第 9 回インターネットテクノロジーワークショップ
The Ninth Workshop on Internet Technology(WIT2008)
2008 年 6 月

可用帯域の測定に基づくマルチパス VPN システム

釘本　健司† 　瀬林　克啓† 　明石　 修† 　丸山　 充†

† NTT 未来ねっと研究所　〒 180–8585 東京都武蔵野市緑町 3–9–11
E-mail: †{kugimoto.takeshi, sebayashi.katuhiro, akashi.osamu, maruyama.mitsuru}@lab.ntt.co.jp

あらまし　近年, 安価な広帯域アクセス回線が普及するにつれ, 遠隔の拠点を低コストで結ぶインターネット VPN が運用されるようになってきた. インターネット VPN のうち, トラフィックを複数のネットワークに分散して広帯域化をはかるものを, 本稿ではマルチパス VPN と呼ぶ. ネットワークの可用帯域は経路によって異なるにも関わらず, 既存のマルチパス VPN では可用帯域の違いを考慮していないため, 回線容量および VPN 装置の持つパフォーマンスを十分に生かせない場合がある. そこで我々は, ネットワークの可用帯域の違いを考慮したマルチパス VPN システムを提案する. マルチパス VPN システムは複数のネットワーク接続点を持つ. 対向する装置間で接続点の組合せを変えることにより, ネットワークの経路をある程度自由に選ぶことができる. 我々が提案するシステムでは, 全ての可能な経路について個別の可用帯域を測定し, 測定結果から VPN 装置全体としての可用帯域が最大となるように接続点の組合せを決定する. これにより, マルチパス VPN システムとしてのパフォーマンスの向上を狙う. 本稿では, 検討中のシステム概要について述べる. また, システムの有効性の見通しを得るための予備実験として, 実際のアクセス回線を用いて, 対向する接続点間の可用帯域の時間的な変動の測定を行ったので, 測定結果を報告する.

キーワード　インターネット VPN, マルチパス, 可用帯域

Multipath VPN system based on available bandwidth measurement

Takeshi KUGIMOTO†, Katsuhiro SEBAYASHI†, Osamu AKASHI†, and Mitsuru MARUYAMA†

† NTT Network Innovations Labs.　Midori-cho 3–9–11, Musashino-shi, Tokyo, 180–8585 Japan
E-mail: †{kugimoto.takeshi, sebayashi.katuhiro, akashi.osamu, maruyama.mitsuru}@lab.ntt.co.jp

1. はじめに

近年, 安価な広帯域のアクセス回線が普及するにつれ, 遠隔地を低コストで結ぶインターネット VPN が運用されるようになってきた. イベント中継, 特設スタジオなどの放送の現場においても, リアルタイムストリーミングや, 放送素材映像を迅速に放送局に伝送するためのインターネット VPN サービスが注目されている. 従来, このような用途には専用線サービスや衛星ネットワークサービスが用いられてきたが, 通信品質の保証という利点があるものの, サービスオーダーから開通までに時間がかかること, 最低契約期間が比較的長期になること, また一般に高価であることなどから, 代替サービスとして低コストのインターネット VPN の使用が検討されてきた. しかし, 素材映像の迅速な伝送のために, 100Mbps の速度が求められている一方で, 現在提供されているアクセスサービスは, 物理速度が最大 100Mbps である上, 実際の可用帯域はそれよりも小さい.

現在, 我々のグループでは, そのような放送現場のニーズに応えるため, マルチパス VPN(Virtual Private Network: 仮想専用線) システムの実現を目指している. マルチパス VPN システムは, B フレッツなどの既存の安価なアクセス回線を複数使用して, 放送素材やストリームを複数ネットワークに分散して伝送する広帯域の仮想専用線システムである. その最大可用帯域は, 対向する装置のネットワーク接続点を結ぶ各ネットワークパスの可用帯域の総和となる.

さて, ネットワークの可用帯域はパスによって異なることが一般に知られている. 可用帯域の違いは, ネットワーク接続点を提供する ISP(Internet Service Provider) 内部網の設備構成やその能力の違いや, ISP を結ぶ中継網の構成や能力に由来する. また, 昼間と夜間ではネットワークの混雑の様相が異なり, ネットワークパスの可用帯域は時刻とともに変化することも知られている. 複数のネットワークに分散してデータを伝送する方式については, これまでにも様々な研究が行われており [1] [2] [3], 製品も市販されている [4] [5]. しかし, 既存のマルチパス VPN システムでは, ネットワークパスの可用帯域の違いを考慮していないため, 可用帯域の狭いネットワークパスを選択してしまい, VPN 装置のパフォーマンスを十分に生かせない場合がある.

そこで我々は, パスの可用帯域の違いを考慮したマルチパス VPN システムの検討を行っている. 本システムは, 対向する VPN 装置のネットワーク接続点間のパスの可用帯域を測定し, 測定結果から VPN 装置全体としての可用帯域が最大となるようにパスを選択することにより, システムのパフォーマンスの向上を狙う.

本稿では, まず, 提案するマルチパス VPN システムの概要と基本機能について述べる. 次に, 提案システムの実用上の見通しを得るために行った予備実験について述べる. 測定実験では, 単体のネットワークパスの可用帯域の評価と, ネットワークパスを組み合わせた合計の可用帯域の評価を目的として, 実際のアクセス回線を用いて測定を行った. また, 現在のところ, 可用帯域の測定は, ダミートラフィックを帯域が飽和するまで流すことによって直接的に行っているが, ネットワークに不必要な負荷をかけないようにするために, 間接的な測定法の確立が必要となる. 我々は, 可用帯域の間接的測定手法の見通しを得るために, RTT と可用帯域の相関を調べる実験を行った. この結果について報告する.

2. 提案するマルチパス VPN システム

本節では, 我々が提案するマルチパス VPN システムについて述べる.

本システムの構成は, マルチパス VPN 装置の基本となる (1) トラフィック分散機能と, (2) パス可用帯域測定機能および, (3) ネットワークパス切替機能の 3 つからなる.

マルチパス VPN システムは, ISP への接続点を両端とする複数のネットワークパスで接続される. マルチパス VPN 装置が設置された拠点間のトラフィックは, これらのネットワークパス上に分散されて伝送される. これが「トラフィック分散機能」である.

また, 本システムの特長は, 対向する接続点の組合せを変更してネットワークパスを選択することで, システム全体の可用帯域を向上させることである. 既存のシステムでは, ネットワークパスの可用帯域の違いを考慮していないため, 可用帯域の狭いパスを選択してしまい, VPN 装置全体としての可用帯域のパフォーマンスを十分に発揮できないことがある. そこで, 「ネットワークパス可用帯域測定機能」を用いてパスの帯域を測定し, 測定結果に基づいて VPN 装置を結ぶネットワークパスの組合せを変えて, システム全体の可用帯域の総和が最も大きくなるように経路設定を行う. これが「ネットワークパス切替機能」である.

以下に, 各機能について詳細に述べる.

2.1 トラフィック分散機能

本機能は, VPN の広帯域化や, 信頼性向上を狙って冗長化を行うために, 入力トラフィックを指定した割合で複数のネットワークを経由して伝送するためのものであり, セレクタ部がその機能を担う.

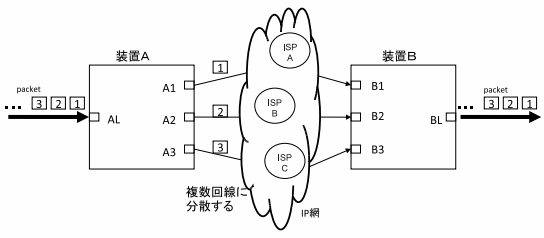

図 1 トラフィック分散機能

組合せ表

	組合せ1	組合せ2	組合せ3	組合せ4	組合せ5	組合せ6
A1	B1 / 10	B1 / 10	B2 / 50	B2 / 50	B3 / 10	B3 / 10
A2	B2 / 10	B3 / 50	B1 / 20	B3 / 50	B1 / 20	B2 / 10
A3	B3 / 10	B2 / 20	B3 / 10	B1 / 10	B2 / 50	B1 / 10
帯域合計Mbps	30	80	80	110	100	80

表 1 ポート間の組合せと可用帯域の総和

図 1 は本機能の概略図である. VPN 装置 A から入力されたパケットは, カプセル化等の伝送に必要な処理を施された後に, パスの可用帯域に応じて複数のネットワークを経由して分散伝送され, 対地の VPN 装置 B で再構成して出力される. 従来のマルチパス VPN 装置では, 分散方式としてラウンドロビン方式が採用されることが多いが, 本機能では可用帯域の向上のために, 測定された可用帯域に応じた割合でパケットを分散して伝送する.

なお, 図 1 中で, 各ポートは物理ポートに限らず, トンネルデバイス等の論理デバイスを含む. また, 単一ストリームのみを扱うように描かれているが, 本システムでは複数ストリームを同時に処理することを想定している. また, 可用帯域の増大や信頼性向上のために, 3 つ以上のネットワークを介して伝送を行うことも想定している.

2.2 パス可用帯域測定機能

本機能は, ネットワークパスの可用帯域を測定する機能である. 装置の使用開始に先だって, ダミートラフィックを流すことにより, パスの可用帯域の最大値, 最小値, 平均値, 偏差などを測定する. この測定結果は, トラフィックの各ポートへの分散の割合と, 後述するネットワークパス選択の根拠となる,

図 1 の構成で, 装置の接続点を両端とするネットワークパスの可用帯域の平均値を測定すれば, パスの可用帯域の平均値を要素とするトラフィックマトリクスが得られる. このトラフィックマトリクスを元に, 例えば表 1 のような組合せ表が得られる. この表は, 各 WAN ポートの対で表されるネットワークパスと, 可用帯域の総和の対応を表したものである. たとえば, 「組合せ 1」のように, 装置 A および装置 B の WAN ポートを, A1 と B1, A2 と B2, A3 と B3 をそれぞれ接続して各々ネットワークパスを構成すれば, 合計の可用帯域は 30Mbps となる. パスの可用帯域の総和が最大値の 110Mbps となるのは, 「組合せ 4」のように A1 と B2, A2 と B3, A3 と B1 を接続して各々のネットワークパスを構成した場合である. すなわち可用帯域を最大とするためには, 次節に述べるネットワークパス切替機能を用いて, WAN ポート間が「組合せ 4」のように接続されるように経路表を操作すればよい.

なお, 各ネットワークパスの可用帯域を単純に足しても, 実際に VPN 装置全体の可用帯域に等しくなるとは限らない. 例えば, 各ネットワークパスが経路の一部を共有しており, かつ, その共有部分の帯域が, 測定された各ネットワークパスの帯域を収容するのに十分な能力を持たず, トラフィックが相互に影響を与える場合である. この場合, VPN 装置全体の可用帯域は, 個別のネットワークパスの可用帯域の総和よりも小さくなる. その意味では, 表 1 の結果のみに頼って組合せを決定することには問題がある.

各ネットワークパスが経路の一部を共有しているかどうかをエンドユーザーが明確に知ることはできないが, 複数トラフィックを同時に流すことによって, 相互の影響をある程度は知ることができる. ただ, 個別のネットワークパスの帯域を測定する場合に比べて, 測定の回数が増えてしまう. 帯域の同時測定に効果があるかどうかは, 実際のネットワーク構成に依存する.

2.3 ネットワークパス切替機能

本機能は, 上記のパス可用帯域測定の結果に基づいて, マルチパス VPN 装置のネットワークパスを切替える機能である. 図 2 のように, VPN 装置の各 WAN ポートは, 各々個別の ISP を介して IP 網に接続されている. VPN 装置 A の WAN ポートを出たトラフィックは, インターネット上の複数のパスを通って VPN 装置 B に送られる.

対向する VPN 装置の経路表をそれぞれ操作することで, 装置間のトラフィックの流れを制御することができる. 例えば, 図 2 の実線の矢印は, WAN ポート A1 から B1, A2 から B2, A3 から B3 へと, トラフィックがそれぞれ分散されて転送される様子を表している. 経路表を操作することで, 破線の矢印のように, WAN ポート A1 から B3, A2 から B1, A3 から B2 へと, トラフィックの流れを変更することができる.

装置のもつ WAN ポート数をそれぞれ n 個とし, 対向するそれぞれの装置の WAN ポートが 1 対 1 に接続されるとすれば, その組合せは $n!$ 通りとなる. 可用帯域の測定の結果から, これら $n!$ 個のパターンのなかから, 可用帯域の総和が最も高いものを選ぶ.

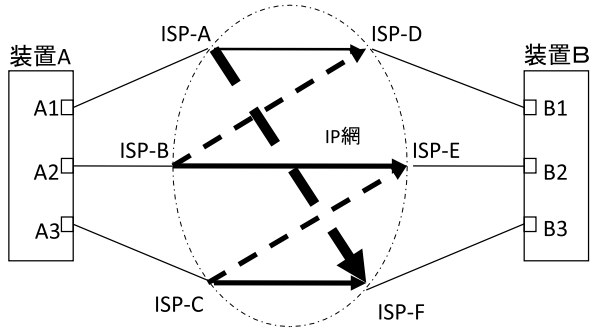

図 2　組合せ切替機能

2.4 本システムの構成例

以上に説明してきた機能を含む, 本システム構成概略を図 3 に示す. システムは, ローカルネットワーク用の LAN ポートと, バッファリングおよびディスオーダリング防止用パケットメモリと, ローカルトラフィックを分散して伝送するための複数の WAN ポートと, 制御部で指定された割合でトラフィックを分散するセレクタと, これらの制御を行う制御部から構成される. 「トラフィック負荷分散機能」は, 制御部の分散制御機能で制御されるセレクタによって実現される. 「ネットワークパス切替機能」は制御部の宛先切替機能とそれによって制御される WAN パケット入出力部により実現される. また, 「パス可用帯域測定機能」は, 「ネットワークパス切替機能」と WAN パケット入出力部に備えられたカウンタにより実現される.

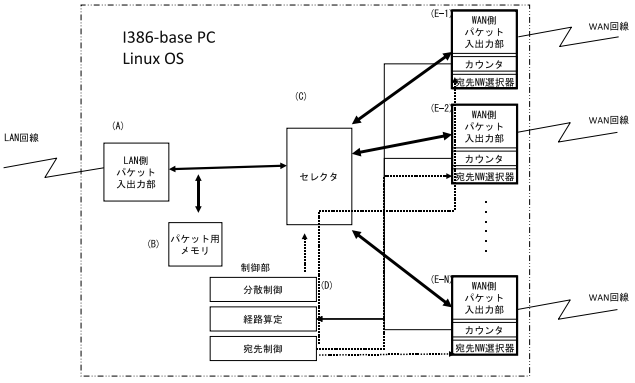

図 3　システム構成概略

3. 測 定 実 験

前節で提案したマルチパス VPN システムを使うことにより, ネットワークパスの可用帯域を最大に利用して, マルチパス VPN システム間の可用帯域を向上させることが可能になる. ISP 間のネットワークパスの可用帯域に違いがあればあるほど, 我々のシステムは有効であると考えられるが, 実際にどのぐらいの違いがあるのかを調べた研究が見当たらなかった. そこで, 本節では, 我々が検討しているシステムが, 現実のネットワークにおいて, どの程度の有効性を持つのかを検証するために, 実際に複数のアクセス回線を設置して測定実験を行った. 以下では, ネットワークパスの可用帯域の様相を調べ, また ISP 間接続の組合せ切替えの効果を確認するための予備的な測定実験の結果を報告する.

3.1 測定環境と測定条件

本稿での測定環境について述べる. ネットワークパスの可用帯域等の測定は, それぞれ 3 つのアクセス回線を接続した 2 台の PC を用いて行った. アクセス回線として B-flets 回線を利用し, 各々異なる ISP に加入している. 回線は全て同じ場所に設置されている. また, 測定に用いた PC は, CPU として Pentium4 3.4GHz, 主メモリとして 2Gbytes, 4 つの GbE ポートを持つ. 搭載された GbE ポート 4 つが同時に 800Mbps の速度で通信可能な性能を有することを事前測定により確認しており, PC の性能が測定上のボトルネックとはならない. また, 使用 OS は CentOS/Linux Release 5 である. ブロードバンドルータの影響を排除するため, CentOS 標準搭載の PPPoE を用いて, 各ポートをそれぞれ別々の ISP と直接に接続している.

可用帯域の測定ツールとして定評のある iperf [6] を使用した. iperf では測定に UDP と TCP のいずれも使用できるが, パケット損失が発生しない最大の速度を測定するために, セルフクロッキングの動作でスムーズなデータ転送が行われることから TCP を用いた. なお, TCP window size はデフォルトの 16KBytes である.

3.2 ネットワークパス単体の可用帯域の評価

時間変動などの様相を知るため, ネットワークパス単体の可用帯域を測定した. ISP 間の可用帯域の測定は iperf を使用し, 対向する 3 組の ISP 間にトラフィックを流し, 10 秒ごとの可用帯域の測定をトータルで 3600 秒間にわたって行った. これにより, 回線に流すことのできるトラフィックの最大値を見積もる. なお, 測定間隔を 10 秒とした理由は, 本システムでは秒単位の細かな可用帯域の変動は, パケットメモリによるバッファリングで吸収することを想定しているからである.

図 4 のグラフは, ISP-A と ISP-D, ISP-B と ISP-E, ISP-C と ISP-F の 3 つの ISP の組合せで構成したネットワークパスの可用帯域を測定した結果である. グラフから, ネットワークパスの可用帯域が大きく異なっていることがわかる. ISP-A から ISP-D の可用帯域は, ISP-C から ISP-F の帯域の半分程度しかない. ネットワークパスよって可用帯域が異なることは, 一般にも経験されることであるが, このグラフからその事実が裏付けられる.

また, グラフからは, ネットワークパスの可用帯域が約 10Mbps の範囲で細かく変動している様子がわかる. 確実にデータ伝送を行うためには, 測定された可用帯域よりも約 10Mbps 少ない送信速度にする必要があると思われる. さらに, グラフ全体からは少し長い時間単位で可用帯域が大きく変化している様子が見える. 特に ISP-B と ISP-E の間の可用帯域の変動が大きい. マルチパス VPN において, 可用帯域を常に確保しておくためには, このロングレンジの変化を早めにとらえて, ネットワークパスの切替えなどを適切に行う必要がある.

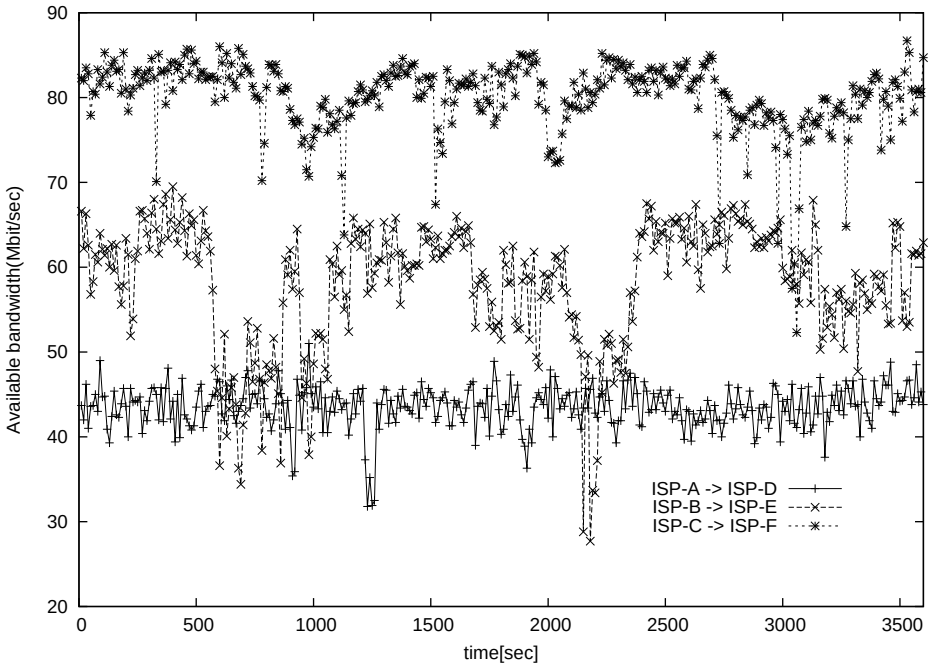

図 4　ネットワークパスごとの可用帯域の違い

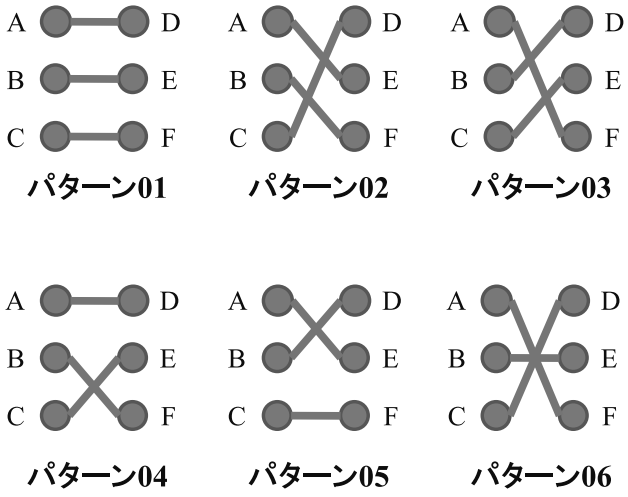

図 5　ネットワークパスのパターン

3.3　ネットワークパスを組合せた合計の可用帯域の評価

この測定の目的は, ネットワークパスの変更によるパフォーマンス向上が可能かどうか, その有効性の見通しを得ることである. そのために, 図 5 に示すようなパスの組合せパターンについて, それぞれ可用帯域の総和の時間変化を調べた.

可用帯域の測定は, iperf を使用し, 図 5 に示す 6 つのパターンで, A,B,C の ISP グループと D,E,F の ISP グループとの間を接続して行った. 1 つのパターンの測定時間は 60 秒とし, 1 回合計 360 秒の測定を 20 分ごとに 24 時間にわたって行った. 測定結果を図 6 のグラフに示す. このグラフから以下のことが分かった.

・合計の可用帯域の範囲

合計の可用帯域は最大で 215Mbps, 最小で 130Mbps である. 素材伝送に求められる可用帯域は最低 100Mbps であり, 最低 100Mbps がシステムの制約となるとすれば, 3 回線で十分との見通しが得られた.

・合計の可用帯域の時間変動

グラフからは時刻によって可用帯域が大きく変動している様子が見てとれる. とくに 20 時頃から 3 時頃までの間は, 可用帯域が大きく落ち込んでいる. 各パターンの可用帯域の時間変化を見てみると, 最大の可用帯域となるパターン Pattern01, Pattern02, Pattern04, Pattern05 の 4 つが頻繁に入れ替わっている. これらのパターン内の可用帯域の差は最大 10Mbps である. その一方で, Pattern03, Pattern06 のように, 可用帯域が一度も最大とならないパターンもある.

・パターン毎の合計の可用帯域の平均値

測定した各パターンの合計の可用帯域から, その平均値を計算した結果を表 2 に示す.

表 2　各パターンの可用帯域の平均値

pattern01	201.77 (Mbps)
pattern02	201.89 (Mbps)
pattern03	180.44 (Mbps)
pattern04	199.67 (Mbps)
pattern05	199.43 (Mbps)
pattern06	183.69 (Mbps)

この表からも, Pattern03, Pattern06 は, 他の 4 つのパターンに比べて可用帯域が 20Mbps ほど少ないことがわかる. このようなパターンを早期に見つけて避けることが, パフォーマンスの向上のための最低条件である.

3.4　可用帯域の合計の最大値の推移

図 7 のグラフは, 図 6 のグラフ中で, 可用帯域の総和が最大となるパターンだけをプロットしたものである.

このグラフからは, 同じパターンが数回連続する傾向が見られる. さらにデータを詳しく見てみると, このグラフの全区間で, 可用帯域が最大となるパターンの持続率は平均 1.8 である. ここで持続率とは, 同一パターンが連続する回数の平均値とする. 持続率が 1.8 であることから, あるパターンの可用帯域が最大となったとき, 次に可用帯域が最大となるのも同じパターンである可能性が高いと言える.

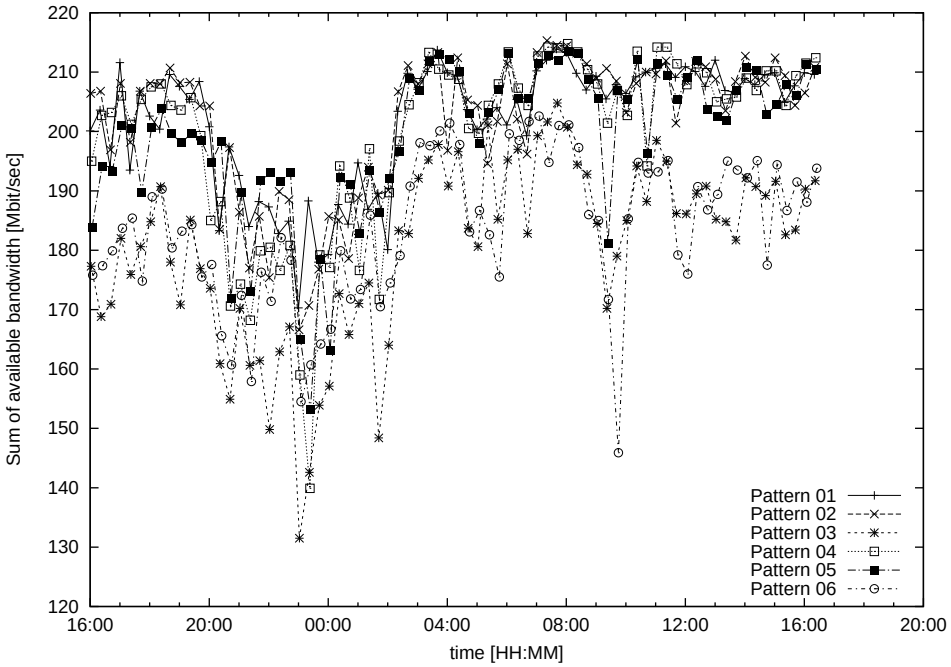

図 6　パスの合計帯域の推移

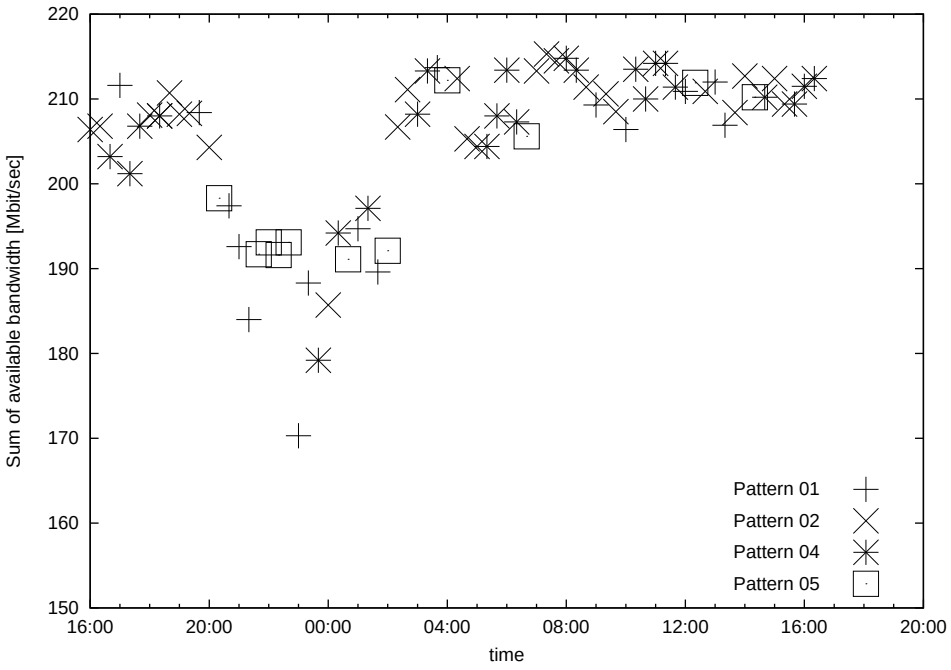

図 7　可用帯域の合計の最大値の推移

・知見を利用した帯域推定アルゴリズム

上記の知見を利用して, 全体の可用帯域の平均値を上げるようにネットワークパスを設定するアルゴリズムを検討した. アルゴリズムは, 「ある時点の測定で可用帯域が最大となるパターンを, 次のパターンとして選択する」単純なものである. なお, 初期パターンを Pattern01 とした. 計算の結果, 可用帯域の平均値は 201.49Mbps となった. この値は, 表 2 の Pattern01, Pattern02, Pattern004, Pattern05 のパターンと同程度であり, この程度の単純な推定アルゴリズムでも実用のものとして使用できる見通しを得た. なお, 合計の可用帯域が最大となるパターンを完全に予測できるとすれば, その平均値は 205.02Mbps となる.

3.5　ネットワークに負荷をかけない可用帯域測定法の検討

可用帯域を調べるために, 現在は iperf を使って測定している. iperf は, ネットワークの限界までダミートラフィックを流して, 可用帯域を直接に測定するツールである. ネットワークに不必要に過大な負荷を与えるため, 他のサービスに影響を与えてしまう.

マルチパス VPN 装置での可用帯域測定法としては, iperf と同様の方法を採用することはできるだけ避けなければならない. そこで, 可用帯域を間接的に推定する技術が求められる.

・RTT と単一のネットワークパスの可用帯域の関係

ネットワークパスの可用帯域の減少は, ネットワークの混雑の結果として現れてくるはずである. ネットワークが混雑する

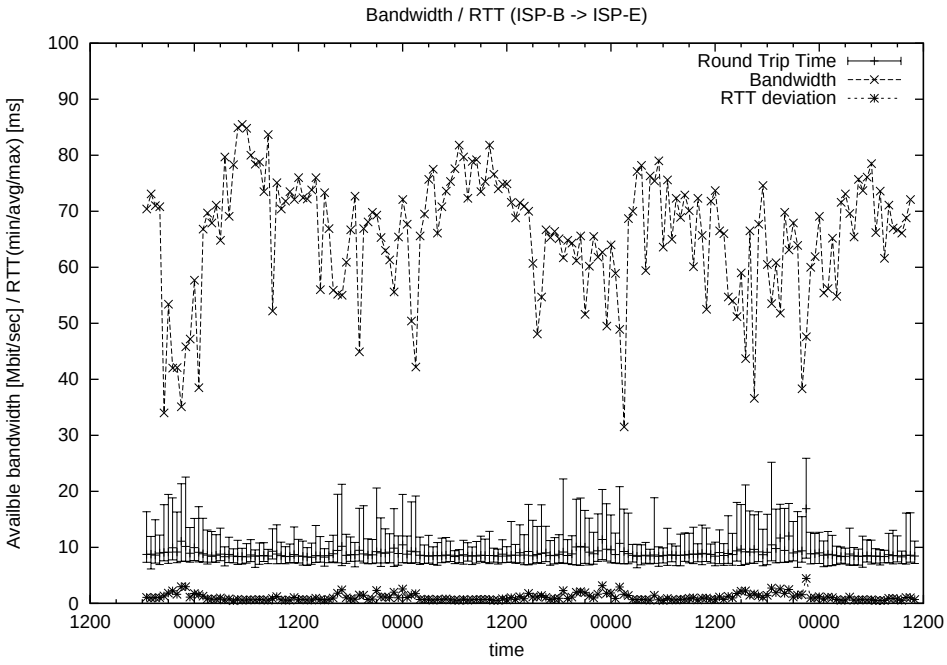

図 8　RTT と可用帯域の時間変化

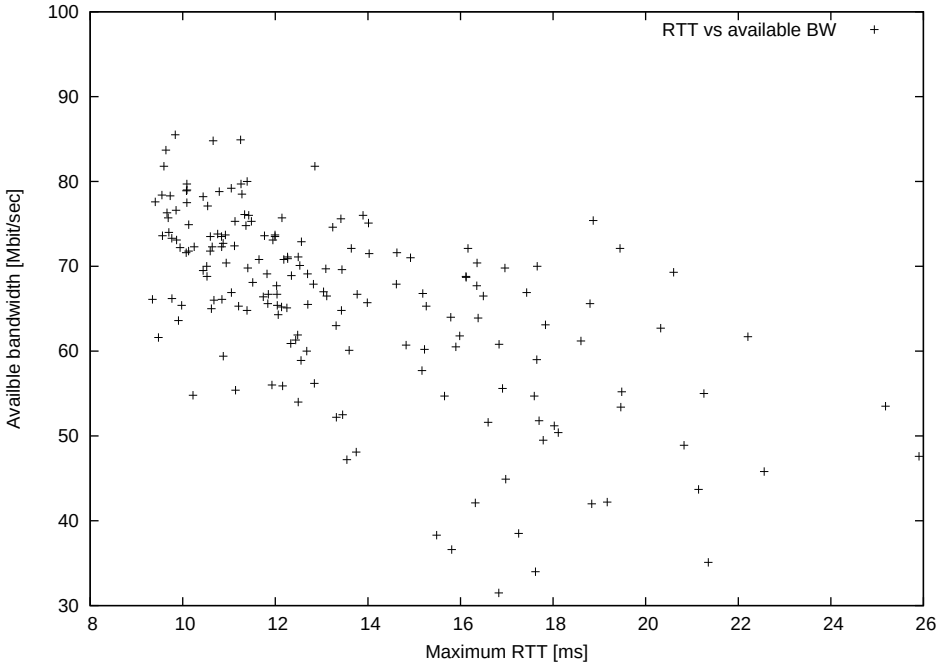

図 9　RTT の最大値と可用帯域の相関

ほど, パケットが中継ノードの Queue に滞留する時間が増えるはずなので, 当然 RTT も増大するはずである. 我々は, RTT を観測することによって, 間接的に可用帯域を推定できるのではないかと考えた.

・RTT と可用帯域の時間変化の測定

3.1 節と同じ測定環境で, 単一のネットワークパスの RTT と可用帯域測定を行った. 可用帯域の測定には iperf を, RTT の測定には ping コマンドを使用した.

図 8 のグラフは, 可用帯域と RTT の 4 日間の時間変化を表したものである. 真中の RTT のバーは最大値, 最小値, および平均値を表している. 毎日 0 時付近に可用帯域が減少しているときに RTT の最大値は大きくなっており, RTT の最大値と可用帯域には相関があるように見える.

・RTT と可用帯域の相関と可用帯域の推定

そこで, 図 9 のように, RTT の最大値と, 対応する可用帯域をプロットしてみた.

このグラフで RTT の最大値が 16ms 以下の領域では, 可用帯域の相関が見て取れる. この領域では可用帯域の推定がある程度可能である.

一方, RTT の最大値が 16ms を超える領域では, 誤差が大きくなってしまい相関が見えにくくなっている. この領域で RTT の最大値から可用帯域を推定することは難しい. ただ, RTT の最大値がこの領域に入っている場合には, できるだけこのネットワークパスを選択しないようにすることで, 装置全体の可用帯域の向上が期待できる.

・測定技術の関連研究

近年, オーバーレイネットワーク, P2P, ストリーミングなど, ネットワークパスの帯域測定を必要とするアプリケーションが多く現れてきており, 様々な測定法の研究が行われている [7] [8]. 測定法として, 試験パケットを送受信して行うアクティブ計測と, 実トラフィックを観測するパッシブ計測がある. 試験パケットはネットワークに余計な負荷を与えるため, 可能な場合はパッシブ計測が望ましいが, パッシブ計測を行うにはネットワークの管理権限を必要とすることが多く, 提案されている測定法のほとんどが, エンドホストのみで計測することが可能なアクティブ計測によるものである.

アクティブ計測の例として, (1) Variable Packet Size (VPS), (2) Packet Pair/Train Dispersion (PPTD), (3) Self-Loading Periodic Streams (SLoPS), (4) Trains Of Packet Pairs (TOPP) などがある.

VPS は, Bellovin, Jacobson らが最初に提案した計測法で, 複数の試験パケットをサイズを変化させて送り, 計測された RTT の差分により帯域を推定する測定法である. Pathchar [9] として実装されている.

PPTD では, 同じサイズの試験パケットを正確な時間間隔で連続して送り, 終点ノードで受信時の正確な時間間隔を計測し, 時間間隔の変化からパスの帯域を推定する.

SLoPS では, 同じサイズの 100 以上の試験パケットを正確なレート R で終点ノードに送り, 終点ノードでパケットの遅延を測定する. 単位時間に送る試験パケットの数を変えて遅延を測定し, 遅延の値が大きくなりはじめるレート R を探る. このレート R が可用帯域となる.

TOPP は, 基本的なアイディアは SLoPS と同じだが, 可用帯域だけでなく, 容量 (capacity) も測定可能なことに特長がある.

今回, 我々が推定に用いたアイディアは, RTT の値の変化から帯域の推定を試みるという意味では, SLoPS や TOPP に近いものである. しかし, いずれの測定法もネットワークが飽和してしまうまでパケットを送ってしまう. 我々はできる限りネットワークに影響を与えないように測定することを目標としており, これらの研究成果を参考にしつつ, よりネットワークに与える負荷の少ない測定法を追求したい.

4. 今後の課題

2.3 節において, WAN ポート間を 1 対 1 に接続することを仮定しているが, ネットワークの状況によっては 1 対多の接続をした場合が有利となる場合もあり得る. 1 対多で接続する場合, 組み合わせは $n!$ 通りではなく, n^2 通りとなり, 組合せ数は増大する.

また, それぞれの装置の持つ WAN ポートを同数としているが, 状況に応じて異なるポート数を持つことも可能である. 各装置のポート数を n, m とし, 1 対多の接続を許せば, 組合せの数はさらに大きくなる. さらに, 多対多で接続する場合もありうる. 多対多接続の場合, パケットを複製して運ぶことにより信頼性の向上を見込むことができる. 今回は 1 対 1 の接続のみの検討を行ったが, 接続の自由度を上げることで, 実際にマルチパス VPN の性能向上につながるかどうかを検討する.

また, 本稿では同一ロケ内に設置された 6 本のアクセス回線による測定実験について述べたが, 今後は他地域にも実験回線を増設し, 地域間のトラフィックの様相を調査して, より広範囲なデータの収集と解析を進め, 帯域推定のアルゴリズムのブラッシュアップ, 可用帯域の間接推定法の調査・検討を行う予定である.

5. ま と め

本稿では, ネットワークパスの可用帯域を考慮したマルチパス VPN システムを提案した. このシステムは, 可用帯域の大きなネットワークパスを選択することにより, システム全体としてのパフォーマンスの向上を狙ったものである. また, 提案システムの実用化の見通しを得るために, 実際のアクセス回線を用いて予備的な測定実験を行った. この測定実験の結果から, ネットワークパスの可用帯域に実際に違いがあること, ネットワークパスを適切に選ぶことで VPN システムのパフォーマンスを向上させ得ることを確認した. また, 可用帯域の測定時のネットワークへの負荷を減ずることを目的として間接測定法の検討を行った. RTT とパスの可用帯域の相関から, RTT の最大値の観測に基づいてパスの可用帯域を推定し得る可能性を示した.

文 献

[1] 林孝典, 山崎真一郎, 森田直人, 相田仁, 武市正人, 土居範久, 「インターネットを用いた複数経路データ伝送方式の性能評価」, 電子情報通信学会論文誌 B, Vol. J84-B, No.3, pp.523-533, 2001

[2] 通信・放送機構, 「分散型ネットワークの高信頼化技術に関する研究開発プロジェクト成果報告書」, "URL: http://koukai.nict.go.jp/doc/result/10960311399_01.pdf", 2000

[3] 渡部郁恵, 岡部寿男, 中村素典, 「複数経路を活用した TCP-Friendly なストリーミングシステムの設計と実装」, 信学技報 IA-2006-37, 電子情報通信学会, pp.37-42, 2007

[4] FatPipe Networks Inc, "FatPipe MPVPN provides the highest level of VPN security", "URL http://www.fatpipeinc.com/mpvpn/index.html", 2007

[5] Alaxala Networks Corp, "AX2000R Software Manual", "http://www.alaxala.com/jp/support/manual/AX2000R/HTML/KAISETSU/0001.HTM", 2005

[6] Iperf Project, "URL http://dast.nlanr.net/Project/Iperf/"

[7] R. Prasad, C. Dovrolis, M. Murray, K. C. Claffy, "Bandwidth Estimation: Metrics, Measurement, Techniques, and Tools", IEEE Network , Vol.17, Issue 6, pp.27 - 35, Nov-Dec 2003.

[8] 鶴 正人, 尾家 祐二, "インターネット品質管理における計測技術の最新動向", Technical report of IEICE CQ, Vol.103, No.444, pp.37-42, CQ2003-70, 2003.

[9] Van Jacobson, Pathchar, "URL http://www.caida.org/tools/utilities/others/pathchar/"