L-001

フィルタリングルール最適配置問題の解法
A Solution for Optimum Filtering Rules Allocation

嶋 良平* 田中 賢* 三河 賢治†
Ryohei Shima Ken Tanaka Kenji Mikawa

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，ネットワーク機器での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招く．本研究では，複数のインタフェースを持つネットワーク機器におけるフィルタリングルールの配置を工夫することで，フィルタリングに伴う通信の遅延を軽減する方法を提案する．

2 フィルタリングルール最適配置問題

本研究では，図 1 のような 3 つ以上のインタフェースを持つネットワーク機器を対象とする．フィルタリングルールは各インタフェースに適用され，in 方向と out 方向を指定することができる [1]．

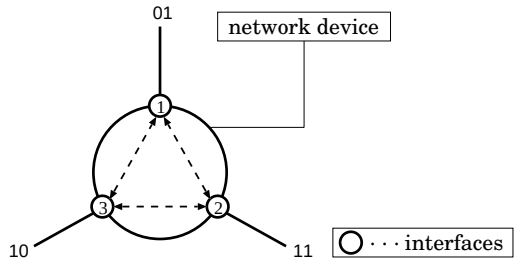

図 1: 複数のインターフェースを持つネットワーク機器

2.1 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．

$$R = \langle R_1^{\{P,D\}}, R_2^{\{P,D\}}, ..., R_n^{\{P,D\}}, R_{n+1}^{\{P,D\}} \rangle \quad (1)$$

ルールセットにおける i 番目のルールを R_i と表す．P,D は評価型を表し，P は転送許可 permit，D は転送拒否 deny を表す．ネットワーク機器に到着したパケットは，ルール R_1 から順番に評価されて転送可否が判断される．デフォルトルール R_{n+1} では，R_n で評価型が決まらなかったすべてのパケットにデフォルトの評価型を与える．

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．

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

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) R によるフィルタリングの遅延 $L(R)$ は以下のように表される．

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

定義 2.4 (重複) R_i で評価型が決まり，R_{i+1} を R_i の手前に移動したとき R_{i+1} で評価型が決まるようなパケットが存在するとき，R_i，R_{i+1} は重複しているという．

2.2 機器全体のフィルタリングの遅延

j 番目のインタフェースにおける，in 方向に適用されたルールセットを RI^j と表し，out 方向に適用されたルールセットを RO^j と表す．このとき，全ルールセット $\mathbb{R}$ は以下のように表される．

$$\mathbb{R} = \langle (RI^1, RO^1), ..., (RI^m, RO^m) \rangle \quad (4)$$

また，m 個のインタフェースを持つネットワーク機器全体のフィルタリングの遅延 $L(\mathbb{R})$ は以下のように表すことができる．

$$L(\mathbb{R}) = \sum_{j=1}^{m} (L(RI^j) + L(RO^j)) \quad (5)$$

各ルールセットによるフィルタリングの遅延 $L(RI^j)$, $L(RO^j)$ は式 (3) を用いて表される．

フィルタリングルール最適配置問題とは，各インタフェースにおけるフィルタリングルールの配置を再構成することで，L を最小にする $\mathbb{R}$ を求める問題である．

*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

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.

3 配置の再構成手順

配置によって $L(\mathbb{R})$ を小さくする方法は，各ルールセットにおけるルールを他のルールセットに移動し，移動したルールどうしを併合することである．

ルールを移動するための必要条件は，移動対象となるルールの送信元アドレスに関する条件部分と，宛先アドレスに関する条件部分が，いずれかのインタフェースの下のアドレス範囲に限られていることである．これを満たさない場合，ポリシーが変わってしまいパケットフィルタリングが正しく動作しなくなる可能性がある．また，重複している複数のルールはまとめて移動する必要性があり，個別に移動することはできない．

ルールを併合をするための条件と手順は，フィルタリングルール再構成法 [2] で議論した方法にもとづく．

(再構成手順)

(1) ルールセット RI^1 におけるルール R_1 に着目し，移動可能なら対応するルールセットの R_n となる位置に移動する．

(2) (1) をデフォルトルールを除く最後のルール R_n まで繰り返す．

(3) (1)，(2) をルールセット RI^m まで繰り返す．

(4) (1)∼(3) をルールセット RO^j においても同様に行う．

(5) 併合可能なルールを併合し，ルール数を減らす．

4 配置の再構成例

以下に，in 方向に適用された 3 つのルールセットについて，提案した手順による再構成例を示す．

各ルールのアドレスの条件部分を次のような論理式で表す．

$$R_i^{\{P,D\}} = b_1 b_2 ... b_l / b_1 b_2 ... b_l \quad (b_i \in \{0, 1, *\}) \qquad (6)$$

ここでは，/ で区切られた前半のビット列が送信元アドレスを表し，後半のビット列が宛先アドレスを表している．各ビット列は任意の l ビットで表される．$*$ はワイルドカードマスクが適用される部分を示している．例えば $R_1^D = 01/10$ は，1 番目のルールにおいて，送信元アドレスが 01，宛先アドレスが 10 であるパケットを転送拒否することを表す．

図 1 における，再構成前の各ルールセットとそれぞれの遅延は表 1 のようになる．

表 1: 再構成前の各ルールセット

(a)$\lvert RI^1\rvert$=34	
RI^1	$\lvert RI_i^1\rvert$
R_1^D=01/**	10
R_2^P=01/10	4
R_3^D=01/10	7
R_4^P=01/11	3
R_5^D=**/**	10
$L(RI^1)$=91	

(b)$\lvert RI^2\rvert$=34	
RI^2	$\lvert RI_i^2\rvert$
R_1^D=10/**	7
R_2^P=10/01	5
R_3^P=10/11	2
R_4^D=**/**	20
$L(RI^2)$=83	

(c)$\lvert RI^3\rvert$=30	
RI^3	$\lvert RI_i^3\rvert$
R_1^D=11/**	9
R_2^P=11/01	6
R_3^P=11/10	3
R_4^D=**/**	12
$L(RI^3)$=66	

再構成前の遅延 $L(\mathbb{R})$ は 240 である．

手順による再構成後の各ルールセットとそれぞれの遅延は表 2 のようになる．in 方向と out 方向の二段のフィルタになることから，in 方向のルールセットのデフォルトルールの評価型が permit になる必要がある点に注意されたい．

表 2: 再構成後の各ルールセット

(a)$\lvert RI^1\rvert$=34	
RI^1	$\lvert RI_i^1\rvert$
R_1^D=01/**	10
R_2^P=**/**	24
$L(RI^1)$=34	

(b)$\lvert RI^2\rvert$=34	
RI^2	$\lvert RI_i^2\rvert$
R_1^D=10/**	7
R_2^P=**/**	27
$L(RI^2)$=24	

(c)$\lvert RI^3\rvert$=30	
RI^3	$\lvert RI_i^3\rvert$
R_1^D=11/**	9
R_2^P=**/**	21
$L(RI^3)$=30	

(d)$\lvert RO^1\rvert$=27	
RO^1	$\lvert RO_i^1\rvert$
R_1^P=1*/01	11
R_2^D=**/**	16
$L(RO^1)$=27	

(e)$\lvert RO^2\rvert$=25	
RO^2	$\lvert RO_i^2\rvert$
R_1^P=*1/10	7
R_2^D=01/10	7
R_3^D=**/**	11
$L(RO^2)$=43	

(f)$\lvert RO^3\rvert$=20	
RO^3	$\lvert RO_i^3\rvert$
R_1^P=01/11	3
R_2^P=10/11	2
R_3^D=**/**	15
$L(RO^3)$=37	

再構成後の遅延 $L'(\mathbb{R})$ は 195 となり，遅延が 81%に軽減されたことがわかる．

5 おわりに

本論文では，パケットフィルタリングのモデルをもとにフィルタリングルール最適配置問題を形式化した．ルールを移動するための条件と手順を提案し，移動後のルール併合による有効性を例示した．再構成後のルールセットに関しては，上位のルールで評価型が決まるパケットが多くなるようにルールを入れ換えることで，更に遅延を軽減できる場合がある．

今後は，ルールの移動によって遅延が軽減できる場合についてより詳細に議論し，その十分条件を明らかにしたい．また，ルーティングを含めた効率化や本手法の有効性についても検討したい．

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.

Copyright © 2011 by Information Processing Society of Japan and
The Instiute of Electronics, Information and Communication Engineers
All rights reserved.