社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

AIMD 型のウィンドウフロー制御を利用した IP-VPN 公平性制御機構

本田　治† 大崎　博之†† 今瀬　真†† 村山　純一††† 松田　和浩†††

† 大阪大学 大学院基礎工学研究科
〒 565-0871 大阪府吹田市山田丘 1-5
†† 大阪大学 大学院情報科学研究科
〒 565-0871 大阪府吹田市山田丘 1-5
††† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
〒 180-8585 東京都武蔵野市緑町 3-9-11
E-mail: †o-honda@ics.es.osaka-u.ac.jp, ††{oosaki,imase}@ist.osaka-u.ac.jp,
†††{murayama.junichi,matsuda.kazuhiro}@lab.ntt.co.jp

あらまし　近年，既存の IP ネットワークを利用して仮想的な専用線を実現する，IP-VPN (IP-based Virtual Private Network) が注目を浴びている．しかし，従来の IP-VPN では，IP-VPN の顧客間の公平性が保証されないという問題点がある．そこで本稿では，公平な IP-VPN サービスを低コストで実現するための，IP-VPN 公平性制御機構 I2VFC (Inter- and Intra-VPN Fairness Control) を提案する．提案する I2VFC は，入線側と出線側のプロバイダエッジルータの間で，AIMD (Additive Increase and Multiplicative Decrease) 型のウインドウフロー制御を行い，VPN 間公平性を実現する．提案する I2VFC は，VPN 間公平性の基準を，IP-VPN のサービスプロバイダが自由に規定できること，また，プロバイダエッジルータのみを変更するだけでよく，既存の IP ネットワークへ容易に導入できるという点が特徴である．
キーワード　IP-VPN (IP-based Virtual Private Network)，公平性，ウインドウフロー制御，AIMD (Additive Increase and Multiplicative Decrease)

On IP-VPN Fairness Control Mechanism using AIMD Window Flow Control

Osamu HONDA†, Hiroyuki OHSAKI††, Makoto IMASE††, Jyunichi MURAYAMA†††, and Kazuhiro MATSUDA†††

† Gradauate School of Engineering Science, Osaka University
†† Graduate School of Infomation Science and Technology, Osaka University,
Yamadaoka 1-5, Suita, Osaka 565-0871, Japan
††† NTT Information Sharing Platform Laboratories, NTT Corporation,
3-9-11 Midori-cho, Musashino, Tokyo 180-8585, Japan
E-mail: †o-honda@ics.es.osaka-u.ac.jp, ††{oosaki,imase}@ist.osaka-u.ac.jp,
†††{murayama.junichi,matsuda.kazuhiro}@lab.ntt.co.jp

Abstract　In recent years, IP-VPN (IP-based Virtual Private Network) that realizes a virtual dedicated line on the existing IP network has been capturing the spotlight. However, in the conventional IP-VPN, there is a problem that the fairness among IP-VPN customers is not guaranteed. In this paper, we therefore propose an IP-VPN fairness control mechanism called I2VFC (Inter- and Intra-VPN Fairness Control) for realizing a fair IP-VPN service at low cost. Our I2VFC performs an AIMD (Additive Increase and Multiplicative Decrease) window flow control between ingress and egress provider edge routers and realizes fairness among VPNs. Notable features of our I2VFC includes that with our I2VFC IP-VPN service provider can freely specify fairness criteria and that our I2VFC can be easily deployed to existing IP networks since modification only to provider edge routers are necessary.
Key words　IP-VPN (IP-based Virtual Private Network), Fairness, Window Flow Control, AIMD (Additive Increase and Multiplicative Decrease)

1 はじめに

近年，既存の IP ネットワークを利用して仮想的な専用線を実現する，IP-VPN (IP-based Virtual Private Network) [1-4] が注目されている．IP-VPN を用いることにより，従来の専用線に比べてはるかに安価に，仮想的な専用回線を IP ネットワーク上

に構築することができる．しかし，既存の IP-VPN は，IP-VPN の顧客間の公平性が保証されないという問題点がある．これは，IP ネットワークがベストエフォート型のネットワークであるため，IP-VPN もベストエフォート型のネットワークとなるからである．

しかし現実には，IP-VPN のサービスプロバイダは，公平な IP-VPN サービスを提供することが求められている．近年，IP ネットワークのトラヒックエンジニアリング技術に関しては，さまざまな研究が行なわれている．しかし，既存のトラヒックエンジニアリング技術は，公平な IP-VPN サービスの実現には適さない．そこで本稿では，公平な IP-VPN サービスを低コストで実現するための，IP-VPN 公平性制御機構を提案する．

本稿では，文献 [1-4] で提案されている PPVPN (Provider Provisioned VPN) のフレームワーク上で，公平な IP-VPN サービスを，できるだけ低コストで実現することを目標とする．既存の IP-VPN では，IP ネットワークがベストエフォート型のネットワークであるために，あるある VPN が大量のトラヒックを発生させた場合に，他の VPN のスループットが不当に低く抑えられるという問題が発生する．本稿では，コアネットワークには，低コストな既存の IP ネットワークをそのまま利用し，エッジルータ間でウィンドウフロー制御を行うことにより，公平な IP-VPN サービスを実現する手法を提案する．IP-VPN サービスが公平であるとは,「VPN 間公平性」 (inter-VPN fairness) (VPN を契約している顧客間の公平性) および「VPN 内公平性」 (intra-VPN fairness) (同じ VPN に収容されている利用者間の公平性) の両方が満たされていることと定義する．以下では，まず，VPN 間公平性および VPN 内公平性について説明する．

VPN 間公平性とは，VPN を契約している顧客間の公平性を意味する．具体的には，サイト間を接続する VPN のスループット (VPN 内に収容されている全パケットの実効転送速度) の比が，IP-VPN サービスプロバイダが規定する比となっている時，VPN 間公平性が実現されているとする．本稿では，ある VPN に収容されている全パケットの流れを「VPN フロー」と呼ぶ．また，VPN フローの実効転送速度を「VPN スループット」と呼ぶ．つまり，VPN 間公平性が満たされている状態とは，VPN フローごとの VPN スループットの比が，サービスプロバイダが規定する比と一致している状態である．

VPN 内公平性とは，同じ VPN に収容されている利用者間の公平性を意味する．具体的には，同じ VPN に収容されているフロー (プロトコル種別，送信側/ 受信側 IP アドレス，送信側/受信側ポートが等しいパケットの流れ) のスループット (実効転送速度) の比が，すべて等しい値となっている時，VPN 内公平性が実現されているとする．本稿では，VPN に収容されている各パケットの流れを，単に「フロー」と呼ぶ．

本稿では，VPN 間公平性および VPN 内公平性を，低コストで実現するための，IP-VPN 公平性制御機構 I2VFC (Inter- and Intra-VPN Fairness Control) を提案する．I2VFC は，IP-VPN のサービスプロバイダの，プロバイダエッジ (PE; Provider Edge) ルータ (PE ルータ) 上で動作する，ウィンドウフロー制御である．具体的には，入口側のプロバイダエッジ (ingress PE) ルータ (入側 PE ルータ) において，VPN に収容されている複数のフローを，単一の VPN フローとして集約する．さらに，入口側のプロバイダエッジルータと，出口側のプロバイダエッジ (egressPE) ルータ (出側 PE ルータ) の間で，AIMD (Additive Increase and Multiplicative Decrease) 型のウインドウフロー制御 [5-11] を行う．提案する I2VFC は，VPN 間公平性の基準を，IP-VPN のサービスプロバイダが自由に規定できること，また，PE ルータのみを変更するだけでよく，既存の IP ネットワークへ容易に導入できるという点が特徴である．

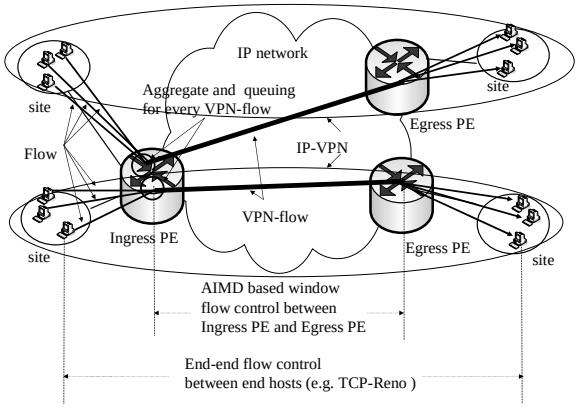

図 1: AIMD 型のウィンドウフロー制御を利用した IP-VPN 公平性制御機構 I2VFC

Fig. 1 I2VFC that realizes fair IP-VPN mechanism by utilizing AIMD window flow control

これまで，TCP のようなエンド-エンド間のフローの公平性に関しては，さまざまな検討が行われたきた [5-11]．一方，IP-VPN における VPN フロー間の公平性に関しては，これまで十分な検討が行われていない．例えば，文献 [12] では，DiffServ に対応した IP ネットワークにおいて，著者らが提案する帯域ブローカを用いることにより，VPN 間公平性を実現する手法を提案している．しかし，文献 [12] の手法では，ネットワーク上のすべてのルータ が DiffServ に対応している必要があるため，現実のネットワークに導入するためには非常にコストがかかるという問題がある．一方，我々が提案する I2VFC は，IP-VPN のサービスプロバイダの PE ルータのみを変更するだけでよく，既存の IP ネットワークへの導入も容易である．

本稿の構成は以下の通りである．まず，2 章では，AIMD 型のウインドウフロー制御の概要を説明し，その公平性について議論する．次に，3 章では，IP-VPN 公平性制御機構の設計目標を述べる．さらに，4 章において，IP-VPN 公平性制御機構 I2VFC の概要および設計目標をどのように達成しているのかを説明する．5 章では，I2VFC の動作アルゴリズムを説明する．最後に 6 章において，本稿のまとめと今後の課題を述べる．

2 AIMD 型のウインドウフロー制御

本章では，提案する IP-VPN 公平性制御 I2VFC が利用している，AIMD 型のウインドウフロー制御の概要を説明し，その公平性について議論する．

AIMD 型のウィンドウフロー制御とは，ネットワーク中で輻輳が発生していない時には，ウィンドウサイズを加算的に増加させ，ネットワーク中で輻輳が発生している時には，ウィンドウサイズを乗算的に減少させるという制御である．AIMD 型のウィンドウフロー制御のパラメータ (1 ラウンドトリップ時間あたりの，ウインドウサイズの線形増加量および乗算減少量) をそれぞれ a および b とする．例えば，AIMD 型のウィンドウフロー制御は，ウィンドウサイズを W とすれば，ネットワーク

中で輻輳が発生していない時には，ウィンドウサイズを a だけ加算的に増加させ，ネットワーク中で輻輳が発生している時には，ウィンドウサイズを $b \times W$ だけ乗算的に減少させる．

AIMD 型のウィンドウフロー制御は，TCP の輻輳回避フェーズでも採用されており，これまでに数多くの研究が行なわれている [5-11].

例えば，文献 [8] では，決定的 AIMD モデル (Deterministic AIMD model) における AIMD 型ウインドウフロー制御のスループットを導出している．決定的 AIMD モデルでは，(1) ウィンドウサイズが一定値を超えた時にのみ，ネットワーク中でパケット棄却が発生すること，かつ (2) ネットワーク中でのパケット棄却は，1 ラウンドトリップ時間中に 1 度しか発生しないこと，を仮定したモデルである．

このモデルのもと，定常状態において，AIMD 型のウィンドウフロー制御に従うフローのスループット T が，近似的に次式で与えられることが示されている．

$$T = \frac{pa(-2+b) + \sqrt{p(-2+b)a(pab - 8b - 2pa)}}{4pbR} \quad (1)$$

$$\simeq \frac{\sqrt{2-b}\sqrt{a}}{\sqrt{2b}R\sqrt{p}} \quad (2)$$

ここで，a および b は，AIMD 型のウィンドウフロー制御のパラメータである．つまり，1 ラウンドトリップ時間あたりの，ウインドウサイズの線形増加量および乗算減少量である．R はネットワークのラウンドトリップ時間，p はパケット棄却率である．

AIMD 型ウインドウフロー制御におけるフローのスループットは，AIMD 型のウィンドウフロー制御のパラメータ a および b，ネットワークのラウンドトリップ時間およびパケット棄却率で決まることがわかる．文献 [5] では，すべてのフローのラウンドトリップ時間が等しく，パラメータ a および b の値が等しく，なおかつネットワークの輻輳通知を同期して受信していれば，すべてのフローに対してボトルネックとなるリンクの帯域が公平に配分されることが示されている．このことは，式 (1) からも確認することができる．

ここで，式 (1) を違った視点から眺めてみる．すると，AIMD 型のウィンドウフロー制御を用いることにより，すべてのフローに対して帯域を公平に配分するだけでなく，「それぞれのフローに対して帯域を任意の比率で配分できる」ことが分かる．つまり，式 (1) は「ネットワークのラウンドトリップ時間 R およびパケット棄却率 p に応じて，パラメータ a および b を適切に設定すれば，フローのスループットを任意の値に制御することができる」ことを意味している．

本稿で提案する I2VFC では，このようなアイディアに基づき，入口側および出口側の PE ルータ間で，AIMD 型のウィンドウフロー制御を行い，VPN 間公平性を実現する．

3 IP-VPN 公平性制御機構の設計目標

本章では，IP-VPN 公平性制御機構の 4 つの設計目標である，

（1） VPN 間公平性 (inter-VPN fairness) を実現

（2） VPN 内公平性 (intra-VPN fairness) を実現

（3） 既存の IP ネットワークへの導入が容易

（4） 転送速度 / VPN 数に関して高いスケーラビリティを実現

のそれぞれについて議論する．

(1) VPN 間公平性 (inter-VPN fairness) を実現

第一の設計目標は，VPN を契約している顧客間の公平性を実現すること，すなわち，VPN 間公平性 (inter-VPN fairness) を実現することである．既存の IP-VPN では，基盤となる IP ネットワークがベストエフォート型のネットワークであるために，VPN 間の公平性が十分に提供されていないのが現状である．しかし，IP-VPN サービスとしては，ある VPN が大量のトラヒックを発生させた場合でも，他の VPN のスループットが不当に低く抑えられないことが望ましい．

また，IP-VPN サービスを提供するのはプロバイダであることを考えると，VPN 間の公平性の基準は，IP-VPN のサービスプロバイダが自由に規定できることが望ましい．例えば，あるボトルネックリンクを共有している複数の VPN フローに対して，均等に帯域を配分するのではなく，VPN の地理的条件 (サイト間の距離やホップ数など) や契約回線速度等に応じて配分できることが望ましい．特に，どのような公平性の基準が適しているかは，IP-VPN のサービスプロバイダごとに異なると考えられるため，IP-VPN 公平性制御機構としては，さまざまな公平性の基準に対応できることが求められる．

また，どのようなタイムスケールで公平性を実現するかも重要となる．数 10 ミリ秒〜数 100 ミリ秒といった細かな粒度での公平性が必要となるのか，それとも数十秒〜数分といった荒い粒度での公平性で十分なのかによって，IP-VPN サービスに要求される機能が大きく異なる．

本稿では，ラウンドトリップ時間の 100 倍程度のタイムスケールで，VPN 間の公平性を実現することを目標とする．これは，以下の 2 つの理由による．(1) 現在，IP-VPN 上を転送されるトラヒックの大部分がデータ系トラヒックであり，ラウンドトリップ時間の 100 倍程度のタイムスケールの公平性が実現されれば十分であること．(2) ラウンドトリップ時間オーダのタイムスケールの公平性を実現するためには，エッジルータの変更では不十分であり，コアルータにも何らかの制御機構を組込む必要がある (つまり，コストが増大する) こと．

(2) VPN 内公平性 (intra-VPN fairness) を実現

第二の設計目標は，同じ VPN に収容されている利用者間の公平性を実現すること，すなわち，VPN 内公平性 (intra-VPN fairness) を実現することである．IP-VPN サービスとして，VPN 間公平性が実現され，VPN を契約している顧客間の公平性が実現されたとしても，実際に VPN を利用している利用者間で不公平性が発生することは望ましくない．ただし，IP-VPN サービスの性質を考えると，VPN 内公平性に対する要求は，VPN 間公平性に比べて，比較的緩いものであると考えられる．一般に，ある VPN 内の利用者に対して，どのように帯域を配分するかは，VPN を契約している顧客が決定すべき内容であり，IP-VPN のサービスプロバイダは関知しない．そこで，IP-VPN 公平性制御機構としては，ある特定のフローのスループットが不当に抑えられなければ十分であると考えられる．

(3) 既存の IP ネットワークへの導入が容易

第三の設計目標は，IP-VPN 公平性制御機構が，既存の IP ネットワークへ容易に導入できることである．IP-VPN がこれだけ普及した要因として，ネットワークのインフラとして，既存の IP ネットワークがそのまま利用できるという点が挙げられる．従って，既存の IP-VPN の枠組をできるだけ変更せずに，公平な IP-VPN サービスを実現できることが望ましい．既存のネットワーク機器に対する変更を最小限に抑えることにより，公平

な IP-VPN サービスが低コストで導入できることが望ましい．

具体的には，IP-VPN のサービスプロバイダが所有する，PE ルータだけに変更を加え，既存のコアルータおよびカスタマエッジルータには変更を加えずに，IP-VPN 公平性制御機構を実現することが望ましい．これは，以下のような理由による．(1) PE ルータは，コアルータと比較すると動作速度が遅く，低コストであること，(2) 一般に，PE ルータは，IP-VPN のサービスプロバイダの管理下にあるが，コアルータは必ずしもそうではないこと，(3) カスタマエッジルータは VPN を契約している顧客の管理下にあるため，IP-VPN のサービスプロバイダの都合で変更することは事実上不可能であること．

(4) 転送速度 / VPN 数に関して高いスケーラビリティを実現

第四の設計目標は，IP-VPN 公平性制御機構が，VPN フローの転送速度および収容する VPN 数に関して高いスケーラビリティを実現することである．近年，ネットワークの高速化が急速に進んでいる．このため，各 VPN ごとに数 Gbps から数十 Gbps のスループットを実現できることが望ましいと考えられる．一方，現在は，企業や組織といった単位で，IP-VPN サービスに加入しているため，IP-VPN のサービスプロバイダが管理する VPN 数はそれほど多くない．しかし今後は，社会構造の変化に伴い，個人の利用者単位で，IP-VPN サービスに加入することも想定される．この場合，IP-VPN のサービスプロバイダが管理する VPN 数は膨大となることが予想されるため，IP-VPN 公平性制御機構が，VPN 数に関して高いスケーラビリティを持つことも重要であると考えられる．

4 IP-VPN 公平性制御機構 I2VFC

本章では，まず，本稿で提案する IP-VPN 公平性制御機構 I2VFC の概要を説明する．その後，3 章で述べた設計目標をどのように達成しているかを説明する．

4.1 I2VFC の概要

図 1 に，提案する I2VFC の概要を示す．I2VFC の核となるのは，IP-VPN のサービスプロバイダの，PE ルータ上で動作する，AIMD 型のウィンドウフロー制御である．

具体的には，入側 PE ルータにおいて，VPN に収容されている複数のフローを，単一の VPN フローとして集約し，VPN ごとの論理キューに格納する．さらに，入側 PE ルータと出側 PE ルータ間で，各 VPN ごとに管理パケットを定期的に交換することにより，ネットワークのラウンドトリップ時間およびパケット棄却率を測定する．入側 PE ルータは，これらの情報をもとに，各 VPN ごとに AIMD 型のウインドウフロー制御を行い，VPN フローからネットワークに送出されるパケット数を調整する．PE ルータ間では，ウィンドウフロー制御のみを行い，再送制御や誤り制御等は行わない．なお，上でいうところの出側 PE ルータから入側 PE ルータの方向にもパケットは転送されている．このため I2VFC では，VPN フローに対し，双方向でウインドウフロー制御を行う必要があることに注意されたい．

PE ルータにおいて，各 VPN ごとに AIMD 型のウィンドウフロー制御を行い，VPN 間公平性を実現する．特に，入側 PE ルータおよび出側 PE ルータ間で管理パケットを交換することにより，ネットワークのラウンドトリップ時間およびパケット棄却率を測定する．これらの測定した値と，IP-VPN サービスプロバイダが規定した公平性の基準をもとに，パラメータ a および b を適切に設定する．これにより，VPN スループットの比を，サービスプロバイダが設定する任意の比率に制御することが可能となる．

VPN 内公平性は，エンド–エンド間で動作する，TCP の輻輳制御機構を利用することによって実現する．つまり，IP-VPN 公平性制御自体は，VPN 内公平性を実現するための積極的な制御は行わない．同じ VPN 内に収容されているフローは，すべてラウンドトリップ時間およびパケット棄却率が等しくなるため，TCP の輻輳制御機構によって十分な VPN 内公平性が実現できると考えられる．

PE ルータ間で転送されるパケットに対しては，カプセル化等の処理は行わない．つまり，VPN に収容されている複数のフローを構成するパケットは，IP-VPN サービスプロバイダのネットワークをそのまま転送される．これは，PE ルータの処理を単純にし，転送速度および VPN 数に関して高いスケーラビリティを実現するためである．

4.2 VPN 間公平性実現のアイディア

VPN 間公平性を実現するための基本的なアイディアは，入側 PE ルータおよび出側 PE ルータ間で動作する，VPN ごとの AIMD 型のウィンドウフロー制御のパラメータ a および b を調整することにより，(ラウンドトリップ時間よりも十分大きい，ある程度大きな時間スケールで考えた場合に) 任意の公平性を実現するというものである．

ここで複数の VPN フローを考える．i 番目の VPN フローに対応する AIMD 型のウィンドウフロー制御のパラメータ a および b を，それぞれ a_i および b_i とする．同様に，i 番目の VPN スループットを T_i，i 番目の VPN のラウンドトリップ時間，パケット棄却率を，R_i，p_i などと表記する．

まず，VPN フロー i および VPN フロー j 間の公平性を考える．ここで，$R_i/R_j = \gamma$，$p_i/p_j = \delta$ であれば，式 (1) より，T_i および T_j の比 η は次式で与えられる．

$$\eta = \frac{T_i}{T_j} \tag{3}$$

$$\simeq \sqrt{\frac{a_i b_j (2 - b_i)}{a_j b_i (2 - b_j) \gamma^2 \delta}} \tag{4}$$

従って，上式で与えられる η が望む値となるように，a および b を設定することにより，任意の公平性を実現できる．例えば，$R_i/R_j = \gamma$，$p_i/p_j = \delta$ の場合に，$a_i = \gamma^2 \delta a_j$，$b_i = b_j$ とすれば，$T_i = T_j$ となる．

より一般的に，VPN i フロー ($1 \leqq i \leqq N$) 間の公平性を考える．ここで，実現したい公平性の基準を，VPN フロー i のスループットの重み r_i によって定義する．つまり，すべての i，j ($i \neq j$) に対して，

$$\frac{T_i}{r_i} = \frac{T_j}{r_j} \tag{5}$$

が成立する時，すべての VPN フローは公平となる．式 (5) を a および b について解くことにより，任意の公平性を実現するような，AIMD 型のウィンドウフロー制御のパラメータ a および b を求めることができる．ただし，式 (5) を満たす a および b の組み合せは無数に存在するため，実際には，その中から AIMD 型のウィンドウフロー制御の過渡特性を考慮して決定する必要がある．

なお，任意の公平性を実現するようにパラメータ a および b を設定するためには，ラウンドトリップ時間 R_i およびパケット棄却率 p_i が既知でなければならない．提案する IP-VPN 公平性制御では，プロバイダエッジルータ間でフィードバック情報

を交換しているため，ラウンドトリップ時間 R_i およびパケット棄却率 p_i ともに容易に測定できる．PE ルータ間のラウンドトリップ時間やパケット棄却率が分かれば十分であり，エンドホスト間のラウンドトリップ時間やパケット棄却率は必要ないことに注意されたい．

4.3 VPN 内公平性実現のアイディア

VPN 内公平性を実現するための基本的なアイディアは，エンド–エンド間で動作する，TCP の輻輳制御機構をそのまま利用するというものである．つまり，IP-VPN 公平性制御は，PE ルータにおいて，VPN 内に収容されている各フローを識別しない．VPN 内に収容されているエンドホスト上で動作する，TCP の輻輳制御機構を利用することによって VPN 内公平性を実現する．

現在，インターネット上のトラヒックの 90 % 以上が TCP によって転送されているため，エンドホスト上で動作する，TCP の輻輳制御機構を利用するという方法は非常に有効であると考えられる．TCP の輻輳回避フェーズは AIMD 型のウィンドウフロー制御を採用しているため，ラウンドトリップ時間およびパケット棄却率が等しい環境下では，ボトルネックリンクの帯域を公平に共有することができる．特に，同じ VPN 内に収容されているすべてのフローは，ラウンドトリップ時間およびパケット棄却率が等しくなることが期待できるため，TCP の輻輳制御機構によって十分な VPN 内公平性が実現できると考えられる．

また，本方式の利点として，PE ルータにおいて，VPN 内に収容されている各フローを識別する必要がないため，PE ルータの高速化が可能であるという点が挙げられる．また，IPSec などを用いて，IP パケットのペイロード部分が暗号化されている場合でも，IP-VPN 公平性制御機構は問題なく動作する．

なお，本方式の欠点としては，同じ VPN 内に収容されている，プロトコル種別の異なるフロー間 (例えば，TCP フローと UDP パケット) の公平性は実現できないという点が挙げられる．しかし，IP-VPN サービスの目的を考えると，VPN 内公平性の厳密な制御は，VPN を契約している顧客が管理している，カスタマエッジルータで行うべきであろう．例えば，カスタマエッジルータにおいて，プロトコルごとの優先制御などを行うことにより，より厳密な VPN 内公平性が実現できると考えられる．

提案する I2VFC では，PE ルータ間で AIMD 型のウィンドウフロー制御が動作し，エンドホスト間で TCP のウィンドウフロー制御が動作する．つまり，PE ルータ間，およびエンドホスト間で，二重にフィードバック型のウィンドウフロー制御が動作することになる．TCP over ABR でさまざまな問題点が指摘されたように [13]，複数のフィードバック制御が相互干渉することにより，全体の性能が低下してしまう危険性も存在する．提案する I2VFC では，二種類のウィンドウフロー制御のタイムスケールを変化させることにより，フィードバック制御の相互干渉を避けている．具体的には，TCP のウィンドウフロー制御は，ラウンドトリップ時間のタイムスケールで動作するため，I2VFC の AIMD 型のウィンドウフロー制御は，ラウンドトリップ時間の 100 倍程度のタイムスケールで動作させる．

5 I2VFC の動作アルゴリズム

本章では，I2VFC の動作アルゴリズムを説明する．

I2VFC では，制御対象となる VPN フローごとに，以下のような処理を行う．

表 1 記号の定義
Table 1 Definition of Symbols

R_I	入側 PE ルータ
R_O	出側 PE ルータ
Δ	管理パケット送信間隔
CI_k	R_I が k 番目に送信した入側管理パケット
CO_k	R_O が k 番目に送信した出側管理パケット
T	ラウンドトリップ時間
p_k	CO_k に記録する (された) パケット棄却率
$\overline{S}$	到着確認済みパケットのシーケンス番号
S_k	CI_k および CO_k に記録されたパケットのシーケンス番号
S_{now}	R_I が現在までに送信したパケットのシーケンス番号
N_k	R_I が CO_{k-1} と CO_k の受信の間に受信したパケットの数
t_k	CI_k の送信時刻
t_{now}	現在時刻
W	ウインドウサイズ
a	1 ラウンドトリップ時間あたりのウインドウサイズ増加量
b	1 ラウンドトリップ時間あたりのウインドウサイズ減少量

(A) AIMD 型のウインドウフロー制御

VPN スループットを制御するため，ウインドウフロー制御によってパケットの送信量を制御する．この制御は，以下の 2 つの動作からなる．

(A-1) 入側 PE ルータにおける送信パケット数の制限

(A-2) 入側 PE ルータにおけるウインドウサイズの更新

(B) 制御に必要なフィードバック情報の取得

I2VFC の制御に必要な情報 (パケット棄却率，ラウンドトリップ時間，送信確認済みのパケットのシーケンス番号) を得るために，管理パケットを入側と出側の PE ルータ間で交換する．この制御は，以下の 4 つ動作からなる．

(B-1) 入側 PE ルータが入側管理パケットを送信

(B-2) 出側 PE ルータが入側管理パケットを受信

(B-3) 出側 PE ルータが出側管理パケットを送信

(B-4) 入側 PE ルータが出側管理パケットを受信

なお，送信確認済みパケットとは，入側 PE ルータが送信し，すでに出側 PE ルータに到着したことがが確認されたパケット，もしくは，入側 PE ルータが送信したが，経路上のルータでの棄却が確認されたパケットを意味する．

I2VFC において，これらの制御 (A-1)〜(B-4) がどのように実行されるのかについて説明する．説明にあたりいくつかの記号を定義した．定義した記号を表 1 に示す．

ある VPN フローに着目すると，およそ以下のような順序で制御が行われる．また，制御が行われる様子を図 2 に示す．

(A-1) 入側 PE ルータにおける送信パケット数の制限

入側 PE ルータ R_I は，ウインドウフロー制御によって送信するパケットの数を制御する．すなわち，R_I は，サイトからパケットを受信すると，R_I が現在までに送信したパケットのシーケンス番号 S_{now} と受信確認済みパケットのシーケンス番号 $\overline{S}$ との差と，ウインドウサイズ W を比較し，次のような処理を行なう．

$$\begin{cases} \text{パケットを送信} & \text{if } S_{now} - \overline{S} \leqq W \\ \text{パケットの送信を停止} & \text{if } S_{now} - \overline{S} > W \end{cases} \quad (6)$$

(B-1) 入側 PE ルータが入側管理パケットを送信

R_I は，パケットを一定個数 (管理パケット送信間隔 δ) 送信するごとに，(制御開始時 k から k 番目にあたる) 入側管理パケット CI_k を生成し出側 PE ルータ R_O に送信する．CI_k に

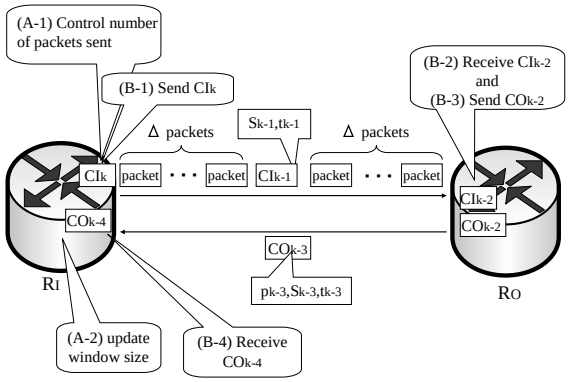

図 2: I2VFC の制御の様子
Fig. 2　Behavior of I2VFC

は，S_{now} と，CI_k の送信時刻 t_k を記録する．

(B-2) 出側 PE ルータが入側管理パケットを受信

CI_k を受信した R_O は，パケット棄却率 p_k を計算する．p_k は，CI_k および CI_{k-1} に記録されていたパケットのシーケンス番号 S_k，S_{k-1} と，R_I が CI_{k-1} と CI_k の受信の間に受信したパケットの数 N_k から，次式で与えられる．

$$p_k \leftarrow \frac{S_k - S_{k-1} - N_k}{S_k - S_{k-1}} \tag{7}$$

(B-3) 出側 PE ルータが出側管理パケットを送信

R_O は，(制御開始時から k 番目にあたる) 受信側管理パケット CO_k を生成し R_I に送信する．CO_k には，p_k，CI_k に記録されていた S_k，CI_k に記録されていた t_s を記録する．

(B-4) 入側 PE ルータが出側管理パケットを受信

CO_k を受信した R_I は，CO_k に記録されているパケット棄却率 p_k を得る．さらに，次式にしたがって，ラウンドトリップ時間 T，送信確認済みパケットのシーケンス番号 $\overline{S}$ を更新する．

$$\begin{aligned} T &\leftarrow t_k - t_{now} \\ \overline{S} &\leftarrow S_k \end{aligned} \tag{8}$$

ここで，t_{now} は現在時刻である．

(A-2) 入側 PE ルータにおけるウインドウサイズの更新

R_I は，p_k をもとに，AIMD のアルゴリズムに従って次式のようにウインドウサイズ W を更新する．

$$W \leftarrow \begin{cases} W + a\frac{\Delta}{W} & \text{if } p_k = 0 \\ W - b \times W & \text{otherwise} \end{cases} \tag{9}$$

通常，入側 PE ルータは，1 ラウンドトリップ時間に，W/Δ 個の出側管理パケットを受信する．このため，$W + a \cdot \Delta/W$ は，Δ や現在の W の値にかかわらず，1 ラウンドトリップ時間あたりに W が a だけ増加することを意味する．

6 ま と め

本稿では，公平な VPN サービスを低コストで実現するためのプロトコル I2VFC を提案した．まず I2VFC の 4 つの設計目標である，(1)VPN 間の公平性の実現，(2)VPN 内公平性の実現，(3) 既存の IP ネットワークへの導入が容易，(4) 転送速度/VPN 数に関して高いスケーラビリティを実現，につい議論した．次に，I2VFC 実現のアイデアである，(1) 入側 PE ルータでフローを集約し，集約したフローに対して AIMD 型ウインドウフロー制御を適用，(2) 制御パラメータを実現したい公平性の基準に応じて適切に設定，(3)TCP-Reno をそのまま利用，について議論した．そして，最後に I2VFC の動作アルゴリズムの詳細を説明した．

今後，シミュレーションによって I2VFC の性能を明らかにする予定である．具体的には，I2VFC の制御パラメータとウインドウフロー制御の過渡特性の関係および I2VFC によって実現できる公平性の精度を明らかにする．また，VPN 数が増加するなどネットワークの状況に変化が起こった場合に，制御のパラメータの設定を自動的に行う方法についても検討する．

文　献

[1] E. Rosen and Y. Rekhter. BGP/MPLS VPNs. *Request for Comments (RFC) 2547*, March 1999.

[2] B. Gleeson, A. Lin, J. Heinanen, and G. Armitage. A framework for ip based virtual private networks. *Request for Comments (RFC) 2764*, February 2000.

[3] A. Malis K. Muthukrishnan. A core MPLS IP VPN architecture. *Request for Comments (RFC) 2917*, September 2000.

[4] Ananth Nagarajan. Generic requirements for provider provisioned VPN. *Internet Draft* <draft-ietf-ppvpn-generic-reqts-02.txt>, January 2003.

[5] D. M. Chiu and R. Jain. Analysis of the increase and decrease algorithms for congestion avoidance in computer networks. *Journal of Computer Networks and ISDN Systems*, 17(1), June 1989.

[6] M. Allman, V. Paxson, and W. R. Stevens. TCP congestion control. *Request for Comments (RFC) 2581*, April 1999.

[7] S. Floyd. Connections with multiple congested gateways in Packet-Switched Networks part 1: One-way traffic. *ACM SIGCOMM Computer Communication Review*, 21(5):30–47, October 1991.

[8] Sally Floyd, Mark Handley, and Jitendra Padhye. A comparison of equation-based and AIMD congestion control, February 2000. available at http://www.aciri.org/tfrc/.

[9] Milan Vojnovic, Jean-Yves Le Boudec, and Catherine Boutremans. Global fairness of additive-increase and multiplicative-decrease with heterogeneous round-trip times. In *IEEE INFOCOM*, pages 1303–1312, 2000.

[10] Deepak Bansal and Hari Balakrishnan. Binomial congestion control algorithms. In *IEEE INFOCOM*, pages 631–640, 2001.

[11] V. M. Ramos Ramos E. Altman, C. Barakat. Analysis of AIMD protocols over paths with variable delay. In *IEEE INFOCOM*, March 2004.

[12] Ibrahim Khalil and Torsten Braun. Edge Provisioning and Fairness in VPN-Diffserv Networks. *JNSM*, 10(1):11–38, March 2002.

[13] Shiv Kalyanaraman, Raj Jain, Sonia Fahmy, Rohit Goyal, Jianping Jiang, and Seong-Cheol Kim. Performance of TCP over ABR on ATM backbone and with various vbr traffic patterns. *ICC*, June 1997.