

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

100430127 李丹薇
渡邊研究室

1. はじめに

現状の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) [1] 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 を実装することにより、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一切許可されない。そこで、本稿では、サーバの横に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。

2. NTMobile の概要

NTMobile は NTMobile を実装した端末 (NTM 端末)、NTM 端末のアドレス管理及びトンネル経路指示を行う DC (Direction Coordinator)、エンドエンドの通信が行えない場合にパケットを中継する 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できる。NTM 端末は起動する時 DC に対して実 IP アドレス登録処理を行い、DC 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る。通信開始時アプリケーションで生成された仮想 IP アドレスに基づいて通信を行う。また、実際の通信では、実 IP アドレスで全てのパケットをカプセル化し、トンネル通信を行う。端末が移動して実 IP アドレスが変化しても、仮想アドレスは変化しないため、通信の継続が可能である。

3. 実現済みの技術とその課題

NTM 端末が一般サーバと通信を行う場合、NTMobile を用いた通信を行えないため、NTM 端末は RS-N (Relay Server type NAT) [2] との間に UDP トンネルを構築する方法が提案され、すでに実現済みである。RS-N は NTM 端末と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。一般サーバは通信相手が RS-N であるものとして認識する。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、一般サーバがグローバル空間に設置されている必要があった。

4. 提案方式

プライベート空間に設置される一般サーバの横に NTMobile 用プライベート中継装置 PRS (Private Relay Server) を設置し、グローバル環境にいる NTM 端末 MN (Mobile Node) からのアクセスを可能とする。

図 1 に提案方式の通信シーケンス及びアドレス遷移を示す。MN は NTM 端末である。PRS は NTM 端末として

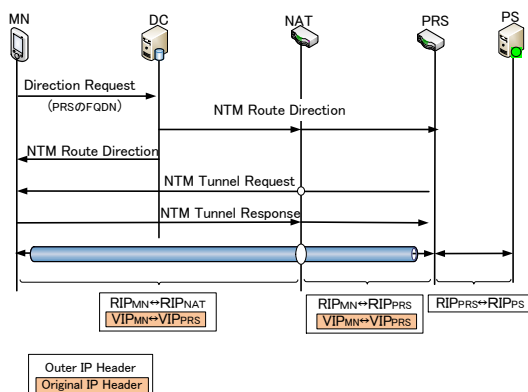


図 1: 通信シーケンス及びアドレス遷移

の機能とパケットの中継機能を合わせ持つ。MN との PRS の実 IP アドレスは DC に登録してあり、仮想 IP アドレスを取得済みであるものとする。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 PS の横に設置し、PS に代わって NTMobile の機能を代行する装置である。

PS の IP アドレスは事前に PRS に登録しておく必要がある。MN から PS へ通信を開始する時、MN は PRS の FQDN を指定して、DC に経路要求 (Direction Request) を行う。DC は MN と PRS に対して経路指示 (NTM Route Direction) を送信する。これを受け取った MN と PRS の間でトンネルを構築する (NTM Tunnel Request/Response)。トンネル構築後の通信において、PRS は MN から受け取った NTM パケットを通常のパケットに戻して PS に転送する。また PS から受信した通常のパケットを NTM パケットに変換して、MN に転送する。この方法により、MN は PS にアクセスがすることができ、かつ NTM 端末が移動しても、通信を継続することができる。

5. まとめ

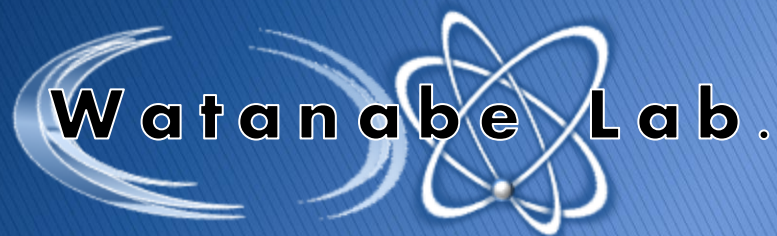
本稿では、プライベート空間内の一般サーバに NTMobile 用プライベート中継装置を設置し、外部からのアクセス及び通信の移動を実現できる手法を提案した。今後、提案方式の実装方法を含めて、評価を進める予定である。

参考文献

- [1] 鈴木秀和, 他: 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] 土井敏樹, 他: 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 Vol.2013-MBL-67, NO.11.

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

理工学部 情報工学科
渡邊研究室
100430127 李丹薇



研究背景

◆ NAT越え問題が発生している

- IPv4ネットワークではNATの利用が一般
- 相手端末がNAT配下に存在すると、インターネット側から通信の開始できない

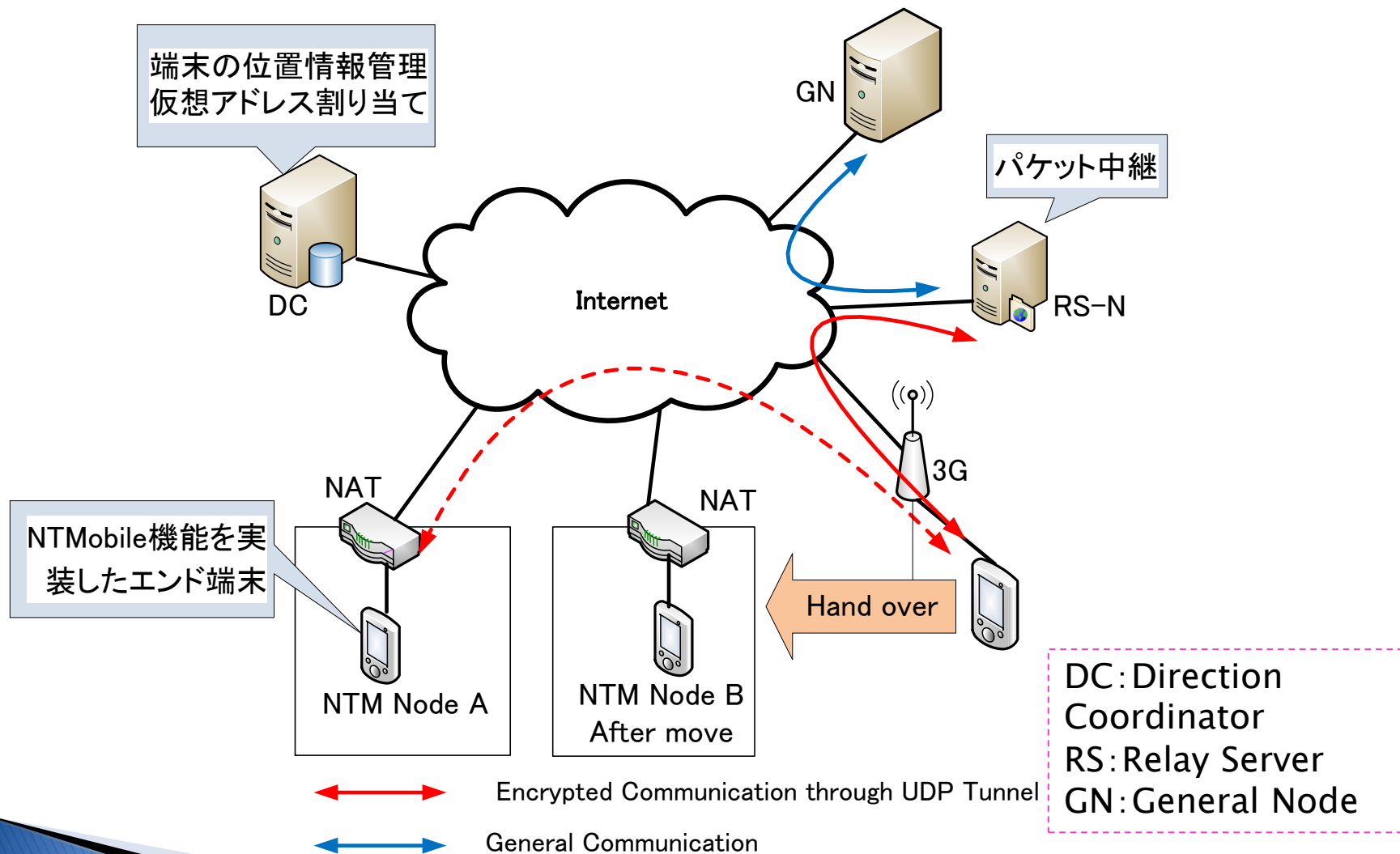
◆ 移動透過性技術が必要

- 公共無線網や携帯端末の発達により移動しながら通信したい要求が増えた
- IPアドレスが通信識別子
- 通信中にIPアドレスが変化すると、通信継続できない



NTMobile(Network Traversal with Mobility)

NTMobileの構成



NTMobileの概要

- ▶ NAT越えと移動透過性を同時に実現
⇒ **NTMobile**(Network Traversal with Mobility)

- ▶ 特徴

- 仮想アドレスの導入
 - 端末に位置に依存しない仮想アドレスを割り当て
- UDPトンネルを利用して通信
 - 実IPアドレスでパケットをカプセル化

研究目的

クライアントとサーバにNTMobileを実装することにより、外部からプライベート空間のサーバにアクセスが可能

問題

一般サーバに手を加えることが許可されない場合がある

➤ 目的

NTMobile用プライベート中継装置の開発

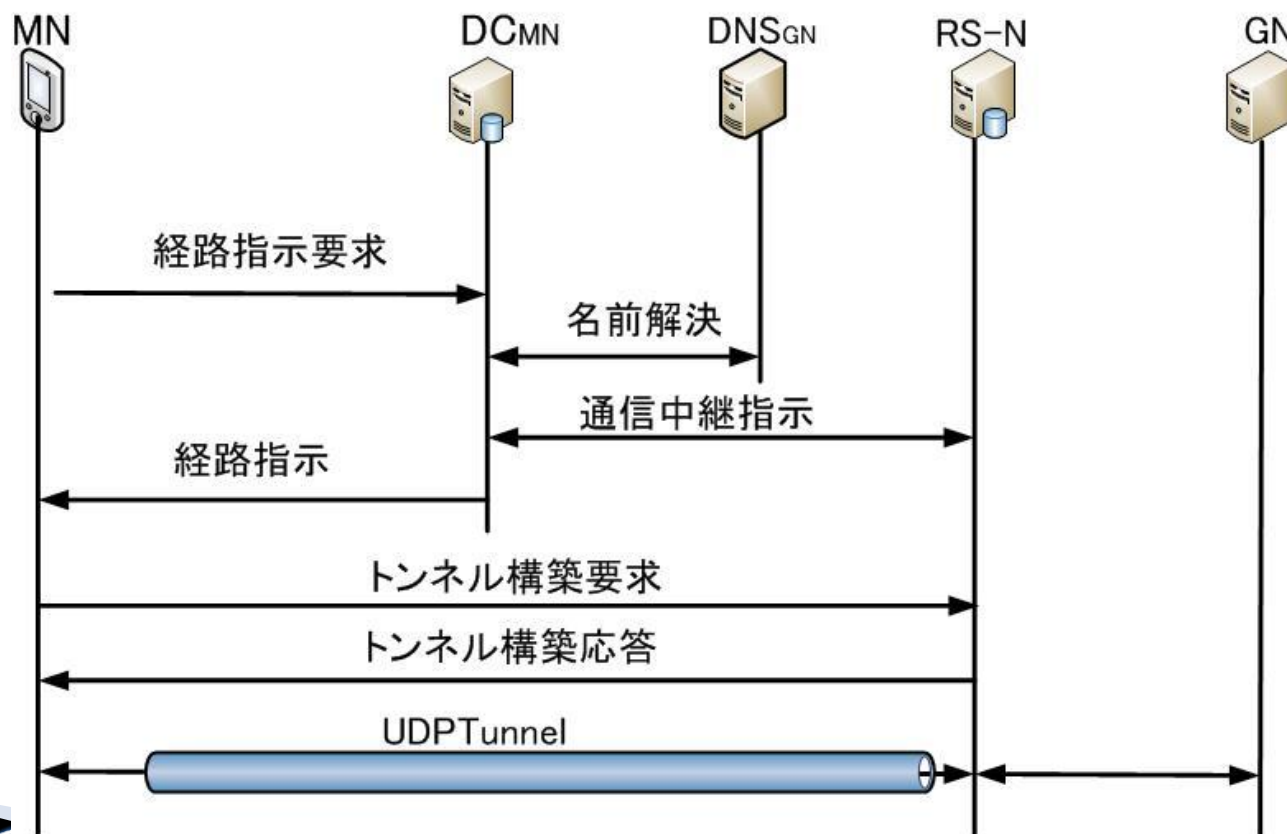
外部からプライベート空間内にアクセスを可能



サーバ横に中継装置を置く

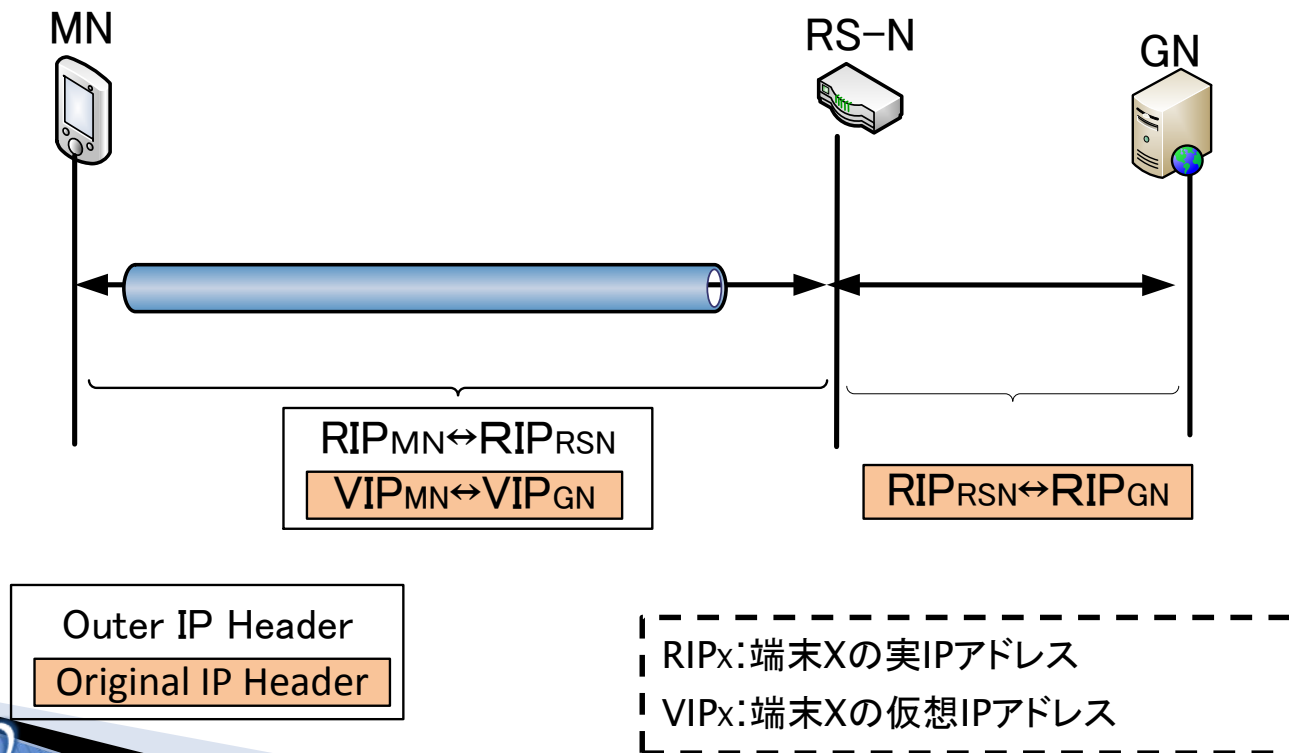
RS-Nを利用した通信シーケンス

- ▶ MNはNTM端末、GNは一般端末
- ▶ MNはアドレス登録済とする



トンネル通信

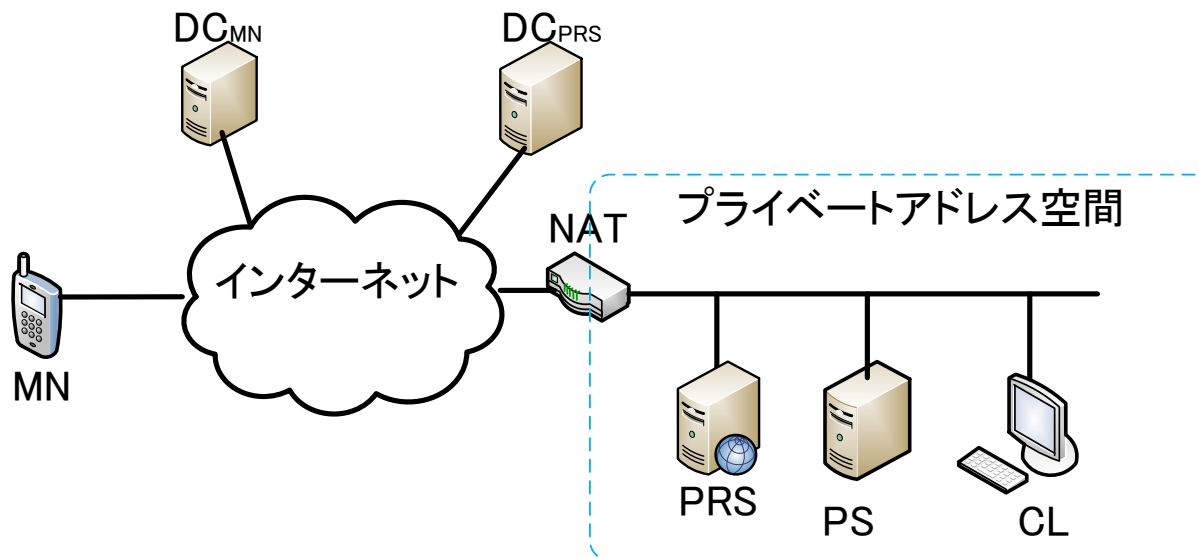
- ▶ トンネル構築後のアドレス遷移
 - GNは通信相手をRS-Nと認識する
 - 仮にGNがプライベート空間に設置されると、RS-NとGNの間にNATが必要となる



提案方式

プライベート中継用NTMobile装置PRS (Private Relay Server)の導入

- ▶ インターネット側の端末からプライベート空間内の一般サーバにアクセスを可能にする

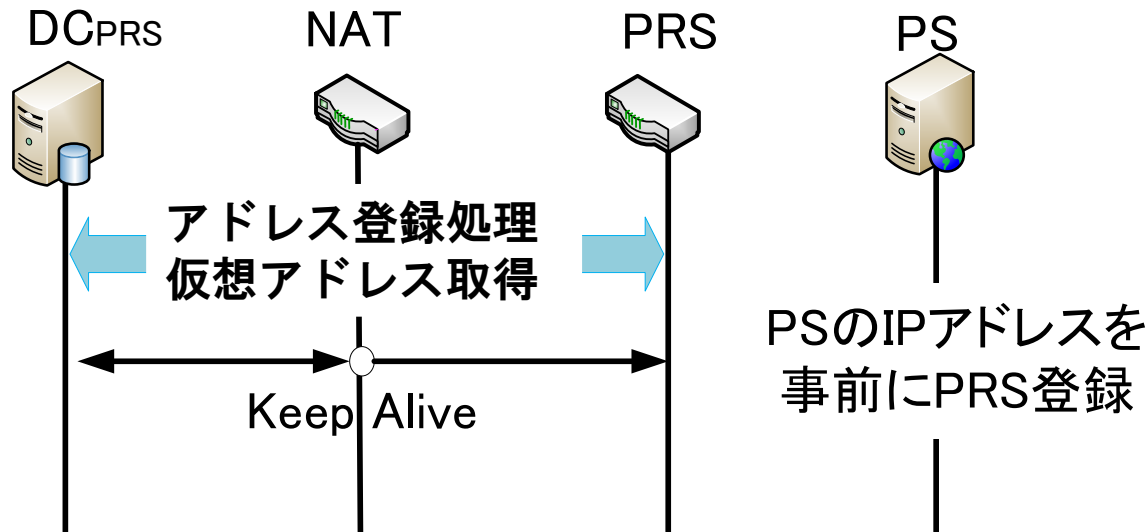


PS (Private server): 組織内や家庭内の一般サーバ

CL: PSを利用している一般のクライアント端末

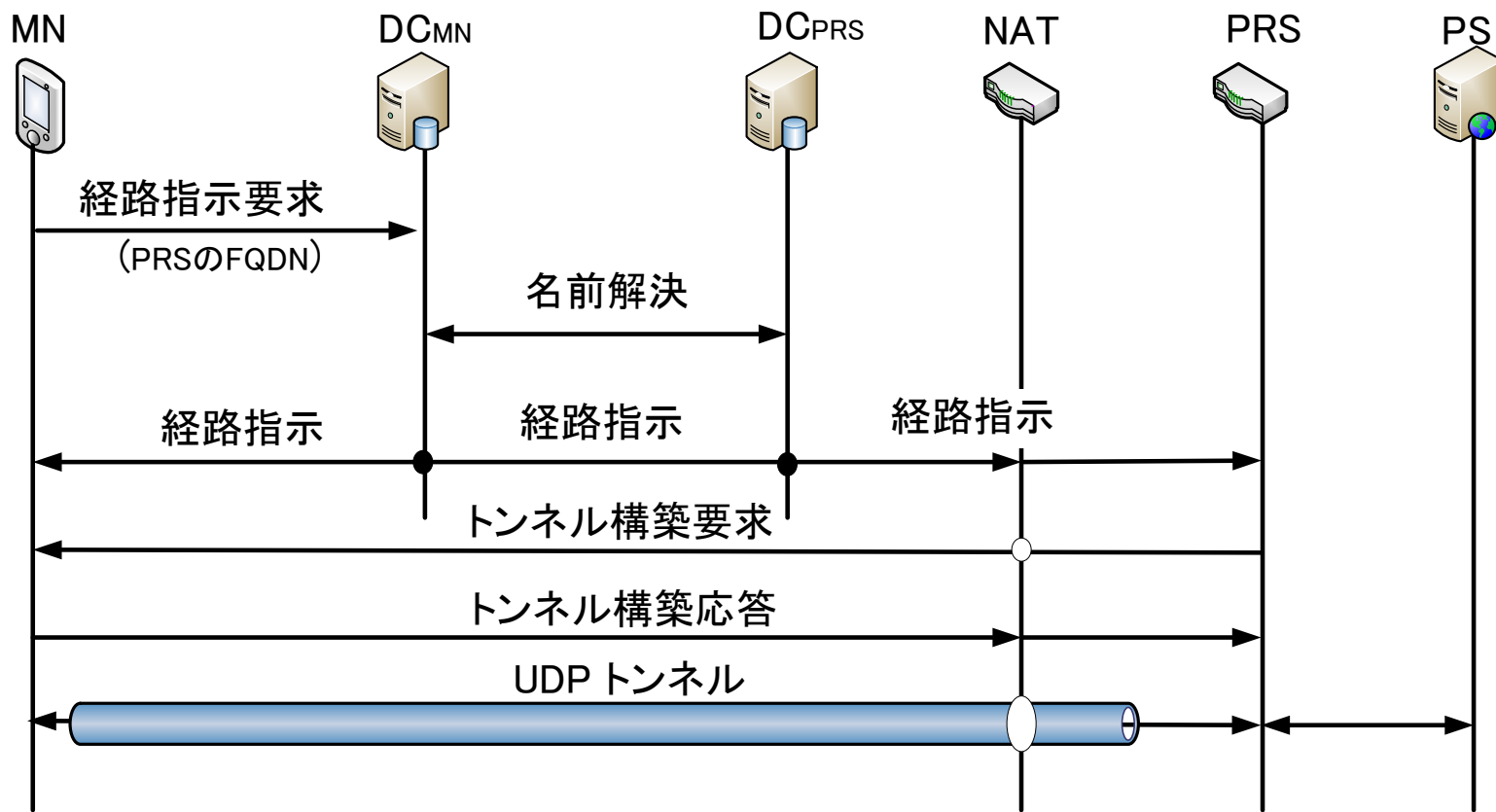
提案方式の通信シーケンス(アドレス取得時)

- PRSはPSに代わって、NTMobileの機能を代行する装置
- PSのIPアドレスは事前にPRSに登録
- PRSはDCとの間でKeep Alive



提案方式の通信シーケンス

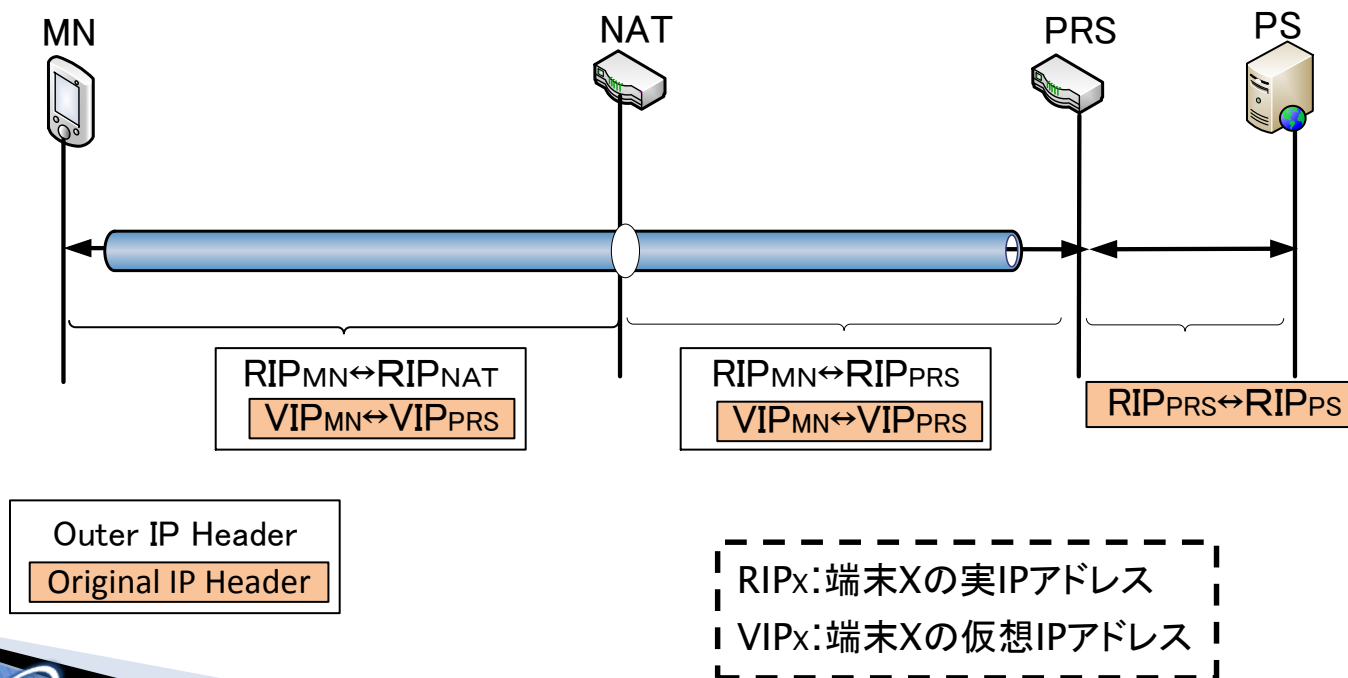
- ▶ MNはPRSのFQDNを指定して通信開始



提案方式のトンネル処理

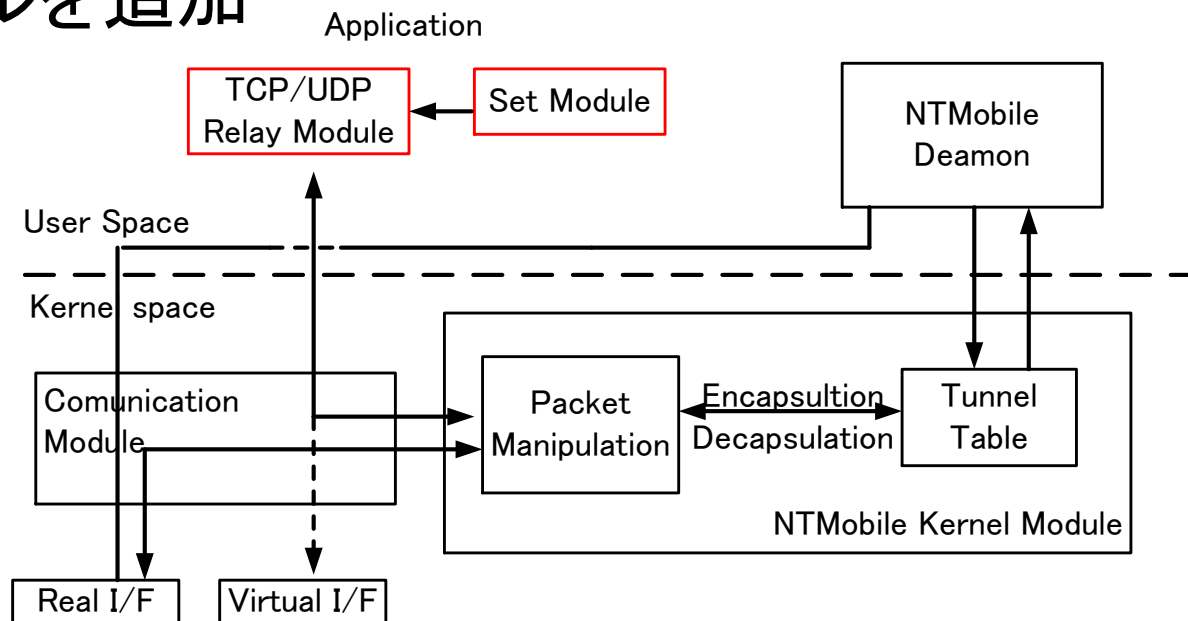
▶ トンネル構築後の通信

- MNは仮想IPアドレスを実IPアドレスでカプセル化し、NATに送信
- PRSはアドレス変換したパケットをPSに送信する



PRS実装方法

- ▶ アプリケーション上でTCP/UDP中継モジュールを追加
- ▶ PSのIPアドレスを事前に登録するため、設定モジュールを追加



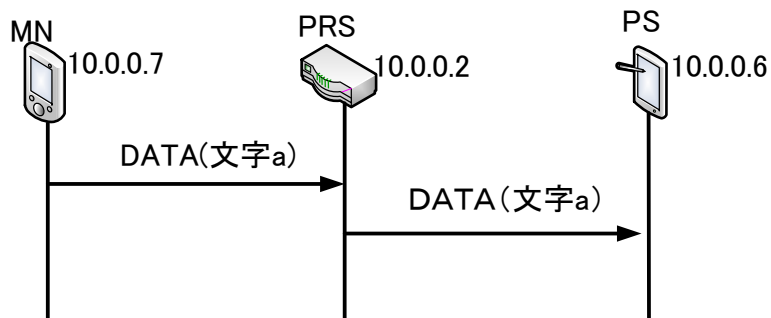
NTMデーモン: アドレスの確認とトンネル構築処理

NTMカーネル: トンネルテーブルに従って、パケットのカプセル化/デカプセル化及び暗号処理

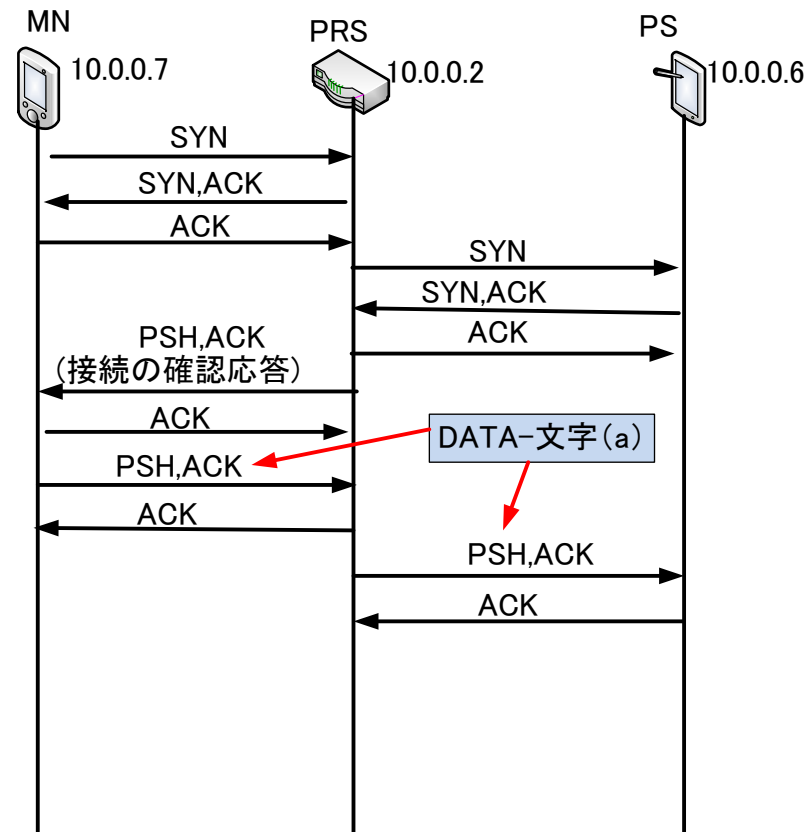
試作結果

- ▶ **TCP/UDPモジュール**で通信できるかを検証済み

UDPの場合通信シーケンス



TCPの場合通信シーケンス



まとめ

- NTMobile概要の説明
- プライベート空間内の一般サーバにアクセスを可能にする提案方式
 - PRS中継装置を導入
- 実装方法
- 今後の予定
 - 提案方式の実装設定と評価

ご清聴ありがとうございました