5ZB-05

QUICを用いたNTMobileの暗号化エンドツーエンド通信の提案

堀崎　翔太 †1　加藤　宏理 †2　鈴木　洸太 †2　鈴木　秀和 †2　内藤　克浩 †3
†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

IPv4/IPv6 混在環境において，移動透過性と通信接続性を実現する技術として，NTMobile（Network Traversal with Mobility）が提案されている [1]．NTMobile ではエンドツーエンド（以後，E2E）の暗号化通信を行うことができるが，NTMobile を利用するためにはファイアウォールのポート開放が必須である．そのため，端末が接続しているネットワークによっては NTMobile による通信が失敗する可能性がある．

本稿では次世代 HTTP プロトコルとして標準化された QUIC を利用して，ファイアウォール（以後，FW）の影響を受けずに NTMobile の E2E 暗号化通信の実現を提案する．

2　NTMobile

NTMobile は移動しても変化しない仮想 IP アドレスを利用して，アプリケーション通信を行う．仮想 IP アドレスを指定した IP パケットを実ネットワークでルーティングさせるために，端末に割り当てられている実 IP アドレスを用いて UDP/IP でカプセル化をする．図 1 に通信開始時に行う NTMobile トンネル構築処理を示す．NTM 端末のアドレス情報を管理する DC（Direction Coordinator）へトンネル構築要求に基づいて，NTM 端末間で暗号鍵の交換および E2E で UDP トンネルを構築する．以後，NTM 端末間の通信は元の仮想 IP パケット部分は全て暗号化され，UDP トンネルにより通信相手 NTM 端末まで届けられる．

しかし，NTMobile の制御メッセージは UDP4330 番ポートを利用するため，ファイアウォールで NTMobile の通信を許可する必要がある．自分の管理できるネットワークの FW であれば変更できるが、通信相手や上流のネットワークに存在する FW の 4330 番ポートが閉じられていると NTMobile のシグナリングやトンネル通信のパケットが通過できなくなる．

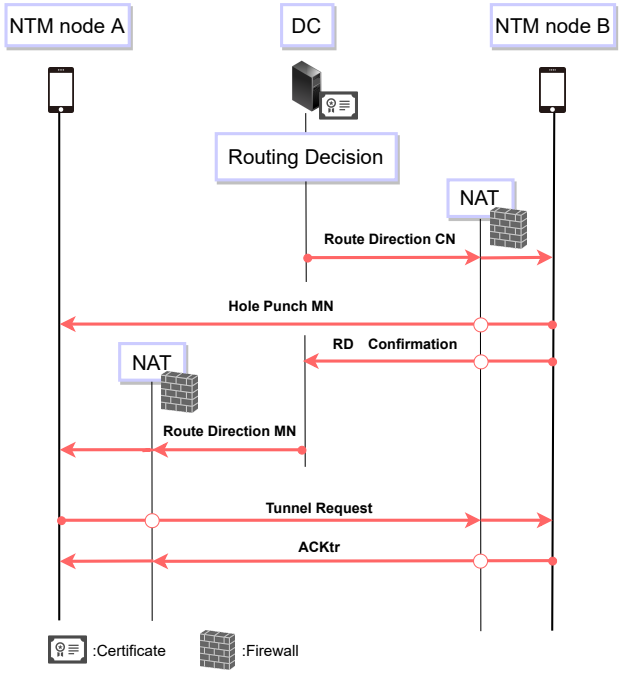

図 1　NTMobile のトンネル構築処理

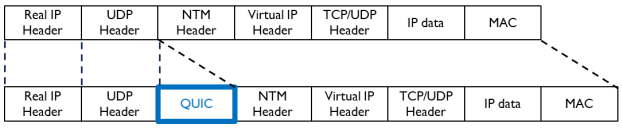

図 2　従来手法と提案手法によるパケットフォーマットの比較

3　提案手法

3.1　概要

前述の課題を解決するために，UDP で定義されているシグナリング，トンネル通信を図 2 にように QUIC[2] で置き換える．QUIC は HTTP/3 で採用されているプロトコルであるため普及に伴って FW を越えることが期待できる．また，HTTP/3 以外のプロトコルへの適用も検討されており，UDP ベースで実装されているため NTMobile との親和性が高い．

3.2　シグナリング処理

QUIC による暗号化通信の実現には通信相手端末が公開鍵証明書を保有し，証明書に基づく認証が前提になる．従来の NTM 端末は公開鍵証明書を保有していないため，新たに証明書を発行・管理する仕組みが必要となる．文献 [3] では，公開鍵証明書に基づく NTMobile の

A Proposal of Encrypted End-to-End Communication for NTMobile Using QUIC

Shota Horisaki[†1], Hirotoshi Kato[†2], Kota Suzuki[†2], Hidekazu Suzuki[†2] and Katsuhiro Naito[†3]
[†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

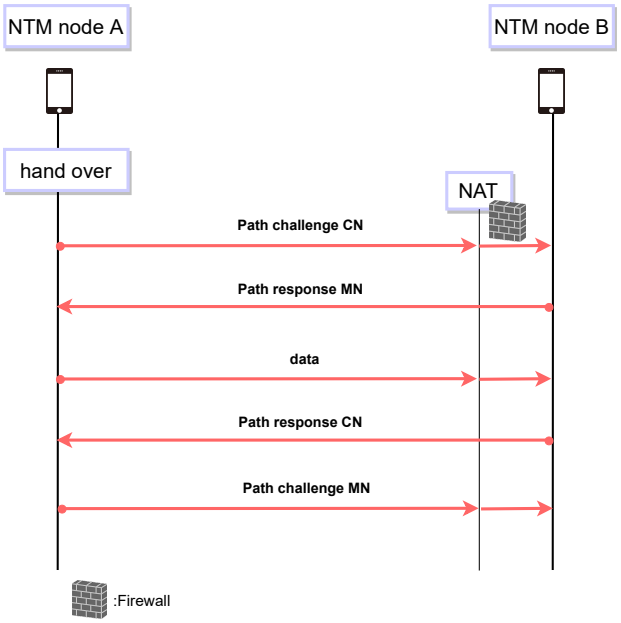

図 3　提案手法によるトンネル再構築処理

仕様を検討している．この仕様を反映することにより，エンド端末間で QUIC を利用した暗号化通信が可能になる．

NTM ヘッダ内でエンド端末や端末間のトンネル通信を判断する識別子（Communication IDentification）を廃止し，QUIC ヘッダに含まれる Connection ID によって判断を行う．それに伴い，各サーバのテーブル情報に Connection ID を新たに記録させる．

3.3　トンネル通信

トンネル構築完了後，NTM 端末が別のネットワークへ移動した際，従来の NTMobile は図 1 に示したように DC を経由してトンネル構築処理を再度行う必要があった．

提案手法によるトンネル再構築処理はハンドオーバー前後の Connection ID の対応を関係づけることで通信を維持させる．図 3 のように E2E でトンネルを再構築できるようになるため接続時間の短縮が期待できる．上記の手法が適用できるのは非ハンドオーバ端末側のネットワークに存在する NAT が Full Cone NAT を想定しており，Restricted cone NAT，Port restricted cone NAT，Symmetric NAT のいづれかが存在する場合は従来手法を用いる．

4　実装及び比較

4.1　実装

従来の NTMobile のプログラムは C 言語で実装されている．しかし，提案手法では Go 言語を使用する．Go 言語は並列処理が可能であり軽量なスレッドを作れるため NTMobile との相性が良く，QUIC に関するオープンソースソフトウェアライブラリが提供されている．ライブラリには quic-go[4] を利用し，データベース管理システムには MariaDB のバージョン 10.6.4 を使用する．

表 1　従来手法と提案手法のパケットサイズ比較

	従来手法	提案手法
Real IP Header[byte]	20	20
UDP Header[byte]	8	8
NTM Header[byte]	32	16
MAC[byte]	16	16
QUIC Header[byte]		25
IP data[byte]	1,424	1,415

表 2　提案手法のメリットとデメリット

メリット	デメリット
• FW を越えやすくなる • ハンドオーバ時の接続時間の短縮 • エンド端末間での認証	• ヘッダ増大によるスループット低下

4.2　比較

1 パケットで送れるデータサイズを従来手法と提案手法で比較したものを表 1 に示す．提案手法は従来手法の制御パケットに対して NTM ヘッダの変更と QUIC ヘッダの追加を行っている．そのため一度で送ることができるデータサイズは約 0.7% 減少する．しかし，過去の検証結果 [5] から従来手法の NTMobile は十分なスループットを維持しているため提案手法でもアプリケーション性能に影響を及ぼさないことが期待できる．

5　まとめ

提案手法のメリットとデメリットを表 2 として示す．現在の HTTP がファイアウォールを通過するように，QUIC も普及するにしたがって，ファイアウォールを越えることが基本になると考えられる．本稿では QUIC プロトコルを利用した NTMobile の暗号化 E2E の手法を提案した．今後は，検討手法を NTMobile に実装し，動作検証およびスループット性能の評価を行っていく．

参考文献

[1] 上醉尾．他：情報処理学会論文誌，Vol. 54, No. 10, pp. 2288–2299, 2013.
[2] J. Iyengar, et al.: RFC 9000, IETF (2021).
[3] Y. Miyazaki, et al.: Development of Certificate based Secure Communication for Mobility and Connectivity Protocol, Proc. IEEE CCNC 2018, pp. 355–358, 2018.
[4] https://github.com/lucas-clemente/quic-go
[5] 内藤．他：情報処理学会論文誌，Vol. 54, No. 1, pp. 380–393, 2013.