1U-02

NTMobileにおける通信制御機能の提案

金松 友哉 [†1]　大久保 陽平 [†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

筆者らはIPv4/IPv6混在環境において確実な接続性と移動透過性を実現する技術として，NTMobile（Network Traversal with Mobility）を提案している [1]. しかし，従来の仕様では，NTMobileを実装した端末（NTM端末）は無条件でNTMobileのトンネル構築処理および通信を開始する．そのため，特定の相手との通信を拒否したい場合や，NTMobileを使用せず通常の通信を行いたい場合など，ユーザが利用ケースに応じて通信方法を選択することができないという課題がある [2].

本稿では，通信時に用いられる通信相手のFQDNとユーザからの通信方法の要望をもとに，通信可否及び通信経路を選択する手法を提案する．

2　NTMobileの概要

NTMobileでは，DC（Direction Coordinator）が各NTM端末のアドレス情報を管理している．NTM端末が通信を行う際には，DCが通信ペアのアドレス情報をもとに通信経路やトンネル構築指示を行うことでトンネル通信を実現している．また，通信相手がNTMobileを搭載していない一般サーバGS（General Server）である場合やIPv4/IPv6間の通信を行う場合は，中継サーバであるRS（Relay Server）を経由した通信経路とすることにより，IPv4/IPv6間の通信やNTM端末の移動透過性を実現している．

しかし，現在のNTMobileには，図1に示すような2つの課題が存在する．1つ目は通信を開始する際に通信相手の判別を行うことなく，無条件で通信相手とトンネルを構築して通信を開始するため，悪意のある通信相手と通信を行ってしまう可能性がある．2つ目はGSと通信を行う場合，必ずRSを経由した通信を行うため，一般的な通信が可能な場合はNTMobileを使用せず直接経路で通信したい等，ユーザの利用ケースに応じた通信経路の選択ができない．

3　提案手法

図2に提案手法の概要を示す．提案手法では，NTM端末に通信相手のFQDNをもとに作成したフィルタリングルールと通信の可否を記載したACL（Access Control List）を実装する．さらに，ユーザの通信経路を選択を反映させるRouteオプションを実装する．

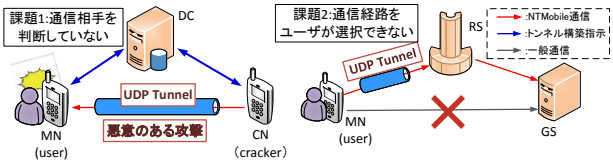

図1　既存手法における課題

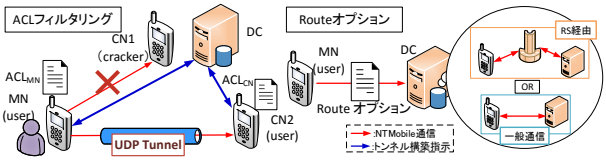

図2　提案手法のoutline

3.1　ACLフィルタリング

ACLフィルタリングとは，通信相手のFQDNを用いて自身のハッシュテーブルに登録されているルールと比較し，許可された通信相手だけにトンネル構築処理およびNTMobileを利用した暗号化通信を行い，許可されていない通信相手とは通信を拒否する機能である．通信を開始する際には，通信開始端末MN（Mobile Node）と通信相手のNTM端末CN（Correspondent Node）の双方で互いのFQDNを用いてACLフィルタリングを行い，ユーザがあらかじめ設定したルールに従って通信の可否を判断する．両端末において通信許可と判断された場合は従来のNTMobileと同様にDCの経路指示に従ってトンネル構築を行う．そのため，例えば指定した相手とだけ通信したい場合や，特定の相手とは通信したくない場合など，通信相手との通信可否が設定できる．

3.2　Routeオプション

NTM端末がGSと通信する場合，DCに送信する経路指示要求メッセージにRSを経由したNTMobile通信を行うか否かを記載したRouteオプション付与できるよう拡張する．DCはRouteオプションを確認し，RSを経由させるか否かを決定する．これにより，ユーザは使用用途に応じて通信経路を選択することができる．例えば，移動透過性をサポートした状態で通信したい場合や，IPv4/IPv6間通信を行いたい場合は，従来のNTMobileと同様にRS経由で通信をする．また，NTMobileの機能は必要とせず，低遅延，高スループットを必要とする

A Proposal of Communication Control for NTMobile
Yuya Kanematsui[†1], Yohei Okubo[†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] Faculty of Information Science, Aichi Institute of Technology

場合，RS 経由させず一般通信を行うことが可能になる．

4 実装

4.1 ACL フィルタリングの実装

ACL を NTMobile のコンフィグファイルとして実装した．ACL に記載されたルールは端末起動時に読み込まれ，ハッシュテーブルとして管理するよう実装した．フィルタリング処理は名前解決を行う際の通信相手の FQDN を用いて ACL ハッシュテーブルを検索し，検索結果によって通信可否を判断するよう実装した．通信が拒否されている場合，名前解決のエラー処理を行うことにより通信相手の IP アドレスが取得できないようにした．

通信相手が CN であった場合，CN 側で設定されている ACL のルールにも従って，経路指示に含まれる FQDN を用いてフィルタリングする．通信が許可されている場合は MN に NTM ACK を返してトンネル構築処理を継続する．拒否の場合は MN に NTM NACK を返し，MN は名前解決エラー処理を行ってトンネル構築処理を中断する．

4.2 Route オプションの実装

経路指示要求にユーザが設定した Route オプションが付与できるように，メッセージフォーマットの Flag フィールドを実装した．RS を経由しない場合，DC は MN へ GS のアドレス情報を付与した経路要求を返信する．その後，MN は NTMobile のトンネル構築処理を終了し，経路指示に付与された GS のアドレス情報に基づいて一般通信を開始する．RS を経由する場合，従来手法と同様の手順により，MN は RS を経由した NTMobile 通信を行う．

5 性能評価

プロトタイプシステムを実装して動作検証を行った結果．ACL フィルタリングと Route オプションの機能が正常に動作することを確認した．これに伴い，提案手法が通信開始時に与える影響を明らかにするために，NTM 端末に実装した ACL フィルタリングのオーバヘッド時間を計測した．測定環境および使用機器の仕様をそれぞれ図 3，表 1 に示す．MN において NTMobile を初期化する処理と CN へ通信を開始する処理を 10 回行った．なお，MN と CN は双方とも，ACL フィルタリングで通信を許可するよう設定した．また，比較のために従来手法の各処理についても同様に測定した．

図 4 に計測したオーバヘッド時間の平均値を示す．NTMobile の初期化処理においては，従来手法が 142.14ms に対し，提案手法の増分は 6.09ms であった．また，NTMobile トンネル構築は従来手法が 81.41ms であるのに対し，提案手法の増分は 3.89ms であり，提案手法のオーバヘッド時間の増分は，従来手法のオーバヘッド時間の約 4% 程と極めて小さいことがわかった．

表 1　測定機器仕様

	MN, CN	DC, RS（仮想マシン）
OS	Ubuntu14.04	CentOS6.8
Kernel	Linux3.13	Linux2.6.32
CPU	Intel CeleronN2820@2.16GHz	AMD Opteron 4180
メモリ	4GB	512MB

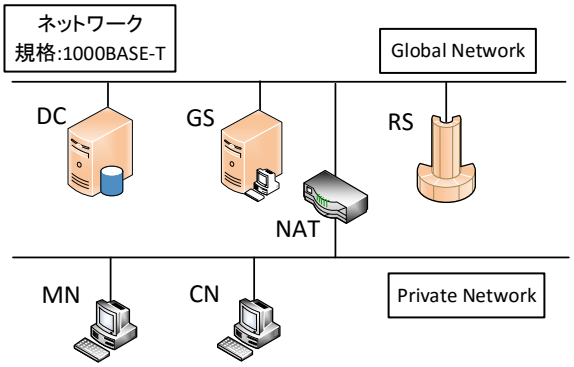

図 3　測定環境

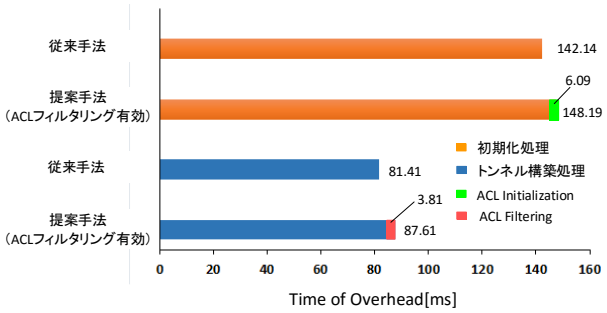

図 4　処理時間の測定結果

さらに，NTMobile のトンネル構築処理は通信開始時のみ行われる処理であるため，提案手法が NTMobile 通信に与える影響は極めて少なく，実用上問題ないと考えられる．

6 まとめ

本稿では通信相手の FQDN を用いた ACL フィルタリングと，ユーザの通信要望を反映する Route オプションを導入することにより，NTMobile における通信制御機能を実現した．提案手法の実装を行い，処理時間を計測した結果，実用上問題ないことを確認した．

参考文献

[1] 上醉尾一真ほか:情処学論, Vol.54, No.10, pp.2288–2299, (2013).
[2] 金松友哉ほか:電気・電子・情報関連学会東海支部連合大会講演論文集, Vol.2016, No.F3-6, (2016).