情報処理学会論文誌 Vol.54 No.1 1–14 (Jan. 2013)

推薦論文

NTMobileにおける移動透過性の実現と実装

内藤 克浩[1,a)] 上醉尾 一真[2] 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]

受付日 2012年4月24日, 採録日 2012年10月15日

概要：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 ネットワークを想定しており, IPv4 ネットワークは十分には検討されていない. 著者らは, 移動透過性と NAT 越え問題の解決を同時に実現する NTMobile (Network Traversal with Mobility) を提案してきた. 本稿では, NTMobile において, 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およびプライベート IP アドレスを用いるネットワークにおいて, 移動透過性の実現方法の詳細と実装方法について提案する. 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, IP データグラムの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.

Realization and implementation of IP mobility in NTMobile

Katsuhiro NAITO[1,a)] Kazuma Kamienoo[2] Takuya NISHIO[1] Tomohiro MIZUTANI[2]
Hidekazu SUZUKI[2] Akira WATANABE[2] Kazuo MORI[1] Hideo KOBAYASHI[1]

Received: April 24, 2012, Accepted: October 15, 2012

Abstract: Recent wireless terminals usually have multiple wireless interfaces, and can switch them to access networks. IP mobility is the technologies that can keep communication when access networks are switched. Most of conventional studies about IP mobility focus on IPv6 networks and those about IPv4 networks are quite few. The Authors have been proposing Network Traversal with Mobility (NTMobile) that can achieve IP mobility and solving the NAT Traversal problem at the same time. In this paper, we will propose the detail of mobility mechanisms and implementation of NTMobile that can achieve IP mobility in global IP networks and private IP networks by introducing virtual IP addresses and constructing tunnels between end terminals. In NTMobile, applications use virtual IP addresses to achieve continuous communication when physical IP addresses change due to switching of networks. We have implemented 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

[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
[a)] naito@elec.mie-u.ac.jp

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, 異なる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]. 一方, IEEE 802. 21 を利用した場合にも, ネットワーク切り替えにともない IP アドレスが変化する.

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, ネットワーク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], [6], [7]. MobileIP は IPv4 ネットワーク用の Mobile IPv4 (MIPv4) [5], [8] と, IPv6 ネットワーク用の Mobile IPv6 (MIPv6)[9], [10] が検討されており, 近年は IPv4/IPv6 ネットワークを同時に利用可能な Dual Stack Mobile IPv6 (DSMIPv6)[11] も提案されている. しかしながら, MIPv4 では, 移動端末宛の通信は必ずホームエージェントと呼ばれる装置を通過する通信を行うため, 通信経路が冗長となる. また, 移動端末からの通信経路を最適化した際には, IP データグラム内の送信元アドレスと実アドレスが異なるため, 一部のルータが IP データグラムを破棄することが知られている [6], [7], [12]. MIPv4 では経路最適化やホームエージェントの二重化は検討されていない一方, MIPv6 では経路最適化手法 [13] を利用することにより, 冗長な通信経路を避けることができ, ホームエージェントの二重化も検討されている [14]. しかし, MIPv6 と MIPv4 には互換性がなく, これらの機能は IPv4 ネットワークでは利用できない . DSMIP は MIPv6 を IPv4 ネットワークにも拡張したものであるため, MIPv4 の経路最適化やホームエージェントの二重化に対する検討課題はそのまま引き継がれている. Host Identity Protocol (HIP) [16] では, IPv4/IPv6 ネットワークを同時に利用可能な手法であるが, Interactive Connectivity Establishment (ICE) [17] を用いたシグナリングコストが高いことが知られている [18]. Session Initiation Protocol (SIP) Mobility [19] は SIP を拡張することにより移動透過性を実現しており, IPv6 ネットワークでの利用は十分に議論されていない. また, SIP Mobility ではアプリケーション毎の対応が必要である.

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)[15]. 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 [20]. Mobile PPC では, IPv4 ネットワークのみを想定しており, エンド端末のみで移動透過性を実現可能な技術である. しかし, エンド端末が NAT 配下に移動した場合, 通信相手の実 IP アドレスが NAT のアドレスとなるため, エンド端末のみによる実 IP アドレスの把握ができなくなる. この問題に対処するためには, NAT 自身を改造するか, 新たな通信シーケンスを定義して NAT のアドレスをエンド端末に伝えるなど, 複雑な処理が必要であった.

また, 著者らは 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(Network Traversal with Mobility) を提案してきた [21]. NTMobile では, IP アドレスが持つノード識別子と位置識別子の役割を分離するため, ノード識別子として仮想アドレスを導入する. また, NTMobile 端末を管理する Direction Coordinator (DC) 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. また, Mobile PPC と同様に経路冗長のない移動透過性を実現可能である. さらに, 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ことができるため, グローバル IP アドレスおよびプライベート 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. 本稿では, 提案してきた NTMobile を実装することにより, グローバル IP アドレスおよびプライベート IP アドレスの区別なく移動透過性を実現可能であることを評価実験から示す. さらに, カーネル空間で IP データグラムの処理を行うことで, 高スループットを実現可能であることも示す.

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 Coordinator (DC), 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. Mobile IP では, Mobile IP 端末の管理と通信中継をホームエージェントが受け持っており, ホームエージェントは通常ホームネットワーク上に設置される. 一方, NTMobile では, NTMobile 端末の管理, 仮想 IP アドレスの管理および通信経路の管理などは DC に集約し, 中継機能は RS に分離している. DC の位置は Domain

Name System(DNS) を用いることにより探索できるため, 設置場所の制約がない. また, RS の位置は DC が管理するため, ネットワーク上の任意の場所に設置可能である. このため, ネットワーク規模およびトラヒック状況などに応じて DC および RS を適切な場所に設置でき拡張性が高い. 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, シームレスな移動を実現可能である.

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ノード識別子である仮想 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であり, 移動透過性を実現することが可能である. なお, NTMobile 端末はアプリケーションが生成する仮想 IP アドレスによる IP データグラムを, 位置識別子である実 IP アドレスを用いてカプセル化することによりトンネル通信を行う.

NTMobile では, カプセル化で利用されるトンネル経路として 2 種類を想定しており, エンド端末間で直接トンネルを構築する場合, 各エンド端末が RS 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, また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, 経路冗長のない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, DC が各エンド端末に指定する 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. NTMobile は Stateful Packet Inspection (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 ルータを想定しており, 既存の NAT ルータの機能を変更することなしに, NAT 越えが実現可能である. そのため, 既存のほとんどのネットワークにおいて移動透過性を実現できる. 以下に NTMobile を構成する端末および装置の機能を説明する.

- Direction Coordinator (DC)
  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. 各 DC 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. また, DC 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. 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 [22]. NTMobile では DC の分散管理を想定しており, 通信先端末を管理する DC を探索するために DNS の機構を利用している. そのため, DC は最低 1 個の管理ドメインを持つ.
- 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 端末と RS 間にトンネルを構築し, RS が一般端末との通信を中継することにより, 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可能な装置である.
- NTMobile 端末
  NTMobile 端末間の通信は DC 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, DC からの指示に応じて, 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う. そして, 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ことで, 両端末が通信可能な状態にする.

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可能である. 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. 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, および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 では, NTMobile 端末が接続してるネットワークを判定するために, NTMobile 端末の実 IP アドレスと NAT の外側 IP アドレスを利用する. 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, および 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, RS を経由して通信を行う. なお, 一般端末が NAT 配下に存在する場合には, 一般端末に向けた通信を開始できないため, RS を経由したとしても, NTMobile 端末の移動透過性は実現できない. 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.

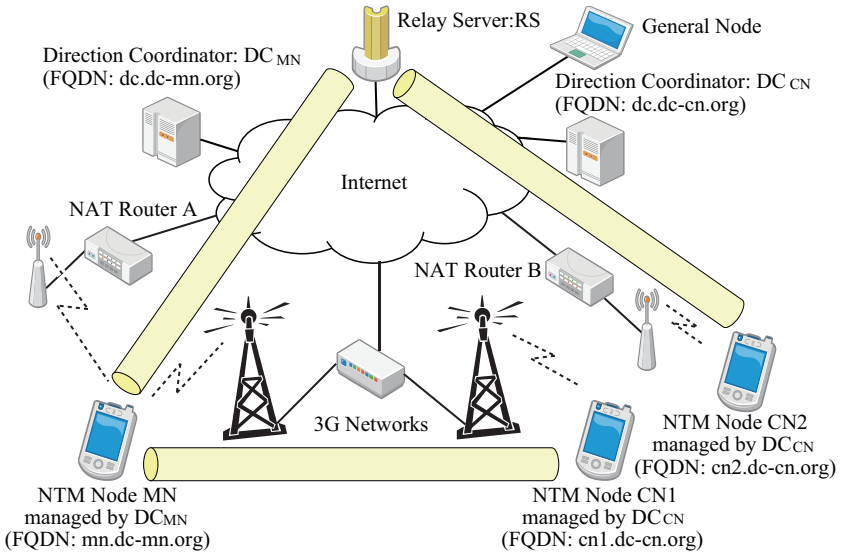


図 1 NTMobile の概要.
Fig. 1 Overview of NTMobile network.

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

G:Global address, P(A):Private address in Network A
P(B):Private address in Network B, P(C):Private address in Network C

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 の場合は Path ID が記録される. また, それ以外のメッセージの場合は Node ID が記録される.
- Registration Request / Registration Response
  NTMobile 端末起動時および移動後, NTMobile 端末のアドレス情報登録に利用されるメッセージを示す.

- NTM Update Request /NTM Update Response
  構築したトンネルに関する情報が経路上のルータなどで破棄されることを防ぐために, 定期的にメッセージ交換を行うメッセージを示す.
- Direction Request
  NTMobile 端末が起動時および移動後, トンネル構築を DC に要求する際に利用するメッセージを示す.
- Route Direction
  DC が NTMobile 端末にトンネル構築に必要な情報を通知し, 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
  DC が RS にトンネル中継に必要な情報を通知し, NTMobile 端末間の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.
- Relay Response
  Relay Direction に対する確認応答メッセージを示す.
- 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た IP データグラムを示す. カプセル化される IP データグラムの送信元アドレスと送信先アドレスに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

NTMobile の大きな特徴は, エンド端末の一方でもグローバル IP アドレス空間に存在する場合, エンド端末間で直接通信を確立できる点である. NTMobile では, NTMobile Daemon がアプリケーション空間において動作しており, NTMobile のシグナリング処理を行う. また, カーネル空間において, IP データグラムのカプセリング処理を行う. そのため, NTMobile を用いた移動透過性を実現するために, 既存の一般アプリケーションの修正は必要ない. 図 3 では, シグナリング処理のうち DNS の A リプライの処理と NTMobile 専用レコードの処理のみ, カーネルモジュールで行っているため, 図では送受信先が明確となるようにアプリケーション空間とカーネル空間で分けて記載する.

なお, 各 DC は NTMobile で想定する移動管理手段 [23] 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 などのアドレス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. ここでは, 通信開始側 NTMobile 端末を MN, 通信相手側 NTMobile 端末を CN と表記する.

グローバル IP とプライベート IP 間のコネクション確立

図 3 は表 1 のパターン 3, 7, 9 に対応するもので, 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.

- アプリケーションによる通信開始要求の検出
  多くのアプリケーションは Fully Qualified Domain Name (FQDN) を用いた通信相手端末の指定を行っており, DNS リゾルバは FQDN に対応する IP アドレスの探索を行う. NTMobile では, DNS リゾルバが送信する A レコードに対する探索をカーネル空間で検出することにより, 通信相手端末が NTMobile 端末であるのか確認を行う. なお, DNS リゾルバ宛の A レコードに対する応答メッセージは, 以下のトンネル確立処理が終わるまで, カーネル空間において一時的に待避を行う.
- 通信相手端末の NTMobile 情報の取得
  NTMobile 端末はカーネル空間において, A レコードで探索された FQDN に対して, NTMobile 専用レコードの探索を行う. 通信相手端末が NTMobile 端末の場合, NTMobile 専用レコードを入手することができ, 通信相手端末のノード ID, 実 IP アドレス, NAT ルータの外側 IP アドレス, 通信相手端末を管理する DC の IP アドレス, 仮想 IP アドレスなどの情報を入手可能となる. なお, カーネル空間で取得した NTMobile 専用レコードの情報は, Netlink ソケットを用いてアプリケーション空間で動作する NTMobile Daemon に通知される.
- トンネル構築の指示要求
  MN は自身の DC に Direction Request を送信することにより, CN とのトンネル構築の指示要求を行う. なお, Direction Request には, MN のノード ID ID*MN, 仮想 IP アドレス VIP*MN, CN のノード ID ID*CN, 実 IP アドレス RIP*CN, DC の IP アドレス RIP*DC-CN, 仮想 IP アドレス VIP*CN が含まれる. また, CN が NAT 配下に存在する場合には, NAT ルータの実 IP アドレスも含まれる.
- トンネル構築の指示
  MN の DC は Tunnel Request を受信することになる CN に対して, CN の DC を経由することにより, Route Direction を送信する. 次に, MN の DC は MN に対して Route Direction を送信する. NTMobile では, DC と DC が管理する NTMobile 端末間, DC 同士, DC と RS との間に信頼関係があることを前提とする. そのため, MN 側の DC と CN との間に信頼関係がない場合も考えられる. そこで, CN に対しては, Route Direction を CN 側の DC 経由で送信する. Route Direction には, 両端末のノード ID, 実 IP アドレス, NAT ルータ

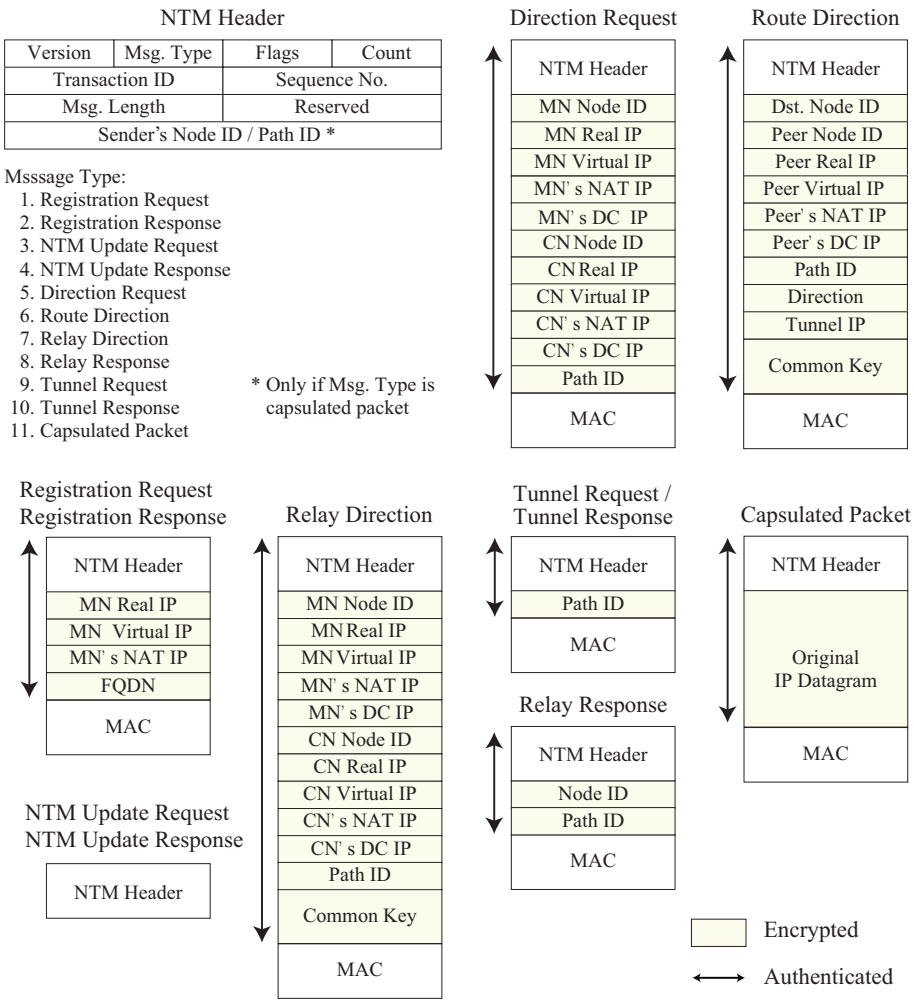


図 2 メッセージフォーマット.
Fig. 2 Message format.

の IP アドレス, 仮想 IP アドレス, DC の IP アドレスに加え, トンネル通信経路を識別するためのパス ID が含まれる. NTMobile では, NTMobile 端末間で構築されるトンネル通信経路を管理するために, パス ID を用いる.

- トンネル構築の要求と応答
  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 を返信することによりトンネル応答を行う. NTMobile では, 構築したトンネルを用いて両エンド端末間の全ての通信を行う. 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.
- A レコードの開放
  アプリケーションの通信を開始させるために, トンネル構築後に待避していた A レコードに対する応答メッセージを開放する.

プライベート IP 間のコネクション確立

図 4 は表 1 のパターン 12, 13, 15, 16, 17 に対応するもので, 両エンド端末が NAT 配下のプライベート IP アドレス空間に存在している場合である. 図 3 と大きく異なる点は, CN 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, RS 経由でトンネル構築を行うのが大きな違いである. なお, DNS を用いた NTMobile 端末の実 IP アドレス情報の取得方法についての説明は図 3 と同様のため省略する.

- トンネル構築の指示要求
  MN は自身の DC に Direction Request を送信することにより, CN へのトンネル構築の指示要求を行う.
- トンネル中継の指示
  DC は Relay Direction を RS 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. また, RS は Relay Response を DC に

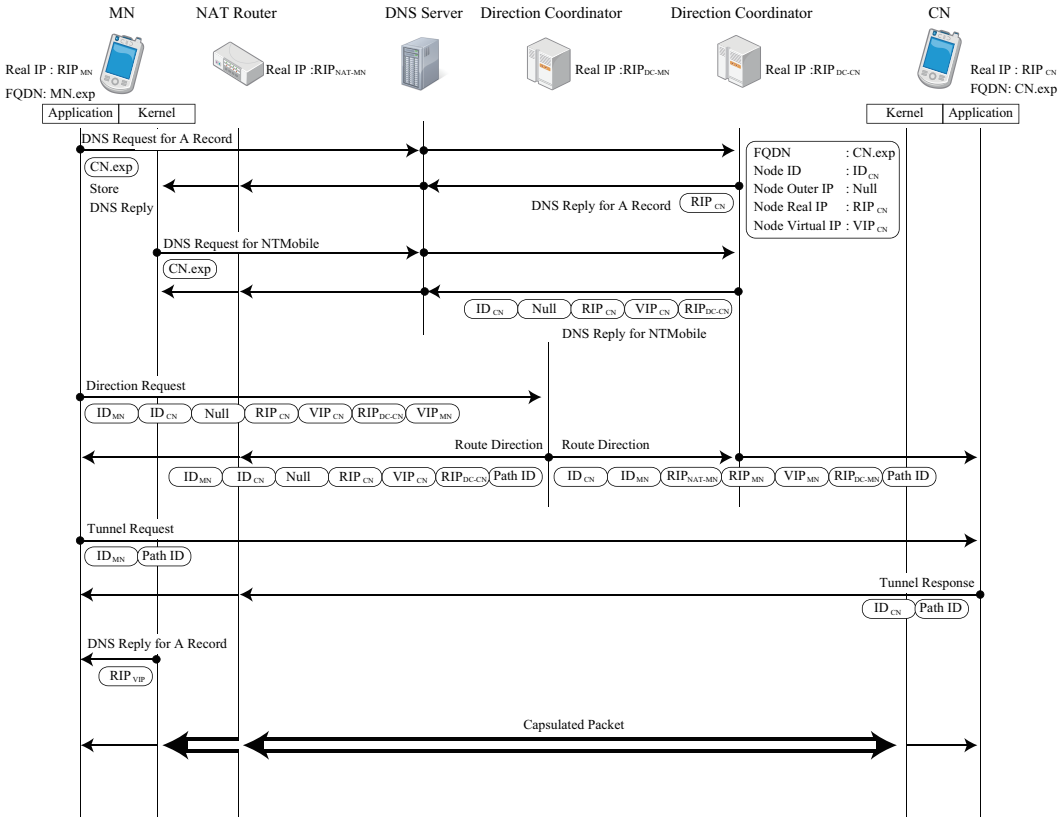


図 3 グローバル IP とプライベート IP 間のコネクション確立.

Fig. 3 Connection process between global IP and private IP.

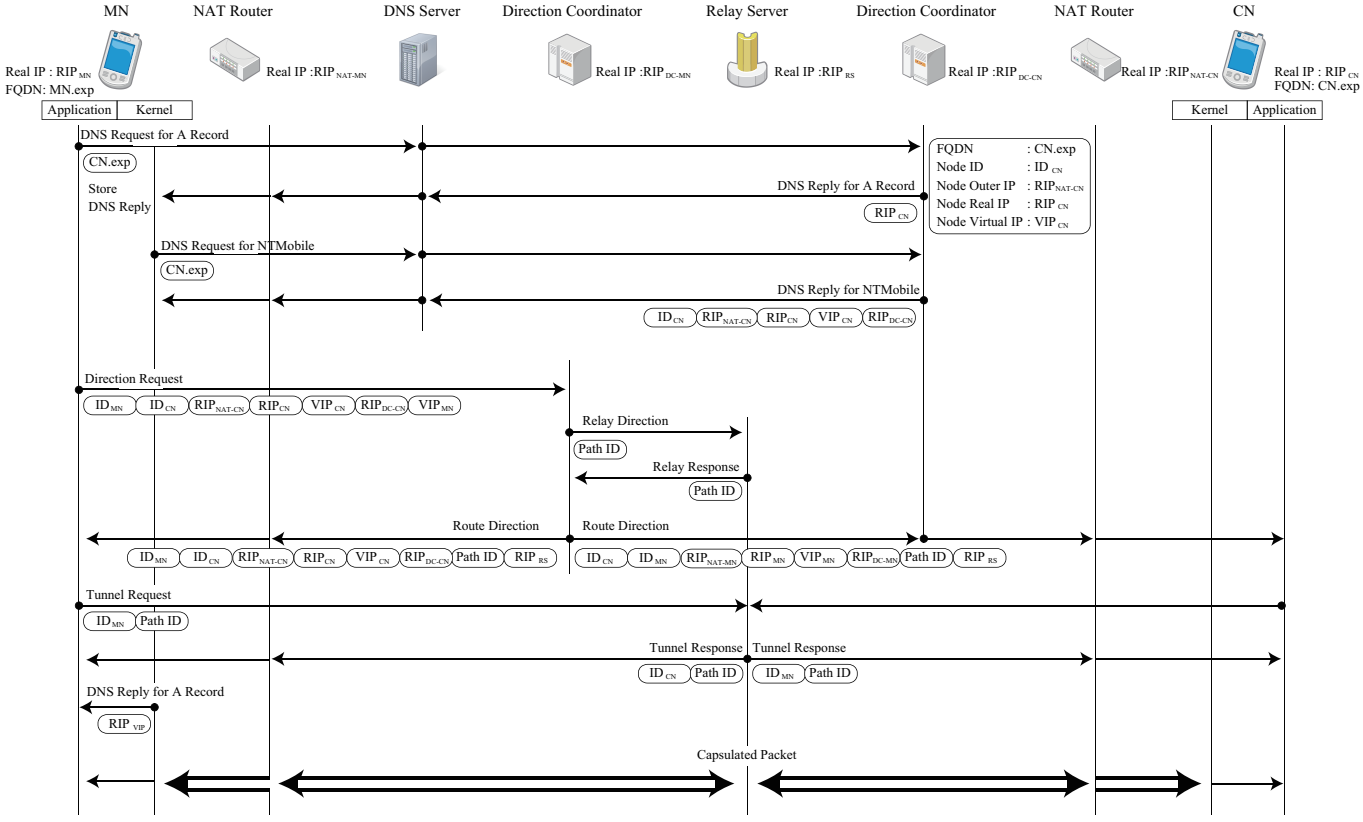


図 4 プライベート IP 間のコネクション確立.

Fig. 4 Connection process between private IPs.

返信することにより, MN と CN 間の中継が可能であることを通知する.

- トンネル構築の指示
  MN の DC は Tunnel Request を受信することになる CN に対して, CN の DC を経由することにより, Route Direction を送信する. 次に, MN の DC は MN に対して Route Direction を送信する. .
- トンネル構築の要求と応答
  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, MN 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 アドレスを監視している. IP アドレスの変化を検出した場合, 新たな IP アドレスを DC 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, MN と CN 間のコネクション再確立を行う.

- トンネル構築の指示要求
  通信に利用する実 IP アドレスが更新された場合, MN は自身の DC に Direction Request を送信することにより, MN と CN 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, DC の IP アドレスに加え, トンネル通信経路を識別するためのパス ID が含まれるため, DC は NTMobile 端末の移動後に利用するトンネル通信経路を把握できる.
- トンネル構築の指示
  MN の DC は Tunnel Request を受信することになる CN に対して, CN の DC を経由することにより, Route Direction を送信する. 次に, MN の DC は MN に対しても Route Direction を送信する.
- トンネル構築の要求と応答
  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, MN 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, MN 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, MN と CN 間のコネクション再確立を行う.

- トンネル構築の指示要求
  通信に利用する実 IP アドレスが更新された場合, MN は自身の DC に Direction Request を送信することにより, MN と CN 間のトンネル再構築の要求を行う.
- トンネル構築の指示
  MN の DC は Tunnel Request を受信することになる CN に対して, CN の DC を経由することにより, Route Direction を送信する. 次に, MN の DC は MN に対しても Route Direction を送信する.
- トンネル構築の要求と応答
  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. 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, この仮想インターフェースに仮想 IP アドレスの割当を行う. NTMobile 端末間の通信では, アプリケーションは仮想 IP アドレスを用いてコネクションを結ぶことにより, NTMobile 端末の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 MN と CN 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, MN と CN の実 IP アドレス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, MN から CN 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, NTMobile ではカプセル化に伴い, NTM ヘッダと Message Authentication Code (MAC) が追加されるため, IP データグラム長が微増する. そこで, 仮想インタフェースの MTU 値を物理インタフェースの MTU 値から NTM ヘッダと MAC 分小さい値とすることで, 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, エンド端末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も移動透過性を実現するために, RS 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. IP データグラムはカー

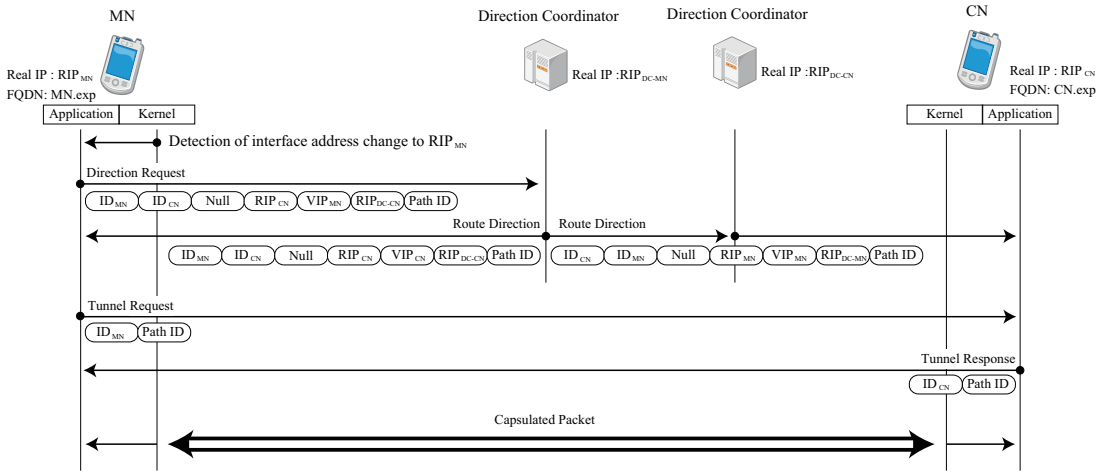


図 5 グローバル IP 間のコネクション再確立.
Fig. 5 Reconnection process between global IPs.

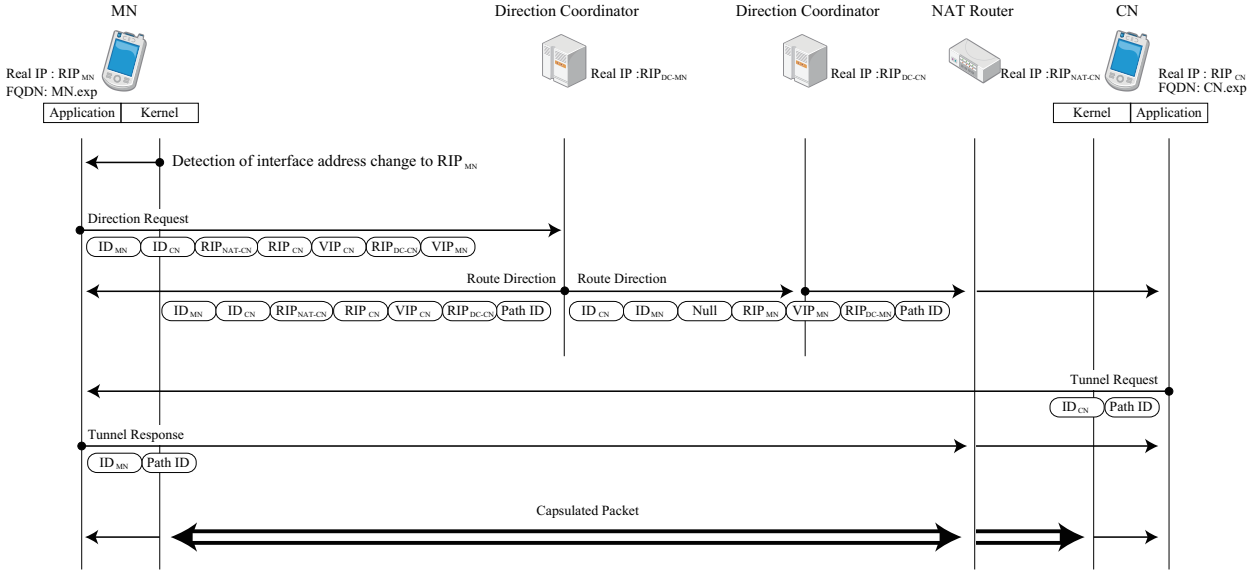


図 6 グローバル IP とプライベート IP 間のコネクション再確立.
Fig. 6 Reconnection process between global IP and private IP.

ネルモジュールにおいてカプセル化され, RS に向けて送信される. RS はこれをデカプセル化し, IP データグラムの仮想 IP アドレスを自身の IP アドレスに変換し, さらに送信元ポート番号を RS において重複しない番号に変換し, 一般端末宛てに送信すること. これにより, 一般端末は通信相手を常に RS と判断するため, 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になる. なお, 一般端末と NTMobile 端末の判断は NTM 専用レコードを取得できたかどうかを確認することにより行う.

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, 携帯端末などでも利用される 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 とカーネル空間で動作する NTMobile Kernel Module 間は Linux の Netlink ソケットを用いて接続する. なお, 一般アプリケーションが IP データグラムの送信元アドレスとして仮想アドレスを利用できるように, 仮想アドレスは仮想インタフェースに割当を行う. また, 仮想アドレスに対する通信は, 仮想インタフェースを利用するように経路情報の設定を行う. 仮想インタフェースは tun/tap を用いて構築する.

ユーザ空間の実装

ユーザ空間の NTMobile Daemon の機能は以下のとおり

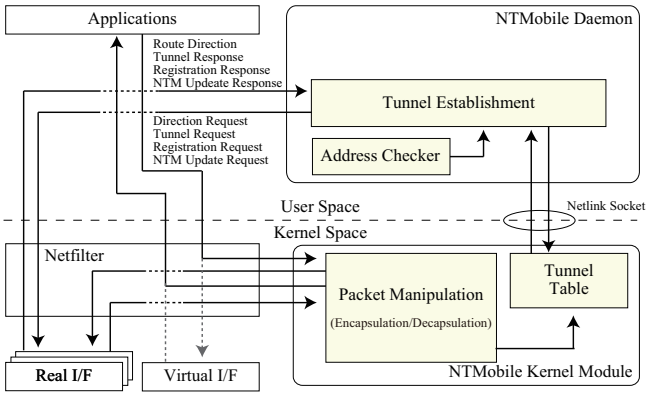


図 7 NTMobile 端末のモジュール構成.
Fig. 7 Module configuration of NTMobile node.

である.

- アドレス確認
  インタフェースの IP アドレスまた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, 必要に応じて新たに接続したネットワークを用いて, 新たなトンネル構築を DC に要求する. また, DC からの経路指示に応じて, NTMobile 端末はエンド端末間または 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 に追加および削除することが可能である. 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およ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およ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の情報に応じて実行される.
- IP データグラムの暗号化および復号処理
  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, 暗号化と復号の処理を行う.

4.2 DC の実装

図 8 に NTMobile の DC のモジュール構成図を示す. DC 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

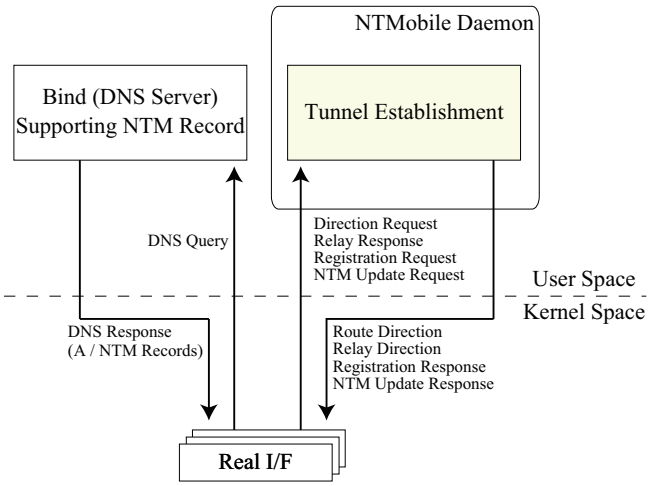


図 8 DC のモジュール構成.
Fig. 8 Module configuration of direction coordinator.

に関する指示を出すことである.

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

- アドレス情報の管理
  NTMobile 端末は起動時および移動時に Registration Request を用いて, 自身の実 IP アドレス情報を DC に送信する. DC は受信する実 IP アドレス情報を NTMobile 用の専用 DNS レコードに保存するとともに, NTMobile 端末のアドレス情報の管理を行う. また, NTMobile では DNS の機構を用いて通信先端末の管理 DC を探索するため, DC は DNS 機能を包括したものとなる.
- 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 端末の実 IP アドレス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, DC 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, DC 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.

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

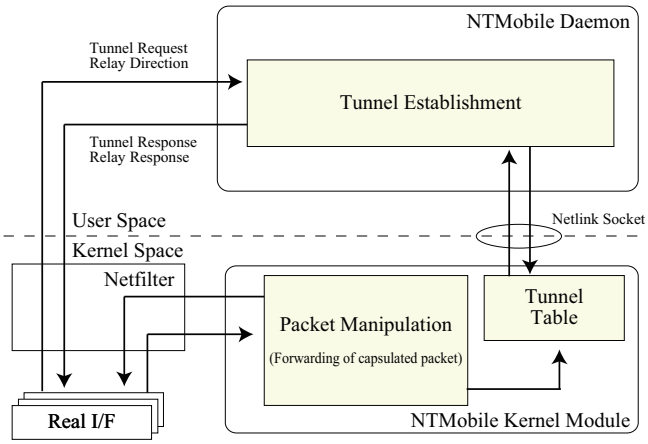


図 9 RS のモジュール構成.
Fig. 9 Module configuration of relay server.

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 の機能は以下のとおりである.

- トンネル中継情報の受信
  RS は DC からトンネル中継で必要となる Path ID および Common Key の情報を受け取ることにより, NTMobile 端末からのトンネル要求の受入待機を行う. なお, Common Key は MN と RS および CN と RS 間の通信を暗号化する際に利用する共通暗号鍵である.
- 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によりトンネル中継を行う.

- NTMobile 端末からのカプセル化された IP データグラムの受信
  NTMobile 端末とのトンネルを通して受信されるカプセル化された IP データグラムを受信し, 宛先端末が NTMobile 端末または一般端末かを判断する.
- NTMobile 端末への中継
  NTMobile 端末宛のカプセル化された IP データグラムを受信した場合, RS はカプセル化された IP データグラムの外側ヘッダの送信元アドレスを RS のアドレスに, 宛先アドレスを該当 NTMobile 端末宛に変更した後, 送信を行う.
- 一般端末への中継
  一般端末宛のカプセル化された IP データグラムを受信した場合, RS は該当 IP データグラム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する. 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

一般にカプセル化処理はユーザ空間とカーネル空間で実現可能である. ユーザ空間でカプセル化処理を行う場合, メモリコピーに伴うオーバヘッドにより, スループット特性の劣化などにつながることが知られている [24].

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, 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 IP データグラムは, Netfilter の NF_INET_LOCAL_OUT にてフックを行うことにより, 送信 IP データグラムの 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 IP データグラムのカプセル化およ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. 受信時は, Netfilter の NF_INET_PRE_ROUTING にてフックを行うことにより, 受信 IP データグラムの 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 IP データグラムのデカプセル化および復号処理を行った後, Netfilter の NF_INET_LOCAL_IN にて sk_buff をチェインに戻す. このように, Netfilter を用いてフックする 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 ではカプセル化処理を行うことにより, 仮想アドレスを用いた IP データグラムを物理アドレスに基づいて配送している. 一般にカプセル化処理のオーバヘッドは大きいことが知られており, カプセル化処理の実装手法は重要となる. 本研究では, NTMobile のカプセル化処理を Linux のカーネルモジュールとして実装しており, iperf [25] を用いることによりスループット測定を実施した. なお, 本評価でのスループットの計算は iperf が転送したデー

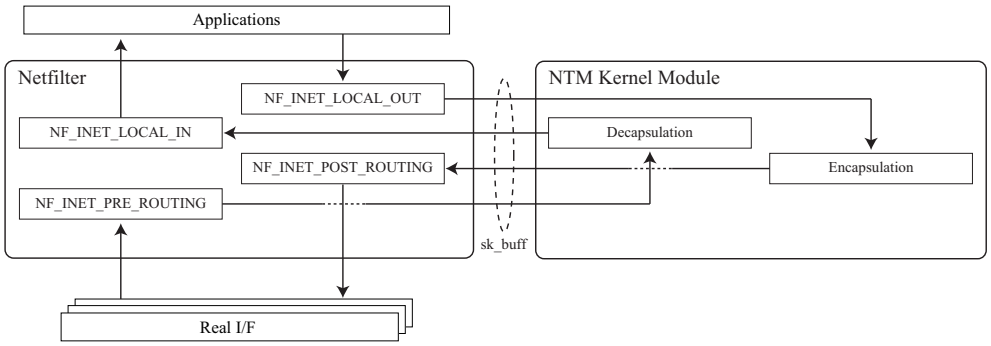


図 10 NTMobile カーネルモジュール構成.
Fig. 10 Configuration of NTMobile kernel module.

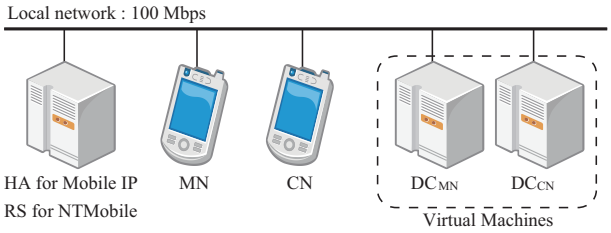


図 11 性能評価モデル.
Fig. 11 Performance evaluation model.

タ量に基づいて計算しているため, デカプセル化された後の IP データグラムで評価している. また, NTMobile で想定するエンド端末間の直接通信および RS を経由する通信について, Transmission Control Protocol (TCP) 及び User Datagram Protocol (UDP) の通信が実現可能であることを確認した. なお, 関係する既存方式として, Linux 用の Mobile IPv4 の実装が入手困難であったため, 既に実装が配布されている Mobile IPv6 を参考値として測定を実施した. Mobile IPv6 の測定では, MN に Mobile IPv6 の実装を導入し, MN と CN はホームエージェント経由で通信を行った. なお, NTMobile と Mobile IPv6 の評価では, 同一のハードウェア及び OS を用いた.

図 11 に性能評価で用いたモデルを示す. 評価環境では, スループットに影響を与えるエンドノードおよび転送処理を行う RS および Mobile IP の Home Agent (HA) を一般的な PC として準備した. また, NTMobile 端末を管理する DC は仮想マシンとして準備した. 表 2 にスループット測定に関する諸元を示す.

図 12 に暗号化処理を行わない場合のスループット特性を示す. 本スループット特性から, 提案方式のカプセリング処理のオーバヘッドが確認可能である. 結果より, 既存の Linux カーネルを用いた場合のスループット特性と比較し, NTMobile 端末間で直接通信した場合のスループットは若干劣化していることが確認できる. しかし, 劣化量はカプセル化に伴い追加される NTM 用のヘッダーサイズの割合に合致しており, カプセリング処理自体のオーバヘッドは極めて小さいことが確認できる. 次に, RS を経由した

表 2 エンドノード, RS, HA の性能評価諸元.
Table 2 Performance evaluation parameters of End-nodes, RS and HA.

OS	Linux
Distribution	Ubuntu 10.04
Kernel version	linux-2.6.32-24-generic
CPU	Intel Core i7 870 2.93GHz
Memory	10 GBytes
Application	iperf
Number of measurements	10

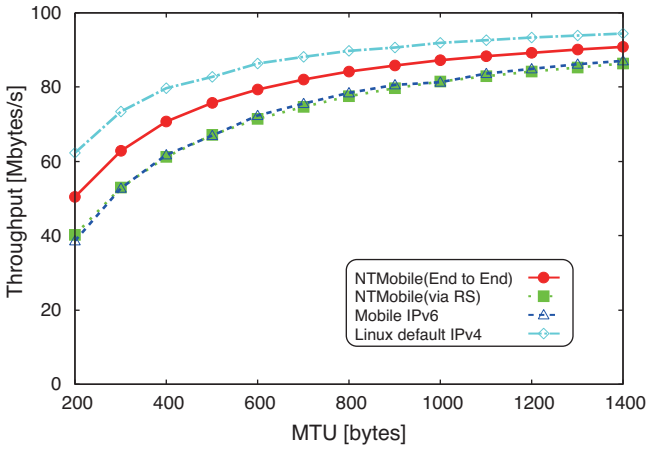


図 12 スループット性能 (暗号化処理なし).
Fig. 12 Throughput performance without encryption.

NTMobile のスループットと, HA を経由した Mobile IPv6 のスループットを比較すると, ほぼ同一のスループットを達成できていることが確認できる. そのため, NTMobile の実装手法は既存の移動透過性技術である Mobile IPv6 における実装と, ほぼ同等のスループット性能を達成していることが確認できる.

図 13 に暗号化処理を行う場合のスループット特性を示す. 本スループット特性から, 提案方式の暗号化処理のオーバヘッドを確認可能である. 結果より, 暗号化処理を行わない場合に比べて, 若干のスループット特性の劣化が確認されるが, NTMobile と Mobile IPv6 の劣化量はほぼ同等

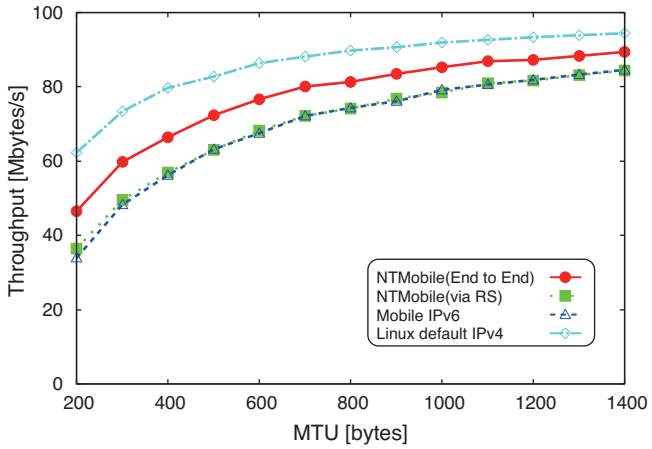


図 13 スループット性能 (暗号化処理あり).
Fig. 13 Throughput performance with encryption.

である. そのため, NTMobile の実装における暗号化処理のオーバヘッドは Mobile IPv6 と同程度であり, 高いスループットを達成可能と考えられる.

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 について, 具体的な実装方法を提案した. 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, 経路冗長のない移動透過性を実現可能である. また, 両エンド端末が 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ことにより, IPv4 ネットワークで想定される全ての状況において, 移動透過性を実現している.

実装では, IP データグラムの処理に伴うスループット特性の劣化を抑えるため, カーネル空間におけるカプセル化およ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, 提案実装方式は既存の Linux カーネルの変更を必要としない上, 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.

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, pp. 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, pp. 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 (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] 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)

[7] 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)

[8] http://www.mip4.org, retrieved (2012)

[9] C. Perkins, D. Johnson and J. Arkko : Mobility Support in IPv6, Revised, RFC 6275, IETF (2011)

[10] M. Ishiyama, M. Kunishi, K. Uehara, H. Esaki, and F. Teraoka : LINA: A New Approach to Mobility Support in Wide Area Networks, IEICE Trans. Comm. , Vol. E84-B, No. 8, pp. 2076-2086 (2001)

[11] H. oliman : Mobile IPv6 Support for Dual Stack Hosts and Routers, Revised, RFC 5555, IETF (2009)

[12] G. Montenegro : Reverse Tunneling for Mobile IP, revised, RFC 3024 (2001)

[13] C. Perkins and D. Johnson : Route Optimization in Mobile IP, draft-ietf-mobileip-optim-11.txt (2001), Work in progress.

[14] A. Patel, Ed. and D. Johnson : Problem Statement for Bootstrapping Mobile IPv6 (MIPv6), RFC 4640 (2006).

[15] H. Levkowetz and S. Vaarala : Mobile IP Traversal of Network Address Translation (NAT) Devices, RFC 3519 (2003)

[16] T. Heer, S. Varjonen : Host Identity Protocol Certificates, Revised, RFC 6253, IETF (2011)

[17] M. Westerlund, C. Perkins : IANA Registry for Interactive Connectivity Establishment (ICE) Options, Revised, RFC 6336, IETF (2011)

[18] P. Nikander, A. Gurtov and T. R. Henderson : Host Identity Protocol (HIP): Connectivity, Mobility, Multihoming, Security, and Privacy over IPv4 and IPv6 Networks, IEEE Communications Surveys & Tutorials, Vol. 12, Issue. 2, pp. 186-204 (2010)

[19] 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 (2008)

[20] 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) (2009)

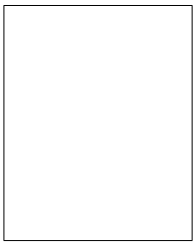
[21] 鈴木 秀和, 水谷 智大, 西尾 拓也, 内藤 克浩, 渡邊 晃 : NTMobile における相互接続性の確立手法と実装, DICOMO 2011 (2011)

[22] A. Gustafsson : Handling of Unknown DNS Resource Record (RR) Types, RFC 3597 (2003)

[23] 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 (2011)

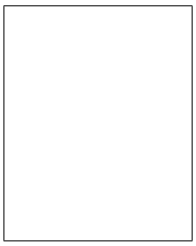
[24] S. Khanvilkar and A. Khokhar :Virtual private networks: an overview with performance evaluation, IEEE Communication Magazine, Vol. 42, No. 10, pp. 146-154 (2004)

[25] http://iperf.sourceforge.net



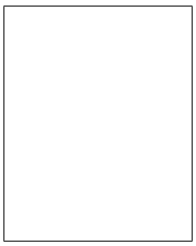
内藤 克浩 （正会員）

1999 年慶大・理工・電気卒. 2004 年名大大学院博士課程後期課程修了. 同年, 三重大・工・電気電子・助手. 2007 年同大・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.



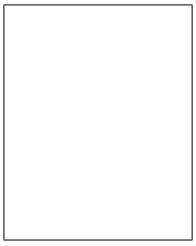
上醉尾 一真 （学生会員）

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.



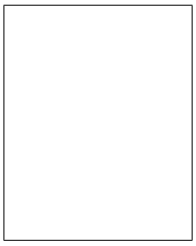
西尾 拓也

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. モバイルネットワークに関する研究に従事.



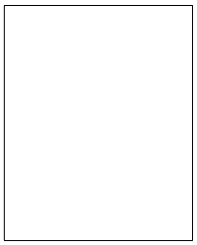
水谷 智大

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）.



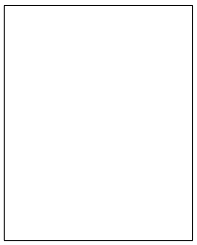
鈴木 秀和 （正会員）

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. 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. 博士（工学）. 電子情報通信学会, IEEE 各会員.



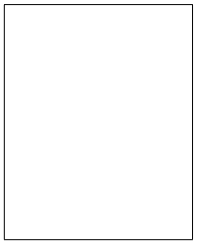
渡邊 晃 （正会員）

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 年名城大学理工学部教授, 現在に至る. 博士（工学）. 電子情報通信学会, IEEE 各会員.



森 香津夫

昭 61 名工大・工・情報卒. 平 12 名大大学院博士後期課程了. 昭 61 年三洋電機 (株) 入社. 以来、交換システム, 移動通信システムの研究開発に従事. 平 7〜平 12(株) ワイ・アール・ピー移動通信基盤技術研究所出向, 平 12 三重大・工・電気電子・助教授, 平 17〜平 18 ロンドン大学キングス校・客員研究員, 平 19 三重大院・工・電気電子・准教授, 平 23 同・教授. 工博. 平 13 年度電子情報通信学会論文賞受賞. 電子情報通信学会, IEEE 各会員.



小林 英雄

昭 50 東北大・工・通信卒. 昭 52 同大学院修士課程了. 同年 KDD 入社. 以来、衛星通信, 移動通信システムの研究開発に従事. 平 10 三重大・工・電気電子・教授. 工博. 無線通信用伝送方式に関する研究に従事. 電子情報通信学会, IEEE 各会員.