LL-008

階層型VPNにおけるQoSおよびアクセスポリシを考慮した経路選択手法

A Routing Method Considering QoS and Access Policy on Hierarchical Virtual Private Networks

岡山 聖彦† 山井 成良† 河野 圭太† 石橋 勇人‡ 松浦 敏雄‡

Kiyohiko Okayama Nariyoshi Yamai Keita Kawano Hayato Ishibashi Toshio Matsuura

1 まえがき

インターネットを介して自組織のネットワークに安全にアクセスするための技術として，仮想プライベートネットワーク (Virtual Private Network，以下 VPN という) が注目されている．ネットワーク接続型 VPN の場合，組織内など同一のアクセスポリシを持つ範囲を VPN ドメインと呼び，VPN ドメインを跨る通信を制御する VPN ゲートウェイ (以下，VGW という) を設置する．組織外にあるクライアントは，VGW との間に VPN リンクを確立することにより，VPN ドメイン内部のサーバと通信することが可能になる．本論文では，特に，VPN ドメインが組織の構造に合わせて階層的に構成されるようなネットワーク (以下，階層型 VPN という) を議論の対象とする．

階層型 VPN において，組織外にあるクライアントが組織内にアクセスするためには，最も外側の VPN ドメインから内側に向かって各階層の VGW を順に辿る必要がある．このとき，大規模な組織では，各地に分散する支社ごとに VGW を置いたり，管理者のみがアクセス可能な VGW を一般ユーザとは別に設けるなど，1 つの VPN ドメインに複数の VGW を設置する場合が考えられる．この場合，クライアント–サーバ間には複数の経路が存在することになるが，効率のよい通信を行うためには，各 VGW のアクセスポリシ (アクセスの可否) を考慮した上で，ユーザ (クライアント) にとって最適な QoS(Quality of Service) を持つ経路を選択する必要がある．階層型 VPN に対応できる既存の VPN リンク確立方式としては，SOCKS5[1] の多段プロキシ機構や SOCK プロトコルバージョン 5 の拡張方式 [2]，仮想パス方式 [3] などがあるが，いずれの方式もこのような機能を持たない．

そこで本論文では，QoS およびアクセスポリシを考慮した経路選択手法を提案する．提案法では，クライアントのアクセス要求を起点に，サーバまでの経路の QoS 情報 (RTT や利用可能帯域など) を収集する．階層型 VPN では，クライアントや各 VGW が直接通信できるのは隣接する VGW までであるため，提案法では，組織の階層構造に従ってバケツリレー方式で QoS 情報の要求メッセージを伝達することにより，クライアントがサーバまでの QoS 情報を収集し，ユーザの要求する QoS に応じた経路選択を行う．このとき，QoS 情報を収集する段階で各 VGW の持つアクセスポリシを参照することにより，QoS だけでなく，VGW 毎に設定されたアクセスポリシを適切に反映した経路選択を可能にする．

以下，本論文が前提とするネットワーク環境について述べた後，提案法の概要と，試作システムの実装と動作確認実験について述べる．

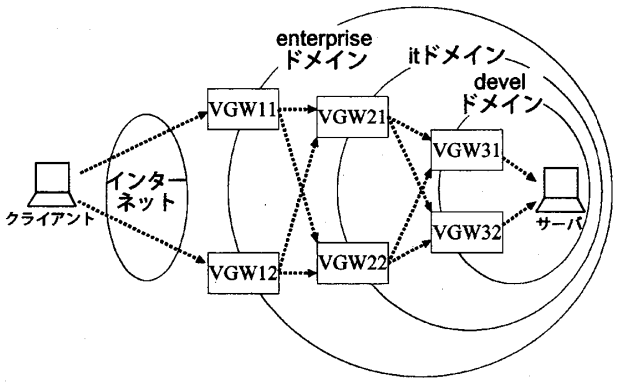

図 1: 階層型 VPN の構成例

2 前提とするネットワーク環境

図 1に，本論文が対象とする階層型 VPN の例を示す．階層型 VPN では，クライアントおよび VGW が直接アクセスできるのは隣接する VGW のみであるため，クライアントが最も内側の VPN ドメインにあるサーバにアクセスするには，クライアントからサーバに至るまでの間にある VGW を 1 つずつ辿る必要がある．通常，VGW は VPN ドメインに 1 つ設置されるが，1 章で述べたように，ネットワーク上の距離を考慮して VPN ドメインへの入口となる VGW を複数設けたり，ユーザごとに複数の VGW を用意する (例えば，一般ユーザ用と管理者用) など，1 つの VPN ドメインに複数の VGW が設置される場合がある．例えば図 1のように，各 VPN ドメインに 2 つの VGW を配置した場合，クライアントからサーバに至るまでに通過する VGW の組合せは 8 通りとなる．本論文では，このような構成の階層型 VPN を前提とし，以下，クライアントがサーバにアクセスするために辿る VGW の組を経路といい，隣接する区間 (クライアント–VGW 間，VGW–VGW 間および VGW–サーバ間) をリンクという．

一般に，クライアント–サーバ間に複数の経路が存在する場合，QoS は選択する経路によって異なる．また，QoS の指標には RTT(Round Trip Time) や利用可能帯域，コストなどさまざまなものがあるが，どれを重視するかはユーザによっても異なる．このため，図 1のように複数の経路が存在する場合には，アクセスポリシの制限によってクライアントのユーザがアクセス不可能な VGW を除いた上で，残った経路の中からユーザが重視する QoS の指標に基づいて最適なものを選択する必要があるが，階層型 VPN に対応可能な既存の VPN リンク確立方式 [1, 2, 3]) はこのよう

†岡山大学, Okayama University

‡大阪市立大学, Osaka City University

な機能を持たない‡.

一方，関連研究として，QoSを考慮した経路制御手法はアドホックネットワークの分野でも研究されており，隣接するホスト(端末)間で情報交換を行いながら，複数のQoS指標に基づいて経路を制御する手法[4]などが提案されている．しかし，このような手法はホスト単位での経路制御を目的としているため，ユーザごとに選択可能な経路が異なるようなネットワーク環境は想定しておらず，また，ユーザの要求するQoSに基づいた経路選択も考慮されていない．

3 QoSおよびアクセスポリシを考慮した経路選択手法

本章では，まず，提案法の基本であるバケツリレー方式によるQoS情報の収集方法について述べた後，これにアクセスポリシを反映させる方法と，QoS情報の収集に必要な通信量を抑制する方法について述べる．最後に，提案法の動作例について述べる．

3.1 QoS情報の収集

2章で述べた階層型VPNでは，特殊な設定(例えばファイアウォールに穴を開けるなど)を施さない限り，直接通信可能なのは隣接するVPNドメインのVGW間のみである．QoSを考慮した経路選択を行うためには，経路上の全リンクのQoS情報が必要であるため，提案法では，クライアントを起点として，QoS情報の要求メッセージ(以下，QoS要求)を隣接するVGWによるバケツリレー方式で最も内側のVGWに送信する．このとき，隣接するVGWが複数ある場合には，同一のQoS要求をすべてのVGWに送信する．一方，要求メッセージを受信した経路上の各VGWは，応答メッセージ(以下，QoS応答)として直下のVPNドメインとの間のリンクに関するQoS情報を上位のVGWを介してクライアントに返す．これにより，クライアントは全経路の全リンクのQoS情報を得るので，ユーザが重視するQoSの指標に基づいて最適な経路を決定することができる．

一方，各リンクのQoS情報を収集する方法としては，各VGWが定期的に計測する方法と，クライアントのアクセス時に計測する方法がある．前者は長期的なトラフィックの傾向(曜日ごとのトラフィックの特徴や1日のトラフィック変動など)を把握する場合に有効であるが，短時間のトラフィック変動を計測しようとすると計測のためのパケットを数多く送受信しなければならないため，場合によってはリンクに大きな負荷がかかる．このため，提案法では，QoSの値をクライアントのアクセス開始時に計測するものとし，計測手段として文献[5, 6]のバックボーン選択手法を利用する．

このバックボーン選択手法では，複数のバックボーンネットワークに接続されたマルチホームネットワークにおいて，対外接続ルータが組織内部のクライアントから送信されたTCPコネクション確立のためのSYNパケットを複製し，すべてのバックボーンを経由して目的のサーバに送信する(利用可能帯域を計測する場合には，連続した2つのSYNパケットを送信する)．そして，サーバから各バックボーンを経由して返された応答パケットのRTTや間隔などから，クライアントのアクセス開始時点でのネットワーク状態に基づいて適切なバックボーンを選択するというものである．したがって，提案法の場合には，クライアントあるいはVGWが隣接する複数のVGWに対して連続した2つのSYNパケットを送信すれば，必要最小限のパケットを用いて各リンクのRTTおよび利用可能帯域を計測することができる．ただし，途中のリンクやVGWが故障している場合などを考慮し，SYNパケットの送信後，一定時間応答のないVGWは除外してQoS要求を送信する．この場合，クライアントは応答のないVGWが接続されたリンクを除外して経路選択を行うことになる．

なお，原理上はQoS応答メッセージにさまざまな指標を付加することが可能であるが，文献[5, 6]のバックボーン選択手法で計測できるのはRTTおよび利用可能帯域のみであるため，本論文ではQoSの指標としてこの2つを扱うものとする．以下，各リンクにおけるRTTおよび利用可能帯域の値の組をリンクコストという．

3.2 アクセスポリシを考慮した経路選択と通信量の抑制

アクセスポリシ，すなわち，VGWがユーザ(クライアント)のアクセス可否を判断するためには，通常はユーザ認証により本人確認を行った上で，ユーザ名に基づいてVGWが保持するアクセスポリシデータベースを参照する．しかし，一般的にユーザ認証には暗号技術が用いられており，経路上のすべてのVGWでユーザ認証を行うと暗号化および復号処理に伴ってユーザの待ち時間が大きくなるため，提案法では，3.1節で述べたQoS要求にクライアントのユーザ名を付加し，これを受信したVGWはそのユーザ名に基づいて，ユーザ認証を行うことなくアクセスの可否を判断するものとする．このとき，アクセスを拒否する場合はその旨をQoS応答として返すとともに，下位のVGWにはQoS要求を送信しない．これにより，アクセスを拒否するVGWを起点とした無駄な要求メッセージを削減することができるだけでなく，クライアントはアクセス不可能なVGWを経由する経路を選択肢から取り除くことができる．なお，VGWでのユーザ認証は経路選択後のVPNリンク確立時に行うため，安全性への影響はないと考えられる．

また，同一VPNドメインに複数のVGWが配置されている場合，3.1節で述べたQoS情報の収集方法を単純に適用すると，直下のVGWは同一クライアントからのQoS要求を，複数のVGWから受信することになる．例えば，図1において，VGW21はVGW11およびVGW12から同一クライアントによるQoS要求を受け取ることになるが，QoS要求が到着する毎に直下のVGWに対してQoS要求を送信するのはトラフィックの無駄である．特に，図1のようにすべてのVPNドメインに複数のVGWが配置されている場合には，同一のQoS要求が指数関数的に増加することになる．このため，(クライアント，サーバ，ユーザ)の3つ組みが同一であるQoS要求をVGWが短期間に重複して受信した場合には，後に受信したQoS要求の処理は行わず，先に受信したQoS要求に対するQoS応答のコピーを送信元に返すものとする．これにより，あるVGWが受信するQoS要求は高々直上VPNドメインのVGW数となり，QoS要求の増加を抑えることができる．

‡SOCK5をベースとする方式は1つのVPNドメインに複数のVGWを登録できるが，耐故障性の向上が目的である．

3.3 動作例

提案法に基づくクライアントおよびVGWの動作例を示す．ネットワークの構成は図1と同一であるものとし，アクセスポリシとして，VGW22のみがユーザokayamaのアクセスを拒否，それ以外のVGWはアクセスを許可するように設定されているものとする．このような構成において，ユーザokayamaが組織外から内部のサーバにアクセスする場合の手順は以下のようになる．

1. クライアントは，VGW11およびVGW12に対して連続した2つのSYNパケットを送信してリンクコストを計測する．そして，各VGWから最初に返ってきた応答パケット(SYN+ACK)を利用してコネクションを確立し，ユーザ名okayamaを含むQoS要求を送信する．このとき，コネクション確立に使用しない応答パケットに対しては，リセットフラグ付きのパケット(RST)を送信することにより，コネクションを強制切断する．
2. VGW11は，QoS要求に含まれるユーザ名を用いて自己のアクセスポリシデータベースを検索し，アクセス許可という結果を得る．そこでVGW11は，クライアントと同様にしてVGW21およびVGW22との間のリンクコストを計測し，各VGWにQoS要求を転送する．

   一方，VGW12もVGW11と同様に動作するが，以降では，VGW11のQoS要求がVGW12よりも早くVGW21およびVGW22に送信されたものとする．
3. VGW11からのQoS要求を受信したVGW21は，VGW11と同様にして，VGW31およびVGW32との間のリンクコストを計測し，QoS要求を転送する．遅れて到着したVGW12からのQoS要求はVGW11からのQoS要求と同一であるため処理を保留し，リンクコストの計測とQoS要求の転送は行わない．

   一方，VGW22もVGW11からのQoS要求を受信するが，アクセスポリシデータベースの検索によりアクセス拒否という結果を得るため，即座にQoS応答(アクセス拒否)を返してVGW11とのコネクションを切断する．遅れて到着したVGW12からのQoS要求も同様に処理する．
4. VGW21からのQoS要求を受信したVGW31およびVGW32は，それぞれ，サーバとの間のリンクコストを計測し，結果をQoS応答としてVGW31に返す．
5. VGW31およびVGW32からのQoS応答を受信したVGW21は，QoS応答のメッセージに手順3で計測したリンクコストを付加し，VGW11およびVGW12に送信する．
6. VGW21からのQoS応答を受信したVGW11およびVGW12は，自身のリンクコスト計測結果をメッセージに付加してクライアントに返す．

以上の手順が完了した段階で，クライアントが計測したリンクコストを加えると，クライアント(ユーザokayama)が選択可能なすべてのリンクコストが得られる．例えば，図2のようなリンクコストが得られたとすると，RTTを重視する場合はVGW11–VGW21–VGW31、利用可能帯域を重視する場合はVGW12–VGW21–VGW32を経由すればよいことがわかるので，ユーザがどちらを重視するかによっていずれかの経路を決定すればよい．

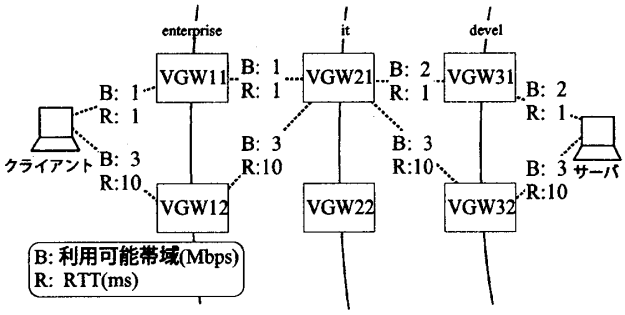

図2: リンクコストの収集結果(例)

4 実装と動作確認

4.1 実装の概要

提案法の実装は，仮想パス方式(文献[3])のクライアントおよびVGWをベースに行った．仮想パス方式はSOCK5のSOCKクライアントおよびSOCKサーバ(VGW)を拡張したものであり，SOCK5のVPNリンク確立方法を変更するとともに，隣接するVGWのIPアドレスをDNSから自動的に得るという改良が施されている．今回は，仮想パス方式のSOCKクライアントおよびSOCKサーバに対して，以下の機能を追加した．

- リンクコスト計測機能
- リンクコスト収集機能
- リンクコストに基づいた経路選択機能

リンクコスト計測機能については，文献[6]のバックボーン選択方法を利用して，クライアントおよびVGWが隣接するVGWとのコネクション確立時に連続する2つのSYNパケットを送信し，最初に送信したSYNパケットと対応する応答(SYN+ACK)パケットの時間間隔をRTT，2つの応答パケットの時間間隔を利用可能帯域とみなした．

リンクコスト収集機能は，隣接するVGWとのコネクション確立後，クライアントのユーザ名を含むQoS要求をバケツリレー方式で送信し，逆の順序でQoS応答をクライアントに返すものである．このとき，3.2で述べたように，各VGWではユーザ名に基づいてアクセス可否を判断し，アクセス不可能なVGWを通るリンクは経路選択から除外するとともに，重複する2番目以降のQoS要求に対しては，最初のQoS要求に対するQoS応答をそのまま返すようにした．なお，収集したリンクコストのクライアントにおける計算方法としては，QoSの指標(RTTおよび利用可能帯域)ごとに重み付けを行った上で，両方を考慮したコスト計算を行うことも考えられるが，今回は単純な方法として，優先するQoSの指標をあらかじめユーザが指定するものとした．すなわち，まず優先するQoSのみを用いて経路の比較を行い，複数の候補が残った場合にはもう一方のQoSを用いて比較する(さらに複数の候補が残った場合はランダムに選択)．

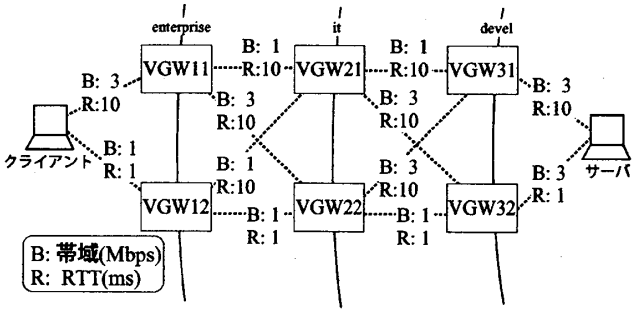

図 3: リンクの QoS パラメータ設定

最後のリンクコストに基づいた経路選択機能はこれまでに述べていないが，VPN リンク確立時に，クライアントが決定した経路に基づいて VGW を辿るために必要である．具体的には，経路決定後のクライアントによる VPN リンク確立時のメッセージに経路情報 (接続すべき VGW の順序) を付加し，VGW はこれに従って次に接続すべき VGW を決定するようにした．

4.2 動作確認実験

提案法の動作を確認するため，図 1とほぼ同様の構成を持つ実験ネットワークを構築し，リンクごとに異なる QoS パラメータを設定して動作確認実験を行った．クライアント，VGW，サーバとして FreeBSD 4.X を搭載する PC/AT 互換機を使用し，各計算機は 100Base-TX の Ethernet で接続した．なお，提案法の実装は仮想パス方式をベースとしているため，VPN ドメイン名から VGW の IP アドレスを得るための DNS サーバや，ユーザ認証に利用する Kerberos の鍵配布サーバ (KDC:Key Distribution Center) などを VGW と同じ計算機で動作させているが，今回の実験ではこれらのサーバに同時にアクセスすることはないので，実験結果に影響を与えることはないと考えられる．

一方，リンクごとに異なる QoS パラメータを与えるため，FreeBSD の dummynet 機能 [7] を利用して，図 3のようにリンクの RTT と帯域を設定した．今回の実験では，同時に複数のクライアントを実行してないため，図 3に示した各リンクの RTT および帯域の値が，リンクコスト計測時の RTT および利用可能帯域となる．

実験方法としては，クライアント上で SOCK クライアントを用いて起動した echo クライアントが，サーバ上の echo サーバに接続する．このとき，SOCK クライアントおよび各 VGW は，3章で述べた経路選択方法に基づいて経路を決定し，その後，仮想パス方式に従って VPN リンクを確立してから，echo クライアントと echo サーバの間で TCP コネクションを確立する．echo クライアント起動時に，ユーザ okayama が優先する QoS 指標として，RTT および利用可能帯域を指定した場合のそれぞれについて 100 回の試行を行い，各試行において選択された経路を調査した．

実験結果は，RTT を優先する QoS 指標として指定した場合，100 回の試行すべてにおいて RTT が最も小さな VGW12–VGW22–VGW32 という経路が選択され，利用可能帯域を指定した場合には，100 回の試行すべてにおいてボトルネックとなるリンクの帯域が最も大きな VGW11-VGW21-VGW31 という経路が選択された．さらに，クライアントおよび VGW のアクセスログを解析することにより，VGW22 のアクセスポリシとしてユーザ okayama のアクセスを拒否するように設定した場合には，VGW22 に接続されたリンクのコストは収集されていないことも確認した．

以上のことから，今回の動作確認実験の範囲では，ユーザが重視する QoS 指標だけでなく，各 VGW に設定されたアクセスポリシも考慮した経路選択を行っていると言える．

5 あとがき

本論文では，階層型 VPN において，QoS およびアクセスポリシを考慮した経路選択手法を提案した．これにより，階層型 VPN において複数の経路がある場合，アクセスする時間および場所によって変化する QoS だけでなく，各 VGW のアクセスポリシを適切に反映した経路選択が可能となる．

今後の課題としては，ネットワークのトラフィックが動的に変化する環境における詳細な性能評価や，VPN リンク確立後の経路方法の検討などが挙げられる．提案法では，VPN リンク確立時に決定した経路は VPN リンク切断まで変更できないが，VPN リンク確立後のネットワークの状態変化に応じて動的に経路を変更できれば，より効率的な通信が行えると考えられる．

謝辞

本研究の一部は，総務省戦略的情報通信研究開発推進制度 (特定領域重点型研究開発プログラム，課題番号 041108001) の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] NEC: *SOCKS Home Page*, http://www.socks.nec.com/index.html.

[2] Kayashima, M., Terada, M., Fujiyama T. and Ogino T.: *SOCKS V5 Protocol Extension for Multiple Firewalls Traversal*, Internet Draft (1997). draft-ietf-aft-socks-multiple-traversal-00.txt.

[3] 岡山聖彦, 山井成良, 金出地友治, 石橋勇人, 安倍広多, 松浦敏雄: 階層型 VPN のための LDAP サーバを用いた経路制御手法, 情報処理学会論文誌, vol.45, no.01, pp.46–55 (2004).

[4] Badis, H., Munaretto, A. and Pujolle, K.: "QoS for Ad hoc Networking Based on Multiple Metrics: Bandwidth and Delay", http://qolsr.lri.fr/.

[5] 岡山聖彦, 山井成良, 島本裕志, 宮下卓也, 岡本卓爾: マルチホームネットワークにおける透過的な動的トラヒック分散, 情報処理学会論文誌, vol.41, no.12, pp.3255–3264 (2000).

[6] 岡山聖彦, 山井成良, 宮下卓也: マルチホームネットワークにおける帯域を考慮したバックボーン選択手法, 情処研報, 2002-DSM-27, pp.1–6 (2002).

[7] Luigi Rizzo, "DUMMYNET", http://info.iet.unipi.it/ luigi/ip_dummynet/.