NTMobileにおける移動透過性の実現と実装

内藤克浩[†1] 西尾拓也[†1] 水谷智大[†2]
鈴木秀和[†2] 渡邊晃[†2]
森香津夫[†1] 小林英雄[†1]

近年の無線端末は複数の無線インタフェースを実装しており，ネットワークにアクセスする際にインタフェースを切り替えて利用可能である．移動透過技術とはアクセスネットワークが切り替えられた場合にも通信を継続可能な技術である．既存の移動透過技術に関する多くの研究では，IPv6 では端末移動を想定しているため IPv6 ネットワークを仮定しており，既存の IPv4 ネットワークは検討されていない．本稿では，仮想 IP アドレスの採用とエンド端末間でトンネル構築を行うことにより，グローバル IP アドレスを用いるネットワーク及びプライベート IP アドレスを用いるネットワークにおいて，移動透過性を実現可能な NTMobile (NAT Traversal with Mobility) の提案を行う．NTMobile では，アプリケーションが仮想 IP アドレスを利用することにより，ネットワーク切り替えに伴う物理 IP アドレスの変化時にも通信を継続可能である．また，NTMobile の実装では，高いスループット性能を獲得するために，パケット操作に関する実装を Linux のカーネルモジュールとして実現している．

Implementation of IP mobility in NTMobile

Katsuhiro NAITO,[†1] Takuya NISHIO,[†1]
Tomohiro MIZUTANI,[†2] Hidekazu SUZUKI,[†2]
Akira WATANABE,[†2] Kazuo MORI[†1]
and Hideo KOBAYASHI [†1]

Recent wireless terminals implement some wireless interfaces, and can switch them to access networks. IP mobility technologies are continuous communication schemes when access networks are switched. According to mobility supports in IPv6, most of the conventional works about IP mobility assume IPv6 networks and do not consider IPv4 networks. Additionally, a few works about IP mobility in IPv4 networks have been considered. In this paper, we propose NTMobile (NAT Traversal with Mobility), in which terminals can achieve IP mobility in global IP networks and private IP networks by constructing tunnels between end terminals. In the NTMobile, applications use virtual IP addresses to achieve continuous communication when physical IP addresses change due to switching of networks. In the implementation of NTMobile, we implement the packet manipulation mechanisms in Linux kernel module to achieve high throughput performance.

1. はじめに

近年のネットワーク技術の発展に伴い，高速無線通信技術を用いたネットワークサービスが急激に普及している．これらのネットワークサービスでは，Internet Protocol (IP) を基盤技術として利用しており，移動端末は IPv4 を用いて通信を行っている．また，近年の移動端末は第三世代携帯電話システムなどのセルラシステムだけではなく，IEEE 802.16e, IEEE 802.11 などの複数の無線通信技術を実装している．そのため，端末は複数の無線ネットワークを切り替えることにより，複数のネットワークに接続することが可能となる[1),2)]．複数のネットワークを跨いだネットワーク切り替え技術をバーティカルハンドオーバーと呼び，IEEE 802.21 ではメディアに依存しないハンドオーバー手法の標準化が進められている[3)]．

アプリケーションは IP アドレスを用いてコネクション管理を行うため，インタフェースの切り替えにより利用する IP アドレスが変化した場合，通信コネクションは切断される．このようなコネクション切断を防ぐ技術は移動透過技術と呼ばれる[4),5)]．IPv6 ネットワークでは端末の移動に対応していることもあり，既存の移動透過性に係る研究の多くが IPv6 を想定している．そのため，既存のインターネットで主に利用されている IPv4 ネットワークでは，これらの技術を活用することが困難な状況である．さらに，既存の移動透過技術の多くはホームエージェントなどの中継装置を経由することが多く，通信を行う両エンド端末が共に移動する場合，両エンド端末を管理する各中継装置を経由することから，オーバーヘッドが大きくなるという課題がある[6)–8)]．

近年のネットワークでは，IPv4 グローバルアドレスの枯渇とセキュリティ確保の観点から，インターネットと組織ネットワーク間に Network Address Translation(NAT) と呼ば

†1 三重大学 大学院工学研究科 電気電子工学専攻
Department of Electrical and Electronic Engineering, Mie University
†2 名城大学大学院 理工学研究科
Graduate School of Science and Technology, Meijo University

れるアドレス変換機構を設置し, 組織ネットワーク内ではプライベートアドレスを利用するネットワーク形態が一般的である．NAT を利用した場合, 内部ネットワークである組織ネットワークは外部ネットワークであるインターネットから隠蔽されることから, インターネット側の端末から組織ネットワーク側の端末に向けて通信を開始することができない (NAT 越え問題)[9]．著者らは NAT 越え問題を解決する移動透過技術として, Mobile PPC を提案してきた[10]．Mobile PPC では, 既存の IPv4 ネットワークを想定しており, エンド端末のみで移動透過性を実現可能な技術であるが, 両エンド端末が NAT 配下に存在する場合などの移動条件には対応が困難であった．また, 通信開始時に割り当てられていた IP アドレスを利用し続けることから, 移動時の IP アドレス管理が煩雑であった．

本稿では, Mobile PPC の課題であった移動条件の制限と IP アドレス管理の煩雑性を解決する手法として, NTMobile(NAT Traversal with Mobility) を提案する．NTMobile では, NTMobile 端末を管理する Direction Server (DS) が仮想 IP アドレスを管理することにより, NTMobile 端末の IP アドレス管理を容易にしている．さらに, Mobile PPC と同様にエンド端末のみで移動透過性を実現可能である一方, 両エンド端末が NAT 配下に存在する場合には, Relay Server (RS) が仲介することにより, 両エンド端末の接続を行うため, グローバル IP アドレス及びプライベート IP アドレスの区別なく移動透過性を実現可能である．そのため, NTMobile は既存ネットワークの変更を必要としないにも関わらず, 両エンド端末が自由に移動可能である．さらに, 基本的に両エンド端末間で直接通信を行うため, スループット性能の劣化も極めて小さくすることが可能であることを実装実験より示す．

2. NTMobile の概要

図 1 は NTMobile で想定するネットワークを示しており, 移動を前提とした処理を行う NTMobile 端末, NTMobile 端末を管理する Direction Server (DS), NAT 配下に存在する NTMobile 端末間の通信を中継する Relay Server (RS) により構成される．DS 及び RS はネットワークの規模に応じて増設することが可能であり, NTMobile 端末が利用する仮想 IP アドレスの管理は DS により行われるものとする．また, 図 1 に示されるように, NTMobile は NTMobile 端末が NAT 配下に存在する場合においても移動透過性を実現可能な方式であり, グローバル IP アドレスを利用するネットワークとプライベート IP アドレスを利用するネットワーク間においても, シームレスな移動が実現可能である．

NTMobile では端末の移動に伴う実 IP アドレスの変化を隠蔽するために, アプリケーションは仮想 IP アドレスを用いて通信を行う．そのため, 端末移動時にもアプリケーションは同一仮想 IP アドレスを継続して利用可能となり, 移動透過性を実現可能となる．なお, NTMobile 端末は仮想 IP アドレスが利用されている IP データグラムをカプセル化することで, 実 IP アドレスを用いたトンネル通信を行う．

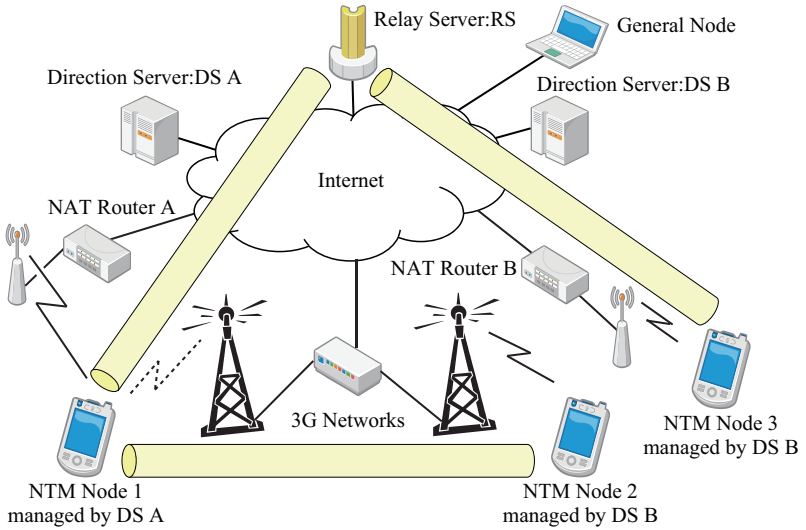

図 1 NTMobile の概要.
Fig. 1 Overview of NTMobile network.

NTMobile では, カプセル化で利用されるトンネル経路は 2 種類想定しており, エンド端末間で直接トンネルを構築する場合と, 各エンド端末がリレーサーバーに対してトンネルを構築する場合がある．利用されるトンネル経路は NTMobile 端末の IP アドレスの種類に依存しており, NTMobile 端末の一方又は両方がグローバル IP アドレスを利用する場合には, エンド端末間で直接トンネルを構築することにより, エンドーエンドの端末のみで移動透過性を実現する．また, NTMobile 端末の両方がプライベート IP アドレスを利用する場合には, 各エンド端末が指定された RS とトンネルを構築することにより, 移動透過性を実現する．なお, NTMobile では SPI などのフィルタリング機能も実装している一般的な NAT をルータを想定しており, NAT ルータの機能変更なしに, NAT 越えが可能な移動透過性を実現可能であるため, 既存の殆どのネットワークにおいて移動透過性を実現可能となる．以下に NTMobile を構成する端末及び装置の機能を説明する．

- Direction Server (DS)
  NTMobile 端末を管理し, NTMobile 端末の移動に伴う各種処理の指示を出す装置である．また, 各 DS は自身に割り当てられた仮想 IP アドレスプールを持ち, NTMobile 端末に重複した仮想 IP アドレスの割当を防ぐ割当管理を行う．なお, DS は Dynamic DNS の機能を包含しており, 各 NTMobile 端末の実 IP アドレスの情報は Dynamic DNS を用いることで登録と更新を行う．また, NTMobile で利用する情報は DNS の専用レコードとして登録することにより, プライマリ DNS 経由の問い合わせにも返答を行う．
- Relay Server (RS)
  通信を行う 2 台の NTMobile 端末が NAT 配下に存在する場合に, NTMobile 端末間の通信を中継する装置である．また, NTMobile 非対応の一般端末との通信においても NTMobile 端末の移動透過性を実現するため, NTMobile 端末と RS 間にトンネルを構築し, RS から一般端末への通信を行うことも可能な装置である．
- NTMobile 端末
  NTMobile 端末間は DS から割り当てられる仮想 IP アドレスを常に利用することにより, 端末移動に伴う実 IP アドレスの変化を隠蔽する．また, DS からの経路指示に応じて, エンド端末間の通信が直接可能な場合には, NTMobile 端末間で直接トンネルの構築を行い, 両エンド端末が NAT 配下に存在する状況では, 各 NTMobile は RS に対してトンネル構築を行う．

3. NTMobile における移動透過性

3.1 移動パターンの分類

NTMobile では, 表 1 に示す移動パターンに対応することにより, 様々な状況における移動透過性を実現する．

表 1 では, NTMobile で想定する移動前と移動後のアドレス変化について記載している．また, 対象となるアドレスの種類として, グローバル IP アドレス空間とプライベート IP アドレス空間を想定している．なお, プライベート IP アドレス空間は, 両エンド端末が同一プライベート IP アドレス空間に存在する場合, 異なるプライベート IP アドレス空間に存在する場合を想定している．NTMobile 端末の通信対象の端末として, NTMobile 端末の場合と NTMobile 非対応の一般端末の場合について記載している．NTMobile の特徴として, NTMobile 端末と一般端末が通信を行う場合, NTMobile 端末同士の通信であっても両端末が NAT 配下に存在する場合は, Relay Server を経由して通信を行う．表 1 には, 各移動パターンの移動後の通信形態についても記載している．なお, 移動パターン 15 において, 通信形態が 2 種類想定されているのは, 無線 LAN 基地局などでは無線端末間の通信を制限する運用も行われており, この場合 NAT 配下の両エンド端末が直接通信することが不可能なためである．

表 1 想定移動パターン．
Table 1 Assumed patterns of terminal movement.

Pattern	NTMobile node	Correspondent node	Tunnel route after terminal movement
1	G ⇒ G	G (NTMobile)	End-to-End
2	G ⇒ G	G (General)	via Relay Server
3	G ⇒ P(A)	G (NTMobile)	End-to-End
4	G ⇒ P(A)	G (General)	via Relay Server
5	P(A) ⇒ G	G (NTMobile)	End-to-End
6	P(A) ⇒ G	G (General)	via Relay Server
7	P(A) ⇒ P(A)	G (NTMobile)	End-to-End
8	P(A) ⇒ P(A)	G (General)	via Relay Server
9	P(A) ⇒ P(B)	G (NTMobile)	End-to-End
10	P(A) ⇒ P(B)	G (General)	via Relay Server
11	G ⇒ G	P(A) (NTMobile)	End-to-End
12	G ⇒ P(A)	P(A) (NTMobile)	via Relay Server
13	G ⇒ P(B)	P(A) (NTMobile)	via Relay Server
14	P(B) ⇒ G	P(A) (NTMobile)	End-to-End
15	P(B) ⇒ P(A)	P(A) (NTMobile)	via Relay Server or End-to-End
16	P(A) ⇒ P(B)	P(A) (NTMobile)	via Relay Server
17	P(B) ⇒ P(C)	P(A) (NTMobile)	via Relay Server

3.2 メッセージフォーマット

NTMobile では, NAT 配下に NTMobile 端末が存在する場合にも移動透過性を実現する．また, NAT 配下に存在する NTMobile 端末に向けて各種メッセージを送信する必要もある．そこで, NTMobile では, NTMobile 専用の同一のポート番号を用いて, 制御メッセージとデータが含まれるカプセル化メッセージなどの全てのメッセージの交換を行う．

図 2 は NTMobile で利用する各種メッセージ内容を示す．本稿では NTMobile のセキュリティに関する言及は特に行わないが, 図 2 には NTMobile で想定する暗号化領域と認証領域も記載する．以下に各メッセージの用途を述べる．

- NTM Header
  NTMobile で利用するメッセージの共通ヘッダを示す．Node ID/Path ID の項目は

Capsulated Packet 以外は Node ID が記録される．

- Registration Request / Registration Response
  NTMobile 端末起動時の位置登録に利用されるメッセージを示す．
- NTM Update Request /NTM Update Response
  NTMobile 端末が移動した際, 位置情報を含む DNS の NTM 専用レコードを更新するために利用されるメッセージを示す．なお, 両メッセージは構築したトンネルが切断されることを防ぐため, 定期的にメッセージ交換を行う際にも利用される．
- Direction Request
  NTMobile 端末が起動時及び移動後にトンネル構築を DS に要求する際に利用するメッセージを示す．
- Route Direction
  該当端末にトンネル構築に必要な情報を含み, DS がトンネル構築を指示する際に利用するメッセージを示す．
- Relay Direction
  RS がトンネル中継に必要な情報を含み, DS がトンネル中継を指示する際に利用するメッセージを示す．
- Tunnel Request / Tunnel Response
  NTMobile 端末がトンネル構築を要求する際に利用するメッセージを示す．
- Capsulated Packet
  NTMobile 端末が通信を行う際に, アプリケーションデータがカプセル化されているメッセージを示す．なお, カプセル化される IP データグラムではエンド端末の仮想 IP アドレスが利用されている．

3.3 起動時のコネクション確立

図 3 は NTMobile 端末同士の通信開始手順を示している．図 3 は通信開始端末が NAT 配下のプライベート IP アドレス空間に存在しており, 通信相手端末はグローバル IP アドレス空間に存在している場合である．なお, 各 DS は NTMobile で想定する移動管理手段[11] により, 各 NTMobile 端末の実 IP アドレス, 仮想 IP アドレス, NAT の IP アドレス, ノード ID など位置情報が既に登録されているものとする．NTMobile 端末は以下の手順に従い, 通信相手端末間のトンネル確立を行う．なお, 本稿では移動透過性の実現に関係する点に特に着目するものとし, DNS を用いた NTMobile 端末の位置情報の取得方法についての説明は省略する．

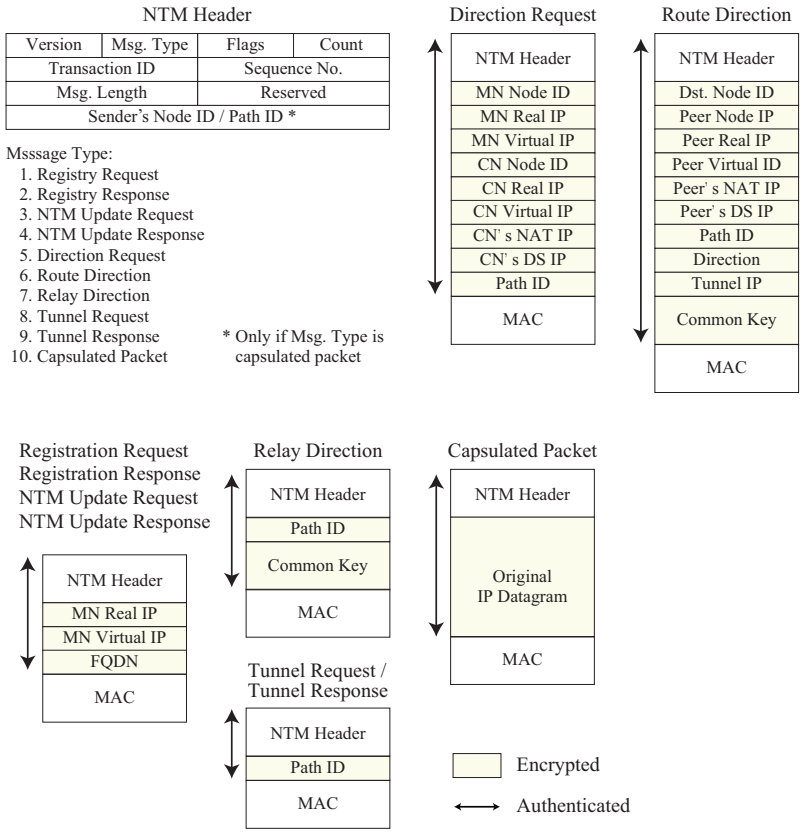

図 2 メッセージフォーマット．
Fig. 2 Message format.

- 指示要求 (Direction Request)
  通信開始端末は自身の DS に Direction Request を送信することにより, 通信相手端末とのトンネル構築の指示要求を行う．なお, Direction Request には, 自身のノード ID AAA, 仮想 IP アドレス VIP_{MN}, 通信相手端末のノード ID BBB, 通信相手端末の実 IP アドレス RIP_{CN}, DS の IP アドレス $RIP_{DS\text{-}B}$, 仮想 IP アドレス VIP_{CN} が含まれる．
- 経路指示 (Route Direction)

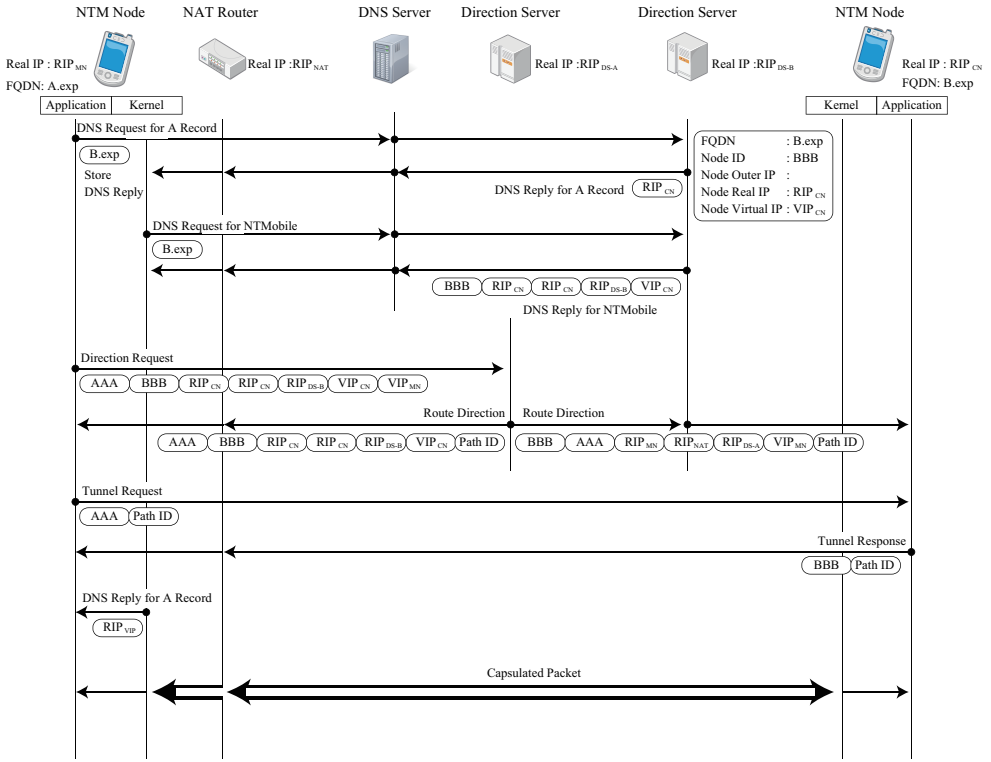

図 3 グローバル IP とプライベート IP 間のコネクション確立.
Fig. 3 Connection process between global IP and private IP.

通信開始端末の DS は通信開始端末と通信相手端末の DS に Route Direction を送信することで, トンネル構築の経路指示を行う．また, 通信相手端末の DS は Route Direction を通信相手端末に転送を行うことで, 通信相手端末にもトンネル構築の経路指示を伝える．なお, Route Direction を通信相手端末の DS 経由で送信するのは, 通信開始端末の DS と通信相手端末間に信頼関係がない場合も考えられるためである．Route Direction には, 両端末のノード ID, 実 IP アドレス, NAT ルータの IP アドレス, 仮想 IP アドレス, 管理 DS の IP アドレスに加え, コネクションを識別するためのパス ID が含まれる．

- トンネル要求/応答 (Tunnel Request / Tunnel Response)

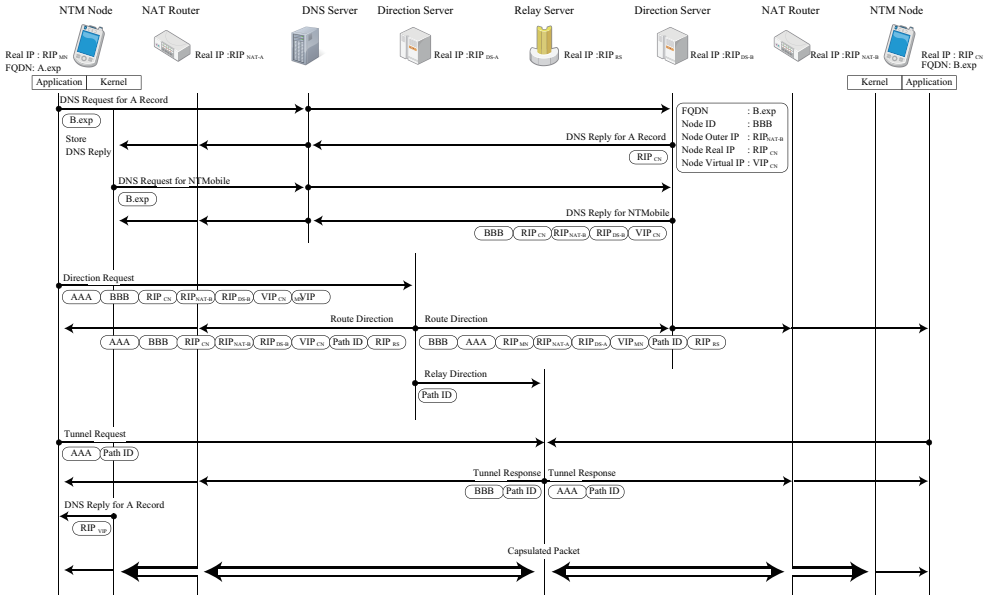

図 4 プライベート IP 間のコネクション確立.
Fig. 4 Connection process between private IPs.

NTMobile では, NAT 配下に存在する NTMobile 端末側から Tunnel Request を送信することにより, 両エンド端末間に通信用のトンネルをエンドーエンドで直接構築するようにトンネル要求を行う．また, Tunnel Request を受信した端末は Tunnel Response を送信することでトンネル応答を行う．NTMobile では, 両エンド端末間の通信を全て構築したトンネルを用いて交換を行う．また, 両エンド端末は仮想 IP アドレスを用いて通信を行うことから, エンド端末の移動に伴いトンネルを再構築した場合にも, 通信を継続することが可能となり, 柔軟な移動透過性を実現可能である．

図 4 は NTMobile 端末同士の通信開始手順を示している．図 3 と大きく異なる点は, 通信相手端末も NAT 配下のプライベート IP アドレス空間に存在している点である．図 3 の場合と基本的な手順は同一であるが, 両エンド端末間で直接トンネル構築を行えないため, Relay Server 経由でトンネル構築を行うのが大きな違いである．

- 指示要求 (Direction Request)

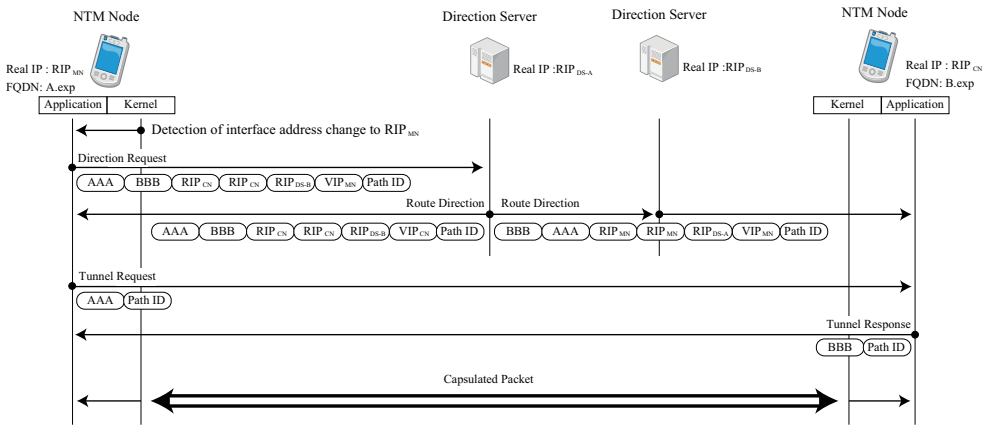

図 5 グローバル IP 間のコネクション再確立.
Fig. 5 Reconnection process between global IPs.

通信開始端末は自身の DS に Direction Request を送信することにより, 通信相手端末へのトンネル構築の指示要求を行う.

- 経路指示 (Route Direction)
  通信開始端末の DS は通信開始端末と通信相手端末の DS に Route Direction を送信することで, トンネル構築の経路指示を行う. また, 通信相手端末の DS は Route Direction を通信相手端末に転送を行うことで, 通信相手端末にもトンネル構築の経路指示を伝える.
- 中継指示 (Relay Direction)
  DS は Relay Direction を Relay Server に送信することで, 指定したパス ID に関するトンネルをリレーするように中継指示を行う.
- トンネル要求/応答 (Tunnel Request / Tunnel Response)
  両エンド端末が RS に向けて Tunnel Request を送信することにより, RS と両エンド端末間のトンネルを構築するようトンネル要求を行う. また, Tunnel Request を受信した RS は Tunnel Response を返信することでトンネル応答を行う.

3.4 移動時のコネクション再確立

図 5 は図 3 のトンネル構築後に, 通信開始端末がプライベート空間からグローバル空間に移動した場合のトンネル再構築手順を示している. なお, NTMobile 端末は自身のインタフェースの IP アドレスを監視する. IP アドレスの変化を検出した場合, 新たな IP アドレスを DS に通知するとともに, 新たなトンネル構築を行う. NTMobile 端末は以下の手順に従い, 通信相手端末間のコネクション再確立を行う.

- 指示要求 (Direction Request)
  通信に利用する実 IP アドレスが更新された場合, 通信開始端末は自身の DS に Direction Request を送信することにより, 通信相手端末間のトンネル再構築の要求を行う. なお, Route Direction には, 両端末のノード ID, 実 IP アドレス, NAT ルータの IP アドレス, 仮想 IP アドレス, 管理 DS の IP アドレスに加え, コネクションを識別するためのパス ID が含まれるため, DS は NTMobile 端末の移動後の通信状況を把握できる.
- 経路指示 (Route Direction)
  通信開始端末の DS は通信開始端末と通信相手端末の DS に Route Direction を送信することで, トンネル構築の指示を行う. また, 通信相手端末の DS は Route Direction を通信相手端末に転送を行うことで, 通信相手端末にもトンネル構築の指示を伝える.
- トンネル要求/応答 (Tunnel Request / Tunnel Response)
  NTMobile では, NAT 配下に存在する NTMobile 端末側から Tunnel Request を送信することにより, 両端末間に通信用のトンネルを構築する. また, Tunnel Request を受信した端末は Tunnel Response を返信する.

図 6 は図 4 のトンネル構築後に, 通信開始端末がプライベート空間からグローバル空間に移動した場合のトンネル再構築手順を示している. 図 5 と大きく異なる点は, 通信開始端末がグローバル空間に移動したため, RS を経由するトンネルを開放し, NTMobile 端末間で直接トンネルを構築する点である. NTMobile 端末は以下の手順に従い, 通信相手端末間のコネクション再確立を行う.

- 指示要求 (Direction Request)
  通信に利用する実 IP アドレスが更新された場合, 通信開始端末は自身の DS に Direction Request を送信することにより, 通信相手端末間のトンネル再構築の要求を行う
- 経路指示 (Route Direction)
  通信開始端末の DS は通信開始端末と通信相手端末の DS に Route Direction を送信することで, トンネル構築の指示を行う. また, 通信相手端末の DS は Route Direction を通信相手端末に転送を行うことで, 通信相手端末にもトンネル構築の指示を伝える.
- トンネル要求/応答 (Tunnel Request / Tunnel Response)
  NTMobile では, NAT 配下に存在する NTMobile 端末側から Tunnel Request を送信

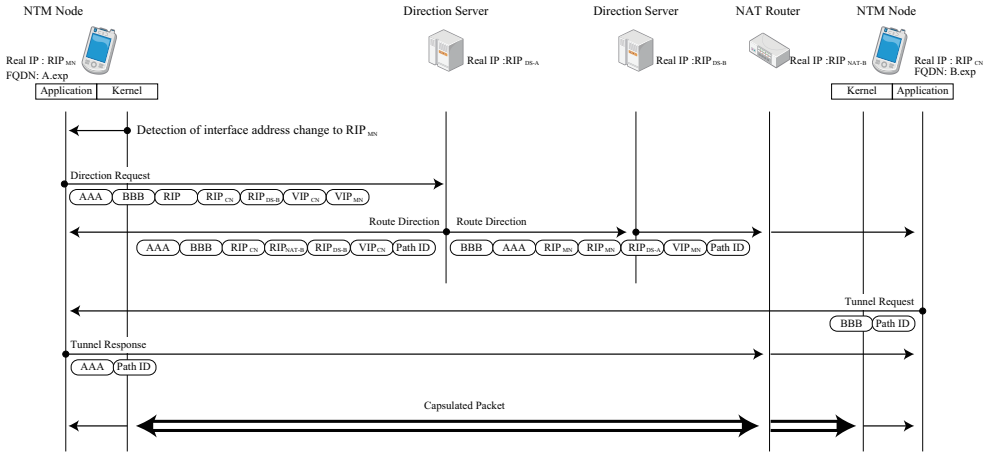

図 6 グローバル IP とプライベート IP 間のコネクション再確立.
Fig. 6 Reconnection process between global IP and private IP.

することにより, 両端末間に通信用のトンネルを構築する．また, Tunnel Request を受信した端末は Tunnel Response を返信する．なお, RS は一定時間トンネルが利用されない場合, 該当トンネルに関する情報を削除するものとする．

3.5 NTMobile 端末の通信

NTMobile では, 実 IP アドレスの変化を隠蔽する手段として, NTMobile 端末内に仮想インタフェースを構築し, 仮想 IP アドレスの割当を行う．NTMobile 端末間の通信では, アプリケーションが仮想 IP アドレスを用いてコネクションを結ぶことにより, 移動透過性を実現している．

- NTMobile 端末間の通信
  アプリケーションが送信した IP データグラムには通信開始端末と通信相手端末の仮想 IP アドレスが記録されている．NTMobile では, カーネル空間に用意したトンネルテーブルを利用することにより, 通信開始端末と通信相手端末の実 IP を用いたカプセル化処理を行う．結果として, 仮想 IP アドレスが記録されている IP データグラムは, 通信開始端末から通信相手端末に到達可能となる．なお, トンネルテーブルはユーザデーモンで交換される NTMobile の制御メッセージに応じて生成するものとする．また, カプセル化に伴いパケットサイズが微増するため, 仮想インタフェースの MTU を調整することで, 物理インタフェースを用いた通信時のフラグメント発生を防いでいる．
- 一般端末との通信
  一般端末との通信では, エンド間のトンネル構築による移動透過性の実現が困難である．そのため, NTMobile では, 一般端末との通信で移動透過性を実現するために, リレーサーバーを経由した通信を行う．アプリケーションは仮想 IP アドレスを用いて一般端末宛の IP データグラムを生成する．そして, IP データグラムはカーネルモジュールにおいてカプセル化され, リレーサーバーに向けて送信される．リレーサーバーは IP データグラムの仮想 IP アドレスを自身の IP アドレスに変換後, 一般端末に IP データグラムを送信することで, NTMobile 端末の移動に伴う実 IP アドレスの変化を隠蔽することが可能である．

4. 実　　装

4.1 NTMobile 端末の実装

図 7 に NTMobile 端末のモジュール構成図を示す．NTMobile は移動透過性を目指した手法のため, 携帯端末などにも実装される Android OS 上で動作することを最終目標としている．そのため, 実装は Linux 上で行っており, 主にユーザ空間とカーネル空間に分離して実装が行われている．また, ユーザ空間で動作する NTMobile Daemon とカーネル空間で操作する NTMobile Kernel Module 間は Linux の Netlink ソケットを用いて接続する．

ユーザ空間の実装

ユーザ空間の NTMobile Daemon の機能は以下の点である．

- アドレス確認
  インタフェースの IP アドレス又はルーチング情報などを確認することにより, NTMobile 端末が新たなネットワークに接続したことを検出する．
- トンネル構築
  NTMobile 端末が新たなネットワークに接続した場合, 必要に応じて新しく接続したネットワークを用いて, 新たなトンネル構築を DS に要求する．また, DS からの経路指示に応じて, NTMobile 端末はエンド端末間又は RS を経由するトンネル要求を行う．

カーネル空間の実装

NTMobile では, Linux カーネル自身の変更を避けるために, Linux の Netfilter 用のカーネルモジュールとして, カーネル空間の実装を行っている．カーネルモジュールを用いているため, モジュールの追加のみで NTMobile の機能を Linux に追加及び削除することが可

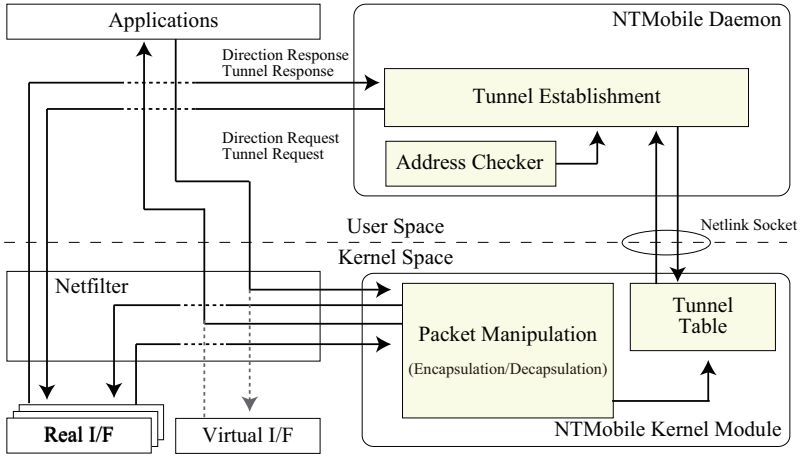

図 7 NTMobile 端末のモジュール構成.
Fig. 7 Module configuration of NTMobile node.

能である．カーネルモジュールの機能は以下の点である．

- IP データグラムのカプセル化及びデカプセル化処理
  NTMobile 端末間の通信はトンネルを経由して行われるため, 仮想 IP アドレスが記録されているアプリケーションが生成した IP データグラムをカプセル化及びデカプセル化する．なお, これらの処理はトンネルテーブルに応じて実施される．
- IP データグラムの暗号化及び復号化処理
  NTMobile 端末間で構築されるトンネル内の通信は暗号化を行うこともでき, トンネルテーブルに保存される各トンネルの鍵情報を用いて, 暗号化と復号化の処理を行う．

4.2 DS の実装

図 8 に NTMobile の DS のモジュール構成図を示す．DS の主な機能は NTMobile 端末に関する情報を DNS レコードとして管理することと, NTMobile 端末にトンネル構築に関する指示を出すことである．

DS の NTMobile の機能は全てユーザ空間に実装されており, NTMobile Daemon の機能は以下の点である．

- 位置情報の管理
  NTMobile 端末は起動時及び移動時に Direction Request を用いて自身の位置情報を

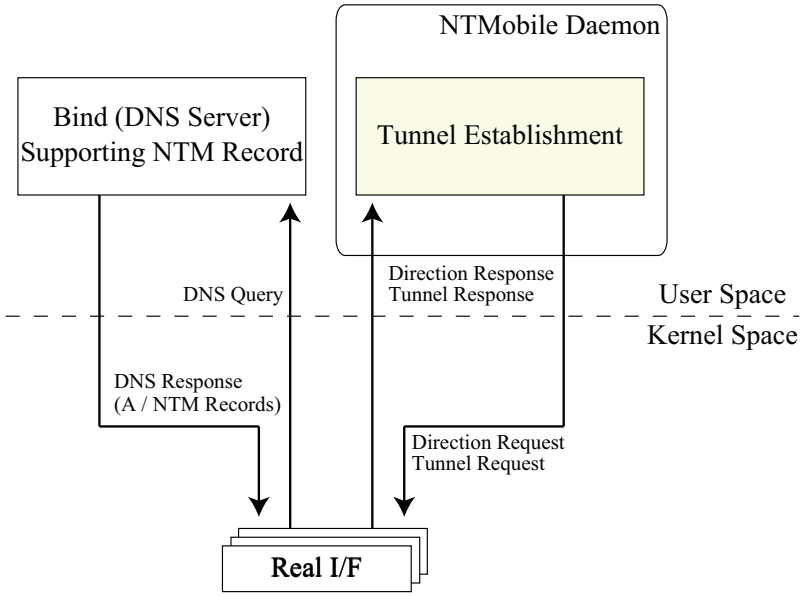

図 8 DS のモジュール構成.
Fig. 8 Module configuration of direction server.

DS に送信する．DS は受信する Direction Request の位置情報に用いて, 現在通信中の NTMobile 端末の情報の管理を行う．

- トンネル構築指示
  NTMobile 端末から送信された Direction Request を受信した場合, 通信を行う両 NTMobile 端末の位置情報を確認することにより, 両 NTMobile 端末に対してトンネル構築を指示する Route Direction の送信を行う．
- トンネル中継指示
  通信を行う両 NTMobile 端末が NAT 配下に存在する場合, DS は RS に対して Relay Request を送信する．また, NTMobile 端末が一般端末と通信を行う際にも, DS は RS に対して Relay Request を送信する．なお, RS を経由する場合には, トンネル要求指示において, NTMobile 端末は RS に対してトンネル構築を行うように要求を行うものとする．

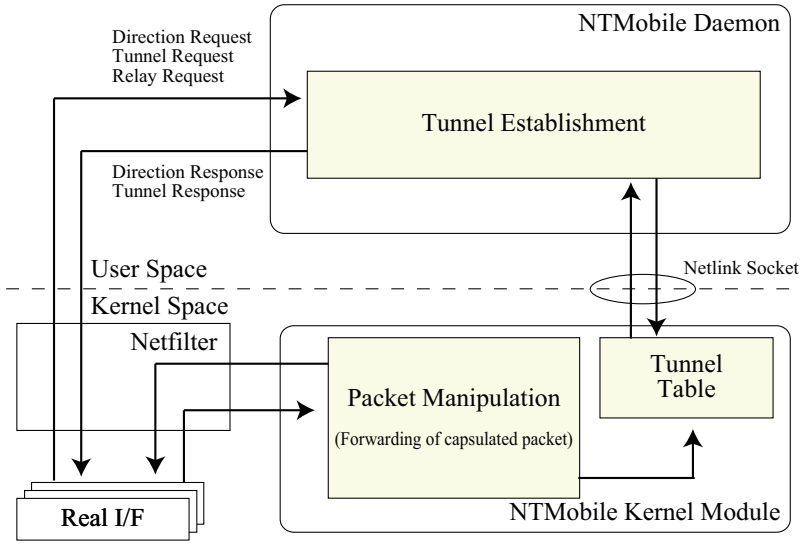

図 9 RS のモジュール構成.
Fig. 9 Module configuration of relay server.

4.3 RS の実装

図 9 に NTMobile の RS のモジュール構成図を示す．RS の主な機能は通信を行う両 NTMobile 端末が NAT 配下に存在する場合, 両 NTMobile 端末と RS がトンネルを構築することにより, 両 NTMobile 端末のトンネル中継を行うことである．また, 一般端末との通信時にも NTMobile 端末の移動透過性を実現するため, RS は NTMobile 端末と一般端末間の通信の中継も行う.

RS の NTMobile の機能はユーザ空間とカーネル空間に実装されている.

ユーザ空間の実装

ユーザ空間に実装される NTMobile Daemon の機能は以下の点である.

- トンネル中継情報の受信
  RS は DS からトンネル中継で必要となる Path ID 及び Common Key の情報を受け取ることで, NTMobile 端末からのトンネル要求の受入待機を行う.
- トンネル構築
  NTMobile 端末からの Tunnel Request に対して Tunnel Response を返信することにより, NTMobile 端末とのトンネル構築を行う．また, Netlink ソケットを用いてカーネルモジュール内のトンネルテーブルに中継に必要となる情報を登録する.

カーネル空間の実装

カーネル空間に実装される NTMobile のカーネルモジュールは, 以下の処理を行うことでトンネル中継を行う.

- NTMobile 端末からの Capsulated Packet の受信
  NTMobile 端末とのトンネルを通して受信される Capsulated Packet を受信し, 宛先端末が NTMobile 端末又は一般端末かを判断する.
- NTMobile 端末への中継
  NTMobile 端末宛の Capsulated Packet を受信した場合, RS は該当 NTMobile 端末宛にアドレスを変更し送信する.
- 一般端末への中継
  一般端末宛の Capsulated Packet を受信した場合, RS は該当パケットのデカプセル化を行った後に, 送信元アドレスを RS のアドレスに変換し, 一般端末に向けて送信される．なお, この際に利用する送信元ポート番号は RS において重複しないように割り当てることにより, RS における NAT 処理を実現する.

4.4 カーネルモジュールの実装

NTMobile では, 移動透過性を実現するためにカプセル化処理を用いたトンネル構築を行う．一般にカプセル化処理を行う方式では, 仮想インタフェースを用いて送信されたパケットをユーザ空間に移動し, ユーザ空間においてカプセル化処理を行う．また, ユーザ空間からカプセル化されたパケットを送信することで, トンネルを構築している．しかし, カーネル空間のパケットを再度ユーザ空間に移動してから処理することは, 大きなオーバーヘッドになり, スループット特性の劣化などの弊害も見受けられる.

NTMobile では, カプセル化処理に伴うスループット特性の劣化を可能な限り防ぐため, 多くのカプセル化手法とは異なり, カーネル内でカプセル化処理を行う．図 10 に NTMobile のカーネルモジュールの設計概要を示す．実装するカーネルモジュールは Linux のネットワーク機能の中核である Netfilter のモジュールとして設計を行う．また, アプリケーションから送信されるパケットデータは, Netfilter の NF_INET_LOCAL_OUT にてフックを行うことで, 送信パケットデータの sk_buff をカーネルモジュールに引き渡す．カーネルモジュールは sk_buff を直接操作することにより, 受信したパケットデータのカプセル化及び暗号化処理を行った後, Netfilter の NF_INET_POST_ROUTING にて sk_buff をチェインに戻す.

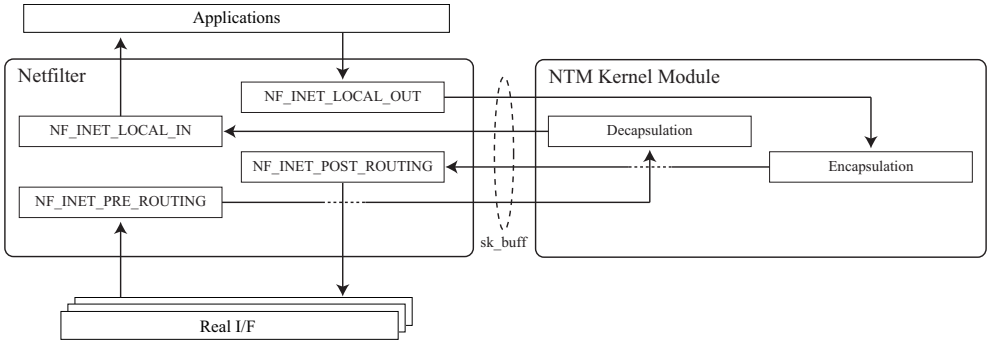

図 10 NTMobile カーネルモジュール構成.
Fig. 10 Configuration of NTMobile kernel module.

受信時は, Netfilter の NF_INET_PRE_ROUTING にてフックを行うことで, 受信パケットデータの sk_buff をカーネルモジュールに引き渡す. カーネルモジュールは sk_buff を直接操作することにより, 受信したパケットデータのデカプセル化及び復号化処理を行った後, Netfilter の NF_INET_LOCAL_IN にて sk_buff をチェインに戻す. このように, Netfilter にてフックする sk_buff をカーネルモジュールで直接操作することにより, NTMobile ではカプセル化に伴うスループット低下を抑制可能な設計としている.

4.5 性 能 評 価

NTMobile では移動透過性を実現するためにカプセル化処理を行う. 一般的にカプセル化処理はオーバーヘッドが大きい事が知られている. そこで, 本性能評価では, 実装を行ったカーネルモジュールのオーバーヘッドの評価を行うために FTP を用いたスループット測定を実施した.

図 11 に性能評価で用いたモデルを示す. 本評価では実装を行ったカーネルモジュールの評価を行うため, 一般的な PC に Linux をインストールし, 有線 LAN を用いて FTP のバルク転送を実施した. 表 2 に評価諸元を示す.

図 12 に FTP で測定を行ったスループット特性を示す. なお, 測定は 10 回行い平均値を記載する. 結果より, 既存の Linux カーネルのみを用いたスループット特性と比較し, 提案方式のカーネルモジュールのスループット特性は数パーセントの特性劣化のみしか発生していないことが確認できる. また, MTU サイズが小さくなるほど, 特性劣化が大きくなる. これは, データサイズに対して, カプセル化で付加される NTM の情報割合が大きくなるため思われる. 結果より, NTMobile で実装したモジュール構成はカプセル化に伴う特性劣化を抑える上で有効であることが確認された.

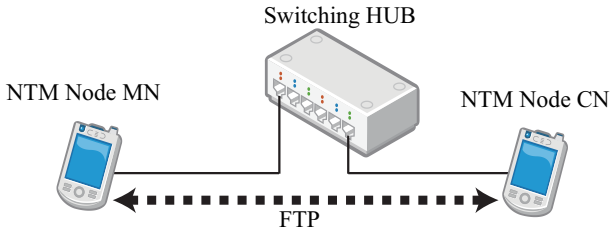

図 11 性能評価モデル.
Fig. 11 Performance evaluation model.

表 2 性能評価諸元.
Table 2 Performance evaluation parameters.

OS	Linux
Distribution	Ubuntsu 10.04
Kernel version	linux-2.6.32-24-generic
CPU	Intel Pentium 4 2.40GHz
Memory	512 MBytes
Application	FTP
Size of transferred data	1.184 GBytes

5. ま と め

本稿では既存の IPv4 ネットワークにおいてエンド端末のみで移動透過性を実現可能な NTMobile の提案を行った. NTMobile では, エンド端末の一方がグローバル IP アドレスを利用している場合にはエンド端末間で直接トンネルを構築することにより, オーバーヘッドの削減を図っている. また, エンド端末が NAT 配下にいる場合のみ, 各エンド端末がリレーサーバーとトンネルを構築するが, 同一のリレーサーバーを経由することで, オーバーヘッドの削減を図っている.

実装では, パケット処理に伴うスループット特性の劣化を抑えるため, カーネル空間でのカプセル化及び暗号化を行う実装とした. また, 既存の Linux カーネルへの影響を最小限に留めるため, 提案方式では Linux のカーネルモジュールの形式で実装を行った. 結果として,

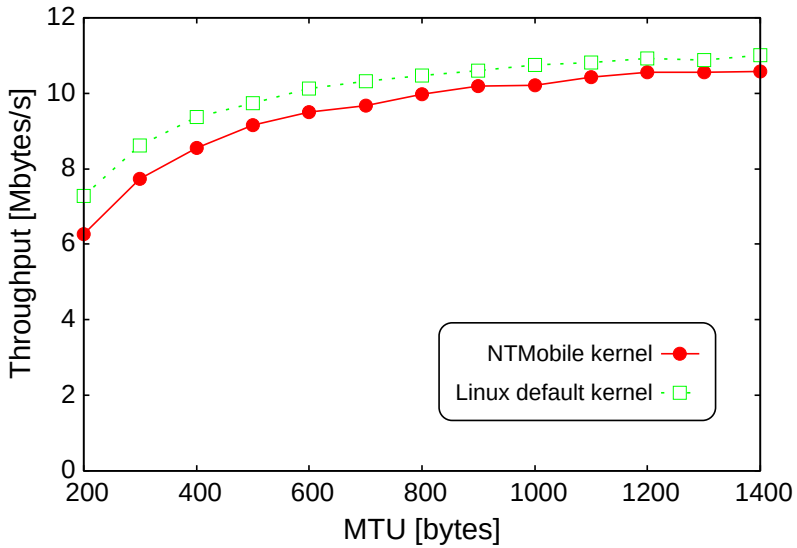

図 12 スループット性能.
Fig. 12 Throughput performance.

提案方式の実装方式はカプセル化に伴うスループット特性の劣化も最小限に抑えており, 高いスループット特性が達成可能であることを評価実験より示した.

謝　　辞

提案方式の実装にあたり様々な協力をして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) M. Buddhikot, G. Chandranmenon, S. Han, Y. W. Lee, S. Miller and L. Salgarelli, “Integration of 802.11 and third- generation wireless data networks,” Proceedings of the IEEE INFOCOM 2003, Vol. 1, Page(s): 503-512, 2003.
2) Q. Zhang, C. Guo, Z. Guo and W. Zhu, “Efficient mobility management for vertical handoff between WWAN and WLAN,” IEEE Communications Magazine, Vol. 41, No. 11, Page(s): 102-108, 2003.
3) L. A. Magagula and H. A. Chan, “IEEE802.21-Assisted Cross- Layer Design and PMIPv6 Mobility Management Framework for Next Generation Wireless Networks,” Proc. IEEE WIMOB ’08, pp. 159-164, Oct. 2008.
4) D. Le, X. Fu and D. Hogrere, “A Review of Mobility Support Paradigms for the Internet,” IEEE Communications surveys, 1st quarter 2006, Volume 8, No. 1, 2006.
5) C. Perkins, “IP Mobility Support for IPv4, Revised,” RFC 5944, IETF (2010).
6) S. Salsano, C. Mingardi, S. Niccolini, A. Polidoro and L. Veltri ”SIP-based Mobility Management in Next Generation Networks,” IEEE Wireless Communication, Vol. 15, Issue 2, April 2008.
7) M. Bonola, S. Salsano and A. Polidoro, “UPMT: universal per-application mobility management using tunnels,” In Proc. of the 28th IEEE conference on Global telecommunications (GLOBECOM’09) 2009.
8) M. Bonola and S. Salsano, “S-UPMT: a secure Vertical Handover solution based on IP in UDP tunneling and IPsec,” GTTI Riunione Annuale 2010, (online), http://www.gtti.it/GTTI10/papers/gtti10_submission_29.pdf, 2010.
9) H. Levkowetz and S. Vaarala, “Mobile IP Traversal of Network Address Translation (NAT) Devices,” RFC 3519, April 2003.
10) H. Suzuki, K. Terazawa and A. Watanabe, “Implementation of NAT Traversal for Mobile PPC with the Principle of Hole Punching,” in Proc. of the IEEE International Region 10 Conference 2009 (TENCON2009), Nov.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,” DICOMO 2011, Jul. 2011.