3V－1

帯域利用者情報管理による帯域の優先的な利用許可機構の構築

戸田 晴一郎[1] 小川 晃通[1] 徳田 英幸[1,2]

[1]慶應義塾大学大学院 政策・メディア研究科 [2]慶應義塾大学 環境情報学部

1 はじめに

インターネット上で優先的な通信を行なう為に用いる RSVP(Resource reSerVation Protocol)[1] は, 帯域予約要求者が把握できない為, 現状では誰もが帯域予約可能であり不正な予約を拒否できない.

また, ポリシコントロールを行なう為に用いる COPS(Common Open Policy Service)[2] プロトコルや,RSVP で予約者認証を行なう為の提案はそれぞれ行なわれているが公開された実装はなく, それらを統合した予約者識別環境は存在しない.

そこで本稿では RSVP 利用時の予約者認証機構を構築し, 同時に処理軽減の方法について考察する.

2 ポリシコントロール機構

本システムでは, ポリシサーバ (PDP:Policy Decision Point) とポリシクライアント (PEP:Policy Enforcement Point) によって構成される単純なクライアント・サーバモデルを用い, それらの間で COPS プロトコルを用いて帯域予約要求判断を行なう.

PEP はルータ内に存在し,RSVP からのポリシ判断要求の内容を COPS プロトコルに含めて PDP へと転送する. また,PDP は自らが持つ情報と PEP からの情報を比較し, 適切な判断を下す.

3 COPS プロトコルの実装

本システムの実装にあたり, 利用可能な実装が公開されていない COPS プロトコルを, 既存の提案に基づいて実装を行なった.COPS には 10 種のメッセージが規定されており, それらをそれぞれ関数として定義し,PEP,PDP から利用可能とした.

4 予約者識別環境の問題と改善策

本章では提案されている予約者識別環境の問題を挙げ, その改善策を考察する.

キャッシュの利用

RSVP 利用時の帯域予約者を識別する方法として, 現在 [3],[4] が提案されているが, これらの方法を用る場合, PEP が帯域要求情報を受信する度に PDP に対して予約確認を行なわねばならない.

しかし, RSVP は SoftState モデルを採用し, 同一の予約内容を含むリフレッシュメッセージを頻繁に交換する為, 毎回 PDP と通信を行なって予約確認を行なうことは, 冗長な処理となる.

そこで, 本システムでは PEP 内でキャッシュを構築し,PDP の判断とその判断の有効性が保たれる時間を PEP 内に保存する. これにより,RSVP のリフレッシュメッセージが到着した際,PEP 内のキャッシュによって処理時間の軽減が可能となる.

PPDP_ADDR の提案

本システムでは, 一つの PDP が複数の PEP に対応し, ある範囲のポリシドメインを形成する. その際, それぞれの PEP が, 同じメッセージに対して同一の PDP に認証要求を行なうことは冗長な処理である.

そこで本システムでは PPDP_ADDR(Previous PDP Address) を定義し, それにより冗長な処理を軽減する. 図 1 に PPDP_ADDR によって改善されたポリシコントロールモデルを示す.

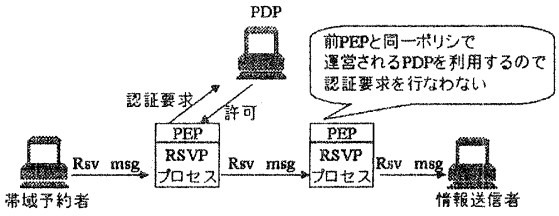

図 1: 改善されたポリシコントロールモデル

これらの改善策を用い, 以下で予約者識別環境の設計と実装を行なう.

5 PDP の設計と実装

PDP は PEP から入力された帯域予約者の情報に基づいて予約の判断を行なう. 以下に段階を踏んで PDP の動作順序について述べる.

メッセージの正当性確認

PDP は PEP からの情報入力を待ち, 入力と共に処理を開始する. 入力された情報には, それが正当なものであると証明する為に情報全体のハッシュ値とそれを暗号化したものが含まれている.PDP は暗号化されたハッシュ値を復号化し, 確認することでメッセージが正当なものであると判断する. 同時にタイムスタンプを利用し, メッセージの再利用を防ぐ.

Resource reservation admission contorol system by user authentication

[1]Graduate School of Media and Governance, Keio University
5322, Endo, Fujisawa, Kanagawa 252, Japan
E-Mail: kiri@ht.sfc.keio.ac.jp
[2]Faculty of Environmental Information, Keio University

予約リストとの比較

PDP内でメッセージが正当なものと確認された場合,PDPは入力データの内容と予約リストとの整合性の確認を行なう.PDPは,予約を許可する者のユーザIDと,予約を許可する時間,そして予約を許可できる帯域要求情報が設定されたリストを持っており,それと比較し,合致した場合に予約許可を通達する.

6 PEPの設計と実装

PEPは,起動と共にRSVPメッセージの入力を待ち,RSVPメッセージ入力に従って処理を行なう.

メッセージの正当性確認

RSVPメッセージの入力があった場合,PEPはフロー情報記述部と,ユーザ情報などを格納したオブジェクトをRSVPメッセージから取り出す.そしてPDPと同様にメッセージの正当性を確認する.

キャッシュ走査

その後,PEPは取り出した予約情報とPEP内部に持つキャッシュ情報とを比較し,キャッシュ情報に適合するものであればその予約要求の判断をRSVPプロセスに通知する.

PPDP_ADDR検査

PPDP_ADDRに含まれる情報とPEPが接続しているPDPアドレスと比較し,合致した場合その予約要求は採択されたものとし,RSVPプロセスへ予約採択を通知し,キャッシュに情報を書き込む.

PDPへの許可要求

PEP内でのこれまでの処理のどれにも該当しない場合,PEPはCOPSのRequestメッセージを用いてPDPへ許可要求を行なう.その後PDPからの判断に従ってキャッシュに情報を書き込む.そして,RSVPプロセスへ通知を行なうが,その際にPPDP_ADDRを書き換え,新たにハッシュ値を計算してPEPの秘密鍵を用いて暗号化する.

7 暗号化関数の実装

本システムでは安全性を高める為に帯域要求情報やユーザ情報を暗号化して用いている.それらの暗号化,復号化を可能にする為にRSAアルゴリズムを用いた暗号化関数を実装した.

また,RSAでは鍵を生成する際に扱う数字が大きいほど安全性が高まる為,一般の計算機が扱う整数型の範囲を越えた値を扱うことを可能にするGNU MP LIBRARYを利用した.

8 評価

本システムの評価として,PPDP_ADDRの処理軽減の効果を図2の環境で測定した.また,図中のホストAをPEP,ホストBをPDPとして利用した.

また,測定の結果を以下の表に示す.測定はPEP内のメッセージ正当性が確認されてから判断を行なうまでの時間について行なった.

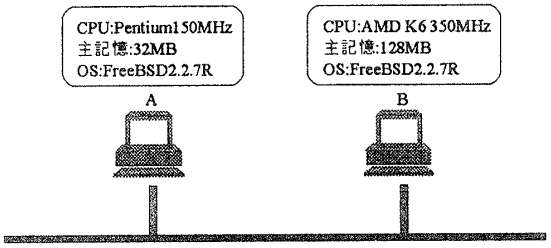

図2: 測定環境

	キャッシュ利用時	PPDP_ADDR利用時	通常時
平均時間	1.14	1.46	174.21
最大時間	1.23	1.56	318.68
最小時間	1.04	1.28	126.90

(msec)

この結果が示すように,キャッシュ利用時だけでなくPPDP_ADDR利用時にもPDPと通信する場合と比べて処理時間の軽減が認められた。

9 まとめと今後の課題

本システムが構築されたことによって,これまで誰もが予約を行なうことが可能であったRSVPに認証機構が加わり,正当な者に対してのみ予約を許可することが可能になった.

今後は動的にPDPに対して予約情報を追加する機構が求められる.また,RSVPはフロー毎の情報を管理して帯域を確保する技術である為,多数のフローが存在する大規模なモデルの場合には管理すべき情報が膨大になり,対応できない欠点を持つ.その為,ポリシドメインを越えて帯域を確保するのは容易ではない.

そこで,今後はRSVPとDiffServ[5]技術を併用しての利用が考えられる.DiffServ技術によってフロー情報を統合し,広域ネットワークでも一般の通信と差別化したサービスの利用が可能になると考えられる.

参考文献

[1] R.Braden, L.Zhang, S.Berson, S.Herzog and S.Jamin, "Resource ReSerVation Protocol (RSVP)", RFC2205, 1997

[2] J.Boyle, R.Cohen, D.Durham, S.Herzog, R.Rajan and A.Sastry, "The COPS (Common Open Policy Service) Protocol", Internet Draft, 1999

[3] S.Herzog, "RSVP Extensions for Policy Control", Internet Draft, 1999

[4] S.Yadav, R.Yavatkar, R.Paddati, P.Ford, T.Moore and S.Herzog, "User Identity Representation for RSVP", Internet Draft, 1999

[5] S.Blake, D.Black, M.Carlson, E.Davies, Z.Wang and W.Weiss, "An Architecture for Differentiated Services", RFC2475, 1998