Vol.2020-MBL-97 No.5
Vol.2020-ITS-83 No.5
2020/11/24

ロードバランサ利用時における NTMobileセッション構築手法の検討

鈴木 洸太[1,a)]　松岡 穂[1]　加藤 宏理[1]　鈴木 秀和[1,b)]　内藤 克浩[2]

概要：インターネット普及により通信トラフィックが増加しているが，多くのシステムでクライアントサーバモデルを使用しているため，トラフィック集中によるサーバ高負荷状態の発生が懸念される．この状態を防ぐ方法としてロードバランサによるトラフィック分散が挙げられるが，IPv4/IPv6 混在環境下で移動透過性及び通信接続性を同時に実現する NTMobile（Network Traversal with Mobility）との併用は検討されていなかった．本稿では NTMobile 環境下においてロードバランサーを導入した際の課題を検証し，併用時に生じる課題を解決するために NTMobile 開始時の処理を変更した新しい仕様について検討する．

キーワード：負荷分散，ロードバランサ，モバイルネットワーク，インターネット保守・管理・運用

A Study on Construction Method of NTMobile Session When Using Load Balancer

Kota Suzuki[1,a)]　Minoru Matsuoka[1]　Hirotoshi Kato[1]　Hidekazu Suzuki[1,b)]　Katsuhiro Naito[2]

1. はじめに

スマートフォンやタブレット等のモバイル端末の増加やインターネットを活用したサービスの普及により，いつでもどこでも誰でもオンラインサービスを利用できる環境になった．これに伴い，モバイル端末のトラフィックも急増している．文献 [1] によると，2017 年における全世界の IP トラフィックの年間ランレートは 1.5 ゼタバイトであるが，2022 年には約 3 倍の 4.8 ゼタバイトに到達すると予測されており，今後もモバイルトラフィックは増加することが考えられる．しかし，多くのオンラインサービスはクライアントサーバモデルで構築されているため，サーバへのアクセスが増加すると，サーバにトラフィックが集中して高負荷状態に陥りやすくなる懸念がある．実際にサーバへのアクセス集中によるサーバ高負荷状態やサーバダウンが発生しており，サービス提供が困難な状態になる事例は存在している [2,3]．そのため，トラフィックの集中によるサーバの高負荷状態の抑制は，オンラインサービスを安定的に提供する上で重要である．

サーバの高負荷状態を抑える手法の 1 つに，サーバを複数台用意し，ロードバランサを用いてクライアントからのアクセスを複数台のサーバへ分散させる方法がある．ロードバランサは特定の負荷分散アルゴリズムに基づいてクライアントからのアクセスをサーバへ振り分けることにより，個々のサーバにかかる負荷の平準化を図る．また，故障や保守により一部のサーバが停止した際にも，他のサーバでサービスを続行させることも可能である．さらに，同一クライアントからのアクセスが複数回ある場合に，全て同じサーバへアクセスを振り分けるようにすることで通信の整合性を保つセッション維持機能なども有する．そのた

[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科
Department of Information Science, Aichi Institute of Technology
[a)] kota.suzuki@ucl.meijo-u.ac.jp
[b)] hsuzuki@meijo-u.ac.jp

© 2020 Information Processing Society of Japan

め，ユーザ数の多いオンラインサービスを提供するサーバにはロードバランサーが導入されることが一般的となっている．

一方，インターネットで利用されている TCP/IP は，端末の移動により接続先ネットワークが変化した場合，端末の IP アドレスも共に変化してしまう．そのため，OS は移動前のフローを識別することが出来ず，通信が断絶してしまう．この課題を解決する技術として移動透過性技術が提案されている [4,5]．さらに，IPv4 ネットワークにはグローバルアドレス空間とプライベートアドレス空間の間に設置される NAT（Network Address Translation）により，双方向通信を自由に開始することができない NAT 越え問題が存在する．さらに，IPv4 と IPv6 の間では互換性が無いため，直接通信を行うこともできない．そのため，モバイル端末の接続先ネットワークの種類や通信相手端末のネットワーク環境に影響されることなく，通信接続性を確保しつつ，移動透過性を実現することが要求されている．

このような背景から，筆者らは IPv4/IPv6 混在環境において通信接続性と移動透過性を同時に実現する技術として NTMobile（Network Traversal with Mobility）を提案してきた [6–8]．NTMobile では，通信開始時に通信相手端末との間にできる限りエンドツーエンドで通信できる通信経路上に暗号化 UDP トンネルを構築し，そこに接続先ネットワークとは独立したエンド端末を識別する仮想 IP アドレスを適用した IP パケットを送信する．端末が移動して IP アドレスが変化した場合は暗号化 UDP トンネルを再構築するが，その中に流す仮想 IP パケットに記載する送信元/宛先 IP アドレスは変化しないため，移動透過性を実現することができる．

しかし，NTMobile を実装した端末がロードバランサーを導入したサーバシステムにアクセスした場合，NTMobile 処理が従来通り正常に動作し，端末移動時にセッションが維持されるのか否か検証されていない．そこで本稿では，NTMobile 環境下において，ロードバランサ使用時でも NTMobile セッションが維持が可能か検証を行う．また，併用時に生じる課題を調査し解消するための手法を検討する．

以下，2 章には NTMobile の概要及びロードバランサ利用時でも NTMobile セッションが維持できるか検証について述べると共に懸念される課題について整理する．3 章では現状の課題を解決するための手法を示し，4 章で提案手法について定性的に評価する．最後に 5 章でまとめる．

2. NTMobile

2.1 概要

NTMobile は，エンド端末の識別子として役割を持つ仮想 IP アドレスと，接続先ネットワークから割り当てられる位置情報としての役割を担う実 IP アドレスの両方を利用することで移動透過性を実現する．エンド端末のアプリケーションで生成される IP パケットは仮想 IP アドレスを利用しており，実際のネットワークでルーティングさせるために実 IP アドレスに基づく UDP/IP ヘッダでカプセル化を行う．

通信開始時において，NTMobile を実装したエンド端末である NTM 端末の間で，暗号鍵の交換や UDP トンネルの動的な構築を行う．仮想 IP アドレスに基づく IP パケットは UDP トンネルを通じて通信相手 NTM 端末へ伝送する．これにより，ネットワークの切り替えや通信経路上にある NAT の影響を受けない通信が可能である．さらに，ハンドオーバにより MN や CN の接続先ネットワークが変化した場合でも，仮想 IP アドレスは変化しないため通信が断絶しない．

2.2 構成

図 1 に NTMobile の構成を示す．NTMobile は，NTMobile がインストールされている端末である NTM 端末の他に，DC（Direction Coordinator）や RS（Relay Server）から構成される．DC は，NTM 端末が通信時に利用する仮想 IP アドレスの割り当て及び管理を行う．さらに，NTM 端末の通信開始時に両端末間で最適なトンネル経路を構築する事ができるよう，関連する端末へトンネル構築に関わる指示を送る．RS は，IP アドレスの違いや NTM 端末がそれぞれ異なる NAT 配下に存在する場合のように NTM 端末間で直接相互通信が行えない場合に通信を中継する．

DC や RS はそれぞれデュアルスタックネットワークに接続されており，運用規模に応じて複数台設置することが可能である．

2.3 トンネル構築

図 2 に NTMobile 通信開始時において，通信開始する端末の MN（Mobile Node）から通信相手端末の CN（Correspondent Node）に対して UDP トンネルを構築する際のシーケンスを示す．MN 内にあるアプリケーションは，通信開始時に CN の IP アドレスを問い合わせるために $FQDN_{CN}$ を含めた DNS クエリを送信する．この DNS クエリを MN にインストールされている NTMobile アプリケーション内の TUN インターフェイスがパケットを取り込む．$FQDN_{CN}$ にはその端末が NTM 端末であることを示す文字列が含まれており，NTMobile アプリケーションはこの文字列の有無で通信相手が NTM 端末であるかを判断する．$FQDN_{CN}$ から CN は NTM 端末であると判断した場合は，MN の管理先 DC（DC_{MN}）へ CN の仮想 IP アドレスなどのアドレス情報を問い合せる Direction Request を $FQDN_{CN}$ を含めて送信する．なお，CN は一般端末であると NTMobile アプリケーションが判断した場合は以下のトンネル構築処理は行われない．MN から

© 2020 Information Processing Society of Japan

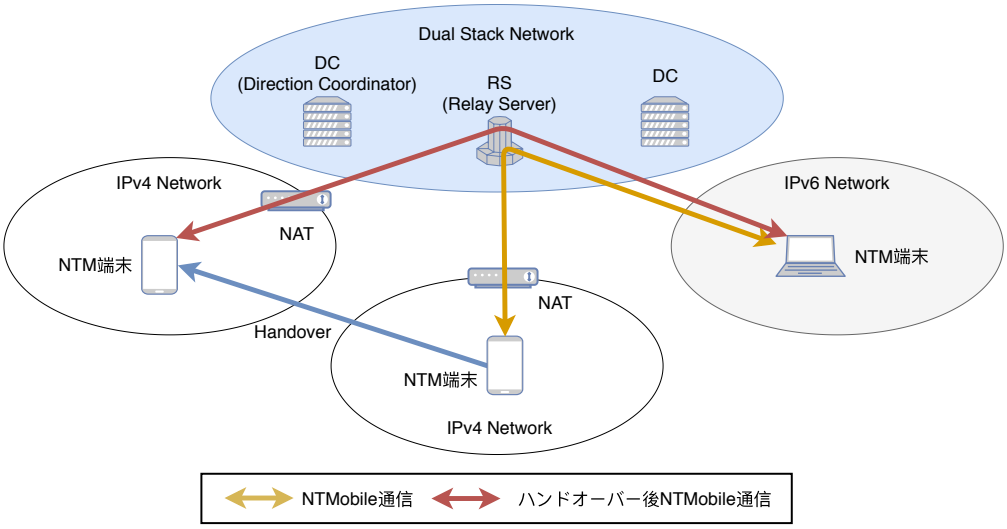


図 1 NTMobile の構成

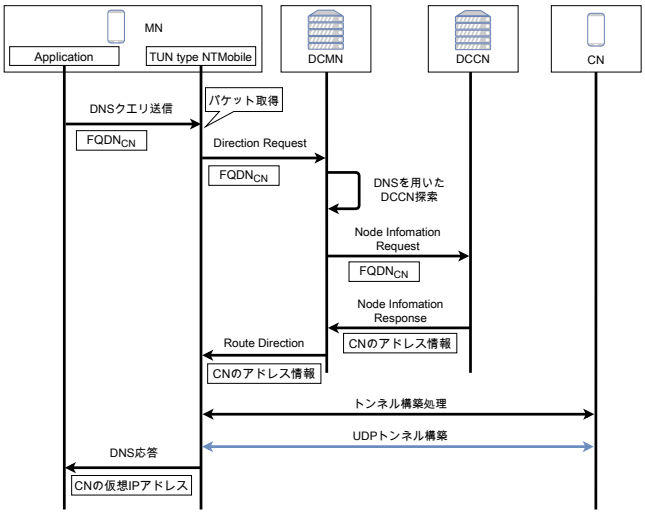


図 2 NTM 端末間におけるトンネル構築処理

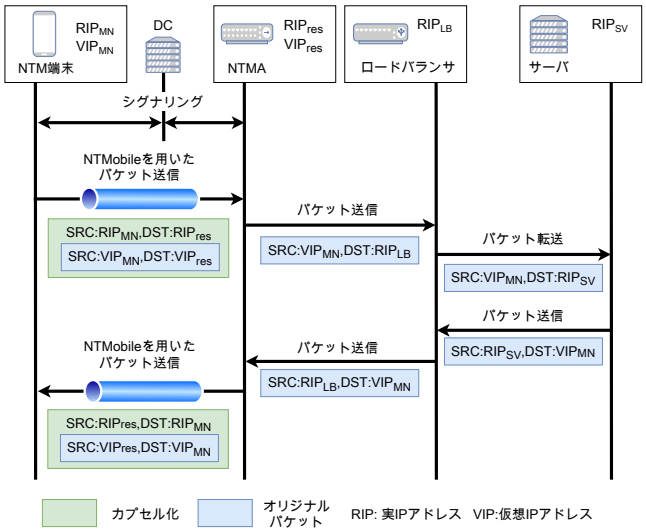


図 3 ロードバランサ使用時における NTMobile に基づく想定される通信シーケンス

の Direction Request 内に含まれている $FQDN_{CN}$ を基に CN を管理している DC（DC_{CN}）を探索する．探索後，DC_{MN} は DC_{CN} へ CN のアドレス情報の提供を要求する Node Infomation Request を送信する．DC_{CN} はメッセージ内に含まれている $FQDN_{CN}$ を基に CN のアドレス情報を DC_{MN} へ返す．DC_{MN} は得られた CN のアドレス情報を MN の NTMobile アプリケーションへ転送する．NTMobile アプリケーションは CN と UDP トンネルの構築処理を開始し，CN の仮想 IP アドレスを DNS 問い合わせ結果としてアプリケーション側へ返す．これにより，MN 側のアプリケーションは通信相手の IP アドレスを CN の仮想 IP アドレスと認識する．上記の流れでシグナリング処理を行うことにより，MN は CN と NTMobile に基づく通信を行うことが可能である．

2.4 想定される運用環境

NTMobile 利用時においても，通信トラフィックが増加した場合にロードバランサを用いてサーバが持つ負荷を分散させる必要はある．**図 3** に NTMobile とロードバランサ併用時に想定される通信シーケンスを示す．NTMobile に基づく通信は，NTM 端末とロードバランサに取り付けられる NTMA(NTMobile Adaptor) 間で行われる．NTMA は組み込み機器など一般的にソフトウェアをインストールやプログラムの改造をすることが出来ない端末でも NTMobile 通信を利用可能にするためのアダプターである [9]．NTMA を用いることにより，ロードバランサを改造することなく NTMobile を利用することができる．

しかし，NTMobile に基づく通信は NTM 端末と NTMA 間で行われ，実 IP アドレスに基づく UDP/IP ヘッダは NTMA で除去される．そのため，ロードバランサは仮想 IP アドレスに基づくパケットを扱うこととなる．仮想 IP アドレスによるパケットにおいても適切にパケット分散及びセッション維持が可能であるか検証する必要がある．

© 2020 Information Processing Society of Japan

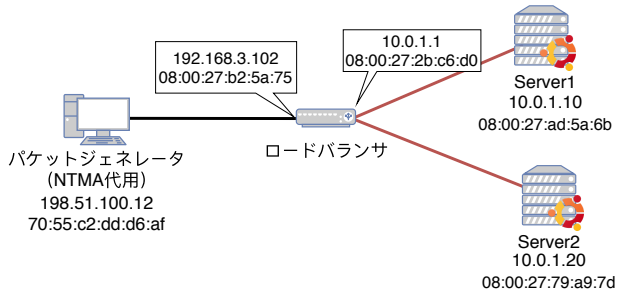


図 4 検証環境の概要

2.5 併用の検証

仮想 IP アドレスに基づくパケットを適切に負荷分散及びセッションの維持が可能であるか確認するために簡易的な環境を構築し検証を行う．**図 4** に検証環境の概要を示す．

ロードバランサは LVS（Linux Virtual Server）[10] を利用した．LVS はオープンソースで開発が進められている，Linux 上で動作する負荷分散ソリューションソフトウェアである．主に，トランスポート層までの情報を基に負荷分散を行う IPVS [11] とアプリケーション層までの情報を用いて負荷分散を行う KTCPVS [12] から構成されている．本稿では，NTMobile が UDP/IP ヘッダでカプセル化を行っているため，IPVS を用いてロードバランサを構築した．また，仮想 IP アドレスに基づくパケットでも動作が可能か確認するために，パケットジェネレーターを用いて仮想 IP アドレスに基づく擬似パケットを作成する．パケットジェネレーターより作成した疑似パケットを幾つか送信し，Wireshark を用いてパケットの流れを観察した．

図 5 にロードバランサにおいてパケットジェネレーター側ネットワーク，サーバ側ネットワークそれぞれにおいて Wireshark を用いてパケットキャプチャを行ったときの様子及び IPVS によるセッションテーブルの様子を示す．図 5 中の赤枠はパケットジェネレータより送信されたパケットの流れを黄枠はサーバから送信されたパケットの流れを示している．また，下部のセッションテーブルは IPVS で保持しているセッションの情報を示したものである．図より，仮想 IP に基づくパケットでも既存のロードバランサで適切に負荷分散を行えることを確認した．

2.6 併用時の課題

仮想 IP アドレスに基づく通信でもロードバランサにより負荷分散及びセッションの維持を適切に行うことができることを確認した．しかし，NTMobile ではシグナリングを行うために，NTMA が持つ NTMobile 用の FQDN を利用する．NTMobile 用の FQDN は，その端末が NTM 端末であることを示す特定の文字列が FQDN 内に存在するため，一般的に用いられている FQDN とは異なる．そのため，サーバやロードバランサと NTMobile に基づく通信を行うためにはサーバやロードバランサが持つ FQDN を NTMobile 用の FQDN に変更する必要がある．

3. 提案手法

3.1 概要

サーバ側端末を示す情報として FQDN を持つが，NTM 端末から通信する場合はシグナリングを行うために NTMobile 用の FQDN，一般端末からの通信など NTMobile を利用しない場合は一般 FQDN のように NTMobile 利用の有無により使用する FQDN が変化してしまう．しかし，この手法では NTMobile に基づく通信を行うために，DNS クエリ送信時点で NTMobile 用の FQDN を含める必要があることから，ユーザが困惑する要因の一つになり得る．この変化を防止するために本稿では，CNAME レコードを用いることにより，一般 FQDN を用いた場合でも通信相手端末が NTM 端末である場合は NTMobile のシグナリングが行える手法を検討する．この場合，一般 FQDN を含めた DNS クエリを用いて通信開始した場合でも，DNS からの応答内に一般 FQDN の別名として NTMobile 用の FQDN が定義された CNAME レコードが存在する場合，通信相手端末は NTM 端末であると判断が可能である．

さらに，CN が NTM 端末であるかどうかを DNS 問い合わせ結果から判断するため，シグナリングを開始するタイミングを従来の「DNS クエリの送信時点」から「DNS 問い合わせを受け取った時点」に変更する．

3.2 NTM 端末検知

ユーザが一般 FQDN を用いて通信開始した場合でも，通信相手端末が NTM 端末である場合に NTMobile のシグナリングを開始できるようにするために，CNAME レコードを利用する．CNAME レコードとは，正規 FQDN 名に対するエイリアスとして別名を定義する DNS のレコードである．CNAME レコードにより定義された別名に対して名前解決を行った場合でも，正規 FQDN 名で名前解決した時と同様の問い合わせ結果が得られる．

本稿では，CNAME レコードを用いて NTMobile 用の FQDN を一般 FQDN の別名として DNS に定義する．これにより，ユーザが一般 FQDN を用いて名前解決を行った場合でも，DNS 問い合わせ結果内の CNAME レコードから NTMobile 用の FQDN を得ることができるため，CN が NTM 端末であることを検知することができる．

3.3 トンネル構築処理開始タイミング

CN が NTM 端末であるかどうか判断するために CNAME レコードを用いるため，判断できるタイミングは DNS からの応答が来たタイミングとなる．そのため，NTMobile のシグナリングを開始するタイミングを従来の DNS クエリ送信時から，DNS クエリの受信時に仕様変更を行う．以

© 2020 Information Processing Society of Japan

パケットジェネレータ側ネットワーク

	Time	Source IP address	Destination IP address		Port
19	16:18:13.727943965	198.51.100.12	192.168.3.102	UDP	60 40000 → 50000 Len=4
21	16:18:16.729299291	198.51.100.12	192.168.3.102	UDP	60 40000 → 50000 Len=4
24	16:18:19.729562528	198.51.100.12	192.168.3.102	UDP	60 40000 → 50000 Len=4
28	16:18:25.791746074	10.0.1.20	198.51.100.12	UDP	42 2914 → 40000 Len=0
29	16:18:26.792331106	10.0.1.20	198.51.100.12	UDP	42 2915 → 40000 Len=0

サーバ側ネットワーク

	Time	Source IP address	Destination IP address		Port
249	16:18:13.727963039	198.51.100.12	10.0.1.20	UDP	46 40000 → 50000 Len=4
250	16:18:16.729319136	198.51.100.12	10.0.1.20	UDP	46 40000 → 50000 Len=4
251	16:18:19.729579132	198.51.100.12	10.0.1.20	UDP	46 40000 → 50000 Len=4
252	16:18:25.791726539	10.0.1.20	198.51.100.12	UDP	60 2914 → 40000 Len=0
253	16:18:26.792314452	10.0.1.20	198.51.100.12	UDP	60 2915 → 40000 Len=0

セッションテーブル

```
IPVS connection entries
pro expire state       source              virtual             destination
UDP 01:05  UDP         198.51.100.12:40000 192.168.3.102:50000 10.0.1.20:50000
```

図 5 Wireshark による各ネットワーク上でのパケットキャプチャ結果及び IPVS セッションテーブルの内容

下，シグナリング開始タイミング変更後のトンネル構築処理について，CN が NTM 端末である場合と一般端末である場合のように場合分けして説明する．

3.3.1 CN が NTM 端末である場合

図 6 に CN が NTM 端末である場合におけるトンネル構築処理シーケンスを示す．NTM 端末内のアプリケーションが通信開始するために生成した DNS クエリは，NTMobile アプリケーションは取得せずに DNS サーバへ送信する．DNS からはクエリ内に含まれる FQDN に対する問い合わせ結果を MN に返すが，NTMobile アプリケーション内の TUN インターフェイスがその DNS 問い合わせ結果メッセージを取り込む．NTMobile アプリケーションは取り込んだ DNS 問い合わせ結果に含まれている ANSWER SECTION の内容を確認し，CNAME レコードで NTMobile 用の FQDN が別名として定義されているか確認する．NTMobile 用の FQDN が別名として定義されている場合，CN は NTM 端末であると判断しトンネル構築処理を行うためのシグナリングを開始し，DC_{MN} へ Direction Request を NTMobile 用の FQDN を含めて送信する．

以降は，従来と同様な手順でトンネル構築処理が行われる．

3.3.2 一般端末との通信時

図 7 に CN が一般端末である場合におけるトンネル構築処理シーケンスを示す．NTM 端末内のアプリケーションが通信開始するために生成した DNS クエリは，3.3.1 節と同様に NTMobile アプリケーションでは取得せずにそのまま DNS サーバへ送信し，DNS からの問い合わせ結果を MN 内の NTMobile アプリケーションの TUN インターフェイスが取り込む．DNS 問い合わせ結果に含まれている ANSWER SECTION の内容を確認し，CNAME レコードで NTMobile 用の FQDN が別名として定義されているか確認する．ここで問い合わせ結果内の CNAME レコードで NTMobile 用の FQDN が別名として定義されていなかった場合，CN は一般端末であると判断し，トンネル構築処理は行わずに DNS 問い合わせ結果をそのままアプリケーション側へ転送する．アプリケーションは DNS 問い合わせ結果内から一般端末の IP アドレスを抽出し，一般通信を開始する．

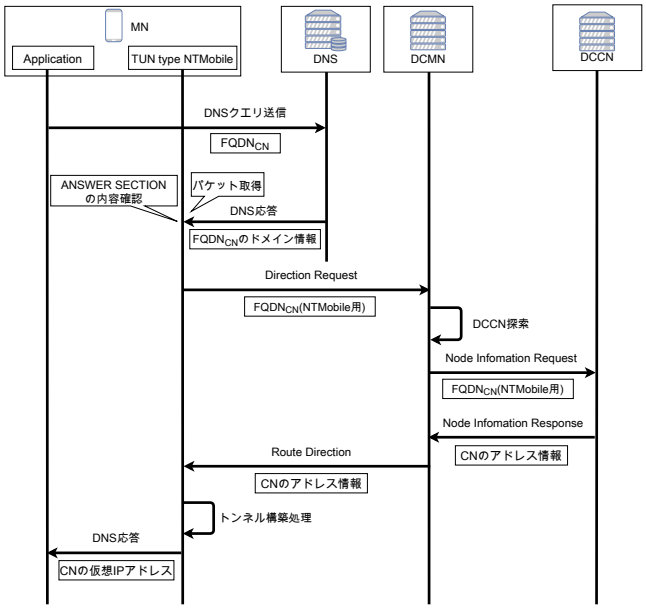


図 6 提案手法によるトンネル構築処理シーケンス

4. 評価

本稿で提案した手法について，従来手法と 3 つの項目に関して比較し定性的に評価を行った．**表 1** に提案手法と従来手法の比較表を示す．

運用時の制約について，従来では NTMobile に基づく通信を行うために，NTM 端末であることを示す文字列が含まれている NTMobile 用の FQDN を用いる必要がある．そ

© 2020 Information Processing Society of Japan

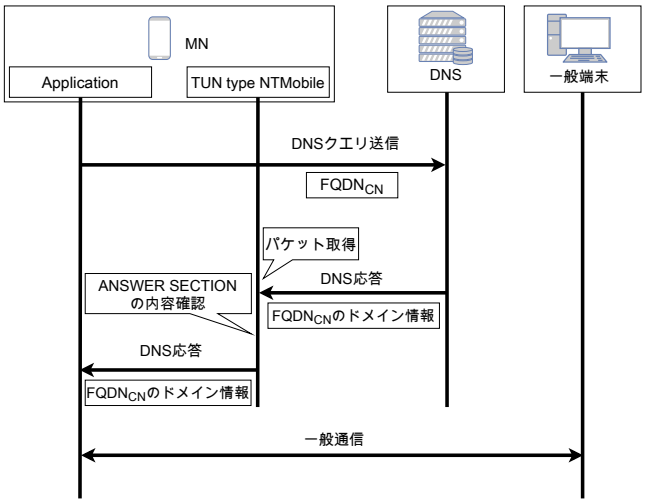


図 7 提案手法による一般端末との通信開始時における処理シーケンス

表 1 従来手法と提案手法の比較

	従来手法	提案手法
運用時の制約	×	○
導入の容易さ	×	○
トンネル構築処理時間	○	×

のため，NTMobile 環境下で運用する場合はサーバやロードバランサが持つ FQDN を NTMobile 用の FQDN に変更する必要があった．提案手法では，CNAME レコードにより本来持つ FQDN の別名として NTMobile 用 FQDN を定義する事により，本来の FQDN と同様なものとして NTMobile 用の FQDN を扱うことができるため，本来の FQDN を用いた場合でも NTMobile に用いるトンネルの構築を行う事が可能である．また，導入の容易さに関しても提案手法では FQDN を変更する必要がないことから，従来手法より容易な導入が可能である．

トンネルの構築処理時間について，提案手法ではトンネル構築処理を開始するタイミングを DNS 問い合わせ結果を受け取った時点に変更した．そのため，提案手法では従来手法と比較して DNS 問い合わせ 1 往復分の通信時間が増加する．しかし，DNS 問い合わせは処理負担が大きい処理ではないため，この処理により提案手法での性能が大幅に低下するとは考えにくい．そのため，上記については運用上問題無いと考えられる．

5. まとめ

本稿では，ロードバランサと NTMobile を併用について簡易的な環境下で検証を行い，NTMobile のセンションが適切に保持できることを確認した．さらに，NTMobile 利用時と非利用時においてサーバ側端末を表す FQDN が NTMobile 用の FQDN と一般 FQDN で変化してしまう課題に対し，CNAME レコードを用いて NTMobile 用の FQDN を一般 FQDN の別名として定義する．また，NTMobile シグナリング開始タイミングを NTMobile アプリケーション内の TUN インターフェイスが DNS 問い合わせ結果を取り込んだ時点に仕様変更する．これにより，FQDN を変更することなく NTMobile を利用することが可能である．

今後は，詳細を検討した後に実装及び性能評価を行う予定である．

参考文献

[1] Cisco: Cisco Visual Networking Index（VNI）：予測とトレンド、2017 〜 2022 年ホワイトペーパー，https://www.cisco.com/c/ja_jp/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. (2020/04/14 参照).
[2] LOHACO:【お詫び】アクセス集中によりサイトにつながりにくくなっておりました，`https://lohaco.jp/info/maintenance/info\_20200306.html`. (2020/10/07 参照).
[3] 一般財団法人国際ビジネスコミュニケーション協会：申込受付中断のお詫びと 2020 年 10 月 4 日 TOEIC Listening & Reading 公開テスト申込受付方法を抽選方式へ変更のお知らせ，`https://www.iibc-global.org/iibc/press/2020/p161.html`. (2020/10/07 参照).
[4] Le, D., Fu, X. and Hogrefe, D.: A review of mobility support paradigms for the internet, *IEEE Communications Surveys Tutorials*, Vol. 8, No. 1, pp. 38–51 (2006).
[5] C.Perkins: IP Mobility Support for IPv4, Revised, RFC 5944, IETF (2010).
[6] 鈴木秀和，上醉尾一真，水谷智大，西尾拓也，内藤克浩，渡邊晃：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. 367–379 (2013).
[7] 内藤克浩，上醉尾一真，西尾拓也，水谷智大，鈴木秀和，渡邊晃，森香津夫，小林英雄：NTMobile における移動透過性の実現と実装，情報処理学会論文誌，Vol. 54, No. 1, pp. 380–393 (2013).
[8] 上醉尾一真，鈴木秀和，内藤克浩，渡邊晃：IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価，情報処理学会論文誌，Vol. 54, No. 10, pp. 2288–2299 (2013).
[9] 尾久史弥，納堂博史，鈴木秀和，内藤克浩，渡邊晃：NTMobile 機能を持つアダプタの実現方式の検討，マルチメディア，分散協調とモバイルシンポジウム 2017 論文集，Vol. 2017, pp. 402–408 (2017).
[10] : The Linux Virtual Server Project, `http://www.linuxvirtualserver.org/index.html`. (2020/05/07 参照).
[11] : IPVS Software - Advanced Layer-4 Switching, `http://www.linuxvirtualserver.org/software/ipvs.html`. (2020/10/11 参照).
[12] : KTCPVS Software - Application-Level Load Balancing, `http://www.linuxvirtualserver.org/software/ktcpvs/ktcpvs.html`. (2020/10/11 参照).

© 2020 Information Processing Society of Japan