複数ドメインを経由するAFサービスのための コードポイント再設定方式の提案

本久　勝一†　　福岡　寛之††　　馬場　健一†††　　下條　真司†††

† 大阪大学大学院情報科学研究科
†† 通信・放送機構
††† 大阪大学サイバーメディアセンター
〒 567–0047 大阪府茨木市美穂ヶ丘 5–1
E-mail: †hisa@ist.osaka-u.ac.jp, ††fukuoka@ais.cmc.osaka-u.ac.jp, †††{baba,shimojo}@cmc.osaka-u.ac.jp

あらまし　Diffserv は IP ネットワークに QoS を提供するアーキテクチャの一つである．この Diffserv には最低帯域保証を実現する AF PHB が規定されている．AF はパケットに廃棄優先度を設定し，高廃棄優先度のパケットから廃棄することにより低廃棄優先度のパケットの廃棄を防ぎ，QoS を提供する PHB である．しかし，複数ドメインを経由する AF を提供する場合，ドメインの境界でドメイン間契約により廃棄優先度の再設定が行われる可能性がある．このため，複数ドメインを経由する AF では通信品質が低下し，定められた QoS を提供することができない．本研究ではドメインの境界で行われる新しい廃棄優先度の再設定方式を提案する．提案方式は優先度の変更されたパケットを他のパケットと区別することにより QoS を保証する方式である．提案方式の基本的な性能を知るため UDP トラヒックを用いたシミュレーションを行った．その結果，提案方式では従来方式よりも通信品質の低下を防ぎ，定められた QoS を提供できることを示した．

キーワード　サービス品質, Diffserv, AF サービス, DSCP 再設定

An Effective Remarking Scheme for Diffserv AF Service through Multiple Domains

Shoichi MOTOHISA†, Hiroyuki FUKUOKA††, Ken-ichi BABA†††, and Shinji SHIMOJO†††

† Graduate School of Information Science and Technology, Osaka University
†† Telecommunications Advancement Organization of Japan
††† Cybermedia Center, Osaka University
5–1 Mihogaoka, Ibaraki, Osaka 567–0047, Japan
E-mail: †hisa@ist.osaka-u.ac.jp, ††fukuoka@ais.cmc.osaka-u.ac.jp, †††{baba,shimojo}@cmc.osaka-u.ac.jp

Abstract　Diffserv is a type of architecture that aims to provide QoS in the IP networks, and the AF service class in Diffserv realizes minimum bandwidth guarantee by the use of differentiated drop precedence property marked in the DSCP field on each packet. The packets comply with the guaranteed bandwidth are protected in the network by means of the differentiated forwarding behavior based on the DSCP value. In the context of multiple domains environment, however, QoS of individual flow is not always preserved due to the re-marking behavior forced at the domain boundaries. Focusing on this point, this paper proposes a new packet re-marking scheme that can improve per-flow QoS of AF service traversing multiple domains of Diffserv networks. The basic concept of the scheme is to distinguish packets re-marked to out-of-profile at the domain boundaries from those already marked as out-of-profile at the time of entering the network, and to give chances to the re-marked packet to recover back to in-of-profile that can enjoy its rightful QoS within the networks. Basic performance of the proposed scheme is evaluated through simulation study. Basic performance of the proposed scheme is evaluated through simulation study, and the rsults show its effectiveness in preserving QoS of the inter-domain flows.

Key words　QoS, Diffserv, Assured Forwarding, DSCP Re-marking

1. はじめに

インターネットを利用するアプリケーションの多様化により，インターネットに様々なサービス品質 (Quality of Service; QoS) が要求され，QoS を保証するための機構が必要となっている．こうした QoS を制御するアーキテクチャの一つとして Diffserv (Differentiated Service) [1] が提案されている．Diffserv はアプリケーションに応じたフローに属するパケットをクラス分けし，クラスごとに QoS を制御するアーキテクチャであり，“スケーラビリティ” と “構成の容易さ” を併せ持つ技術である．Diffserv は IP ヘッダの TOS フィールドを DSCP (Diffserv Code Point) [2] と再定義し，クラスを識別するための値を設定する．Diffserv では現在，仮想専用線を提供する EF (Expedited Forwarding) [3] と最低帯域保証を提供する AF (Assured Forwarding) [4] の 2 つの PHB (Per Hob Behavior) が標準化されている．AF はパケットに最大 3 段階の廃棄優先度を設定することができ，この廃棄優先度を利用することにより最低帯域保証を提供することができる．AF を使って最低帯域保証を提供する場合，ユーザとドメインの間に保証する最低帯域を定めたサービスプロファイルを契約する．ネットワークは，ドメインの入口のエッジルータにおいてユーザが送信したパケットの到着レートを測定し，パケットをサービスプロファイル内 (in-of-profile) とそれ以外 (out-of-profile) に分類し，それぞれ優先あり，なしの情報を DSCP に設定する．優先権ありのパケットを IN パケット，優先権なしのパケットを OUT パケットと呼ぶ．次に，ドメイン内のコアルータでは DSCP の値に基づいて，OUT パケットを積極的に廃棄することにより IN のパケットの損失を防ぎ，ユーザに対して最低帯域を保証する．すなわち，AF のパケット廃棄優先度のうち，2 つを使って最低帯域保証を実現している．

最低帯域保証を複数のドメインを経由するフローに対して提供する場合，ドメインの境界でドメイン間契約に基づき DSCP の再設定が行われる．ドメイン境界のエッジルータでは，IN パケットの到着レートを測定し，ドメイン間契約のレートを上回る IN パケットを OUT パケットに変更する [5]．ドメインの境界を通過する IN パケットのレートは，ネットワーク内の他のトラヒックの影響やトラヒックの集約によりジッターが生じ変動する．この変動によりパケット到着レートがドメイン間契約レートより大きくなることがあるため，ドメインを経由すればするほど IN から OUT に再設定されるパケット数が多くなり，IN パケットは減少する．すなわち，IN パケットから OUT パケットへの再設定により，当初 IN であったパケットのパケット損失率が高くなり，ユーザに対してサービスプロファイルで定めた品質を保証することができなくなる場合がある [6]．特に，途中のドメインで輻輳が起きている場合には，著しいパケット損失を引き起こす．また，同じサービスプロファイルでも IN パケットの割合が異なってくるためドメイン内のフローよりドメイン間のフローが不利になり，公平性に欠ける結果につながる．本研究ではドメインを経由するごとの IN パケットの減少は，ドメイン境界での DSCP 再設定方式に問題があると考え，ドメイン間のフローの品質を保証するドメイン境界での新しい DSCP 再設定方式を提案する．

提案方式では IN から OUT に再設定されるパケットに IN/OUT とは別の廃棄優先度を設定し，ドメインの境界で到着レートが契約レートより小さければ再設定されたパケットを IN パケットに戻すことができるようにする．これにより，複数ドメインを経由する場合の IN パケットの減少を防ぐ．

本稿においては，2. 章で本稿で対象とするネットワークについて述べる．3. 章では提案するコードポイント再設定方式について説明し，4. 章では提案方式を評価するためのシミュレーションとその結果を示し考察を述べる．最後に 5. 章でまとめを述べる．

2. 対象とするネットワーク

図 1 に本研究で対象とする，複数ドメインを経由して AF サービスを提供する場合のネットワークモデルを示す．ここでは Source と Destination 間で通信を行うとし，Source 側で Domain A とサービスプロファイルを契約する．まず Source が送信したパケットが Domain A のエッジルータに到着すると，エッジルータは後に示す到着レート測定アルゴリズムを用いてパケットの到着レートを測定し，そのパケットがユーザとドメイン間で定められた契約レート以内かどうかを判定する．その結果，契約レート以内であったパケットには IN，それ以外のパケットには OUT の DSCP の設定が行われる．これらの処理が行われた後，パケットはコアルータに送られる．コアルータではパケットの順序入れ替えを起こさせないためクラスごとに IN/OUT のパケットを同一のキューに入れ，後に示すキューイングアルゴリズムに従って制御を行い，輻輳時に OUT パケットを優先的に廃棄する．Domain A のコアルータを経由して Domain B のエッジルータに到着したパケットは IN と OUT に分類され，IN パケットは Domain A, B 間のパケット到着レートの測定が行われ，契約レートを超えた IN パケットは OUT パケットに再設定される．Domain B, C でも同様な処理が行われ，パ

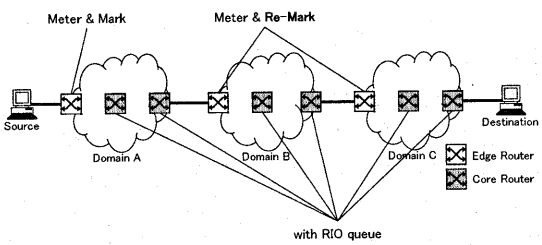

図 1　ネットワークモデル

ケットは Destination に届けられる．また，ドメインを経由する際，DSCP の設定が行われたパケットに対して shaping/policing を行う方法も提案されているが，余剰帯域を有効利用するため，本研究では shaping/policing を行わないものとする．

エッジルータで行われるパケット到着レートの測定のアルゴリズムとして TSW (Time Sliding Window) 方式 [7] が提案されている．TSW 方式ではパケット到着時に以下の式に従いパケットの到着レート $rate_n$ を計算する．

$$rate_n = \frac{rate_{n-1} \times Itvl + size}{t_n - t_{n-1} + Itvl}$$

$rate_n$ ： パケット到着レート

$size$ ： 到着パケットのパケットサイズ

t_n ： 現在時刻

$Itvl$ の値はドメインごとに定めることになるが，[7] では 1 秒と設定することを推奨している．本研究では全てのドメインで $Itvl$ の値は 1 秒とする．

ドメイン内で用いられるキューイングアルゴリズムとして RED (Random Early Discard) [8] をベースとした RIO (RED with IN and OUT) [9] を用いる．RED はしきい値を設定し，平均キュー長がそのしきい値以上になった場合，パケットを廃棄するキューイングアルゴリズムである．RIO は IN と OUT に対して独立した RED パラメータを設定するため，IN と OUT に別々のしきい値が設定される．この時，OUT から先に廃棄するため OUT のしきい値を IN のしきい値よりも小さく設定する．輻輳が生じ，平均キュー長が長くなり OUT のしきい値を超えると，到着する OUT パケットは廃棄されるが，IN のしきい値は OUT のしきい値よりも大きいので，IN パケットは廃棄されない．このように，RIO は輻輳時に OUT パケットを先に廃棄し，IN パケットの廃棄を防ぐことができる．

3. 提案するコードポイント再設定方式

複数ドメインを経由する AF サービスを行う場合，ドメイン間で DSCP の再設定が行われることにより，IN パケットが減少し，ユーザにサービスプロファイルで契約した品質を提供することができない．この問題点を解決するため，本研究ではエッジルータでの新しいコードポイント再設定方式を提案する．提案方式は，ユーザ・エッジルータ間で設定された OUT パケットと，ドメイン境界で再設定により発生した OUT パケットを DSCP で区別し，ドメイン境界においてパケット到着レートが測定された時，契約レートに余裕があれば再設定により発生した OUT パケットを IN パケットへ再び戻すことを可能とする方式である．これにより，複数のドメインを経由することによる IN パケットの減少を抑え，品質の劣化を防ぐ．

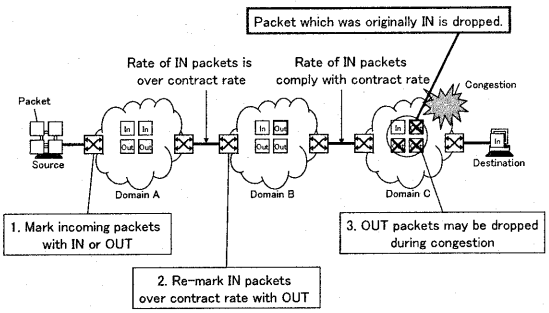

図2 従来方式

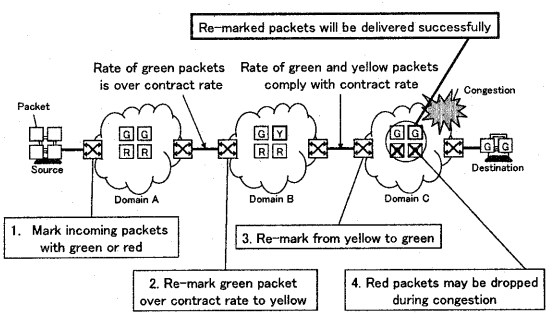

図3 提案方式

提案方式では AF の持つ 3 つの廃棄優先度を用い green, yellow, red に分け DSCP に設定する．まず，エッジルータにおける DSCP の設定方法について述べる．従来のユーザ・ドメイン間の契約レートに基づく DSCP の設定値である IN/OUT を green/red に設定する．ドメイン間の契約レートに基づき設定を行う場合，従来の方式では IN から OUT になるパケットの DSCP を yellow に設定する．つまり，これによりユーザ・ドメイン間で契約レートを超過することにより設定される OUT パケットとドメイン間での契約レートを超過することにより設定される OUT パケットを区別して取り扱うことができる．DSCP に yellow を設定したパケットはドメイン間での到着レート測定の際，従来の方式における IN パケットと同様に扱うとする．すなわち，green パケットと yellow パケットを観測対象とし，契約レート内のパケットであれば DSCP に green を設定し，契約レートを超えるパケットは DSCP に yellow を設定する．

次にコアルータにおけるパケットの扱いについて述べる．コアルータにおいては 3 段階の廃棄優先度を利用し，前節に述べた RIO を用いて制御を行うことが可能である．ただし，本研究では従来方式との比較を行うため，green パケットを従来方式の IN パケットと同様に in-of-profile として扱い，yellow パケット，red パケットを従来方式の OUT パケット同様に out-of-profile として扱うこととする．

従来方式では，ユーザ・ドメイン間で in-of-profile であったという情報がドメイン境界での再設定で失われてしまうが，提案

方式ではユーザ・ドメイン間で in-of-profile であったパケットは DSCP が変更されても yellow パケットとするため情報を失うことはない．従って，途中のドメインのエッジルータにおいて，契約レートを超過していると判断されたパケットも，他のドメインのエッジルターで契約レート内に十分収まるパケットは，再び green に設定することが可能である．これにより，複数ドメインを経由するごとに in-of-profile のパケットが減少することが避けられ，ユーザ・ドメイン間の契約レートに沿った性能が得られる．

図 2，3 で従来方式と提案方式それぞれの具体的な動作について示す．図では Source から Destination へパケットを送信する．従来方式では図 2 のように，Source が送信したパケットは Domain A の入口で IN と OUT に DSCP が設定される．これらのパケットが Domain A, B 間に到着したとき，Domain A, B 間にドメイン間契約レートを超える IN パケットが到着していれば，IN パケットの一部は OUT パケットに再設定される．Domain B を経由して Domain B, C 間に到着したとき，Domain B, C 間に到着する IN パケットのレートがドメイン間契約レートより小さければ，到着するパケットはそのままの DSCP で送出される．Domain C 内で輻輳が発生した場合，Domain A 内で IN であった OUT パケットも他の OUT パケットと同様に廃棄され，ユーザ・ドメイン間で契約された品質を保つことができない．提案方式では図 3 にように，Source が送信したパケットは Domain A の入口で green と red に設定される．そして，Domain A, B 間でドメイン間契約を超える green パケットは yellow に再設定される．Domain B 内で，yellow パケットは red パケットと同様の RIO パラメータで処理される．Domain B, C 間では green，yellow をあわせてパケット到着レートを測定し，ドメイン間契約レートより到着レートが小さければ yellow を green に再設定する．Domain C 内で輻輳が発生しても，Domain A で green であったパケットは Domain B, C 間での DSCP 再設定により，green パケットとして到着しているので廃棄されず Destination に届けられ，ユーザ・ドメイン間で契約された品質を保つことができる．

4. 提案方式の評価

本研究では提案方式の基本的な性能を評価するため UDP トラヒックを対象としたシミュレーションを行った．まず，複数ドメインを経由するフローにおける DSCP の再設定が行われるパケット数について調査し，提案方式と従来方式を比較する．そして，再設定の効果がパケット損失率にどのように影響するかを調査する．最後に，ドメイン間フローとドメイン内フローの双方が存在する場合のパケット損失率を測定し，フロー間の公平性を調査する．また，シミュレーションは Network Simulator version 2 (ns–2) [10] を用いて行った．

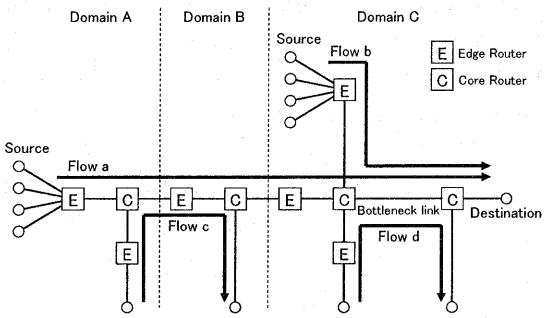

図 4　シミュレーションモデル

4.1 シミュレーションモデル

図 4 にシミュレーションモデル示す．各リンクは伝搬遅延を 1 ms，帯域は十分大きく，パケットの廃棄は Domain C のボトルネックリンク以外では起きないものとする．エッジルータではパケット到着レートの測定および DSCP の設定を行い，パケット到着レートの測定のアルゴリズムは TSW 方式を用いる．コアルータは単一の RIO キューから構成されていて，キューのバッファサイズは 200 packet，RIO キューパラメータは，IN に対して $(min_{in}, max_{in}, Pmax_{in}) = (100, 150, 0.02)$，OUT に対して $(min_{out}, max_{out}, Pmax_{out}) = (50, 100, 0.1)$ と設定する．$min, max, Pmax$ はそれぞれ廃棄開始しきい値，完全廃棄しきい値，最大廃棄確率である．発生するトラヒックは UDP フローとし，パケットサイズは最大値 1500 byte，平均 1000 byte，分散 1000 byte^2 の正規分布に従い，到着はポアソン分布に従うものとする．また，Domain A, B 間，Domain B, C 間とも契約レートはそれぞれ 20 Mbps とする．

4.2 DSCP 再設定パケット数の変化

図 4 の Flow a を 1 Mbps，20 本の UDP トラヒックとし Flow b, c, d を 0 Mbps の状態とする．また，Flow a のユーザ・ドメイン間の契約レートは十分に大きく，Domain A のエッジルータに到着するパケットは全て in-of-profile となるものとする．この状態で Domain A, B 間および B, C 間で DSCP 再設定されるパケット数を測定するシミュレーションを行った．

表 1 に Domain B および C のエッジルータに到着したパケットの DSCP を再設定した結果を示す．Flow a はあわせて 20 Mbps の UDP トラヒックであり Domain A, B 間の契約レート 20 Mbps

表 1　ドメイン入口でのパケット数

	DSCP	Domain B ingress		Domain C ingress	
Conventional	Total	7486073	(100%)	7486073	(100%)
	IN	7450456	(99.524%)	7436151	(99.333%)
	OUT	35617	(0.476%)	49922	(0.667%)
Proposed	Total	7494078	(100%)	7494078	(100%)
	green	7455264	(99.482%)	7455520	(99.485%)
	yellow	38814	(0.518%)	38558	(0.515%)
	red	0	(0%)	0	(0%)

と等しいが，パケットの到着間隔の変動により，一時的にドメイン間の契約レートを超えてパケットが到着することがある．このため，従来方式，提案方式共に，Domain A, B 間で約 0.5 % のパケットが再設定され，OUT および yellow になっている．従来方式では Domain B, C 間でさらに IN から OUT への再設定が起こり，Domain C 内の OUT パケット数は Domain B 内の OUT パケット数より，さらに 40 % 増加している．しかし，提案方式では，Domain B, C 間に到着する green, yellow をあわせて到着レートを計算するため，契約レートを超え，yellow に再設定されるパケット数は Domain A, B 間で yellow に再設定されるパケット数とほぼ同じ値となっている．このため，提案方式では複数ドメインを経由するごとに IN パケットが減少することを防いでいると言える．

4.3 パケット損失率への影響

図 4 の Flow a を 1 Mbps，x 本の UDP トラヒック，Flow b を 0 Mbps，Flow c を 5 Mbps の UDP トラヒック，Flow d を 25 Mbps の UDP トラヒックとする．Flow a および Flow c のユーザ・ドメイン間の契約レートは十分大きく，エッジルータに到着したパケットは全て in-of-profile となり，Flow d 契約レートは 0 Mbps で到着パケットは全て out-of-profile となるものとする．また Domain C にあるボトルネックリンクの帯域を 25 Mbps とする．このときの Flow a のパケット損失率を測定するシミュレーションを行った．

図 5 に Flow a のフロー数を X 軸としたときのパケット損失率を示す．比較対象としてドメイン間の契約レートが十分に大きく，ドメイン境界で DSCP の再設定が起こらない場合のパケット損失率 (No Re-marking) を併せて示す．従来方式では Flow c の影響から x の値が 15 本以上で Domain A, B 間に到着する IN の到着レートがドメイン間契約レートの 20 Mbps を超えるため，IN から OUT への再設定が頻繁に起こる．従来方式では

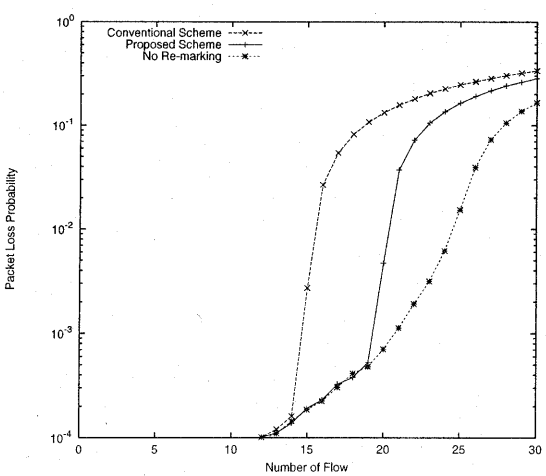

図 5　複数ドメインを経由するフローのパケット損失率

Domain A, B 間で OUT になったパケットが Domain C 内のボトルネックリンクで廃棄されるため，パケット損失率が高くなっている．一方，提案方式では，x が 15 本以上で従来方式と同様 Domain A, B 間で green から yellow への DSCP の再設定が起こる．しかし，Domain B, C 間に到着した green と yellow のパケットはドメイン間契約レートの 20 Mbps を基に DSCP を再設定される．このため，x の値が 20 本より小さい場合はボトルネックリンクに到着するパケットのほぼ全てが green パケットであるため性能限界である全パケットが IN でボトルネックリンクに到着する場合のパケット損失とほぼ同じになっている．また，x の値が 20 本以上でも，20 Mbps 分のパケットは green パケットとなって Domain C 内に送信されるため，従来方式より提案方式の方がパケット損失率が小さくなっている．

4.4 ドメイン内フローとの公平性

図 4 の Flow a を 1 Mbps，x 本の UDP トラヒック，Flow b を Flow a と同じく 1 Mbps，x 本の UDP トラヒック，Flow c を 10 Mbps の UDP トラヒック，Flow c を 30 Mbps の UDP トラヒックとする．Flow a, b, c のユーザ・ドメイン間の契約レートは十分大きく，エッジルータに到着したパケットは全て in-of-profile となり，Flow d の契約レートは 0 Mbps で到着パケットは全て out-of-profile となるものとする．また，Domain C にあるボトルネックリンクの帯域を 30 Mbps とする．このときの Flow a, b のパケット損失率とスループットを測定するシミュレーションを行った．

図 6 はフロー数を変化させたときパケット損失率を示すグラフであり，図 7 はフロー数を変化させたときの 1 フローあたりのスループットを示すグラフである．従来方式では x の値が 10 本より小さい時，ドメイン内フローとドメイン間フローとの間でパケット損失率，スループット共に差はない．しかし，x の値が 10 本になると Domain A, B 間の契約レートと Domain A, B 間に到着する IN パケットのレートが同じになる．このため，x の値が 10 本以上になると，頻繁に契約レートを超えて IN パケットが到着し，そのパケットは OUT パケットに再設定される．OUT パケットはボトルネックリンクで廃棄されやすいので，x の値が 10 本以上になるとドメイン内フローと比べてドメイン間フローはパケット損失率が高くなる．また，スループットも低下し，ドメイン間フローとドメイン内フローとの間で公平性が保たれていない．一方，提案方式では x の値が 10 本以上になると，従来方式と同様に Domain A, B 間で green から yellow への再設定が生じる．しかし，Domain B, C 間で green と yellow のパケット到着レートがドメイン間契約レートの 20 Mbps より小さければ Domain A, B 間で yellow に再設定されたパケットも green に再設定さる．すなわち，x の値が 20 本より小さい場合，ほとんどのパケットは green の状態でボトルネックリンクに到着する．このため，ドメイン間フローとドメイン内フローとの

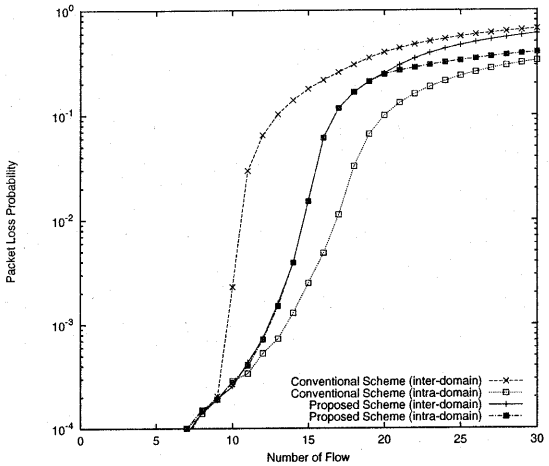

図6 ドメイン間フローとドメイン内フローのパケット損失率

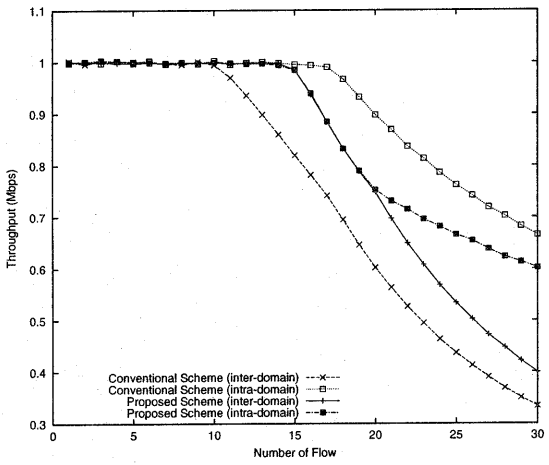

図7 ドメイン間フローとドメイン内フローのスループット

間でトラヒック条件に差が小さく，パケット損失率，スループット共にほぼ同じ値となっており，公平性が保たれている．例えば $x = 15$ の時，従来方式のドメイン間フローのパケット損失率は 1.784×10^{-1}，ドメイン内フローでは 2.494×10^{-3} となっており 100 倍近い差があるのに対し，提案方式のドメイン間フローのパケット損失率は 1.529×10^{-2}，ドメイン内フローでは 1.512×10^{-2} となっておりフロー間の差が小さい．また，スループットも従来方式では，ドメイン間フローが 0.820 Mbps，ドメイン内フローが 0.995 Mbps と 0.175 Mbps の差があるのに対し，提案方式はドメイン間フローでは 0.985 Mbps，ドメイン内フローでは 0.984 Mbps と差が小さい．x の値が 20 本を超えると提案方式でもドメイン間フローが不利になるが，従来方式のフロー間の差よりも，提案方式のフロー間の差の方が小さく，提案方式の効果が出ていることが言える．

5. ま と め

本研究では複数ドメインを経由して AF サービスを提供する場合，ドメイン境界での IN パケットの再設定による品質が劣化する問題を解決する，新しいコードポイント再設定方式を提案した．提案方式の基本的な性能評価のため UDP トラヒックによるシミュレーションを行った結果，提案方式では従来方式よりも IN パケットの減少を防ぎ，パケット損失率を減させ，ドメイン内フローとドメイン間フローの間の公平性を保つことを示した．

今回は提案方式の基本的な性能を調査するため UDP トラヒックを用いたが，本来 AF サービスは TCP での利用を想定している．このため，提案方式が TCP のフロー制御にどのような影響を及ぼすかを，今後調査していく．

文 献

[1] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss, "An Architecture for Differentiated Services," *RFC 2475*, Dec. 1999.

[2] K. Nichols, S. Blake, F. Baker and D. Black, " Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," *RFC 2474*, Dec. 1998.

[3] V. Jacobson, K. Nichols and K. Poduri, "An Expedited Forwarding PHB," *RFC 2598*, June 1999.

[4] J. Heinanen, F. Baker, W. Weiss and J. Wroclawski, "Assured Forwarding PHB Group," *RFC 2597*, June 1999.

[5] W. Fang, "The "Expected Capacity" Framework: Simulation Results," *Princeton University Technical Report*, TR-601-99, Jan. 1998.

[6] K. Kumazoe, Y. Hori, T. Ikenaga and Y. Oie, "Quality of Assured Service through Multiple DiffServ Domains," *IEICE Transactions on Information and Systems*, Vol.E85-D, No.8, pp.1226-1232, Aug. 2002.

[7] W. Fang, N. Seddigh and B. Nandy, "A Time itiding Window Three Colour Marker (TSWTCM)," *RFC 2859*, June 2000.

[8] S. Floyd and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," *IEEE/ACM Transactions on Networking*, Vol. 1, No. 4, pp. 397-413, Aug. 1993.

[9] D. D. Clark, W. Fang, "Explicit Allocation of Best Effort Packet Delivery Service," *IEEE/ACM Transactions on Networking*, Vol. 6, No. 4, pp. 362-373, Aug. 1998.

[10] The VINT Project, "Network Simulator version 2," `http://www.isi.edu/nsnam/ns/`.