6T-07

VPNServiceを利用した移動透過性の実現方式の提案

黒宮 魁人 [†1]　清水 一輝 [†2]　鈴木 秀和 [†2]　内藤 克浩 [†3]　渡邊 晃 [†2]
[†1] 名城大学理工学部　[†2] 名城大学大学院理工学研究科　[†3] 愛知工業大学情報科学部

1　はじめに

スマートデバイスの爆発的な普及によってモバイルデータトラフィックの逼迫が問題になっている．そのためモバイルネットワークに流れるデータをWi-Fiを用いて固定回線にオフロードすることが望まれる．しかし異なる事業者間でデータオフロードを行うとIPアドレスが変化するため通信を継続できない．この課題を解決できる有力な手段の一つとして通信データのカプセル化がある[1]．スマートデバイスにパケットのカプセル化を提供する技術としてVPNServiceがある．VPNServiceはもともとVPN通信を行うための技術であり，移動透過性の実現を主目的としたものではないが，この技術を用いることにより移動透過性を容易に実現できる．本稿では，NAT越え技術と移動透過性を同時に実現するNTMobileをVPNService上で実現し，中でも移動透過性に係る処理をどのように実現すべきかを検討したので報告する．

2　カプセル化通信の有用性とNTMobile

2.1　カプセル化の有用性

IPアドレスを利用した通信ではIPアドレスが通信識別子としての役割と位置識別子としての2つの役割を持っている．そのため，移動してIPアドレスが変化すると通信識別子が変わるため通信が途切れるという課題がある．カプセル化技術を利用すると通信識別子と位置識別子をそれぞれ別のIPアドレスに担わせることができる．パケットを送信する際には通信識別子として機能するIPアドレスで作成したパケットをそのままIPデータとみなし，位置識別子として機能するIPアドレスをヘッダにした新たなパケットを作成する．アプリケーションは通信識別子として機能するIPアドレスを利用して通信を行うため，位置識別子として利用されるIPアドレスが変化しても影響を受けない．

2.2　NTMobile

NTMobileはNAT越え通信と移動透過性を同時に実現する技術である．NTMobileを実装した端末は，NAT

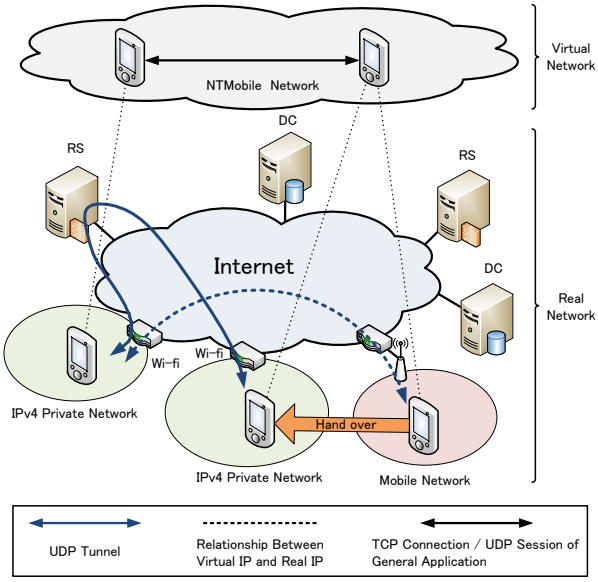

図1　NTMobileの構成図

の有無に関係なく双方向の通信開始が可能で，かつ通信中に移動しても通信を継続できる．図1にNTMobileの構成図を示す．NTMobileは移動によって変化しない仮想IPアドレスが定義されており，通信識別子として用いている．仮想IPアドレスはDC（Direction Coordinator）から重複しないように割り振られる．DCはアドレスの配布の他に通信経路の指示も行なう．両端末が異なるNAT配下に存在する場合は通信の中継を行うRS（Relay Server）を経由した通信となる．NTMobileによる通信は，仮想IPアドレスに基づくパケットを全て実IPアドレスによりUDPでカプセル化する．このため，端末が移動して実IPアドレスが変化してもアプリケーションに影響を与えることなく，新たなトンネル経路で通信を継続することができる．

3　VPN技術とVPNService

VPN技術は端末がパケットのカプセル化を行うことにより，異なるアドレス空間を経由した相互通信を可能とする技術である．VPNを利用した通信で使用されるパケットは基本的にカプセル化を行う際に全て暗号化され，拠点間の接続やリモートアクセスなどのセキュアな通信を行うために用いられることが多い．

多くのVPN技術では，TUNと呼ばれる仮想インタフェースを作成してカプセル化に利用するが，インタ

Proposal of realization method of IP Mobility using VPNService
Kaito Kuromiya[†1], Kazuki Shimizu[†2], Hidekazu Suzuki[†2], Katsuhiro Naito[†3] and Akira Watanabe[†2]
[†1] Faculty of Science and Technology, Meijo University
[†2] Graduate School of Science and Technology, Meijo University [†3] Department of Information Science, Aichi Institute of Technology

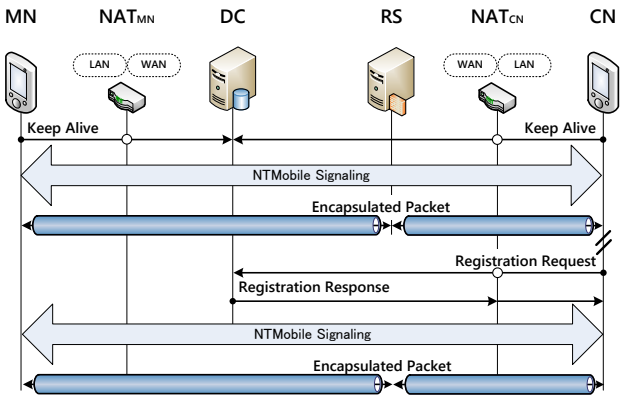

図 2　移動処理を含めたシーケンス図

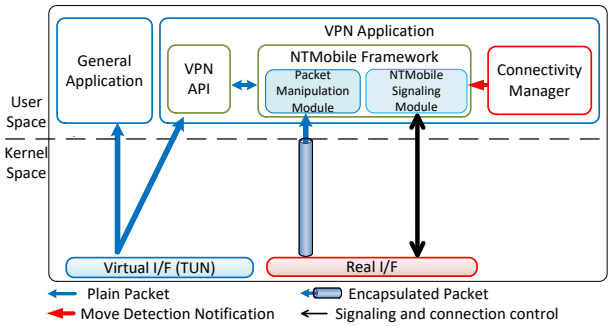

図 3　VPN アプリのモジュール図

フェースを端末に追加するためには root 権限が必要となる．スマートデバイスが提供する VPNService はモバイルアプリケーション開発者向けに root 化せずに VPN 通信を提供するための API として Android4.0 以上の端末で提供されている．VPNService を利用することで仮想インタフェースの作成や仮想インタフェースに届いたパケットをそのまま取得することが可能となるため，独自の VPN を利用した通信を行うアプリケーションが作成できる．

4　Android における NTMobile の実現方式

4.1　実現の経緯

VPNService の特徴に注目し，我々は NTMobile を VPNService 上で実現する方法を検討してきた [2]．NTMobile を実現するライブラリ（NTMfw）は C で記述されており，様々な OS にそのまま移植できる．Android においても VPN アプリとして移植を終え，一般アプリケーションの通信に NAT 越えなどの NTMobile の機能を一部を実現できることを確認した．しかし移動透過性の実現においては，移動を検出する適切な方法がなく実現できていなかった．理由は OS ごとに NIC の名称が異なっていたり，スマートデバイス特有のインタフェースが存在することから，アドレス変化を異なる OS で共通に検出することが難しいためである．

4.2　NTMobile の移動通信シーケンス

図 2 に移動に係る NTMobile の通信シーケンスを示す．MN(Mobile Node) と CN(Correspondent Node) は立ち上げ時に DC に実 IP アドレスを登録後，仮想 IP アドレスを取得する.Keep Alive は DC に定期的に送信するパケットであり，端末が NAT 配下に存在していても DC から通信経路の指示を受けることができる．通信開始時に MN/DC/RS/CN がシグナリング処理を行うことにより MN-CN 間に UDP トンネルが構築される．図 2 では両端末が NAT 配下であるため，RS を経由したトンネル経路となる．通信の途中で CN の IP アドレスが変化した際には，まず次の通信の受信に備え，DC に新しい IP アドレスを登録する（Registration）．続いて通信開始時と同じシグナリング処理を行うことでトンネル経路を再生成する．これによりユーザアプリケーションはトンネル経路の変化に気づくことなく通信を継続できる．

4.3　Android におけるアドレス変化検出

移動に関わるアドレス変化を確実に検出するため（図 2 に示した斜線部），Android では VPN アプリ内（Java）で実現する．図 3 に VPN アプリのモジュール構成を示す．VPN アプリは，NTMobile に関わる処理を実行する NTMfw ライブラリを内蔵し，VPNService と NTM ソケット通信を仲介する．さらにアドレス変化検出クラスを NTMfw とは独立してもつ．アドレス変化検出クラスは ConnectivityManager を使用して実現する．Android 端末のネットワーク接続状況が変化すると CONNECTIVITY_ACTION がブロードキャストされる．そのため CONNECTIVITY_ACTION を受信するためのレシーバを準備することにより，スマートデバイスのアドレス変化を検出できる．このアドレス変化をトリガとして，VPN アプリは NTMfw に新たなトンネル生成を実行させる．

5　まとめ

本稿では，VPNService 上で NTMobile を実現し，アドレス変化検出を Android 用に NTMfw から独立させることにより，移動透過性を実現する方式について提案した．今後は提案方式の実装と評価を行う予定である．

参考文献

[1] 内藤克浩ほか： NTMobile における移動透過性の実現と実装，情報学論，Vol. 54，No.1，pp.380–393 (2013).

[2] 山田貴之ほか： IPv4/IPv6 混在環境に対応した VpnService 型 NTMobile の性能評価，DICOMO2015 論文集，Vol. 2015，No.1，pp.1784–1791 (2015).