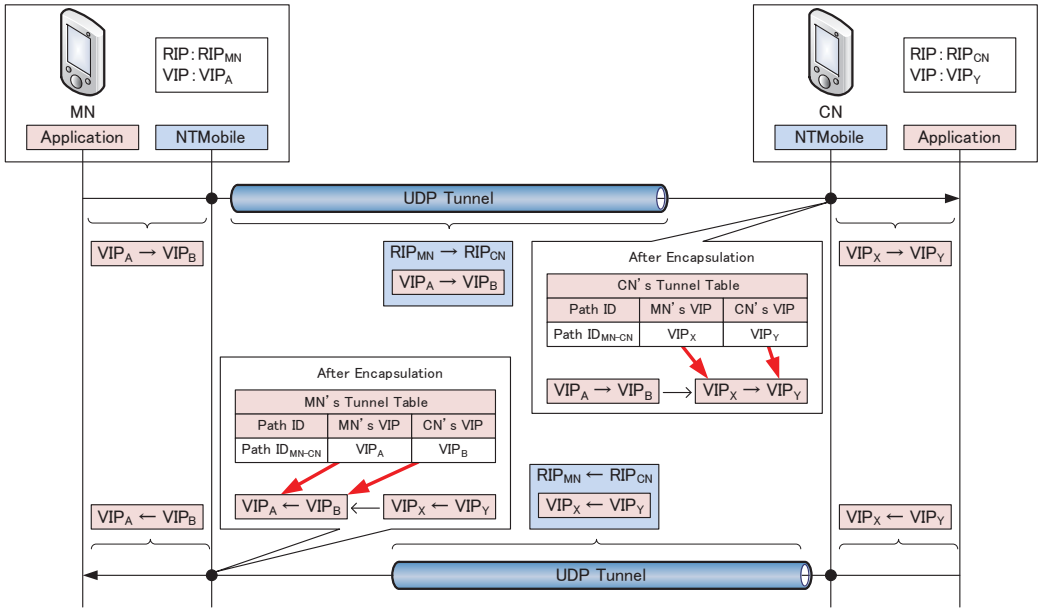

図 6 トンネル通信時のアドレス遷移

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の仮想 IPv4 アドレスとして設定した IP アドレスを検索する．その後，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．

6. 評価

図 8 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，プライベートネットワークへと直接接続している．また接続は 1000BASE-T による有線 LAN 接続である．本来は，NTM 端末で一意な仮想 IPv4 アドレスを生成するが，今回はアドレス生成処理が未実装であるため，通信相手の仮想 IPv4 アドレスを静的に設定した．

MN と CN 間で iperf[*1] を用いた TCP 通信を行い，スループットの測定を行った．ここでは，従来の NTMobile

[*1] http://sourceforge.net/projects/iperf/

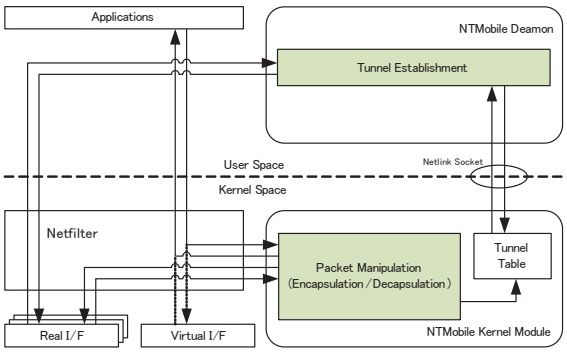

図 7 NTM 端末のモジュール構成

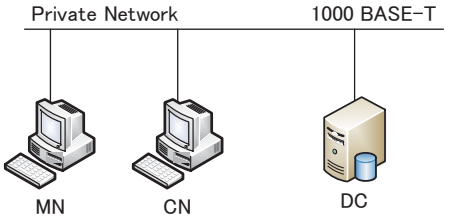

図 8 ネットワーク構成

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

によるトンネル通信と提案方式によるトンネル通信のスループットを比較した．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 回行い，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．従来方式に比べて提案方式のスループットは 0.5%低い値となった．この結果より，提案方式の通信において，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．

7. まとめ

本論文では，NTM 端末内部で仮想 IPv4 アドレスを自律的に生成し，通信する端末間の仮想 IPv4 アドレスを端末内部で管理する手法を提案した．この手法により，NTMobile 全体で仮想 IPv4 アドレス領域を共有する必要がなくなるため，限られた仮想アドレス領域で大規模に NTMobile を運用することが可能となった．また，DC が仮想 IPv4 アドレスを管理する必要がなくなり，運用が容易になった．Linux 上で提案方式の実装を行い，動作を検証した．これまでの NTMobile と提案方式を用いて NTM 端末間のトンネル通信によるスループットを比較し，提案方式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．

今後は，提案方式による NTM 端末と一般端末との通信を可能にするための検討を行う．

参考文献

[1] 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).
[2] 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).
[3] 上醉尾一真，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).
[4] 納堂博史，鈴木秀和，内藤克浩，渡邊　晃 : NTMobile における自立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).
[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. MBL, [モバイルコンピューティングとユビキタス通信研究会研究報告]，Vol.2013-MBL-67, No.11, pp. 1-6(2013).
[6] C. Perkins. : IP Mobility Support for IPv4, Revised, RFC5944, IETF(2010).
[7] H. Levkowetz and S. Vaarala. : Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC3519, IETF(2003).
[8] モバイル・無線-モバイル IP，アドホックネットワーク (2010). http://www.ieice-hbkb.org/files/04/04gun_05hen_01.pdf
[9] H. Soliman.: Mobile IPv6 Support for Dual Stack Hosts and Routers, RFC5555, IETF (2009).
[10] S. Bradner.: Benchmarking Methodology for Network Interconnect Devices, RFC2544, IETF(1999).