科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１６　日現在

機関番号：　３２７０２
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００９９

研究課題名（和文）通信の遅延を最小化する最適パケットフィルタの実現

研究課題名（英文）A Filtering Rule Optimization Method for Minimizing Communication Latency

研究代表者
田中　賢（Tanaka, Ken）

神奈川大学・理学部・教授

研究者番号：５０２７２８１０

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：インターネット上の危険な通信を除去する手法にパケットフィルタリングがある。近年ネット上の脅威が増加するにつれフィルタリングに起因する通信の遅延が増大しており、とりわけ動画や音声などの通信品質が損なわれつつある。本研究では、この通信の遅延を削減するために、フィルタ内に記述されているルールを最適化する方法を考案し、その有効性を実験的に明らかにした。

研究成果の概要（英文）：Packet filtering is a function of communication appliance for rejecting dangerous packets. In these days increasing threats in the internet cause the latency of communication gears to glow up. Hence, the quality of packet communications, especially of movies or voice, has been seriously degraded. In our studies, we proposed a optimization method for filtering rules in network gears and we showed the effectiveness of our method empirically. Our method makes it possible to realize secure network communications.

研究分野：　総合領域

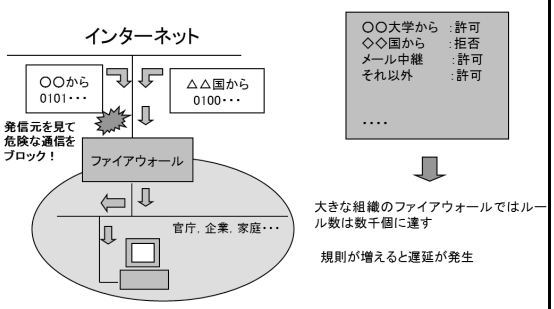
科研費の分科・細目：　情報学・計算機システム・ネットワーク

キーワード：　ネットワークセキュリティ技術

１．研究開始当初の背景

近年、インターネット上の脅威が増加するにつれ、企業や研究機関のファイアウォールで記述されるパケットフィルタのルール数は増加の一途をたどっている。ファイアウォールではすべての到着パケットについて最悪すべてのルールによるチェックを行うため、ルールが増加するにつれチェックに起因する通信の遅延が問題となる。インターネット電話や動画配信など、実時間性が求められるサービスにおいては、ファイアウォール内での遅延がサービス品質の著しい低下を引き起こす。このような遅延はファイアウォール内部の処理段階で発生するため、通信回線の増速では対処できない。また、ネットワーク管理者には外部の脅威が除去されたことを確認する手段がないため、追記されたルールを削除することもできず、遅延は増大する一途をたどっている。現在、企業や研究機関などのファイアウォールにおいて記述されているルール数は数千の規模に達している。インターネット上の脅威は今後も増加する一方であることから、安全性を確保した形でサービスの品質を保っていくためには、ファイアウォール上のパケットフィルタにおける遅延を最小化する何らかの技術が不可欠である。

これまで、パケットフィルタを最適化するさまざまな研究が行われてきた。探索木を用いてルールを高速に探索する方法の有効性はフィルタの構成に依存し、理論的な計算量の下界の問題もなお残されている。一方、ルールそのものを再構成することで、フィルタの負荷を下げる手法についても報告されているが計算量の問題が存在する。



２．研究の目的

本研究では、ルールの構成と配置を最適化することで転送の遅延を最小にする方法を構築した。これによって、従来問題となっていた通信の遅延問題の解決を目指した。フィルタリングルールの最適化は、従来技術者の経験やスキルに負う作業であったため、最適性が保証されず、場合によっては不適切な記述により逆に遅延を増大させたり、セキュリティ上の危険を引き起こす可能性があった。本研究ではそのような問題の発生を回避する最適化法を検討した。

３．研究の方法

我々は、ルールの構成を最適化する様々なアルゴリズムを考案した。提案した方法を対象として、実際のネットワーク通信に対する通信の遅延を計測し、その有効性を検証した。

４．研究成果

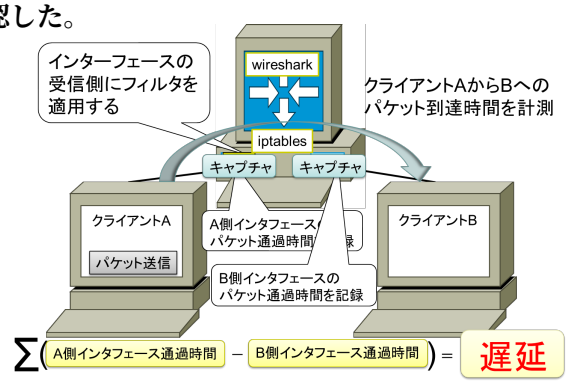
(1)我々はまず、ルールのグループ化による最適化法を考案した。従属関係にあるルールをまとめ、独立なルールとして扱い入れ換えを行うことで、複雑な従属関係をもつルール同士で遅延の削減を可能とした(論文 3)。

(2)また、ルールを入れ替える際に遅延が減少する十分条件を求め、これに基づく最適化アルゴリズムを提案した(論文 2)。

(3)次に、遅延の原因となる評価パケット数の大きなルールを、ルールを再帰的に辿ることで従属ルールとともに上位に移動する方法を考案した(論文 1)。ルールを再帰的に辿ることで、ルール間に存在する任意の従属関係に対応できる最適化法を実現した。

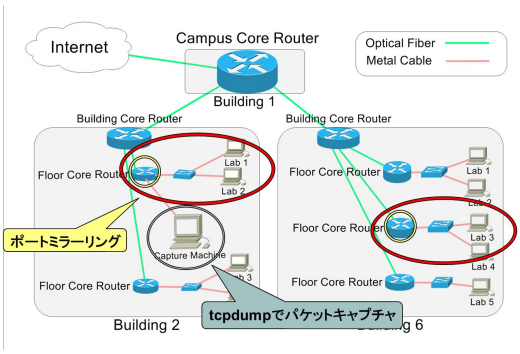
これらの方法は、いずれもルール数に対して多項式時間のアルゴリズムであり現実的なネットワーク機器で実装可能である。コアルータからアクセスルータまでパケット通信を行う様々なネットワーク機器において適用できることから、ネットワーク全体の通信の品質を向上することに広く貢献する。

(4)これらの結果を踏まえ、下図のようにクライアント A、B で通信を行い、A から B への到達時間を計測した。フィルタリングルール最適化前と最適化後での遅延を計測したところ、ルールやパケットの頻度分布に応じて、最大 10%程度まで遅延を軽減できることを確認した。



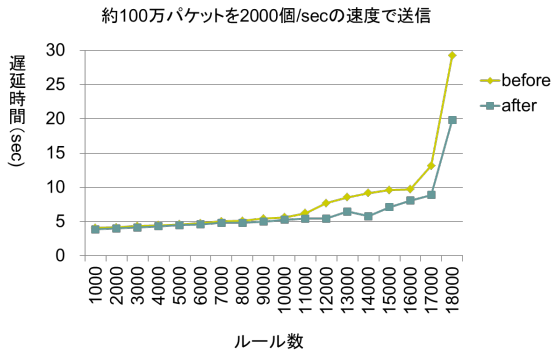
(5)さらに、学内 LAN 上でキャプチャしたパケットを対象として最適化アルゴリズムの有効性検証実験を検証した。学内 LAN 上のフロアスイッチにおいてポートミラーリングを設定し、tcpdump を用いてフローをキャプ

チャした。



神奈川大学平塚キャンパスにおいて、上図のようにパケットキャプチャを行い、個人情報などを含むペイロードを削除した後に同様の方法で遅延を計測した。

キャプチャ作業から実験に至るまで、大学の情報セキュリティ担当者や法務関係者と議論を重ね、プライバシー保護や個人情報の取り扱いについては十分配慮した。



約 100 万パケットを 2000 パケット/sec の速度で送信したところ、ルール数が多いほど顕著な遅延の減少を確認できた。ルール数が 17000 の場合、40%程度の遅延の削減を確認した。

現在はこれらの結果を踏まえたネットワーク実証実験を詳細に行い、その成果をまとめた外部発表の準備を行っている。

本研究の成果により、インターネット上に存在する様々なネットワーク機器の負荷が広く軽減される。本研究の成果は、インターネット全体にわたる通信・サービス品質の向上に対し、今後長期にわたり貢献できる。

５．主な発表論文等

〔雑誌論文〕（計３件）

1. Optimization of packet filter with maintenance of rule dependencies, K. Tanaka, K. Mikawa, K. Takeyama, IEICE Commun. Express, 査読有,Vol.2, No.2, 80-85 (2013)
2. A heuristic algorithm for reconstructing a packet filter with dependent rules, K. Tanaka, K. Mikawa, M. Hikin, IEICE Trans. Commun., 査読有, Vol.E96-B, No.1, 155-162 (2013)
3. ブロック分割によるパケットフィルタ最適化問題の一解法，三河賢治，田中賢，小出淳一，電子情報通信学会論文誌 B，査読有，Vol.J94-B，No.10，1408-1417 (2011)

〔学会発表〕（計７件）

4. パケットフィルタリング最適化法の有効性について，野村圭太，田中賢，三河賢治，情報科学技術フォーラム講演論文集, 第 4 分冊，査読無，291-292 (2013)
5. フィルタリングポリシー記述言語でのルール最適化について，秋山匠，田中賢，三河賢治，電子情報通信学会ソサイエティ大会講演論文集，査読無，93 (2012)
6. 制約ルール集合上のパケット分類の領域計算量に関する考察，三河賢治，田中賢，電子情報通信学会ソサイエティ大会講演論文集 2，査読無，25 (2011)
7. パケットフィルタリングの多段化による遅延の軽減法, 阿部貴紀, 田中賢, 三河賢治, 情報科学技術フォーラム講演論文集, 第 4 分冊，査読なし，177-178 (2011)
8. フィルタリングルール最適配置問題の解法，嶋良平，田中賢，三河賢治，情報科学技術フォーラム講演論文集, 第 4 分冊, 査読無, 175-176(2011)
9. 任意のビットマスクに対応した階層型トライの提案，長谷川創，三河賢治，田中賢，電子情報通信学会総合大会講演論文集 2，査読無，197(2011)
10. 多段化によるパケットフィルタリングの効率化，阿部貴紀，田中賢，三河賢治，電子情報通信学会総合大会通信講演論文集 2，査読無，563(2011)

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
http://www.cs.info.kanagawa-u.ac.jp/

６．研究組織

(1)研究代表者

田中　賢（TANAKA, Ken）
神奈川大学・理学部・情報科学科・教授
研究者番号：50272810

(2)研究分担者

三河賢治（MIKAWA, Kenji）

新潟大学・情報基盤センター・准教授
研究者番号：00344838