M-004

QUIC-CYPHONIC における経路最適化処理の仕様検討
Specification Review of Route Optimization Process in QUIC-CYPHONIC

六鹿 太智[1)]　内藤 彩乃[2)]　鈴木 秀和[3)]
Taichi Mushika　Ayano Naito　Hidekazu Suzuki

1　はじめに

IP 通信における通信接続性と移動透過性を同時に実現する技術として，QUIC-CYPHONIC（QUIC-based CYber PHysical Overlay Network over Internet Communication）が提案されている [1]．QUIC-CYPHONIC では，異なる NAPT 配下のデバイス間通信をクラウドサーバ経由で中継することにより通信接続性を実現している．しかし，暗号化通信経路の冗長化や中継サーバにおける負荷集中による通信性能の低下が課題となっている．

本稿では，QUIC のコネクションマイグレーション機能を応用し，中継サーバ経由の暗号化通信経路をエンドツーエンド通信へ動的に切り替える経路最適化手法の仕様を検討する．

2　QUIC-CYPHONIC

図 1 に QUIC-CYOHONIC の概要を示す．QUIC-CYPHONIC は，CYPHONIC を導入した CYPHONIC ノードと CYPHONIC クラウドサービスにより構成される．CYPHONIC ノードは通信開始時に DNS による通信相手の名前解決処理を実行するが，これをトリガとして QUIC-CYPHONIC による経路選択処理，トンネル構築処理が行われる．経路選択処理では，NMS（Node Management Service）が通信ペアとなる CYPHONIC ノードのネットワーク情報に基づいて両 CYPHONIC ノードに暗号化通信経路を指示する．その後のトンネル構築処理では，CYPHONIC ノードは NMS からの指示に従って動的に QUIC トンネルを構築する．

両 CYPHONIC ノードが共に NAPT 配下に存在する場合は，中継サーバである TRS（Tunnel Relay Service）に対してそれぞれ QUIC トンネルを確立する．その後のアプリケーション通信は TRS 経由で行われる．

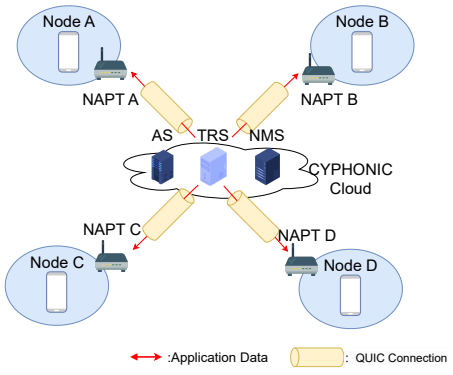

図 1　QUIC-CYOHONIC の概要

1）名城大学大学院理工学研究科　Graduate School of Science and Technology, Meijo University
2）愛知工業大学情報科学部　Faculty of Information Science, Aichi Institute of Technology
3）名城大学情報工学部　Faculty of Information Engineering, Meijo University

3　コネクションマイグレーション

QUIC では，コネクションの識別を 4 タプルから独立した Connection ID（CID）が使用されており，ノードの IP アドレスやポート番号が変わっても通信を継続できるコネクションマイグレーション機能を有している [2]．図 2 にコネクションマイグレーション処理を示す．以後，通信開始側および通信相手側 CYPHONIC ノードをそれぞれ Node I，Node R と表記する．まず，Node I は Node R と QUIC シグナリングを実行してコネクションを確立する（CID=I0, R0）．その後，両ノードはコネクションマイグレーションで使用する CID（I1,R1）を “NEW_CONNECTION_ID” フレームに含めてそれぞれ交換する．その後，アプリケーション通信は R0 および I0 を指定したストリームとしてやり取りされる．

ここで，Node I がネットワークを移動して IP アドレスが変化すると，事前に共有していた I1 と R1 を用いてパス検証を実施する．パス検証では，“PATH_CHARENGE” および “PATH_RESPONSE” フレームを用いて両ノード間で同じ乱数値の交換ができるか確認する．パス検証を完了することにより，新しい CID によるストリームとして通信を継続することができる．

4　検討手法

QUIC-CYPHONIC では，NAPT 配下の CYPHONIC ノード間の通信がすべて TRS を経由してしまうため，TRS に負荷が集中してしまう課題がある．この課題を解決するには，通信を TRS 経由から CYPHONIC ノード間の直接通信になるように経路最適化を行う必要がある．そこで，QUIC のコネクションマイグレーションを応用することにより，TRS 経由のストリームから CYPHONIC ノード間の直接経路によるストリームへ切り替える．

図 3 に経路最適化までの通信シーケンスを示す．Node I および Node R が接続する LAN を構成する NAPT

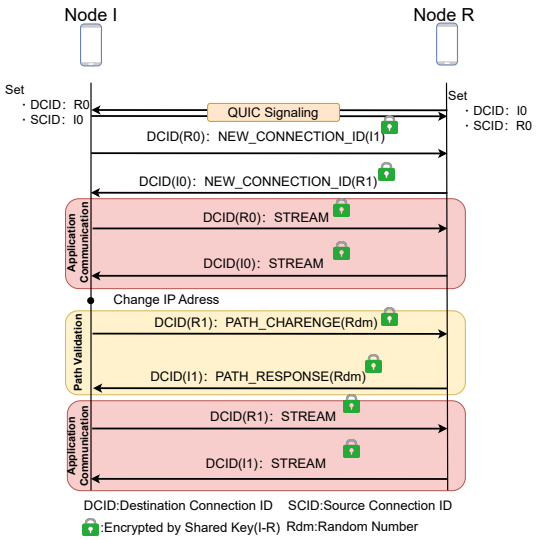

図 2　コネクションマイグレーション

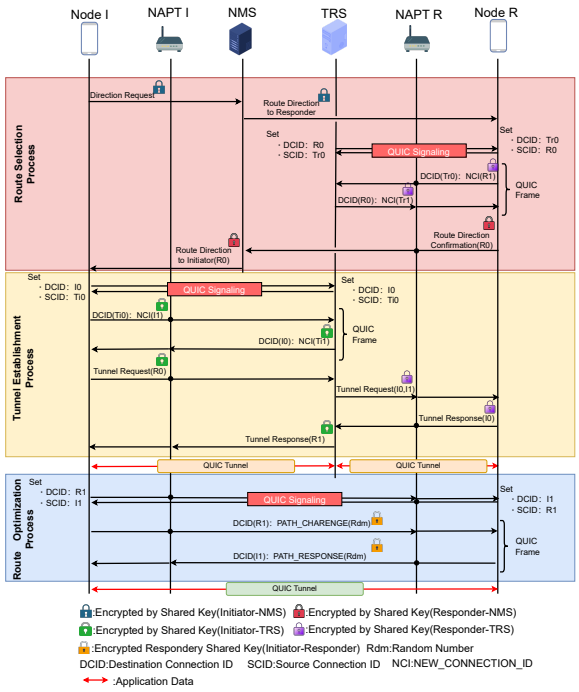

図 3　経路最適化までの通信シーケンス

を，それぞれ NAPT I，NAPT R とする．RFC5780 [3] では，NAPT の種類はマッピング動作とフィルタリング動作の組み合わせで 9 パターンに分類できると示されている．本稿における検討では，NAPT R のマッピング動作は Endpoint-Independent Mapping，フィルタリングは動作 Endpoint-Independent Filtering であることを前提とする．

4.1　経路選択処理

Node I が NMS へ Direction Request を送信して経路選択処理を開始する．Node I と Node R が共に NAPT 配下に存在するため，NMS は Node R へ Route Direction を送信し，TRS へ暗号化通信経路を構築するよう指示する．Node R は TRS と QUIC シグナリグを行い，TRS との QUIC トンネル通信のための CID R0，Tr0 を交換する．さらに，“NEW_CONNECTION_ID”（以後，NCI）によりコネクションマイグレーションで使用する CID R1，Tr1 を交換する．この時，TRS は自身の CID Tr0 を Key として，Node R から通知された NCI に含まれる CID R1 を管理する．また，TRS は Node R の CID R0 を Key として Node R のコネクションを管理する．その後，Node R は NMS を経由して自身の CID R0 を Route Direction に含めて Node I へ通知する．

4.2　トンネル構築処理

Node I は NMS からの指示に従って，TRS に対して QUIC シグナリグと NCI の交換を行い，CID I0，Ti0，I1，Ti1 を共有する．この時，TRS は CID Ti0 を Key として，Node I のから通知された CID I1 を管理する．また，TRS は Node I の CID I0 を Key として Node I のコネクションを管理する．その後，Node I は Route Direction で受け取った R0 を記載した Tunnel Request を TRS へ送信する．TRS は R0 から Node I の通信相手のコネクションを特定し，CID I0，R1 を Tunnel Request に含めて Node R に送信する．Node R は CID I0 をそのまま Tunnel Response に含め，TRS に送信する．TRS は Node I のコネクションの特定と CID R1 を Tunnel Response に含めて Node I に送信を行う．その後，Node I は TRS を経由して Node R とアプリケーション通信を開始する．

表 1　経路最適化の結果

経路最適化パターン	該当数
○	27
△	26
□	4
×	24
合計	81

4.3　経路最適化

TRS 経由のトンネル通信と並行して，Node I と Node R 間で経路最適化処理を実施する．Node I は NMS から通知された情報を用いて，NAPT R に対して QUIC シグナリグを実行すると，NAPT R は Node R へ転送して Node I と Node R 間の QUIC シグナリングが始まる．ここで，NCI を CID とした新たなコネクションを確立する．

その後，パス検証を完了することにより，暗号化通信経路を TRS 経由からノード間のエンドツーエンドへと切り替える．このプロセスにより，新たに確立したコネクション上でアプリケーションデータを送受信される．

5　評価

4 章で述べたとおり，NAPT は 9 種類に分類できるため，NAPT I と NAPT R の組み合わせを想定すると 81 通りある．しかし，特定の NAPT の組み合わせの場合，QUIC シグナリングを Node I と Node R 間で実施できない場合がある（NAT 越え問題）．そこで，どの NAPT の種類の組み合わせであれば，検討手法による経路最適化が可能か検討した．

表 1 に経路最適化の可否を検討した内容を示す．表中の記号は以下の通りである．

- ○：Node I から Node R に対して実行した経路最適化処理が成功する場合．
- △：Node I から Node R への経路最適化は失敗するが，その後に Node R から Node I への経路最適化処理を実行することで成功する場合．
- □：△ でも経路最適化は失敗するが，再度，Node I から Node R への経路最適化処理を実行すると成功する場合．
- ×：経路最適化は不可能な場合．

検討した結果，約 70%の NAPT の組み合わせで経路最適化が可能であることがわかった．

6　まとめ

本稿では，QUIC のコネクションマイグレーション機能を応用し，エンドツーエンド通信へ動的に切り替える経路最適化手法の仕様を検討し，NAPT の挙動の違いによる経路最適化処理の可否について示した．

今後は，検討手法を QUIC-CYPHONIC に実装し，実環境における経路最適化処理の検証を行う予定である．

参考文献

[1] S. Horisaki, et al.: CYPHONIC-over-QUIC: Secure End-to-End Communication Architecture Traversing Firewalls/NATs, *Journal of Information Processing*, Vol. 32, pp. 509–519, 2024.

[2] J. Iyengar, et al.: QUIC: A UDP-Based Multiplexed and Secure Transport, RFC 9000, IETF, 2021.

[3] C. Jennings, et al.: NAT Behavior Discovery Using STUN, RFC 5780, IETF, 2010.