L-002

パケットフィルタリングの多段化による遅延の軽減法

A Delay Reduction Method for Packet Filtering by Multi-Stage Network Gears

阿部　貴紀* 田中　賢* 三河 賢治†
Takanori Abe Ken Tanaka Kenji Mikawa

1 はじめに

インターネット上の脅威の増加や運用ポリシの複雑化に伴い，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性を増している．通常，管理者には外部の脅威が取り除かれたことを確認する手段がないため，ひとたび追加されたフィルタリングルールは消去されることはない．このため，フィルタリングルールは増加しつづけ，やがて通信の遅延やサービス品質の低下を引き起こす．ヘッダやルールがより複雑になる IPv6 上のフィルタリングにおいて，この問題はより顕著になる．パケットフィルタリングの効率を上げる 1 つの方法は，複数のネットワーク機器を同時に用いて並列に計算を行なうことであるが，ルールは順を追って適用される必要があるため，単純な並列化では対応が困難である．本稿では，[1] で提案したパケットフィルタリングの理論モデルにもとづき，複数のネットワーク機器を順に接続してフィルタを多段化したときのフィルタリングの効率について検討する．

2 パケットフィルタリングのモデル

L3 スイッチやルータ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 [1]．R_i は i 番目のフィルタリングルールを表し，P は転送許可を，D は転送拒否をそれぞれ表す．また, フィルタのルール数は $n+1$ とする．最後の $n+1$ 番目のルールはデフォルトルールで上位のルールで評価型が決まらなかった全てのパケットに対してデフォルトの評価型を与える．

ルール R_1^P
ルール R_2^D
ルール R_3^P
⋮
ルール R_n^P
ルール R_{n+1}^D

図 1: パケットフィルタリングのモデル

定義 2.1 (ルールセット) n 個のフィルタリングルールで構成されるルールセット R は以下のように表される．

$$R = \langle R_1, R_2, R_3, ..., R_n, R_{n+1} \rangle \tag{1}$$

定義 2.2 (評価パケット数) R_i 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．

このとき，総パケット数 $|R|$ は以下のように表される．

$$|R| = \sum_{i=1}^{n} |R_i| + |R_{n+1}| \tag{2}$$

各々のパケットに対して適用されたルールの総数を，そのパケットの評価の際に生じた遅延と考える．デフォルトルールについては，条件の評価が伴わないことに注意して，フィルタリングの遅延を以下のように定義する．

定義 2.3 (フィルタリングの遅延) ルールセット R による遅延 $L(R)$ を以下のように定義する．

$$L(R) = \sum_{i=1}^{n} i|R_i| + n|R_{n+1}| \tag{3}$$

3 多段フィルタ

3.1 多段フィルタの効果

ここではデフォルトルール以外の n 個のルールを l 台のネットワーク機器に均等に分割して多段化することを考え，図 1 のモデルを図 2 のような多段化されたパケットフィルタリングモデルに対応付ける．l は多段化のネットワーク機器の段数を表し，k は i 番目のルールが属すネットワーク機器の番号を表す．

多段化されたパケットフィルタリングは，パイプライン処理のように動作する．各々のパケットが 2 段目のネットワーク機器に達したとき，次のパケットのフィルタリングが開始されるため，到着パケットのフィルタに要する時間を削減でき遅延の軽減をはかれる．

3.2 多段フィルタのモデル

ここでは，多段フィルタの効果について考察する．多段化された l 台のネットワーク機器は，同期的に動作すると仮

*神奈川大学大学院理学研究科情報科学専攻
†新潟大学学術情報基盤機構情報基盤センター

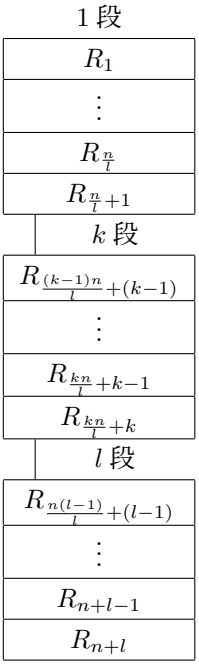

図 2: 多段フィルタのモデル

定する．つまり，1 台目のみにパケットが送られてくれば 1 台目だけでフィルタリングを行なうが，2 台目のフィルタリングを行なう時は 1 台目と 2 台目のフィルタリングを同時に開始する．以降 3 台目は 1 台目と 2 台目と同時にフィルタリングを開始していく．図 3 に多段化によるフィルタの時間推移を，多段化を行わない $l = 1$ と多段化を行う $l = 2$ の場合について示す．

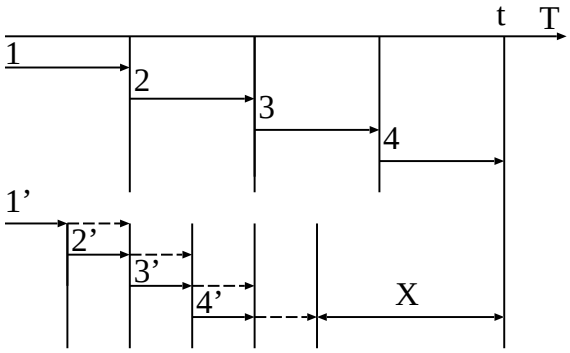

図 3: ネットワーク機器の多段化

図 3 の 1,2,3,4 と 1’，2’，3’，4’ の実線は送られてきたパケットがネットワーク機器で評価されている間を表し，点線は多段化した時の 2 段目のネットワーク機器で評価されている間を表している．4 と 4’ は時間 t に送られてきているパケットの最後のパケットである．X の部分が多段化することによって軽減された遅延である．

1’，2’，3’ は次のネットワーク機器にパケットが送られると同時に次のパケットのフィルタリングが開始されるので，1 段目のネットワーク機器の評価時間のみで求めることができる．4’ は 2 台のネットワーク機器の評価回数を求める必要があるが，本稿では概算値として，4’ も 1’，2’，3’ と同様に考える．よって遅延は 1 台あたりのルール数を求め，それに総評価パケット数をかければよい．

$$L(R)' \fallingdotseq (\frac{n}{l})|R| \tag{4}$$

ここでは，多段化による効率を，多段化を行なっていないフィルタリングの遅延の式 (3) の L に対する多段化の式 (4) の L' の比を考える．$\sum_{i=1}^{n} |Ri|$ は一様頻度のもとでルール数 m ビットのとき 2^m と考える．

$$\frac{L'(R)}{L(R)} = \frac{(\frac{l}{n})|R|}{\sum_{i=1}^{n} i|R_i| + n|R_{n+1}|} \tag{5}$$

簡単化のために，$\forall_i |R_i| = 1$ とし，式を整理すると以下の式のように表せる．

$$\begin{aligned} &= \frac{(\frac{l}{n})2^m}{\sum_{i=1}^{n} i|R_i| + n(2^m - n)} \\ &= \frac{\frac{n}{l}}{\frac{n(n+1)}{2^{m+1}} + n(1 - \frac{n}{2^m})} \end{aligned} \tag{6}$$

ルール数 n に比べて 2^m の方が十分大きいことから，以下の式が成り立つ．

$$\begin{aligned} &\fallingdotseq \frac{\frac{n}{l}}{n} \\ &= \frac{1}{l} \end{aligned} \tag{7}$$

(7) より，遅延の比は l に逆比例することがわかる．パケットフィルタリングにおいては，ネットワーク機器の多段化によって効率的なスケーラビリティが得られるといえる．

4 今後の課題

本稿では多段化によるパケットフィルタリングの効率化の有効性を検討した．フィルタリングルールは適用順序を保ったまま適用される必要があるため，単純な並列化は困難であるが，本手法は順序を保った形での並列化が可能な点が特徴である．

今後は隣接するネットワーク機器への転送に伴う遅延を考慮した形での遅延の定式化と多段化の有効性の検討，ネットワーク機器を用いた実験を行っていく．

参考文献

[1] 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.