L-034

パケットフィルタリングルールの最適配置法

Optimum Allocation Method of Packet Filtering Rules

嶋 良平* 田中 賢*
Ryohei Shima Ken Tanaka

1 はじめに

広域帯のアクセス網が普及するにつれ，ネットワーク機器におけるパケットフィルタリングが重要度を増している [1]．パケットフィルタリングは，ネットワーク機器に一定の負荷を与え，パケット転送の遅延を引き起こし、サービス品質の低下を引き起こす．複数のインタフェースを持つネットワーク機器において，パケットフィルタリングは通常入力インタフェースで一括して実行される．このフィルタを複数の出力インタフェースに分割することで，ネットワーク機器の負荷を軽減し効率化をはかる方法を提案する．

2 パケットフィルタリングルール

2.1 パケットフィルタリングのモデル

ネットワーク機器におけるパケットフィルタリングは，図 1 のようにモデル化できる [2]．図中，R_i は i は番目のフィルタリングルール，n はフィルタを構成するルールの数である．P と D は各ルールの評価型で，P によってパケットの転送許可を，D によってパケットの転送拒否を表す．ネットワーク機器にパケットが到着すると，ルール R_1 から順に適用し，転送可否の判断をする．ルール R_n では，それ以前のルールで評価型が決まらなかったすべてのパケットについて，デフォルトの評価型を与える．

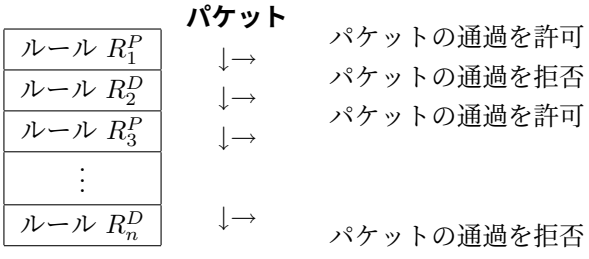

図 1: パケットフィルタリングのモデル

各ルールの条件式は，以下のような論理式 (1) とする．

$$R_i = b_0 b_1 \cdots b_m (b_i \in 0, 1, -) \tag{1}$$

アドレスやポート番号などの条件をマスク記号-を伴った論理式とする．例えば,「R_3^P = 00-1」は，3 番目のフィルタリングルールで「00-1」というアドレスの転送を許可することを表す．

2.2 評価パケット数とフィルタリング負荷

定義 1 各ルールで評価型が決まるパケットの数を評価パケット数と呼び，$|R_i|$ と表す．

全てのアドレスから同じ頻度でパケットが到着するとしたとき、一組のルール R によるフィルタリング負荷 $L(R)$ は式 (2) のように定義される．

$$L(R) = \sum_{i=1}^{n} i|R_i| \tag{2}$$

3 分割の効果

3.1 分割後のフィルタリング負荷と効率化条件

分割後の m 組のルール R によるフィルタリング負荷を $L_{seg}(R)$ と表す．$L_{seg}(R)$ は，異なる m 組のフィルタリングルールごとに式 (2) を用いて加算した，式 (3) のように表せる．

$$L_{seg}(R) = L(R^1) + L(R^2) + \cdots + L(R^m) \tag{3}$$

フィルタの分割が有効となる条件は式 (4) のようになる．

$$L(R) > L_{seg}(R) \tag{4}$$

3.2 ルール数と分割数による負荷の変化

デフォルトルールを除くルール数 n と分割数 m の 2 つのパラメータによって分割の効率が変化する．ここでは，デフォルトルールを除くルールにマスクを含まない場合の効果を求める．そのとき，それぞれの評価パケット数は全て 1 になる．図 2 のような n 個のルールを m 等分割できるフィルタリングルールを考え，その負荷の変化を求める．

分割前
R_1
R_2
R_3
⋮
R_n
R_{n+1}

⇒

分割後		評価パケット数
R_1^1	R_1^m	1
⋮	⋮	⋮
$R_{\frac{n}{m}}^1$	$R_{\frac{n}{m}}^m$	1
$R_{\frac{n}{m}+1}^1$	$R_{\frac{n}{m}+1}^m$	$2^k - \frac{n}{m}$

図 2: m 分割するルールと評価パケット数

*神奈川大学大学院理学研究科情報科学専攻

分割後のルールのビット数が k ビットであれば，表 1 の条件における $L_{seg}(R)$ は式 (4) のように表せる．

$$L_{seg}(R) = m(\sum_{i=1}^{\frac{n}{m}} i + (\frac{n}{m}+1)(2^k - \frac{n}{m})) \quad (5)$$

式 (4) を用いて，k=8 でルール数 n と分割数 m が変化するときの負荷差 $L(R) - L_{seg}(R)$ の様子を図 3 に示す．

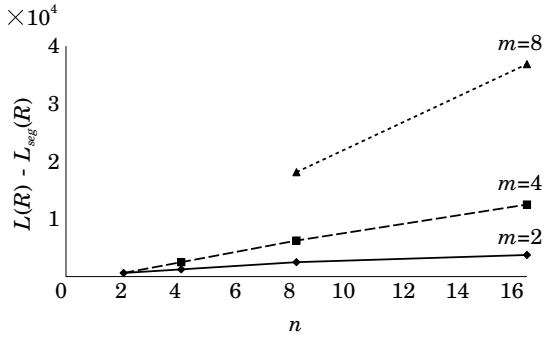

図 3: ルール数増加に伴う分割数毎の負荷差

$L(R) - L_{seg}(R)$ の値が大きいほど分割による効果が大きくなる．ルール数と分割数が増加するほど負荷の軽減率が上昇する．

4 フィルタの分割法

4.1 分割手順

入力インタフェースのフィルタリングルールの宛先アドレス部分を元にしてルールを分割していく．分割したルールのまとまりを分割後のフィルタとし，それぞれ対応する出力インタフェースにフィルタリングルールを適用する．

4.2 分割例

以下に，提案した手順によるフィルタの分割例を示す．ここで，/の前のビット列は宛先アドレスを表す．0，1 の 2 つのネットワークに各ルールを割り当てる．

1. R_1^D に着目．0 は一致するのでルールを割り当てる．1 は一致しないので割り当てない (表 1).

表 1: R_1^D までの分割結果

分割前	分割後 (0)	分割後 (1)
R_1^D=0/1000	R_1^{1D}=0/1000	
R_2^P=-/10--		
R_3^P=0/1110		
R_4^D=1/0011		
R_5^P=1/0-1-		
R_6^P=0/0101		
R_7^D=-/----		

2. R_2^P に着目．マスクなので 0，1 の両方にルールを割り当てる (表 2).

表 2: R_2^P までの分割結果

分割前	分割後 (0)	分割後 (1)
R_1^D=0/1000	R_1^{1D}=0/1000	R_1^{2P}=-/10--
R_2^P=-/10--	R_2^{1P}=-/10--	
R_3^P=0/1110		
R_4^D=1/0011		
R_5^P=1/0-1-		
R_6^P=0/0101		
R_7^D=-/----		

3. R_7^D まで比較を繰り返し行い，フィルタの分割が終了する (表 3).

表 3: R_7^D までの分割結果

分割前	分割後 (0)	分割後 (1)
R_1^D=0/1000	R_1^{1D}=0/1000	R_1^{2P}=-/10--
R_2^P=-/10--	R_2^{1P}=-/10--	R_2^{2D}=1/0011
R_3^P=0/1110	R_3^{1P}=0/1110	R_3^{2P}=1/0-1-
R_4^D=1/0011	R_4^{1P}=0/0101	R_4^{2D}=-/----
R_5^P=1/0-1-	R_5^{1D}=-/----	
R_6^P=0/0101		
R_7^D=-/----		

$$\begin{cases} L(R) = 166 \\ L_{seg}(R) = L(R^1) + L(R^2) = 64 + 47 = 111 \end{cases}$$

$L(R) > L_{seg}(R)$ となり，分割により負荷を 66.9% に軽減できた．

5 おわりに

本研究では，フィルタの分割によるフィルタリング負荷の効率化法と分割手順を示した．一方，フィルタをインタフェースに分割することで，外側から内側に向けてルーティングされるパケットの数も増加する．今後はフィルタリング負荷とルーティング負荷を合わせた評価法を検討する必要がある．また，フィルタの位置が変わることによって起こるセキュリティの問題についても検討する必要がある．

参考文献

[1] Jeff Sedayao(著), 岡利章,(監訳), 生田りえ子 (訳),"Cisco IOS アクセスリスト,"オライリー・ジャパン,2002.

[2] 田中賢, 伊藤聖,"ネットワーク機器の負荷を軽減するフィルタリングルール再構成法,"信学論 (B),vol.J88-B,No.5,pp.905-912,May.2005.