L-017

パケットフィルタで処理可能なパケット数の上限と下限について
Upper and Lower Bounds for the Number of Evaluated Packets by Filter

小出 淳一§　浜元 信州†　田中 賢‡　三河 賢治†
Junichi Koide　Nobukuni Hamamoto　Ken Tanaka　Kenji Mikawa

1. はじめに

ネットワークには，コンピュータウイルス混入や不正アクセス，サービス不能攻撃等を目的とした悪意ある通信も流れており，近年コンピュータや企業内ネットワークに甚大な被害を与えている．パケットフィルタは，ネットワークを流れる通信がコンピュータや企業内ネットワークに侵入する前に，パケットフィルタ内の各ルールと通信を照合し，特定の通信を許可／拒否して，セキュリティ事故を未然に防ぐための手段である．

最適なパケットフィルタを構成する問題 NP-完全であることが証明されており，ネットワーク機器の負荷を低減するようなパケットフィルタを現実的な計算量で構成するための方法論は，多くの研究者によって現在も試行錯誤の段階にある．著者らは，各々の部分集合が互いに独立となるようなパケットフィルタの分割方法を考案し，各部分集合で処理可能なパケット数の指標に基づいて部分集合を並べ替える方法を提案した[1]．

本研究では，前述の文献[1]で求めた指標の上限と下限を分析し，どの程度ネットワーク機器の負荷を低減することに貢献できるか，この指標の正当性を評価する．

2. 準備

パケットフィルタを通過するパケットを文字列長 m のビット列として，パケットを許可／拒否するフィルタリングルールを次式

$$R_i = b_1 b_2 \ldots b_m, \qquad b_i = \{0,1,-\}$$

で表す．式中 '-' は 0 と 1 のどちらにも合致する記号でドントケアと呼ばれる．特に，パケットの許可／拒否を明示する場合は，R_i^A（許可），R_i^D（拒否）で表し，A と D をそれぞれパケットの評価型と呼ぶ．パケットフィルタは，フィルタリングルールの順序付き集合として，次式

$$\mathcal{R} = \langle R_1, R_2, \ldots, R_n \rangle$$

で表す．

フィルタを通過するパケットは，フィルタ内の上位のルールから順に各ルールと比較されて，あるルールと一致するパケットは，ルールの評価型によってフィルタの通過を許可／拒否される．ルール R_i に一致したパケット（すなわち R_i で評価されたパケット）の総数を評価パケット数と呼び，$\|R_i\|$ で表す．R_i で評価可能なパケットであっても，R_i より上位のルールで評価済みの場合は $\|R_i\|$ にカウントされない．R_i で評価可能なパケット数は，R_i のドントケア数 d だけに依存し，その数は 2^d である．R_i で評価可能なパケット数を $|R_i|$ で表す．本研究では，パケットの到着頻度分布が一様であると仮定して，$\mathcal{R}$ のフィルタリング負荷を次式

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

で表す．

本稿で扱うフィルタリングのモデルでは，フィルタ $\mathcal{R}$ を通過するパケットは，フィルタ内の上位のルールから順に各ルールと比較される．このため，ルールを単純に入れ替えると，本来，拒否されるはずのパケットが許可されたり，許可されるはずのパケットが拒否されたりと，フィルタのポリシーが変わってしまう可能性がある．このような事象は，パケットの評価型と合わせて，次に示すルール間の依存関係に起因する．

定義 1.（重複）$R = b_1 b_2 \ldots b_m$ と $R' = b'_1 b'_2 \ldots b'_m$ をフィルタリングルールとする．各ビットについて，次の条件式 (1) $b_i = b'_i$ (2) $b_i = '-'$ または $b'_i = '-'$，のうち，どちらか一方を満たしているとき，R と R' の関係を重複と呼び，R と R' に重複するパケットを $R \odot R'$ で表す．

定義 2.（包含）R と R' をフィルタリングルールとする．次式 $|R \odot R'| = |R|$ を満たすとき，R と R' の関係を包含と呼び，R は R' を包含する．

定義 3.（一部重複）フィルタリングルール R と R' について，R と R' は重複であるとする．次式 $|R| > |R \odot R'|$ と $|R'| > |R \odot R'|$ を同時に満たしているとき，R と R' の関係を一部重複と呼ぶ．

定義 4.（独立）R と R' をフィルタリングルールとする．次式 $|R \odot R'| = 0$ を満たすとき，R と R' の関係を独立と呼ぶ．

3. 独立ルール集合

ルール間の関係が独立であれば，どちらか一方のルールを削除したり順位を入れ替えたりしても，フィルタのポリシーは変わらない．著者らは，ルール間の独立関係をフィルタに拡張し，$\mathcal{R}$ を独立ルール集合と呼ばれる部分フィルタに分割する方法を提案した[1]．

定義 5.（独立ルール集合）$\forall x \in D_i$ と $\forall y \in D_j$ $(i \neq j)$ について，$|x \odot y| = 0$ を満たし，かつ r が最大となるように $\mathcal{R}$ を $D_1, D_2, \ldots, D_r$ に分割する．このとき，各 R_i を独立ルール集合と呼ぶ．

独立ルール集合は，次の 2 つの性質を持つ．

性質 1. フィルタ $\mathcal{R}$ 上の任意の独立ルール集合 D について，$\forall x \in D$ と $\forall y \in \mathcal{R} \setminus D$ は独立である．

§ キャノン・イメージング・システムズ株式会社
Canon Imaging Systems Inc.
† 新潟大学　Niigata University
‡ 神奈川大学　Kanagawa University

性質 2. フィルタ $\mathcal{R}$ 上の任意の独立ルール集合を D とする．$\forall x, y \in D$ について，$|x \odot z| > 0$ と $|y \odot z| > 0$ を満たす $z \in D$ が存在する．

各独立ルール集合で評価可能なパケットの総数を計算して，その値の降順に集合を並べ替えると，$\mathcal{R}$ のフィルタリング負荷を小さくすることができる．しかしながら，各集合で評価可能なパケットの総数を現実的な計算量で求めることは難しいため，文献[1]では，独立ルール集合で評価可能なパケット数の予測値を導入し，これを見込み評価パケット数と称した．

実際，独立ルール集合 D に属するルール数 $\#(D) = n$，集合に属するルールのうち最大のドンドケア数 d として，文献[1]では，見込み評価パケット数を $2^d/n$ とした．

4. パケット数の上限と下限

見込み評価パケット数が実際の独立ルール集合で評価可能なパケットの総数に近いものであれば，フィルタリング負荷の低減に貢献する．本節では，独立ルール集合で評価可能なパケットの総数の上限と下限を示し，見込み評価パケット数として適当な値を考察する．

定理 1. $\mathcal{R}$ で評価可能なパケットの総数は $\mathcal{R}$ 上のルールの順序に依存しない．

（証明）$\mathcal{R}$ 上の連続するルール R_i と R_{i+1} を入れ替える場合を考える．入れ替える前の評価パケット数の合計は，当然，$\|R_i\| + \|R_{i+1}\|$ である．一方，入れ替えた後のルールを $R'_i = R_{i+1}$ と $R'_{i+1} = R_i$ とすると，それぞれの評価パケット数

$$\|R'_i\| = \|R_{i+1}\| + \|R_i \odot R_{i+1}\|$$
$$\|R'_{i+1}\| = \|R_i\| - \|R_i \odot R_{i+1}\|$$

から，評価パケット数の合計

$$\|R'_i\| + \|R'_{i+1}\| = \|R_i\| + \|R_{i+1}\|$$

を得る．以上より，連続するルールの入れ替えを繰り返して，あるルールを任意の順位に移動しても $\mathcal{R}$ で評価可能なパケット数の総数は変わらない．ゆえに，定理は証明された．

定理 2. 独立ルール集合 D について，D で評価可能なパケットの総数の下限 $E_{\min}$ は次式

$$E_{\min} = 2^d$$

で与えられる．d は D に属するルールの最大のドントケア数である．

（証明）$|R_i| = 2^d$ とする．R_i は最大のドントケア数を持つので $\|D\| \geq 2^d$ が言える．R_i と独立もしくは一部重複となるルールが D に存在すると，R_i 以外で評価可能なパケットが存在するため，$\|D\| > 2^d$ となる．一方，R_i と包含となるルールが D に存在しても，R_i が他のルールを包含するため，$\|D\| = 2^d$ となる．ゆえに，最大のドントケア数を持つルールが他のすべてのルールを包含するならば，$E_{\min} = 2^d$ が成立する．

次に，$\|D\| = 2^d$ を仮定する．定理 1 より，R_i を先頭に移動しても $\|D\| = 2^d$ となるから，$\|D\| = \|R_1\| = 2^d$ が成立する．したがって，R_1 より下位のルールの評価パケット数は 0 である．これは，定義から，R_1 が下位のルールを包含している．ゆえに，$\|D\| = 2^d$ ならば，最大のドントケア数を持つルールが他のすべてのルールを包含する．

以上，最大のドントケア数を持つルールが他のすべてのルールを包含するとき，かつそのときに限り，命題が成立することが証明された．

定理 3. 独立ルール集合 D について，$\#(D) = n$ とする．D で評価可能なパケットの総数の上限 $E_{\max}$ は次式

$$E_{\max} = n \cdot 2^d - (n-1)$$

で与えられる．d は D に属するルールの最大のドントケア数である．

（証明）省略

5. まとめ

本稿では，独立ルール集合で評価可能なパケット数の上限と下限を与えた．文献[1]で導入された見込み評価パケット数は，各独立ルール集合で評価可能なパケット数の下限の平均値であった．実際，上限と下限は n 倍程度の差である．今後は，本稿で求めた上限と下限から，フィルタリング負荷の減少に効果のある見込み評価パケット数を検討する．

謝辞

本研究の一部は内田エネルギー科学振興財団の助成を得て行われた．

参考文献

[1] 小出淳一，三河賢治，田中賢，“パケットフィルタリング最適化問題における多項式時間アルゴリズム”，第 7 回情報科学技術フォーラム講演論文集，第 4 分冊，pp. 151-152 (2008)

[2] 昆金学，田中賢，“適応型パケットフィルタリングの構成法”，電子情報通信学会 2008 総合大会講演論文集，pp. 185 (2008)

[3] 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”，電子情報通信学会論文誌，Vol. J88-B, No. 9, pp. 905-912 (2005)