L-031

実 IP ネットワーク上の近接性を反映する VPN のためのネットワークトポロジ決定方式

A Proximity-Aware Overlay Network Topology Management Method for VPNs

堀 賢治† 吉原貴仁† 堀内 浩規†
Kenji Hori Kiyohito Yoshihara Hiroki Horiuchi

1. はじめに

個人や企業が迅速，容易かつ安全に遠隔共同作業をできるようにするため，利用者の要求に応じてインターネット上にオーバレイネットワークとして動的に構築される VPN (Virtual Private Network, 仮想専用網)が期待されている．この際，VPN ルータ数が変化しても VPN 内の到達性を維持するため，VPN ルータの VPN トンネル(仮想経路)終端数を一定数以下に抑えながら，VPN のトポロジを決定する必要がある．これに対し次数(VPN ルータに接続する VPN トンネル数)が一定となる正則グラフを利用する従来方式では VPN のトポロジに実ネットワークのトポロジが反映されず通信遅延の増大を招く問題がある．そこで本稿では VPN ルータ間の通信遅延削減を図るため，ホップ数で表した近接性や回線帯域幅といった実ネットワークのトポロジを考慮してトポロジを決定する方式を新たに提案し，通信遅延の観点からシミュレーションによる提案方式の評価結果を示す．

2. 想定環境

本稿において想定するネットワーク環境の例を図 1 とともに以下に示す．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，遠隔し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，第三者が盗み見ることを困難にしたネットワークを指す．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．

また，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[1]を想定する．[1]では 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．VPN トラヒックを特定のユーザネットワークへとルーティングするために，VPN 管理サーバは当該ユーザネットワークの IP プレフィクスを持つ IP アドレス(以下，VPN ルータアドレス(図 1 の各“V”)を VPN ルータに一つ設定する．さらに当該 VPN ルータを始点とする VPN トンネルの終点となる VPN ルータアドレス(以下，トンネルピアアドレス)を設定する必要がある．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))となっている．

3. VPN トポロジ決定における課題と従来方式の問題点

3.1 VPN トポロジ決定における課題

VPN 管理サーバは参加する VPN ルータの台数を事前に知らないため，VPN ルータ参加時に動的に，VPN 内が連結となるように VPN トポロジを決定し，トンネルピアアドレスを VPN ルータに設定する．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(以下，VPN トンネル終端数)はそ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．よって 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 への最短経路が R1→R4→R2 となっているように，マルチホップトポロジを導入して VPN トンネル終端数を制限しなければならない課題がある．

3.2 従来方式の問題点

3.1 で先述した課題解決の一環として，[2]をはじめとする方式が従来報告されている．

[2]はファイル共有を目的としたオーバレイネットワークのトポロジを動的に決定する方式であるが，以下のように VPN 管理サーバによる動的な VPN トポロジ決定にも利用できる．

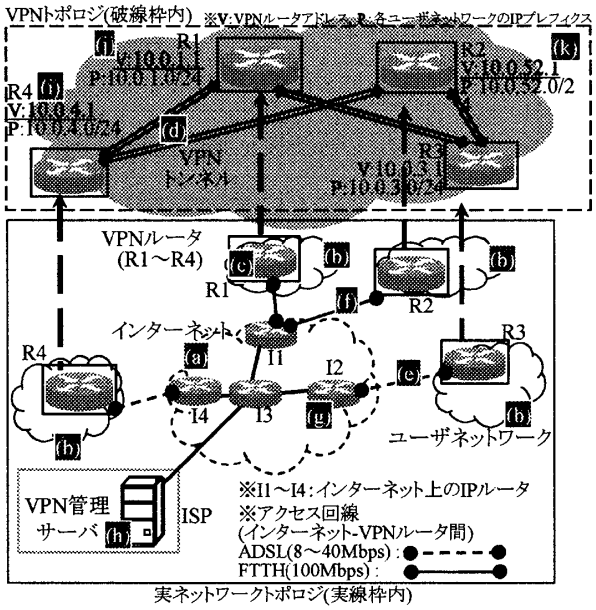

図 1 想定するネットワーク環境の例

(1) VPN 管理サーバが VPN ルータから参加要求を受信した際，まず VPN ルータに未使用の VPN ルータアドレスを割当てる．同時に VPN ルータアドレスの SHA1 によるハッシュ値(以下，ノード ID)を求め，VPN 管理サーバは VPN ルータアドレスとノード ID との対応関係を記憶する．

(2) 次数が VPN トンネル終端数の制限値以下である de Bruijn グラフを利用し，VPN トラヒックを転送すべき次ホップのノード ID を求める．求めたノード ID から，(1)で記憶した対応関係より VPN ルータアドレスを求めてトンネルピアアドレスとする．

(3) de Bruijn グラフの頂点の数に比して VPN ルータ数は殆どの場合極めて小であるため，VPN ルータアドレスとは対応関係にない頂点とノード ID が数多く存在する．各 VPN ルータはこれらを仮想的な経由 VPN ルータとして扱い，VPN トラヒックをルーティングする．

しかしながら[2]は実ネットワークを反映したトポロジ決定ができず，以下(1)，(2)の問題点がある．

(1) 2 つの VPN ルータ間の実ネットワーク上での近接性，具体的にはホップ数の大小といったパラメータによらず，ノード ID の関係だけで 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 ルータによって VPN トンネル終端数が大きくばらつく場合があり，アクセス回線帯域幅の比較的狭い VPN ルータにおいて VPN トンネル終端数が比較的大きくなるといった通信遅延を増大させる現象を招く．

4. 提案方式

提案方式では 3.2 に述べた従来方式を基本に，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 ルータとの実ネットワーク上での近接性やアクセス回線帯域幅を反映することにより，3.2 に述べた問題点を解決する．

尚，以下では VPN 管理サーバは実トポロジおよび 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 ルータの参加要求の際にアクセス回線帯域幅を通知可能であるものとする．

4.1 実ネットワーク上での近接性の反映方式

実ネットワーク上での近接性を反映するために，まず VPN 管理サーバに表 1 のような「ノード 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)と対応するノード ID(表 1(b)列)を SHA1 により求め，更に求めた全てのノード ID について，これが次ホップとするノード ID(表 1(c)列)，およびそれに対応する VPN ルータアドレス(表

†(株)KDDI 研究所 (KDDI R&D Laboratories Inc.)

表1 ノードID表

(a) VPN ルータ アドレス	(b) (a)に対応する ノードID	(c) (b)が次ホップとするノード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

(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	↑	↑
...	...	...

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)を運用中に記録する.

次にVPNルータから参加要求を受信したVPN管理サーバは, 既に参加しているVPNルータの中から, 予め把握している実トポロジの情報を利用して, 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, これを次ホップとする未使用のVPNルータアドレスをノードID表から求めて, 参加を要求するVPNルータに割り当てる.

例えば図1のVPNトポロジにおいてVPNルータR2だけがVPNに未参加であり, 今VPN管理サーバはR2から参加要求を受信したとする. この場合, R1, R3, R4の中ではR2が実トポロジにおいてR1に最も近い. このためVPN管理サーバはR1のVPNルータアドレス10.0.1.1(表1"★")が次ホップとする未使用のVPNルータアドレス10.0.52.1(表1"☆")を決定しR2に割当てる. この結果, R1とR2の間にVPNトンネルが接続される.

これによって実ネットワークのホップ数がより小さいVPNルータ間にVPNトンネルが多く接続されるため, 多くのVPNトラヒックはより少数のVPNルータやインターネット上のIPルータを経由してルーティングされるようになり, 通信遅延の削減効果が期待できる.

4.2 アクセス回線帯域幅の反映方式

アクセス回線帯域幅が比較的大きいVPNルータ程, 実際のVPNトンネル終端数がより多くなるようにするために, まず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, ノード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.

(c)列には管理者が予め設定する, あるランクの値を持ったVPNルータアドレスを割当てるに相応しいVPNルータのアクセス回線帯域幅の範囲が列挙される. 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.

次にVPNルータから参加要求を受信したVPN管理サーバは, 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. これにより, アクセス回線帯域幅の狭いVPNルータほど少数の, 広いVPNルータほど多数のVPNトンネルが終端され, 通信遅延の削減効果が期待できる.

尚, 4.1の方式と4.2の方式とのどちらを優先するかは, 管理者が予め決定してVPN管理サーバに入力する.

表3 シミュレーション設定

VPNルータ数	64, 128, 256, 512[台]
VPNトンネル終端数上限	VPNルーター台あたり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	1024[台]
インターネット内IPルータ間回線帯域幅	すべて1[Gbps]
インターネット内IPルータ間接続トポロジ	ランダムに生成した一つのトポロジを全ての試行で共通に使用
VPN管理サーバ⇔インターネット間回線帯域幅	1[Gbps]
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近接性により決定.

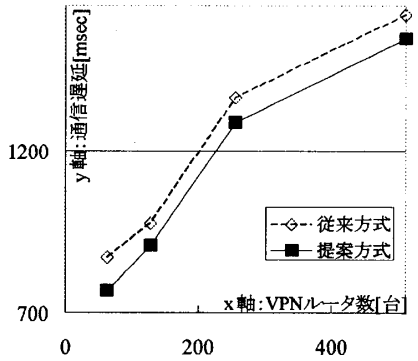

図2 通信遅延の評価結果

5. シミュレーションによる評価

提案方式により通信遅延がどの程度削減されたか確認するため, シミュレータソフトウェアns2を用いて評価を行った.

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, VPNルータ数を変えて複数回行った. ただし大規模なネットワークを模すためインターネット内部のIPルータ数を増やし, ランダムな接続トポロジとした. 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後, 一度に1台, 0.2から4秒までのランダムな時間間隔で各VPNルータをVPNに参加させる.
(2) 全てのVPNルータから同時に, ランダムに決定する他のVPNルータ1台へと, 1秒間隔で10回, 1500bytesの測定用パケットを送信する.
(3) 1個の測定用パケットが送信開始されてから, 受信完了するまでの時間を測定する.
(4) 10秒毎に送信先VPNルータを切替える.
(5) (4)の送信先の切替え回数がVPNルータ数に等しくなった時点で測定終了とする.
(6) (5)の全ての測定結果について平均値を求める.

5.2 評価結果

図2に示した評価結果より, 3.1に示した従来方式に比して提案方式は5～12%程度の通信遅延を削減できることが分かる. 特にVPNトンネル終端数のばらつきが大きい, VPNルータ数が256までの範囲では従来方式と提案方式との差は相対的に大きくなる傾向にある.

6. おわりに

本稿では実ネットワークのトポロジを反映するVPNトンネルトポロジ決定方式を新たに提案し, シミュレーション評価によって通信遅延の削減効果を確認した. 最後に, 日頃ご指導頂く(株)KDDI研究所浅見所長, 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, "パーソナル用途向けインターネットVPNの自動設定方式," FIT2004講演論文集 L-010, Sep.2004.
[2] F. Kaashoek and D. Karger, "Koorde: A simple degree-optimal distributed hash table," In Proc. of 2nd IPTPS, Berkeley, CA, Feb. 2003.