平成26年度　卒 業 論 文

和文題目

プライベート空間のサーバにアクセスが可能な NTMobile用プライベート中継装置の提案

英文題目

Proposal of NTMobile private relay device that Enables Access to the Server in Private Address Area

情報工学科　渡邊研究室

(学籍番号: 100430127)

李　丹薇

提出日: 平成 27 年 2 月 12 日

名城大学理工学部

内容要旨

IPv4 ネットワークの大きな課題として，インターネット側の端末から NAT 配下の端末に通信を開始できない NAT 越え問題があり，その解決が望まれている．また，公共無線網の普及や携帯端末の発達により，通信中にネットワークを切り替え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．我々は，NAT 越え問題の解決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．プライベートアドレスを持つサーバに NTMobile を実装することより，インターネット側の端末からこのサーバに対してアクセスが可能になる．しかし，サーバに手を加えることは許可されないことが多い．そこで，本論文では，サーバの横に NTMobile 用プライベート中継装置を設置して，インターネット側からプライベートサーバへの通信開始を可能にする方式を提案する．

目 次

第1章　はじめに

現在のネットワークはIPv4ネットワークを使用しており，その最も大きい課題はアドレスの枯渇問題であり，長期的な解決策としてはIPv6に移行するが，IPv4アドレスとIPv6アドレスは互換性がないため，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，IPv4とIPv6の混在環境が続くと想定されている．また，短期的な解決策として，インターネットと家庭内や企業内のネットワークの間にNAT(Network Address Translation)を導入し，プライベートアドレスを利用して通信を行っている．しかし，グローバルネットワーク側の端末からNAT配下の端末に通信を開始できないNAT越え問題が発生し，通信接続性を確保できない課題がある．一方，スマートフォンをはじめとする携帯端末の普及及び公共無線網の発達により，ネットワークの利用需要が急増し，特に移動しながら通信を継続できることが要求されている。しかし，現在のIPネットワークでは，端末に割当たられたIPアドレスを通信識別子として通信を行っている．端末の移動やネットワークの切り替えによって，IPアドレスが変化すると通信が継続できない．このような問題を解決するため，通信中に移動やネットワークの切り替えでも通信を継続できる技術が望まれている．

我々は，通信接続性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は仮想IPアドレスの導入とトンネル技術を用いることにより，NAT越えと移動透過性を実現した技術である．NTMobileの機能を実装した端末（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る．通信開始時アプリケーションは仮想IPアドレスに基づいて通信を行う．実際の通信では，実IPアドレスで全てのバケットをカプセル化し，トンネル通信を行う．

プライベートアドレスを持つサーバにNTMobile機能を実装することより，インターネット側の端末からこのサーバに対してアクセスが可能になる．しかし，サーバに手を加えることは許可されないことが多い．そこで，本論文は，NTMobile機能を拡張し，サーバの横にNTMobile機能を実装したプライベート中継装置を設置して，インターネット側からNAT配下に存在するプライベートサーバへの通信開始を可能にする手法を提案する．中継装置がNTMobileを代行する．中継装置でアドレス変換してサーバにアクセス，サーバは中継装置からアクセスされているように見えるので，ほかのネットワークには一切影響を与えない．

以下，2章でNTMobileにおける一般端末とNTM端末との通信動作について説明し，3章では提案方式について説明する．4章で実装の検討について述べ，5章でまとめる．

第2章　NTMobile

本章では，NAT 越え問題の解決と移動透過性技術を同時に実現する技術 NTMobile について説明する．

この技術は IPv4 ネットワーク想定しており，IPv4 ネットワークは，グローバルアドレスの枯渇でアドレスの消費を抑えるため，NAT というアドレス変換装置を設置し，組織ネットワーク内においているプライベートアドレスを利用するネットワークが一般的である．NAT を利用する場合は，組織内のネットワークは外部ネットワークである IP アドレスから隠蔽されることから，インターネット側から組織内のインターネットへの通信は開始できない．NTMobile は IP アドレスが持つノード識別子と位置識別の役割を分離するため，仮想 IP アドレスを導入し，グローバル IP アドレスとプライベート IP アドレスの区別なく移動透過性を実現する．

2.1　NTMobile の概要

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，アプリケーションで配布された仮想 IP アドレスを自分自身の IP アドレスと認識し，仮想 IP アドレスに基づいて通信を行う．実際の通信は，仮想 IP アドレスに基づくパケットを実 IP アドレスでカプセル化して送信する．

図 2.1 に NTMobile の概要を示す．NTMobile は，NTMobile を実装した端末（NTM 端末），NTM 端末の仮想 IP アドレス管理及び NTM 端末に対してトンネル経路指示を出す DC(Direction Coordinator)，端末同士の直接通信が行えない場合にパケットを中継する装置 RS（Relay Server）によって構成される．DC や RS はグローバルネットワーク上に設置し，ネットワークの規模に応じて複数設置することが可能である．

NTM 端末は実ネットワークから配布された実 IP アドレスと DC から一意的に割り当てられる仮想 IP アドレスの 2 種類のアドレスを持っている．NTM 端末のアプリケーションは仮想 IP アドレスを用いて通信セッションを確立する．また，DC からのトンネル構築指示に従い，エンドエンドの通信の場合は直接トンネル構築を行う．両端末が NAT 配下に存在しエンドエンド通信が行えない場合は，RS を経由してトンネル構築を行う．

DC は NTM 端末の位置情報を管理し，NTM 端末に対して FQDN，NodeID，及び自らのアドレス領域空間から重複が起きないように仮想 IP アドレスを配布する．また，DC は DNS の機能を包含しており，それによって，通信相手端末を検索する．

RS は NTM 端末が異なる NAT 配下に存在する場合または NTM 端末と一般端末（GN）との通信を行う場合にパケットを中継する装置である．後者の RS は RS-N（Relay Server type NAT）と呼び，アドレス変換機能を持っている．以下は本提案に関連する RS-N の動作を示す．

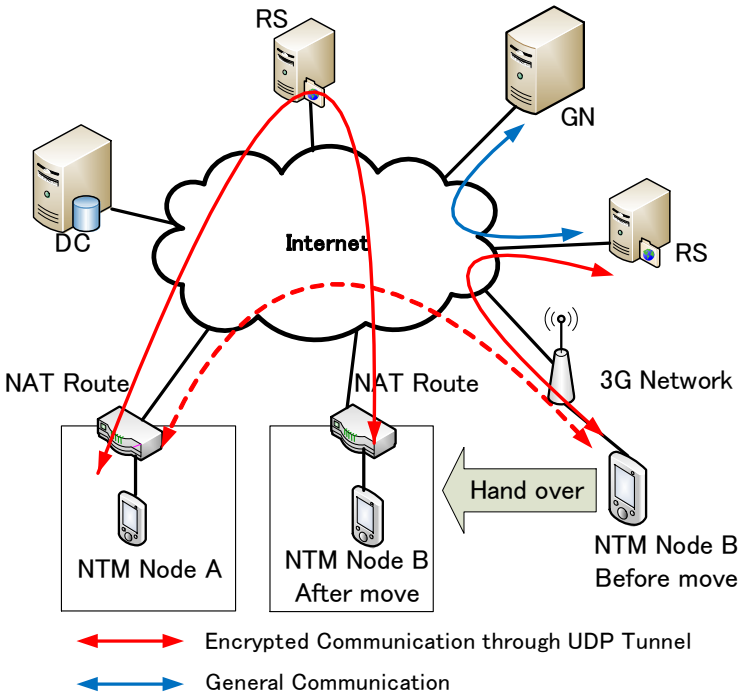

図 2.1　NTMobile の概要

2.2　一般端末と NTM 端末との通信動作

以後の説明では，通信開始側の NTM 端末を MN(Mobile Node)，通信相手側の一般端末 (NTMobile 機能を実装していない) を GN(General Node)，MN を管理する DC を DC_{MN}，GN の FQDN と IP アドレスの関係を管理する DNS サーバを DNS_{GN} とする．また，NTM 端末 MN の実 IP アドレスを RIP_{MN}，仮想 IP アドレスを VIP_{MN} とする．

一般端末と NTM 端末との通信は RS-N を経由する必要がある．RS-N は，アドレス変換型 RS である．RS-N は NTM 端末と一般端末または一般サーバとの間でパケットのカプセル化/デカプセル化，及び仮想 IP アドレスと実 IP アドレスの変換処理を行う．

2.2.1　端末起動時の処理

NTM 端末 MN を起動し，ネットワークに接続する時，自身の FQDN，実 IP アドレス RIP_{MN}，などの端末情報を DC_{MN} に登録する．DC_{MN} は自身のデータベースに MN の端末情報を登録するとともに，MN に対して，仮想 IP アドレス VIP_{MN} を割り当てる．GN 側の FQDN と IP アドレスの関係は DNS_{GN} に登録済みであるものとする．

2.2.2　通信開始時の処理

図 2.2 に NTM 端末 MN と一般端末 GN の通信シーケンスを示す．MN は GN の端末情報を得るため，DC_{MN} に対して，NTM Direction Request を送信し，GN の名前解決とトンネル構築を依頼する．NTM Direction Request を受信した DC_{MN} は DNS の仕組みによって，DNS_{GN} の NS レコードを取得する．DC_{MN} は DNS クエリによって，DNS_{GN} へ TXT レコードの問い合わせを行う．DNS_{GN}

は一般の DNS サーバであるため，TXT コードに応答していない．そこで，DC_{MN} は相手端末が GN であると判断し，DNS_{GN} に対して A/AAAA レコードを送信し，GN のアドレス情報を取得する．DC_{MN} は取得したアドレス情報を載せた NTM Relay Direction を RS-N に送信し，中継指示を行う．DC は NTM Relay Response を受信すると，MN に対して経路指示 NTM Route Direction を送付する．MN はこの指示に従い，MN と RS-N の間でトンネル構築処理を行う．また，MN は GN の仮想 IP アドレス VIP_{GN} を取得し，アプリケーションでは VIP_{GN} を GN の IP アドレスとして認識する．

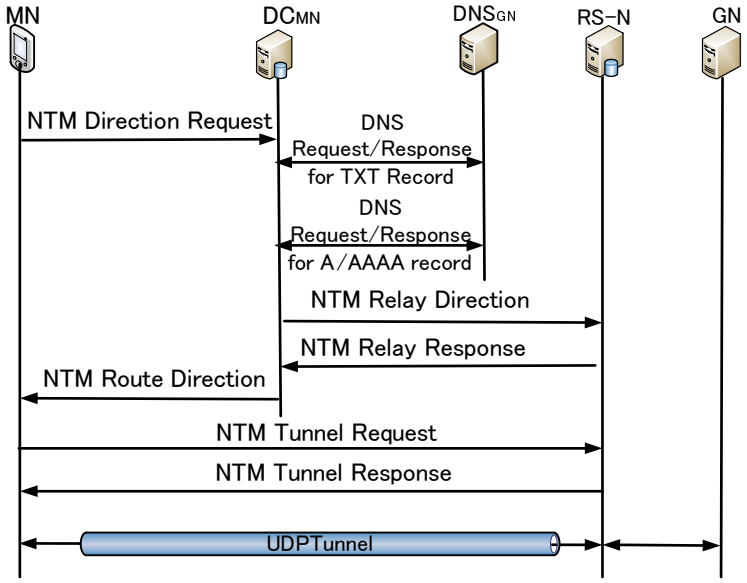

図 2.2　RS-N を経由した通信におけるシーケンス

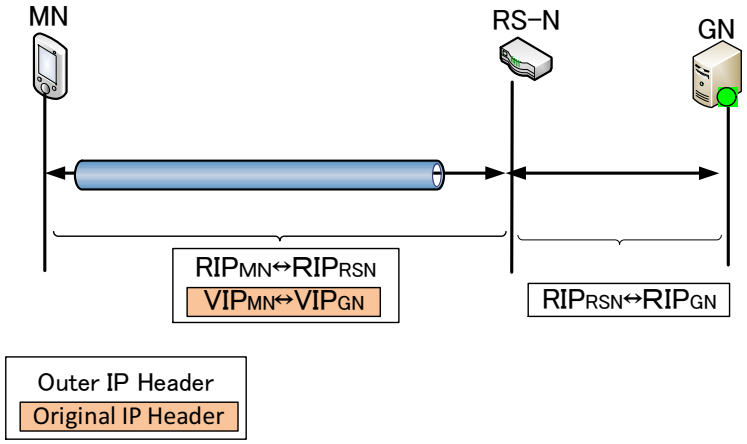

図 2.3　RS-N を用いたトンネル通信におけるアドレス遷移

図 2.3 にトンネル通信のアドレス遷移を示す．MN のアプリケーションで生成された仮想 IP アドレス VIP_{GN} に基づくパケットを実 IP アドレスでカプセル化し，RS-N に送信する．RS-N は受け

取ったパケットをデカプセル化し，元のパケットを取り出し，仮想 IP アドレスを実 IP アドレスに変換する．その後，RS-N はアドレス変換したパケットを GN に送信する．また，GN は RS-N にパケットを送信する場合にも同様である．RS-N は宛先と送信元の両方のアドレスを変換する点が一般 NAT 動作とは異なる．GN は RS-N から返信が開始されたものと認識する．MN が移動して実 IP アドレスが変化しても，GN はそのことに気付かず，返信は継続される．

2.2.3 課題

NTM 端末と一般端末との通信は RS-N を中継して通信を行うことにより，NTM 端末が移動しても移動透過性を実現できる．しかし，この方式では，一般端末がグローバル空間に設置されている必要がある．本論文の目的は外出していても，自宅や社内のサーバにアクセスを可能にすることであり，このままでは要求を満たすことができない．次章において，組織内又は家庭内のサーバにアクセスを可能な手法について述べる．

第3章　提案方式

3.1　ネットワーク構成と前提条件

図 3.1 に提案方式のネットワーク構成図を示す．提案方式ではグローバルネットワーク側の端末から NAT 配下に存在するプライベートサーバにアクセスを可能にするため，NTMobile 機能を実装した中継装置 PRS(Private Relay Server) を新たに提案する．PS（Private Server）は組織内又は家庭内の一般サーバで，NAT 配下のプライベートアドレス空間内に設置されている．PRS はプライベート空間に設置し，PS に代わって NTMobile の機能を代行する装置である．CL はプライベートアドレス空間内に存在し，PS を利用している一般端末のクライアント端末である．

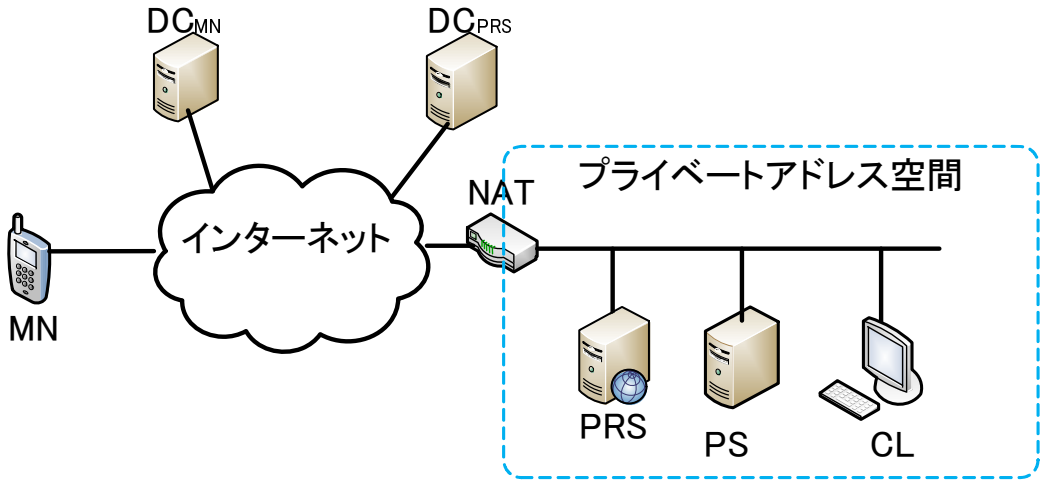

図 3.1　提案方式のネットワーク構成図

MN は NTM 端末である．PRS は NTM 端末としての機能とパケットを中継する機能を合わせ持つ．MN と PRS は起動時，それぞれの DC に対して，実 IP アドレスと FQDN などの端末情報を登録し，DC から仮想 IP アドレス VIP_{MN}，VIP_{PRS} を取得済みであるものとする．PS の IP アドレスは事前に PRS に登録しておく必要がある．PRS は NTM 端末の機能を包含しており，DC に対して，定期的に Keep Alive のメッセージ交換を行っている．

3.2　通信確立手順

図 3.2 に提案方式の通信シーケンスを示す．MN から PS へ通信を開始する時，MN は PRS の FQDN を指定する．DC_{MN} に対して，$FQDN_{PRS}$ を記載した NTM Direction Request を送信し，PRS の

名前解決とトンネル構築指示を依頼する．NTM Direction Request を受信した DCMN は DNS サーバの反復問い合わせることにより，DCPRS を探索する．DCMN は NTM InformationR Request/Response の交換により，PRS の登録情報を取得する．その後，DCMN は MN，PRS の端末情報に応じて適切なトンネル経路を判断し，MN，PRS に対して NTM Route Direction によって，トンネル構築指示（NTM Tunnel Request/Response）を行う．また，PRS 向けの NTM Route Direction は DCPRS を経由する．

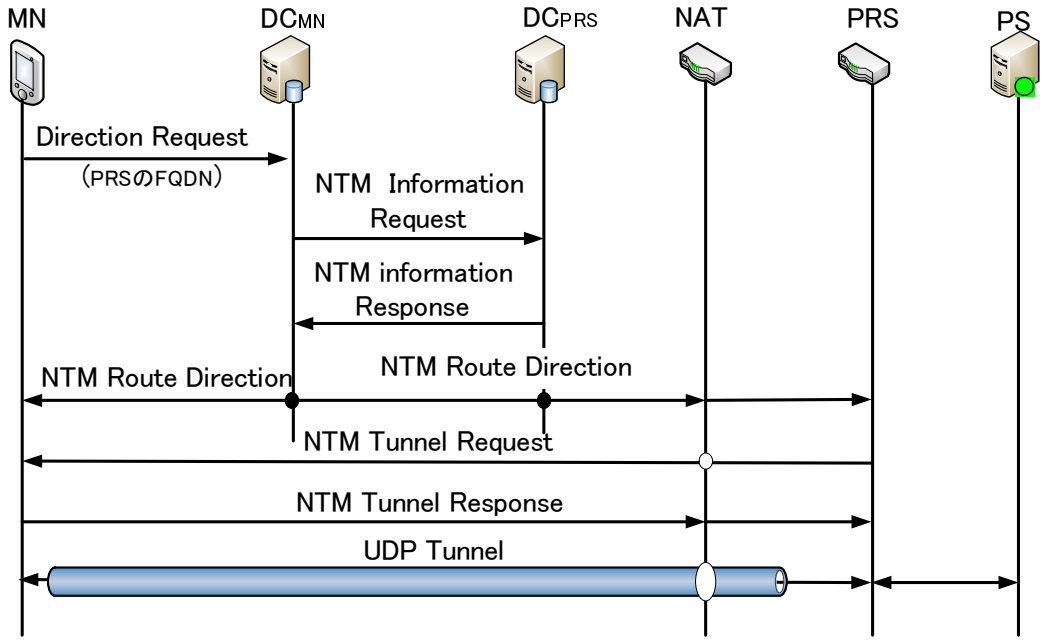

図 **3.2**　提案方式の通信シーケンス

3.3　トンネル通信処理

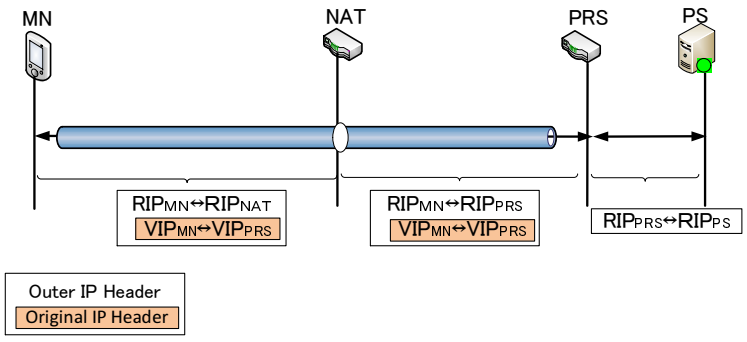

図 **3.3**　提案方式のトンネル通信におけるアドレス遷移

図 3.3 に提案方式のトンネル通信を行う様子を示す．MN と PRS の間の通信は仮想 IP アドレス

に基づいて，通信が行われる．そのため，アプリケーション上で生成されたパケットに仮想 IP アドレス VIP_{PRS} が記載されている．MN は宛先のアドレスである VIP_{PRS} を NTMobile の機能により実 IP アドレス RIP_{NAT} でカプセル化して NAT に送信する．NAT には既に経路が生成されているため，RIP_{NAT} が RIP_{PRS} に変換されて PRS に届く．PRS は受け取ったパケットをデカプセル化し，元のパケットを取り出し，仮想 IP アドレスを実 IP アドレスに変換する．その後，PRS はアドレス変換した通常パケットを PS に送信する．PS は PRS からのアクセスに見えるので，PS と CL の返信には一切影響を与えない．

第4章　実装の検討

4.1　PRS のモジュール構成

提案方式の実装について説明する．図 4.1 は PRS のモジュール構成を示す．

PRS は NTMobile の機能を持つため，モジュール構成は NTMobile 端末と同じく，ユーザ空間動作する NTMobile Daemon とカーネル空間で動作する NTMobile Kernel Module で構成される．但し，PRS はパケットを中継する機能を持っているため，アプリケーションで TCP/UDP 中継モジュール (ソケット通信プログラム) を追加する．さらに，PS の IP アドレスを指定するため，PRS で設定モジュールを追加した（追加したものは赤い点線で表す）．なお，一般アプリケーションが IP データグラムの IP アドレスとして仮想アドレスを利用できるように，仮想インターフェースを割り当てる．次は NTMobile デーモン，NTM カーネル，TCP/UDP 中継モジュールについて説明する．

NTMobile デーモンは DC への NTM 端末情報の登録と仮想 IP のアドレスの取得及び DC からの指示に従ったトンネル構築を行う．

NTM カーネルはトンネルテーブルの情報に応じて，パケットのカプセル化/デカプセル化処理又は暗号化及び復号の処理を行う．

TCP/UDP 中継モジュールは UDP と TCP のソケット通信をアプリケーション上で実装し，パケットを PRS 経由して仮想 IP アドレスを実 IP アドレスに変換し，PS に転送する通信プログラムである．

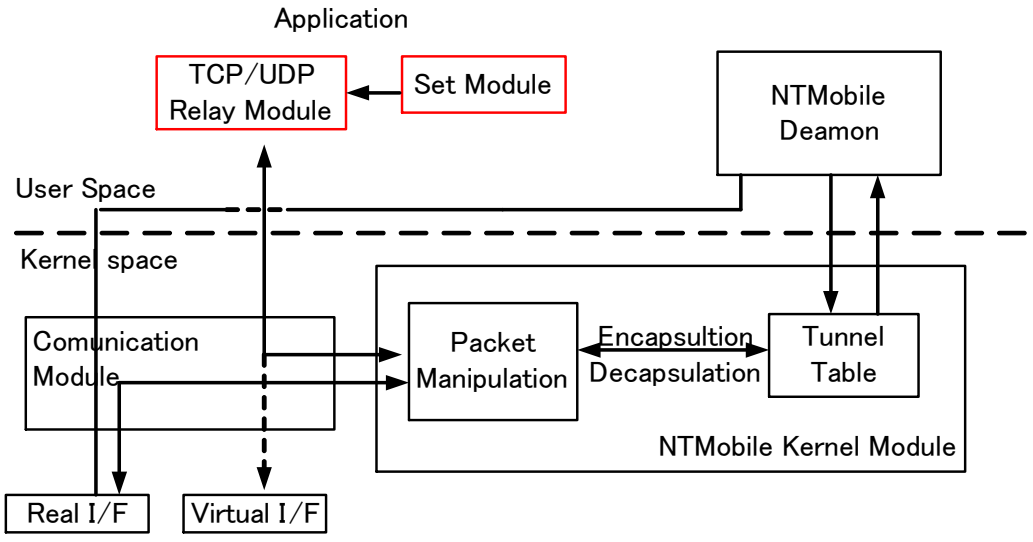

図 **4.1**　提案方式のモジュール構成図

4.2　試作結果

中継装置 PRS に TCP/UDP モジュール（TCP と UDP のソケット通信）を追加して，同じネットワーク環境にいる一般端末（MN，PS）をそれで中継して通信できることを確認した．図 4.2 にソケット通信の試験環境を示す．MN，PS は一般端末であり，PRS は両端末通信時のパケット中継装置である．PRS では UDP の送信と受信，TCP のサーバとクライアントをそれぞれ 1 つのプログラムにした．

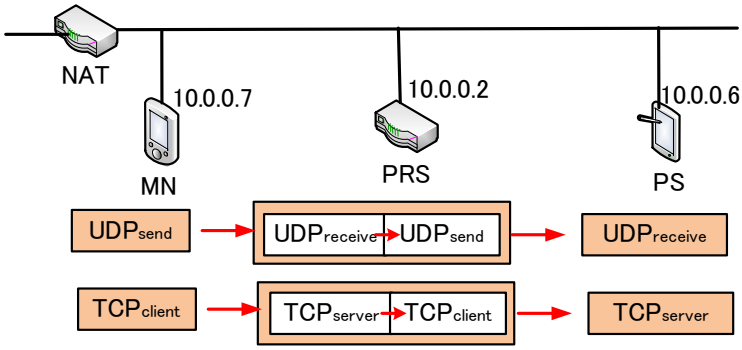

図 **4.2**　ソケット通信試験環境

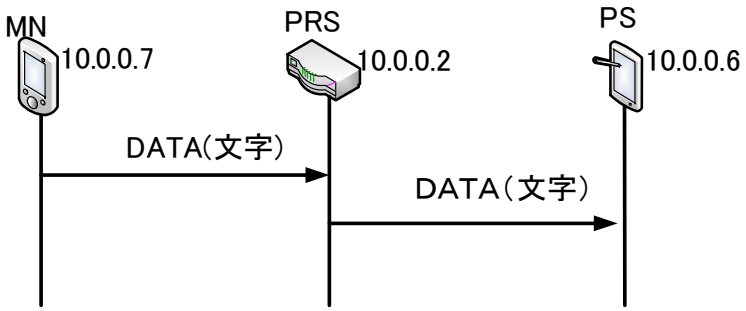

図 **4.3**　**UDP** における通信シーケンス

図 4.3 は UDP 通信において MN から PS にパケットを送信する時のパケットに基づいて通信を行う UDP 通信シーケンスである．MN から飛ばしたパケット (例としてデータ「a」という文字を送る) を PRS に受け取った．PRS は受け取ったパケット（a）を PS に転送される．これによって，パケット中継装置 PRS を経由して通信の接続はできたと考えられる．

図 4.4 は TCP 通信において MN から PS にパケットを送信する時のパケットに基づいて通信を行う TCP 通信シーケンスである．MN が PRS に SYN パケットを送り，接続オープンする．SYN パケットを受け取った PRS が MN に SYN/ACK フラグをセットしたパケットを返信し，MN が PRS に ACK パケットを送ることで通信接続を確立する．また PRS と PS の間でも同じく TCP 通信の接続を確立し，その後，PRS から MN に対して，PS との通信確立できたというメッセージを MN に送って，MN からメッセージを受け取った後，PS に向けって、パケット（例として文字 a）を送

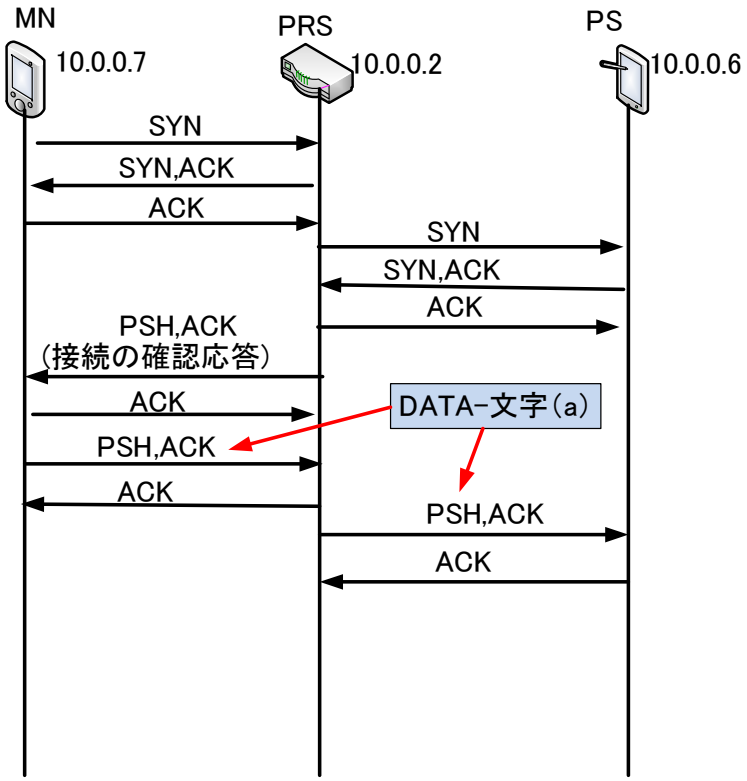

図 **4.4**　**TCP** における通信シーケンス

り出す．PRS は MN から受け取ったパケットを PSH，ACK フラグによって PS に転送する．これによって TCP の場合でも PRS を経由して通信できるのを確認した．

理論上は上記のパケット中継装置 PRS と端末 MN に NTMobile 機能を実装し，さらに MN を NAT の外側に設置し，PRS，PS を NAT の配下に設置すると，MN と PRS の間は NTMobile 技術を用いて，トンネル通信を行い，PRS と PS の間は上記のソケット通信に基づいて通信を行うため，MN から PS との通信は継続できると想定されている．

第5章　まとめ

本論文では，通信接続性と移動透過性を実現できる NTMobile を拡張し，プライベート空間内の一般サーバに NTMobile 用プライベート中継装置 PRS を設置することにより，外部からのアクセス及び通信の移動を実現できる手法を提案した．提案方式では PRS をサーバの代わりに，NTMobile の機能とパケット中継する機能を実行することで実現できる．

今後は提案方式の実装完了し，評価を行う予定である．

謝辞

本研究にあたり，多大なるご指導とご教授を賜りました，渡邊晃教授に心から感謝いたします．

また，本研究を進めるにあたり，御意見ならびに御助言を受け賜りました，名城大学理工学研究科　鈴木秀和助教，愛知工業大学情報科学部情報科学科　内藤克浩准教授に心より感謝致します．最後に，本研究を進めるにあたり，数々の有益な御助言を賜りました，渡邊研究室および鈴木研究室の諸氏に感謝します．

参考文献

[1] 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.1-13(Jan.2013).

[2] 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，Jan.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，Oct.2013.

[4] 廣瀬達也，鈴木秀和，内藤克浩，渡邊晃:NTMobile を用いたネットワークモビリティの提案，情報処理学会研究報告，2013-MBL-69(8)，pp.1-5，Dec.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，2013-MBL-67(10)，pp.1-8，Sep.2013.

[6] 納堂博史，鈴木秀和，内藤克浩，渡邊晃:NTMobile における自律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，Jan.2013.

研究業績

研究会・大会等（査読なし）

（1）李丹薇，廣瀬達也，鈴木秀和，内藤克浩，渡邊晃：プライベート空間のサーバにアクセスが可能なアダプタ型 NTMobile 装置の提案，平成 26 年度電気・電子・情報関係学会東海支部連合大会論文集，Sep.2014.