6E-5

遅延を考慮した VPN トポロジ決定方式の評価

堀 賢治　吉原貴仁　堀内 浩規
株式会社 KDDI 研究所

1. はじめに

IP ネットワーク上にオーバレイネットワークとして VPN(仮想専用網)を動的に構築する際，VPN ルータ数の増加に伴い，ルータ間を結ぶ VPN トンネル(仮想経路)も増える．一方，一台の VPN ルータが始点や終点となることのできる VPN トンネル数(VPN トンネル終端数)にはメモリ容量から上限がある．このため，始点から終点に至るまでに 2 つ以上の VPN トンネルを経由する必要が生じるが，通信遅延の増大を招く課題がある．この課題に対し筆者らは，VPN トンネルを設定する管理サーバが，始点から終点に至るまでに経由するルータ数(以下，ホップ数)やアクセス回線帯域幅といった遅延要因を考慮しながら，VPN トンネル終端数が一定数以下となる VPN トポロジを決定することで，通信遅延の削減を図る方式を提案している[1]．本稿ではシミュレーションにより，提案方式が決定するトポロジの有効性を，ホップ数と VPN トンネル終端数の観点から評価する．

2. 想定するネットワーク環境および VPN 構築方式

2.1 想定するネットワーク環境

図 1 の実線枠内がインターネット(図 1(a))とユーザネットワーク(図 1(b))からなる実ネットワークのトポロジ(以下，実トポロジ)を，破線枠内が実ネットワーク上にオーバレイネットワークとして実現された VPN のトポロジ(以下，VPN トポロジ)を表す．

本稿で VPN とは，地理的に離れたユーザネットワーク間の IP トラヒック(以下，VPN トラヒック)を，各ユーザネットワークとインターネットとを接続する VPN ルータ(図 1(c))間で暗号化転送することで，通信の機密性を確保するネットワークである．2 台の VPN ルータ間に動的に設定される暗号化転送経路を VPN トンネル(図 1(d))と呼ぶ．実ネットワークにおいてユーザネットワークとインターネットとは ADSL(図 1(e))または FTTH 等(図 1(f))のアクセス回線によって接続され，その帯域幅はアクセス回線の種類によって異なる．また，インターネット内は I1～I4 で表される IP ルータ(図 1(g))で構成される．

2.2 VPN 構築方式

VPN を動的に構築する方式として，ISP (Internet Service Provider)に置かれた VPN 管理サーバ(図 1(h))が全ての VPN ルータを自動設定する方式を想定する．このため VPN ルータは参加，離脱要求を VPN 管理サーバに送信することで，いつでも任意の VPN へ動的に参加，離脱できる．

また，各ユーザネットワークがそれぞれ異なる IP プレフィクス(図 1 の各“*P*”)を利用する L3-VPN を想定する．ただしプレフィクス長は固定の値とする．

L3-VPN の場合，VPN トラヒックのルーティングのために，VPN 管理サーバは VPN ルータからの VPN 参加要求受信に際し，VPN 内が連結となるように VPN トポロジを決定し，VPN ルータの IP アドレス(VPN ルータアドレス，図 1 の各“*V*”)，および当該 VPN ルータの始点と対向する終点(以下，トンネルピア)の VPN ルータアドレス(以下，トンネルピアアドレス)とを VPN ルータに自動設定する．例えば図 1 の R4(VPN ルータアドレス 10.0.4.1，図 1(i))のトンネルピアアドレスは 10.0.1.1(R1 の VPN ルータアドレス，図 1(j))と 10.0.52.1 (R2 の VPN ルータアドレス，図 1(k))となる．IP プレフィクスは VPN ルータアドレスとプレフィクス長とから一意に定まる．

3. 動的な VPN トポロジ決定における課題と従来方式の問題点

3.1 動的な VPN トポロジ決定における課題

VPN トンネル終端数は VPN ルータの搭載メモリ量に依存し，多くの市販製品では数十が上限である．このため VPN ルータ数が数十を超える場合，例えば図 1 破線枠内で R1 から R2 への VPN トポロジ上の最短経路が R1→R4→R2 となっているように，複数の VPN トンネルを経由すること(以下，マルチホップトポロジ)で VPN トンネル終端数を制限しなければならない．しかしながらこのとき，図 1 実線枠内では R1→I1→I3→I4→R4→I4→I3→I1→R2 を経由しなければならないといったように，実トポロジ上のホップ数が増加し通信遅延の増大を招く課題がある．

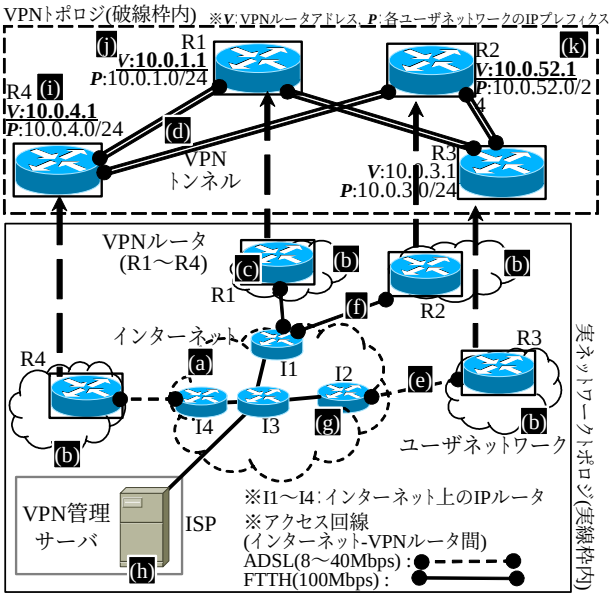

図 1 想定するネットワーク環境の例

3.2 従来方式の問題点

3.1 で先述した課題解決のため，VPN ルータに予め割当てられた IP アドレスの SHA1 ハッシュ値(ルータ ID)から，正則連結グラフの一つ de Bruijn グラフを利用し，一定次数以下のオーバーレイネットワークトポロジを決定する方式[2]が従来報告されている．しかしながら[2]は以下 2 つの問題点がある．

(1) 2 つの VPN ルータ間のホップ数の大小によらず VPN トポロジが決まるため，VPN トラヒックが多くの VPN ルータやインターネット上の IP ルータを経由し，通信遅延の増大を招く可能性がある．

(2) VPN トンネル終端数に VPN ルータのアクセス回線帯域幅が反映されないため，アクセス回線帯域幅の比較的狭い VPN ルータが多くの VPN トンネルを終端して VPN トラヒックが集中する場合があり，通信遅延の増大を招く可能性がある．

4. 遅延を考慮した VPN トポロジ決定方式

筆者らの提案方式[1]では，従来方式[2]を基本に，VPN 管理サーバによる VPN ルータアドレス決定の際，既に VPN に参加している他の VPN ルータとのホップ数や，インターネットとのアクセス回線帯域幅を考慮することにより，従来方式の問題点を解決する．以下に[1]の概要を示す．

4.1 前提

提案方式では，VPN 管理サーバとアクセス回線を同一 ISP が提供することで，実トポロジおよび VPN ルータ間のホップ数を ISP の持つ実トポロジ情報から把握することができ，また各 VPN ルータが参加を要求する際に，VPN ルータはアクセス回線帯域幅を VPN 管理サーバに通知できるものとする．

4.2 基本方針

(1) ホップ数を考慮するため，VPN 管理サーバに表 1 のような「ルータ ID 表」を新たに導入する．

VPN 管理サーバは予め全ての VPN ルータアドレス(表 1(a)列)と対応するルータ ID(表 1(b) 列)を SHA1 により求め，更に求めた全てのルータ ID について，該当するルータの次ホップとなるルータのルータ ID(表 1(c) 列)，およびそれに対応する VPN ルータアドレス(表 1(d) 列)を全て求めて記憶する．これらの値は実トポロジには依存せず，de Bruijn グラフの構築規則と SHA1 により決まる．また当該 VPN ルータアドレスの使用状態(表 1(e) 列)を運用中に更新する．

(2) アクセス回線帯域幅を考慮するため，VPN 管理サーバに VPN ルータアドレスの「ランク表」(表 2)を新たに設ける．ここで「ランク」とは，ルータ ID 表(表 1)の(d)列において，ある VPN ルータアドレスが出現した回数と定義する．ランク表の(a)列には全ての VPN ルータアドレス，(b)列には(a)列の VPN ルータアドレスのランクが列挙される．

Evaluation of Delay-Sensitive Overlay Network Topology Decision Method for VPNs, Kenji HORI, Kiyohito YOSHIHARA and Hiroki HORIUCHI, KDDI R&D Laboratories Inc.

表 1 ルータ ID 表 注:"↑"は上の欄と同じ値であることを示す.

(a) VPN ルータアドレス	(b) (a)に対応するルータ ID	(c) (b)が次ホップとするルータ ID	(d) (c)の VPN ルータアドレス	(e) 使用状態
10.0.53.1	47463cc05a2da28	47463cc05a2da28	10.0.53.1	使用中
10.0.1.1	**59857fe80456583c**	**a84848a4f0bb25c6**	**10.0.52.1**	**使用中**
10.0.52.1	**a84848a4f0bb25c6**	**a84848a4f0bb25c6**	**10.0.46.1**	**未使用**
10.0.48.1	16254c4e0765c50e	↑	↑	未使用
10.0.61.1	166bfcc5d2828421	↑	↑	未使用
10.0.32.1	166dbdc650423d16	↑	↑	未使用
10.0.11.1	323fee92c52f3194	641c122a045930d3	10.0.36.1	未使用
10.0.22.1	33eeadc575bdc041	↑	↑	使用中
...	...	...	...	...

表 2 ランク表 注:"↑"は上の欄と同じ値であることを示す.

(a) VPN ルータアドレス	(b) (a)のランク	(c) (b)に対応するアクセス回線帯域幅の範囲
10.0.53.1	9	100Mbps<
10.0.43.1	6	≦100Mbps
10.0.46.1	↑	↑
10.0.21.1	4	≦50Mbps
10.0.13.1	↑	↑
10.0.28.1	3	≦30Mbps
10.0.53.1	2	≦20Mbps
10.0.36.1	↑	↑
10.0.13.1	↑	↑
...	...	...

(c)列にはランクの値に対応するアクセス回線帯域幅の範囲が列挙される. これらの範囲は予め管理者が設定する. 例えば, VPN ルータアドレス 10.0.36.1(表 1, 2 で灰色のセル)は表 1(d)列に 2 回出現するためランクが 2 である. また管理者はランクが 2 の VPN ルータアドレスを, アクセス回線帯域幅 20Mbps 以下の VPN ルータへと割当てるように設定している(表 2 で枠線を太くしたセル).

(3)VPN 管理サーバが VPN ルータに VPN ルータアドレスを割当てる際に適用する, VPN ルータアドレス決定規則(下記)の優先度を管理者は予め決定し VPN 管理サーバに入力する.

(規則 1**)**既に参加している VPN ルータの中から, 4.1 で述べた実トポロジ情報により, 参加を要求する VPN ルータと実トポロジにおけるホップ数がなるべく近いものを求める. これを次ホップとする未使用の VPN ルータアドレスをルータ ID 表から求めて, 参加を要求する VPN ルータに割り当てる.

(規則 2**)**ランク表より, VPN ルータのアクセス回線帯域幅と対応したランクを持つ, 未使用の VPN ルータアドレスを一つ決定して割当てる.

5. シミュレーションによる評価

提案方式が決定するトポロジの有効性を, ホップ数と VPN トンネル終端数の観点から, シミュレーションにより従来方式と比較評価する. シミュレータソフトウェアには ns2 を用いる.

5.1 評価方法

評価は図 1 と同様に VPN ルータとインターネットが接続された実トポロジを用いて行った. ただし, インターネット内の IP ルータ数を増やしてランダムに接続し, インターネット内の IP ルータ数および VPN ルータ数を変えて複数回シミュレーションを実行した. これらを含めたシミュレーション条件を表 3 に示す. 測定方法は以下の通りである.

(1) シミュレーション開始以降, 一度に一台の VPN ルータを順次 VPN に参加させる.

(2) 全 VPN ルータの参加完了後, 全 VPN ルータ間について実トポロジ上でのホップを求め, その平均値を求める. さらに全 VPN ルータについて VPN トンネル終端数を求める.

5.2 評価結果

図 2 は, 実トポロジ上のホップ数が, 従来方式に比して提案手法では何%削減されたかを示している. 図 2 より, 従来方式に比して提案方式は 5〜14%程度, 実トポロジ上のホップ数を削減する効果が確認できる. 削減度合いはインターネット内のルータ数が 128 の時に顕著(10〜14%)であるが, 512 の場合は 5〜9%とやや効果が少ない. これは提案方式ではある二台の VPN ルータ間のホップ数を重視してトンネルピアを決定するため, 一部の VPN ルータ間のホップ数が遠くなる場合もあり, インターネット内のホップ数の増大が原因と考えられる.

一方, VPN ルータ数の増加に対しては削減度合いが次第に増加する傾向にある. これはトンネルピアとして選択可能な VPN ルータ数の増加に起因すると考えられ, 大規模な VPN に対してより大きな通信遅延削減効果が期待できる.

表 3 シミュレーション設定

VPN ルータ数	128, 512, 1024[台].
VPN トンネル終端数上限	VPN ルータ一台あたり 12[本].
アクセス回線帯域幅	10〜100[Mbps]の間でランダムに決定.
インターネット内の IP ルータ数	128, 512[台].
インターネット内 IP ルータ間接続トポロジ	インターネット内の IP ルータ数が同一の試行に対し, ランダムに生成した一つのトポロジを共通に使用.
VPN ルータアドレス形式	VPN ルータ数を上限とする自然数.
VPN ルータアドレス決定規則	アクセス回線帯域幅を優先して決定. アクセス回線帯域幅が等しい場合はホップ数により決定.

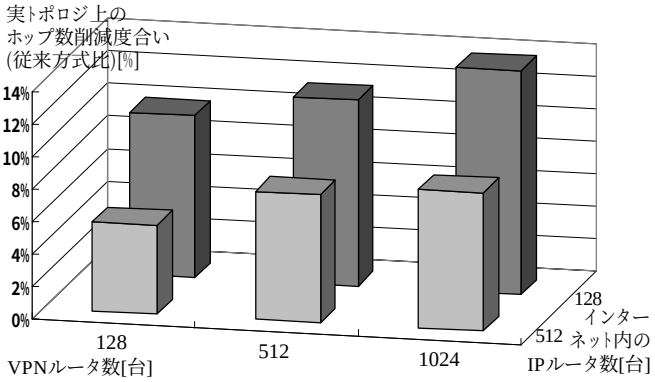

図 2 実トポロジ上のホップ数削減度合い

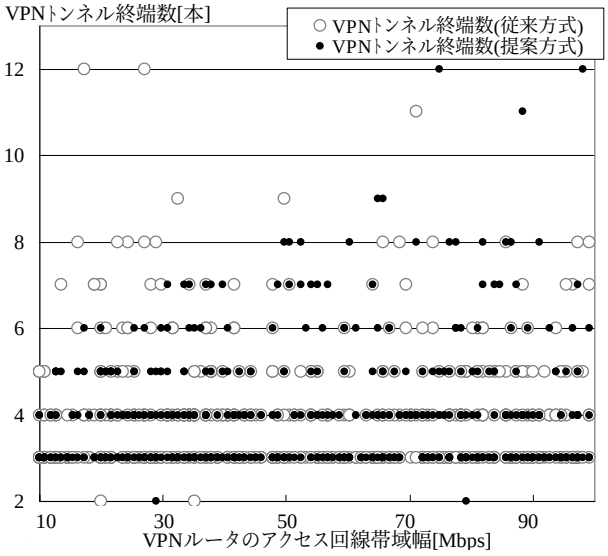

図 3 アクセス回線帯域幅に対する VPN トンネル終端数

VPN トンネル終端数の評価結果として, 紙面の制約によりインターネット上の IP ルータ数が 512, VPN ルータ数が 512 の場合の結果のみ図 3 に示す. 従来方式ではアクセス回線帯域幅によらず VPN トンネル終端数が均一となる傾向にあるのに対し, 提案方式ではアクセス回線帯域幅のより大きい VPN ルータほど多くの VPN トンネルを終端しており, 通信遅延の削減効果が期待できる.

6. おわりに

本稿では遅延を考慮した VPN トポロジ決定方式をシミュレーション評価し, ホップ数の削減効果を確認, さらにアクセス回線帯域幅を反映した VPN トンネル終端数となることを確認した. 最後に, 日頃ご指導頂く(株)KDDI 研究所秋葉所長, ならびに長谷川執行役員に感謝する. なお本研究の一部は, 総務省委託研究「ユビキタスネットワーク技術の研究開発」により実施している.

参考文献

[1] 堀他, "実 IP ネットワーク上の近接性を反映する VPN のためのオーバーレイネットワークトポロジ決定方式, " FIT2005 講演論文集 L-031, pp.73-74 , Sep.2005.

[2] F. Kaashoek and D. Karger, "Koorde: A simple degree-optimal distributed hash table," In Proc. of 2nd IPTPS, Berkeley, CA, Feb. 2003.