2G−2

ユーザ情報を利用したトラフィック制御技術の研究*

森山 斉† 藤崎 智宏† 浜田 雅樹†

NTT ソフトウェア研究所‡

1 はじめに

現在，多くの企業がインターネットに接続し，ネットワーク上の資源を利用できる環境が整いつつある．これら企業は，インターネットに接続するための対外線を保持している．最近では，LAN 内ユーザの増加，WWW（World Wide Web）やストリーミングアプリケーションなどによるトラフィックの増加により，インターネットに接続するための対外線にかかる負担は増加傾向にある．

現在，特定のトラフィックフローの優先処理を目的とするトラフィック制御手法は幾つか存在している．これらは IP アドレス，ポート番号といった情報を用いてトラフィック制御を行っている場合が多い．したがって，組織内ホストの IP アドレスが DHCP を用いて動的に割り振られる場合や，このホストに複数のユーザがログインしてインターネットテレビ会議システムのアプリケーションを利用していた場合，このホストから生成される緊急会議だけのトラフィックフローを特定する事は困難となる．このような場合には，緊急会議を行うユーザの情報を用いれば容易にトラフィックフローを特定化することができる．

そこで，本研究においてユーザ情報を用いたトラフィックフロー優先処理を目的としたトラフィック制御技術の提案を行う．提案するシステムによって，特定のユーザからのパケットを優先してインターネットに接続するための対外線へ通す事ができるようになる．

2 既存技術

現在，トラフィックフローの優先処理を目的としたトラフィック制御機器が幾つか存在している．このような特定のトラフィックフローの優先処理を目的とするトラフィック制御機器は，IP アドレス，ポート番号といった情報を用いてトラフィック制御を行っている場合が多い．しかしながら，これら既存のトラフィック制御手法では以下のような問題が考えられる．

1. 動的な IP アドレスの割当に対応できない問題
   DHCP を利用している環境において，ホストの IP アドレスが動的に変化する場合の状況に対応できない．

2. 同一ホスト上のユーザの区別ができない問題
   同じホストを用いるユーザは，同様の権限を持つ事になり，詳細な優先制御を行えない．
   また，1 つのホストに複数のユーザがログインしている場合に同じホストから送り出されるトラフィックフローを特定する事が難しい．

3. ユーザ間での公平な資源配分ができない問題
   複数のホストを用いるユーザは，各ホスト毎に帯域を割り当てられることになり，他のユーザに対して優位性が生じる．

そこで，トラフィックフローの属性としてユーザの情報（ユーザ ID，アカウント etc.）を利用して，トラフィックフローを特定化する事を考える．

また，トラフィックフロー優先処理に関係する技術として RSVP(Resource reSerVation Protocol)[Bra97] が提唱されている．RSVP は，QoS 保証を行うための帯域予約プロトコルである．リソースを確保するポリシやトラフィック制御モジュール機構に関しては規定がなく，実装ごとに別途用意する必要がある．

RSVP を用いることにより，トラフィックフロー毎に細かな指定が行なえるが，多くのユーザが細かく品質を指定すると回線帯域の利用効率が低下し，優先度の低いユーザは実質ほとんど利用できなくなる問題が生じると考えられる．そこで，利用効率を上げるためにトラフィックフロー毎の重み付けを行なう事を考える．例えば，利用時間に対して優先度が下がるように設定できれば，優先度の低いユーザは実質ほとんど利用できないといった状況を回避できる．

既存技術でのトラフィックフローに対しての重み付けは，各通信毎に行なわれているため短期的なスパンでしか重み付け処理が行なえない．そこで，本研究では，個々のユーザの使用履歴を参照することにより長期的になスパンでの重み付け処理を考える．これにより，既存技術では行なえなかったユーザの利用期間に対して使用制限を実現できる．

しかしながら，トラフィックフローの優先を行なうためには，どのユーザからの要請かを判断する必要がある．すなわち成りすましや改ざんといった手段を回避できなければ，実際にトラフィックフローの優先を行なって良いのかが判断できない．そこで本研究では，ユーザ毎の認証に対して IPsec[Ken98] 等を利用してセキュリティの問題点を解決する．

3 ユーザ情報を利用したトラフィック制御技術

トラフィックフローの優先処理を目的としたトラフィック制御機構に対してネットワーク管理者から要求される条件について，本稿では以下のように考える．

1. 組織内ネットワークは，統一したポリシによって運営できる．

2. 組織内ネットワークのユーザ情報，アプリケーション情報を一意に扱う事ができる．

3. 対外線使用状況に併せたトラフィックフロー優先制御を可能にするため，対外線の使用状況を把握する事ができる．

---

*A Traffic Control Technology using User Information
†Hitoshi Moriyama, Tomohiro Fujisaki, Masaki Hamada
‡NTT Software Laboratories

提案するシステム構成を示す (図 1).

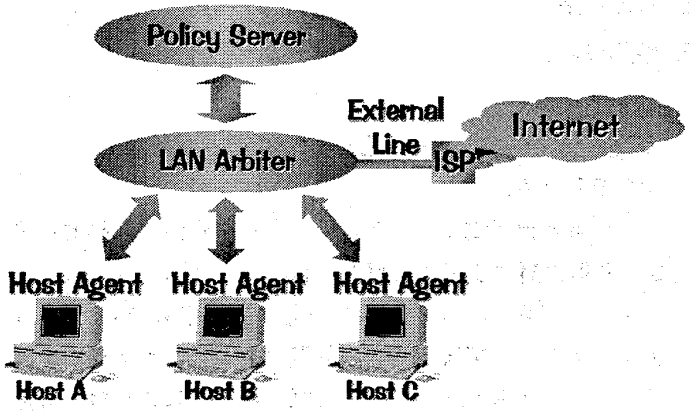

図 1: A system configuration

図における ISP は, LAN へインターネットへの接続ポイントを提供するインターネットサービスプロバイダー, External Line は対外線を表す. 各ホスト (Host A,B,C) 上には HostAgent を実装する. 対外線を通るパケットは, LAN Arbiter を介して ISP に送られる. ここでの, Policy Server, LAN Arbiter, Host Agent の定義を以下に示す.

Policy Server ユーザ情報, アプリケーション情報をもとに対外線に送り出すパケットの優先順位を決定する. ユーザの対外線利用履歴データを利用した時間軸に対して可変なトラフィック制御ポリシを決定する.

LAN Arbiter Policy Server から得たパケット優先順位情報をもとにパケットスケジューリングを行う.

Host Agent LAN Arbiter に対してユーザ情報, アプリケーション情報を送る. また, LAN Arbiter にトラフィックフロー優先処理に対する要請を行う.

3.1 トラフィック制御機構

CBQ[Flo95] では, トラフィックフローに対する動的な重み付けを送出パケット間隔の加重平均を使って実現している.

$$\begin{aligned} f(s,b) &= s/b \\ diff &= t - f(s,b) \\ avg &\leftarrow (1-w)avg + w * diff \end{aligned}$$

ここでの s:送られたパケットのバイト数, b:クラスに割り当てられたバイト数, t:パケット送出間隔, w:重みである. $avg < 0$ でパケットの送出を停止する. また, Hierarchical SCFQ[Rex96] においても動的な重み付けを提案している. しかしながら, トラフィックフローに対しては, ある特定のトラフィックフローといった大まかな内容しか規定されていない. 全てのアドレスとアプリケーションポートの組合せに対して処理を行なうことは大変コストがかかる. またこのコストを軽減するために IP アドレスだけで処理を行なうことが考えられるが, それでは前述の問題に対応できない.

そこで本研究では, ユーザ情報をもとにトラフィックフローの優先処理を行なうことを提案する.

提案する LAN Arbiter のトラフィック制御部を示す (図 2). 入力されたパケット Input Packet は Packet

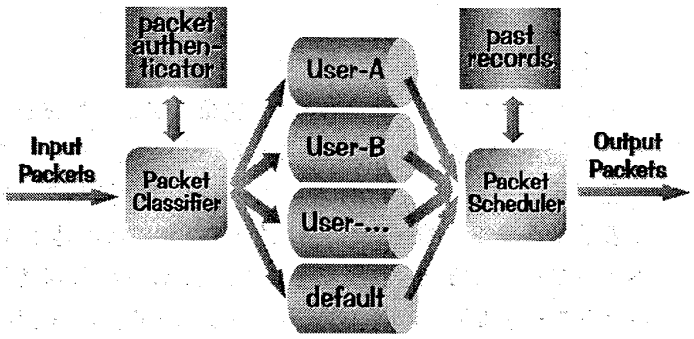

図 2: A traffic control system

Classifier によって識別される. この時, どのユーザから送出されたパケットかを Packet Authenticator が認証を行ない, その情報をもとに個々のキューに入る. 認証に失敗したパケットはデフォルトのキューに入る. Packet Scheduler は, 以前までの利用データを保存する Past record データベースに問い合わせを行なってパケットを順番に取り出す.

現在, 本研究におけるパケットスケジューリングアルゴリズムについては検討段階であるが, アルゴリズムの決定に関して, 以下のような評価基準を考えている.

1. 複数の制御ポリシを容易に実現できる.
2. 実装における処理オーバヘッドが少ない.
3. 処理精度が高い.
4. スケーラビリティがある.

4 今後の予定

今回提案を行なったユーザ情報を利用したパケットスケジューリング機構を実現するアルゴリズムを決定を行なう. また, 情報交換のための実装手法に関して詳細化を行ない, プロトタイプを構築する予定である.

参考文献

[Bra97] Braden, B. ed.: *Resource ReServation Protocol (RSVP) - Version 1 Functional Specification*, September 1997, rfc2205.

[Flo95] Floyd, S. and V. Jacobson: Link-sharing and Resource Management Models for Packet Networks, *IEEE/ACM Transaction on Networking*, Vol. 3, No. 4, pp. 365–386, August 1995.

[Ken98] Kent, S. and R. Atkinson: IP Authentication Header, July 1998, draft-ietf-ipsec-auth-header-07.txt.

[Rex96] Rexford, J. L., A. G. Greenberg, and F. G. Bonomi: Hardware-Efficient Fair Queuing Architectures for High-Speed Network, in *Proceedings of Computer Communications (IEEE Infocom)*, pp. 638–647, March 1996.