QoS制御付き情報コンセントのための遠隔機器制御プロトコル

秋成 秀紀† 西村 浩二‡ 田島 浩一‡ 相原 玲二‡
†広島大学大学院 工学研究科 ‡広島大学 情報メディア教育研究センター

近年のネットワークの普及を受け，大学や公共施設等では情報コンセントを設置し，ネットワークサービスを提供するようになった．そのようなサービスの中には，外部トラフィックの影響を受けやすい実時間トラフィックも多くなりつつある．しかし，すべての利用者に十分な帯域を提供することは困難であり輻輳等によりパケットロスが生じる．そのため特定のパケットを優先するQoS制御が必要となる．そこで，本研究では，我々が提案している情報コンセントにおけるアクセス制御機能のモデルに対してQoS制御機能を導入し拡張することで統一的にアクセス制御，優先制御が行えることを示す．また，モデルに基づく実装とその評価を行う．

A class of Remote Appliance Control Protocol for information outlet systems with QoS control

Hidenori Akinari†, Kouji Nishimura‡, Kouichi Tashima‡ and Reiji Aibara‡
†Graduate School of Engineering, Hiroshima University
‡Information Media Center, Hiroshima University

Recently, information networks have gained a tremendous popularity. Information outlet systems have been installed at universities and public centers to provide various services. The provided services are including stream data delivery such as VCD system which is influenced by other traffic. Sharing of limited resources causes rise of packet loss due to collisions by traffic congestion. A QoS Control is necessary to prevent the packet loss of a specified stream by giving priority to the packets. In this paper, We propose an access control model including QoS control. We also demonstrate an implementation of an information outlet system based on the model and evaluation of the system performance.

1 はじめに

近年のコンピュータの小型高性能化とネットワークの普及に伴い，多くの人々が携帯端末を持ち歩くようになり，コミュニケーションや情報源のひとつとしてネットワークを通して提供されるさまざまなサービスを利用するようになりつつある．これらを受け，大学に代表されるような施設等では，オープンスペースに情報コンセントを設置しネットワークへの接続環境を提供するようになった．このような情報コンセントは，誰でも手軽に利用できる性質を持つため，不正使用によるネットワーク資源の浪費やサービス妨害などからセキュリティを確保するための機能が必要となる．そのため利用者認証による利用資格の有無に基づきアクセス制御を行う情報コンセントシステムの研究がいくつかなされている（これらの研究については，参考文献[1]中の関連研究として挙げられている参考文献を参照されたい）．

一方，ネットワークを通して提供されるサービスの中には，VOD(Video On Demand)に代表されるようにサウンドデータや動画データをネットワーク経由で受信しながら順次再生するストリーミング配信などの実時間トラフィックもあり，これらはますます多くなりつつあり，また個々の要求する帯域も増加傾向にある．一般にこれらのトラフィックは，その他のトラフィックの影響を受けやすい．しかし，情報コンセント利用者のすべてのトラフィックに十分な帯域を提供することは困難であり，ネットワークの集約するアップリンクにおいて，集約トラフィックの帯域がネットワークの収容能力を超えると，輻輳状態となりその結果パケットロスを生じることになる．そこで，情報コンセントにおいて特定のトラフィックを優先的に処理するQoS(Quality of Service)制御が必要となる．また，大学等における教育目的のためのトラフィックも，その目的からその他のパケットよりも優先的な処理を必要とされている．

情報コンセントにおいてQoS制御を行う場合，アクセス制御の場合と同様に利用者単位で管理または制御が出来ることが望まれる．これは，利用者認証を行いその結果に基づき制御を行うことを意味する．我々は，既に情報コンセントにおけるアクセス制御機能のモデル化を行い，そのモデルに対する制御プロトコルとして遠隔制御機器プロトコルRACP(Remote Appliance Control Protocol)の枠組に基づいた提案を行っている．本研究では，このモデルに対してQoS制御機能を導入し拡張することで，統一なコマンドによりアクセス制御，優先制御が行えることを示す．また，QoS制御付き情報コンセントシステムとしてPortGuardシステムの実装とその評価を行い，RACPによる制御の実用性を示す．

2 QoS(Quality of Service)

現在，インターネットにおけるQoS制御に関するさまざまな研究が行われているが，ここでは本研究が対象としている情報コンセントにおけるQoS制御についての考察を行い，我々が提案するQoS制御付き情報コンセントシステムの制御手法とその他の研究について示す．

2.1 情報コンセントにおけるQoS制御

一般に大学や公共施設等における組織内の通信は，広域ネットワークに対する通信に比べて大きな帯域を利用できる．また，情報コンセントで使用されるスイッチや無線基地局も10Mbps~100Mbpsもの転送速度を持つものが使用されている．そのため，大学では，録画した講義を個々の利用者の要求に応じて利用者毎に配信するVODサービスや講義における資料をネットワーク上から取得できるサービスの提供を行うようになり，そこで情報コンセントが使用されるようになりつつある．

しかし，ネットワーク資源は有限であるため情報コンセントに利用している接続装置のアップリンク上では，集約トラフィックの帯域が収容能力を超えると，輻輳状態となりパケットロスを生じてしまう．また，突発的なトラフィックの発生が原因で実時間トラフィックに悪影響を及ぼすことがある．そこで，情報コンセントシステムにおいてトラフィックを区別し，それぞれ異なる取扱いを行うQoS制御機能が必要となる．

情報コンセントシステムにおけるQoS制御の対象となるトラフィックは，図1のように，特定のホストから送信されてくるトラフィックと情報コンセントの利用者端末から送信されるトラフィックの2つに分類することが出来る．

一方，一般に情報コンセントシステムでは，不正使用を防止するためにも利用者認証に基づくアクセス制御と連携して機能することが望まれる．また，特定の人がサービスを利用し続けることは好ましくないため，時間によるサービス制御が行えることも必要である．

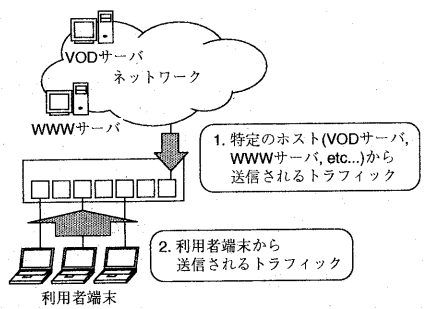

図 1: QoS制御対象トラフィック

2.2 PortGuardシステム

我々は，既に情報コンセントシステムにおけるアクセス制御機能のモデル化を行い，RACPの枠組に従い制御プロトコルを定義している．また，そのプロトコルを使用し，有線LANと無線LAN環境のそれぞれで使用可能な情報コンセントシステムとしてPortGuardシステムを開発し[1][2]，ソースの公開を行っている[7]．そこで，本研究では，この情報コンセントシステムのモデルに先に述べたQoS制御機能と時間による制御機能を取り込み拡張を行うことで，QoS制御可能な情報コンセントシステムを実現する．

情報コンセントにおける必要なQoS機能は，特定のトラフィックに対して他のトラフィックよりも優先的に処理することにより実現できる．そこで，本研究では，サービスの違いを優先度で表現し，その値に基づき処理を行う優先制御方式を用いる．

2.3 その他の研究

本研究での着目点は，情報コンセントシステムのサービスのひとつとしてQoS制御を捉え，認証の結果に基づきアクセス制御とQoS制御が統一的なコマンドにより管理，制御出来ることにあり，このような視点による研究は，ほとんどないのが現状である．その他のアプローチとしては，認証後に既存の方法で制御する方法もあり，そのひとつとしてRSVP(Resource ReServation Protocol)[4]とCOPS(Common Open Policy Service)プロトコル[5]を用いる方法もある．しかし，RSVPではEnd-to-Endでのネゴシエーションを前提としており，アプリケーションレベルでの対応が必要であるが，現状では既存の多くのアプリケーションが未対応であり，利用者が直接機器の制御をすることも現実的ではない．同様にCOPSに対応している機器も現状では少ない．また，情報コンセントにおけるQoS制御では，利用状況に会わせた制御や時間による制御などが必要となり，既存の方法で実現すると，繁雑なシステムとなってしまう．そのため，情報コンセントにおけるこれらの機能を制御する方法としては，本研究のアプローチが自然であると考えられる．

3 モデル化とRACPによる制御

ここでは，我々が既に提案した情報コンセントシステムのアクセス制御モデルに対して，QoS制御に関する機能を導入し拡張したモデルを示し，そのモデルに対する制御プロトコルについて述べる．

3.1 QoS制御付き情報コンセントシステムのモデル化

図2に拡張した情報コンセントシステムのモデルを示す．モデル化した情報コンセントシステムは，内部に複数のVLANを持つ．それぞれのVLANには，複

数の物理ポートを割り当てることが可能であり，また，物理ポートの入出力方向に対して複数のフィルタを設定することにより，一致するパケットの入出力の許可を制御し，QoS 制御のための優先度付けを行う．物理ポートに設定されるフィルタは、リスト構造で管理され，その物理ポートにパケットが到着するとフィルタを順番に評価し，最初に一致したフィルタが適用される．

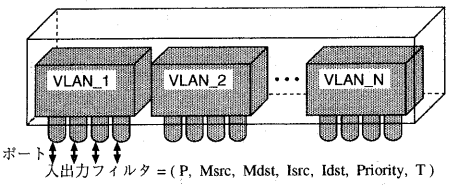

図 2: QoS 制御付き情報コンセントシステムモデル

このフィルタは，対象となるパケットの指定に使用される物理ポート番号 (P)，始点 MAC アドレス (M_{src})，終点 MAC アドレス (M_{dst})，始点 IP アドレス (I_{src})，終点 IP アドレス (I_{dst}) と対象となるパケットの処理を指定する 優先度 ($Priority$)，利用時間 (T) の合わせて 7 項目で構成され，$(P, M_{src}, M_{dst}, I_{src}, I_{dst}, Priority, T)$ のように表すことが出来る．優先度は，フィルタに一致するパケットの処理される優先度を 0~7 の 8 段階で示し，利用時間 (T) とは，設定されたフィルタの有効時間を示す項目である．有効時間の切れたフィルタは無効となり削除される．また各項目には，ワイルドカード "*" を指定することが出来，各項目でワイルドカードが指定された場合の解釈は，表 1 の通りである．

表 1: 各項目でのワイルドカードの意味

項目名	意 味
P	任意の物理ポートに一致
M_{src}, M_{dst}	任意の MAC アドレスに一致
I_{src}, I_{dst}	任意の IP アドレスに一致
$Priority$	デフォルトの優先度
T	無制限の利用時間

本モデルのシステムは，内部に 8 段階の優先度の異なる送信バッファを持ち，フィルタにより優先度付けされたパケットは，その優先度に従いそれぞれの送信バッファに送られる．送信バッファでは，優先度に従いバッファからパケットを送信することで優先制御を実現している．本モデルを用いて，情報コンセントで必要とされる以下の 4 つの制御を表現することが可能である．

- ネットワーク接続制御
- ネットワーク到達制御
- QoS 制御 (優先制御)
- 利用期間制御

ここで，利用目的に応じた QoS 制御のためのフィルタの設定例を図 3 に示す．図では，IP アドレス I_5 を持つ端末を使用する情報コンセントの利用者が VOD サーバから送られてくるパケットに対する QoS 制御の要求に対して，VOD サーバの IP アドレス I_{vod} を始点 IP アドレスに持ち，情報コンセント利用端末の IP アドレス I_5 を終点 IP アドレスとして持つパケットに対して高優先度 (7) のフィルタをアップリンクの入力方向に設定することによって実現している．情報コンセントとして用いる機器によって，使用できる優先度が異なる場合は，IEEE802.1Q のユーザー・プライオリティとトラフィック・クラスの対応付けに従い制御を行う [6].

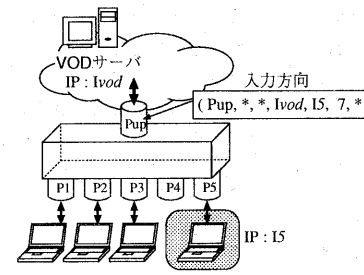

図 3: QoS 制御のためのフィルタ設定例

3.2 RACP によるモデルの制御

RACP は，ネットワークを通して遠隔にある機器を制御するための通信規約である．RACP の特徴としては，制御対象となる機器で必要とされる機能のモデル化を行い，そのモデルに対して制御方法を定義していることが挙げられる．そのため，制御を行う際に，制御対象となる機器の種類やメーカ，本来の制御方式を意識する必要が無く，機器構成の変更が生じた場合にも容易に対応が可能となる．

我々は，既に情報コンセントシステムのアクセス制御機能のモデルに対する制御プロトコルとして RACP を用いており，その枠組に従い VLAN サブユニットコマンドを定義している．そこで以下では，本研究で情報コンセントシステムのモデルに拡張した QoS 制御と利用期間制御のために使用される VLAN サブユニットコマンドについて取り上げる．表 2 には，VLAN サブユニットコマンドの一覧を載せてある．

[QoS 制御] QoS 制御のための優先度フィルタの設定は，フィルタ設定コマンド (FILT) で行う．フィルタの追加・削除は，それぞれ**ADD** または**DEL** 引数を用い，**IN** または**OUT** 引数でフィルタの方向を指定する．フィルタを設定する物理ポートは，VLAN 識別子 (n) と物理ポート番号 ($port$) の組み合わせで指定し，その物理ポートを通過する対象パケットを始点 MAC アドレス (mac_{src})，終点 MAC アドレス (mac_{dat})，始点 IP アドレス (ip_{src})，終点 IP アドレス (ip_{dst}) で指定する．優先度 ($priority$) は，0~7 の 8 段階で指定することが出来る．

表 2: VLAN サブユニットコマンド一覧

コマンド解説	コマンド書式
物理ポート設定	VLAN *n* PORT ADD *port*[*port2*[...]] [*start_time* : *end_time*] [LINKUP] VLAN *n* PORT DEL *port*[*port2*[...]]
フィルタ設定	VLAN *n* FILT ADD {IN|OUT} *port* mac_{src} mac_{dst} ip_{src} ip_{dst} [Priority] [*start_time* : *end_time*] [LINKUP] VLAN *n* FILT DEL {IN|OUT} *port* mac_{src} mac_{dst} ip_{src} ip_{dst}
ステータス表示	VLAN n STAT [{PORT [*port*] | FILT [{IN|OUT} *port* mac_{src} mac_{dst} ip_{src} ip_{dst}]}]
トラップ設定	VLAN n TRAP [ALL|PORT|FILT]
ヘルプ表示	VLAN n HELP [PORT|FILT|STAT]

[利用時間制御] 利用時間制御のための有効時間の指定は，物理ポート設定コマンド (PORT) とフィルタ設定コマンド (FILT) において，開始時間 (*start_time*) と終了時間 (*end_time*) の組合せて，*start_time* : *end_time* のように指定することで行う．終了時間の過ぎた物理ポートは，現在の VLAN から削除され，デフォルトの VLAN に追加される．また，終了時間の過ぎたフィルタは，同様に削除される．

4 実装とその性能評価

この節では，提案したモデルに基づき実装を行った 2 種類のコントローラを用いた QoS 制御付き PortGuard システムについて述べ，性能測定に基づく評価を行う．

4.1 QoS 制御付き PortGuard システム

我々は，既に PortGuard システムのアクセス制御のために，VLAN 機能を持つ Cisco 社のスイッチングハブを制御するスイッチングハブコントローラ (以下，HUBctrl) と機器自身にアクセス制御機能を持たない無線基地局やダムハブのような機器において，アップリンクに接続したホストでフィルタリングを行うことでアクセス制御を実現するフィルタコントローラ (以下，FILTctrl) をモデルに基づき実装している．

そこで，本研究では QoS 制御のために，HUBctrl に対して，Cisco 社の Catalyst3500 XL シリーズの持つ 2 段階の PRIQ(PRIority Queueing) 機能を制御するように拡張を行った．また，QoS 制御機能を持たない機器において，アップリンクに接続したホストで ALTQ(ALTernate Queueing)[3] を制御することで QoS 制御を実現する ALTQ コントローラ (以下，ALTQctrl) をモデルに基づき実装した．ALTQ は，ルータ上でさまざまな種類のキューイング制御を可能とするもので多くの BSD 系の OS 上で実装されている．本研究では，KAME カーネルの FreeBSD 上で ALTQctrl の実装を行った．図 4 に HUBctrl を用いた QoS 制御付き PortGuard システムの概要を (*a*) に ALTQctrl を用いたものを (*b*) に示す．

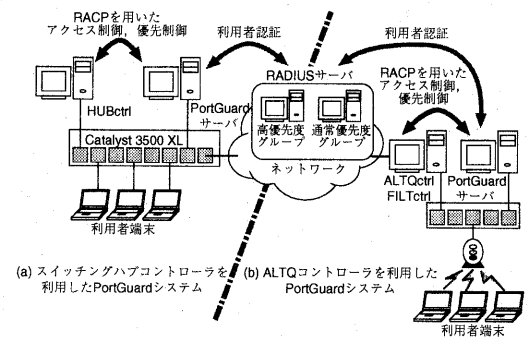

図 4: PortGuard システム概要

本システムでは，図 4 に示されるように高優先度の利用が許可されている利用者の認証情報が登録されている RADIUS サーバと通常の利用者が登録されている RADIUS サーバの 2 台を用いて順に認証を行うことでポリシー制御を行う．高優先の使用資格を持つ利用者の場合は，ネットワークの使用許可 (アクセス制御) に続き，優先許可 (QoS 制御) を行う．

4.2 処理の流れ

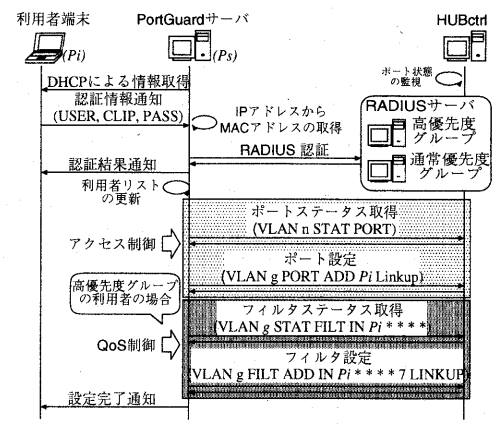

図 5: PortGuard システムの処理手順

HUBctrl を用いた PortGuard システムでの処理の流

れを図5に示す．図中のPortGuardサーバとHUBctrl間の網目掛けの部分が，RACPを用いたアクセス制御とQoS制御の部分であり，RACPを用いることにより統一的なコマンドでアクセス制御とQoS制御が行えていることが分かる．ここでは，HUBctrlを用いた場合の手順のみを載せてあるが，FILTctrlとALTQctrlを組み合わせた環境においても各RACPコマンドの引数を変えることのみで，同様にアクセス制御とQoS制御を実現することができる．このように，RACPを用いて，情報コンセントとして使用している機器の制御方法や機能の相違点を吸収することにより，複数機器の混在する環境での制御を容易にし，また，使用機器の変更における管理コストを抑えることが出来る．

4.3 性能測定

実装したHUBctrlとALTQctrlの性能測定のために図6に示される環境で以下の手順に従いRACPを用いて優先制御を行った．図6中のホストのスペックは、表3に示してある．また，ALTQctrlの測定では，キューイング制御方式としてPRIQとCBQ(Class Based Queueing)をそれぞれ用いて行った．

1. HostAとHostBからHostCに向けて同時にトラフィックを送信(ALTQctrlの測定では，HostDに向けて送信)．
2. スループット測定開始から20秒後にHostBから送信されるトラフィックを優先するようにRACPを用いてフィルタの設定を行う．
3. スループット測定開始から40秒後に，RACPを用いて2で設定したフィルタの削除を行う．

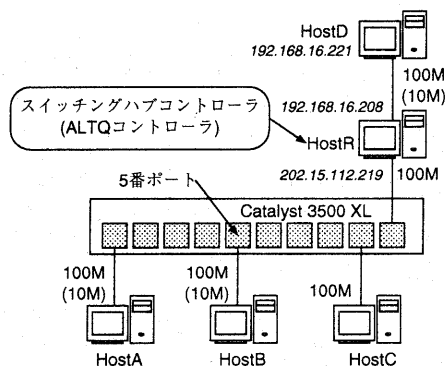

図 6: 測定環境

上記の制御をHUBctrlに対して行った時のスループットを図7に示す．また，図8には，ALTQctrlでPRIQを用いた場合のスループットを示す．図より期待通りの制御結果が得られていることが分かる．

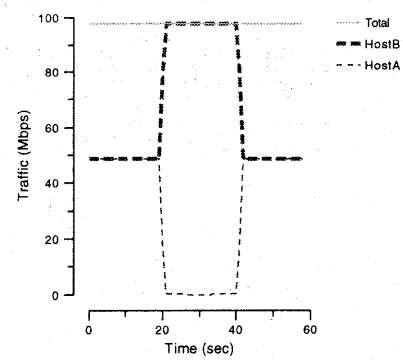

図 7: HUBctrlの優先制御結果

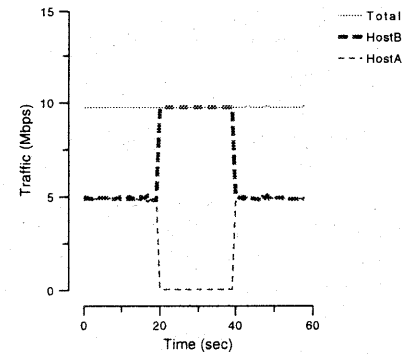

図 8: ALTQctrlの優先制御結果

4.4 通信遅延，処理時間の測定とその評価

RACP制御によるオーバヘッドを考察するために，実装したHUBctrlとALTQctrlに対して優先制御に要する通信遅延と処理時間の測定を行った．各コントローラに接続してから優先度付けを行うフィルタを設定するまでに必要となるRACPコマンドをタイムチャートに沿って示してものを図9に載せてある．括弧に囲まれたRACPコマンドは，ALTQctrlを用いた場合に使用されるものである．図中の(1) ～ (3)の数字は，それぞれ測定区間を示してあり，(1)は，RACPサーバ(HUBctrl，ALTQctrl)に接続要求を出してからフィルタの設定が終わるまでの区間を示し，(2)はフィルタの設定を行うRACPコマンドを送信してから，そのコマンドの応答を受信するまでの区間を表しており，最後の(3)はRACPサーバにおいてフィルタ設定要求を受信してから設定を行うまでの区間を表している．

測定は，HUBctrlとALTQctrlに対しての制御をそれぞれ1000回行った．その測定値を平均したものを表4に示す．

RACPを用いたことによるオーバヘッドは，(1)の設定に要する総時間から(3)の設定変更に要する時間を引いた値であり，性能測定の結果(表4)から約6.4ミリ秒と小さくほとんどないと考えられる．また，実

表 3: 使用機器のスペック

	HostA, HostB	HostC, HostD	HostR
CPU	PentiumIII-866MHz	PentiumIII-750MHz	PentiumIII-500MHz
Memory	128MB		256MB
OS	Vine Linux 2.2.17-0vl10		FreeBSD 4.3-Release + KAME(snap_20010731)

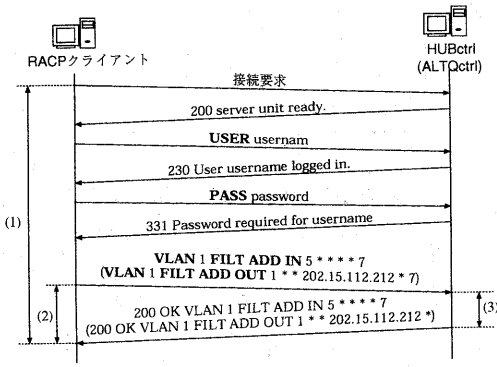

図 9: RACP によるフィルタ設定の流れ

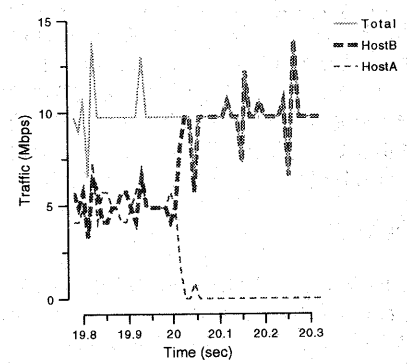

図 10: 19.8~20.3 秒間を 10ms 間隔で表示

装を行った HUBctrl と ALTQctrl による QoS 制御のために必要な処理時間も，より時間を要した HUBctrl においてもおよそ 800 ミリ秒であり，実用上十分に耐えうると考えられる．

表 4: 測定結果

測定区間	ALTQctrl	HUBctrl
(1) 設定に要する総時間	6.9545	753.4765
(2) フィルタ設定に要する時間	0.9648	747.5232
(3) 設定変更に要する時間	0.6334	747.2021
往復応答時間:(2)-(3)	0.3314	0.3211
RACP オーバヘッド:(1)-(3)	6.3211	6.2744

(単位:ミリ秒)

また，ALTQctrl は，QoS 制御を PC ベースのルータ上に組み込むまれたキューイングシステムを利用することで実現しているため，設定したフィルタが実際に反映されるまでの遅延が考えられる．そこで，スループットの測定から 20 秒後に RACP による制御を行った図 8 のグラフの 19.8~20.3 秒間を 10 ミリ秒間隔で表示したものを図 10 に示す．

図 10 から 20 秒後のおおよそ 100 ミリ秒以内に設定が反映されていることが分かり，実用上問題ないと考えられる．

5 おわりに

本研究では，情報コンセントシステムにおける QoS 制御についての考察を行い，次に RACP の枠組に従い拡張した QoS 制御付き情報コンセントシステムのモデル化とそれを制御するための RACP コマンドについて述べた．また，実際にモデルに基づき実装した HUBctrl と ALTQctrl を用いて QoS 制御を可能とした PortGurad システムの構築を行い，RACP を用いることにより統一的なコマンドでアクセス制御と QoS 制御が可能になることを示した．また，性能測定を通じて本提案手法と実装したシステムが実用に耐えうることを示した．

参考文献

[1] 西村 浩二, 秋成 秀紀, 相原 玲二: “遠隔機器制御プロトコルによる情報コンセントのアクセス制御”, マルチメディア, 分散, 協調とモバイル (DICOMO 2000) シンポジウム論文集, pp.523-528(2000)

[2] 野村 嘉洋, 秋成 秀紀, 田島 浩一, 西村 浩二, 相原 玲二: “遠隔機器制御プロトコル RACP を用いた無線 LAN 認証システム”, 情処研報, DSM-22-8, pp.45-50(2001).

[3] Kenjiro Cho, “Managing Traffic with ALTQ”, In Proceeding of USENIX 1999 Annual Technical Conference: FREENIX track, Monterecy CA, Jun. 1999

[4] R. Branden, L. Zhang, S. Berson, S. Herzog, S. Jamin, “Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification”, RFC2205, Sep. 1997

[5] D. Durham, Ed., J. Boyle, R. Cohen, S. Herzog, A. Rajan, A. Sastry, ”The COPS (Common Open Policy Service) Protocol”, RFC2748, Jan. 2000

[6] IEEE: ”IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks”: IEEE Std 802.1Q (1998)

[7] 広島大学情報メディア教育研究センター (情報通信基盤系): PortGuard, on-line available at http://www.portguard.org/