

総ネットワークコストを最小化する 仮想ファイアウォール機能の配備法

B-14 Flexible deployment of virtual firewall function NFV-based network with minimum total network cost

内谷 玲香[†] 肥田 健一郎[†] 栗林 伸一[†]

Reika UCHIYA, Ken-ichiro HIDA and Shin-ichi KURIBAYASHI

[†] 成蹊大学理工学部 [†] Faculty of Science and Technology, Seikei University

1. まえがき

ネットワーク仮想化技術NFV(Network Functions Virtualization)に基づくネットワークでは、様々なネットワーク機能をソフトウェアにより仮想的に実現し、容量も設置場所も自由に選択することができる。そのため、NFVベースのネットワークを経済的に設計・構築するためには、どれだけの容量のネットワーク機能をどこに配置するかが重要な課題となる^[1]。本論文では、仮想ファイアウォール機能を対象に、その配備法と配備指針を明らかにする。

2. ファイアウォール機能配備に関する基本的な考え方と配備アルゴリズム

ファイアウォール機能は一般的に外部からの攻撃に対応するものであり、受信側に設置することが基本となる。しかし、ファイアウォールでフィルタリングされる無駄なトラフィックを例えば送信側で事前にフィルタリングすれば、無駄な中継帯域や中継分経路選択機能にかかるコストを無くすことができる。ただし、**パケットフィルタリング機能**（事前に登録されたIPアドレスとポート番号でフィルタリング）のように事前に一度設定すれば対応できるものは候補となるが、送信側の数が多くかつリアルタイムに連携が必要なファイアウォール機能については膨大な処理がかかるため対象外と考えられる。そこで筆者らは、受信側に設置するパケットフィルタリング機能を対象とする全ての送信側に追加配置することによる増加コスト (C_1) と、それにより削減される全てのの中継帯域&中継分経路選択機能コストと削減される受信側ファイアウォールコストの総和 (C_2) を比較し、 $C_1 < C_2$ となれば対象となる送信側全てにパケットフィルタリング機能を追加配置する（移動ではない）配備アルゴリズムを提案した^[1]。本論文では、提案配備アルゴリズムが全てのケースを比較しコストが最小となる形態（最小解）にどれだけ近い最終形態を提供できるか、また定量評価から得られる配備指針を中心に提案する。

3. 評価結果と考察

3.1 評価条件

総ネットワークコストの値で評価を行う。ネットワークを構成するためには経路選択機能と回線帯域が必要であるため、総ネットワークコストにはファイアウォール機能、パケットフィルタリング機能のほかに経路選択機能と回線帯域のコストを含める。ネットワークモデル、評価パラメータ、中継トラフィックを踏まえた経路選択機能配備アルゴリズム、シミュレーションツールも含め、文献^[1]と同じ評価条件で実施する。また、経路選択機能と回線帯域については入出力分と中継分に分けられ、各コスト算出法は文献^[1]を参照のこと。さらに、規制係数Prは入力トラフィックが追加設置するパケットフィルタリング機能を通過する割合（つまり $(1-Pr)$ は規制される割合）、コスト比Wcは回線帯域コストとファイアウォールコストの比、フィルタリング機能コスト係数fはファイアウォール機能全体のコストを占めるパケットフィルタリング機能のコストの割合をそれぞれ示す。

3.2 評価結果と考察

主な評価結果を図1と図2に示す。縦軸はパケットフィルタリング機能を送信側に追加配置しない場合の

の総ネットワークコストで正規化した値を示す。これらから以下の諸点が明らかである。

1) Prが小さいほど総ネットワークコストを削減できる。

図1の条件では、Prが0.7以下になるような状況でない追加配備する効果がないこと、Wcが大きくなるにつれそのPrの範囲は小さくなる。

2) Pr値が一定値（この値は条件により異なる）以下になると、全ての受信エリアに対応したパケットフィルタリング機能に対応する全ての送信エリアに追加配置する形態が望ましい。

3) 提案アルゴリズムは最小解の約95%に近づいている。

なお、今回の図には含めていないが、Wcが小さくなるほどファイアウォールコストの占める割合が小さくなり、結果として総ネットワークコストも小さくなることを確認している。

4. 今後の課題

今後、仮想キャッシュ機能、仮想DPI機能、仮想圧縮機能などを前提とした配備法を検討する。

<参考文献>

[1] 肥田, 栗林: “ネットワークコストを最小化する仮想経路選択機能と仮想ファイアウォール機能の複数機能配備法”、電子情報通信学会信学技報IN2017-48 (2017.12).

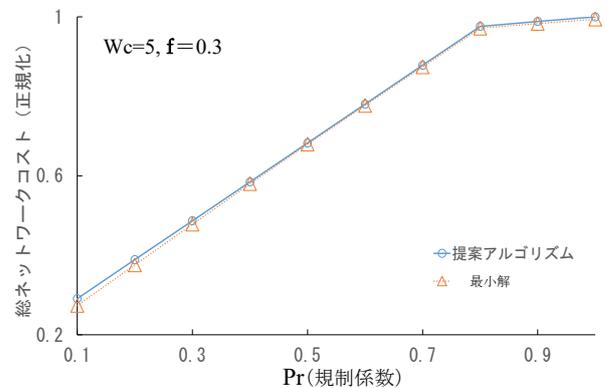


図1. Prによる総ネットワークコスト削減効果

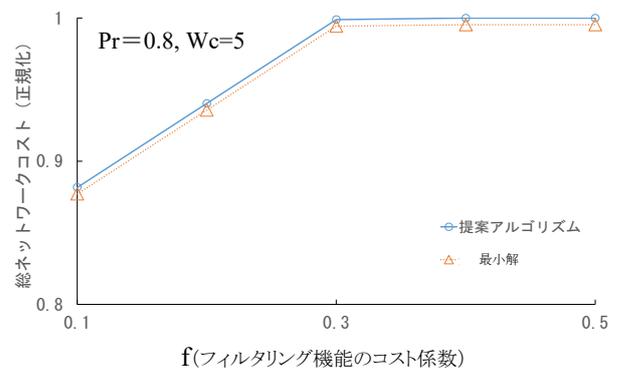


図2. fによる総ネットワークコスト削減効果