様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　８　月　２８　日現在

機関番号：　３２７０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０１６３

研究課題名（和文）遅延時間がルール数に依存しないパケットフィルタの実現

研究課題名（英文）A packet filtering method whose latency does not depends on the number of rules

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）　　3,600,000円

研究成果の概要（和文）：インターネットやモバイルデータ通信では、パケットとよばれるデータのかたまりをやりとりすることで通信が行われている。パケットフィルタリングはコンピュータや通信機器に置いて安全なパケットと危険なパケットを分類する重要な処理である。フィルタリングに用いるルールは外部のリスクが増加すればするほど多くなり減少することはない。このことがパケット転送の遅延を招き、やがて通信品質の低下を引き起こすことになる。本研究ではこの問題を解決するために、ルールが増加しても一定時間でフィルタリングが可能な方法を構築しその有効性を検証した。

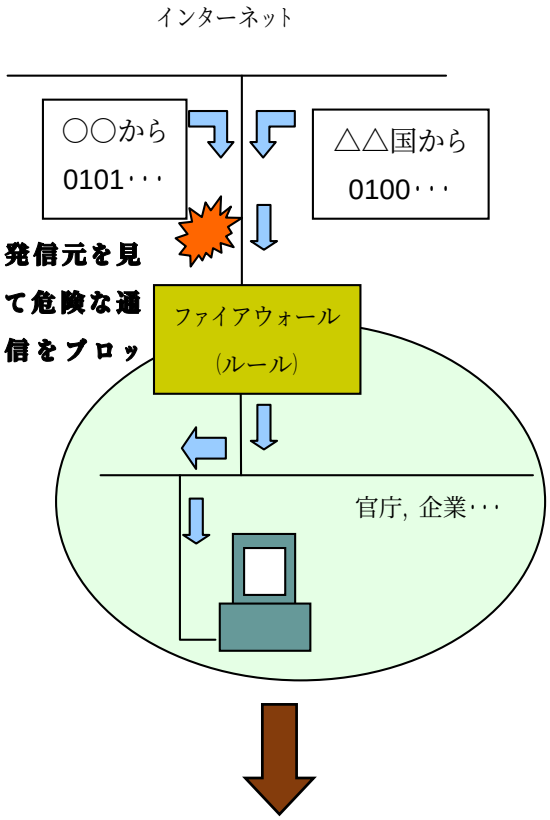
研究成果の概要（英文）：Communications on the Internet and mobile networks are realized on data packets communications. For the sake of communication securities, all packets are filtered on the PC or communication machines. The more the number of risks increases, the more the number of rules on these machines increases and the former never decreases. This causes the speed of communications become slowly and the qualities of services degrade. So we proposed a novel filtering method based on our run-based tries. Based on our method, the latency caused by filtering never increases. We confirmed the effectiveness of our method through network experiments.

研究分野：　ネットワークセキュリティ

キーワード：　パケットフィルタリング　パケット分類　決定木　トライ木

１．研究開始当初の背景

パケットフィルタリングは、ネットワークセキュリティを確保する基本的手法である。フィルタ運用の際は、外部に脅威の存在が認められる度にルールが追加されるが、その脅威が除去されたことを確認する手段がないため 、ルールは増加の一途を辿っていた。このルールの増加がパケット転送の遅延を招き、やがて通信品質の低下を引き起こすことが懸念されていた。



ルールは増加し続ける！ルールが増えると

遅延が発生！！

フィルタリング時間がルール数に依存しない
フィルタリングの方法は？

図１：パケットフィルタリング

フィルタリングの遅延を減少するために、様々なルール順序最適化法が提案されてきた。ルール順序最適化問題はNP-困難であり、現実的なサイズの問題で最適解を得ることが困難な問題であった。このため、多くの発見的手法が開発されていた。しかし、それらのほとんどは限定されたタイプのルールにしか適用できない、大規模なルールセットには適用できないといった問題があり、ルール数の増大に伴う遅延の増大を避けられない、といった本質的な問題があった。

２．研究の目的

本研究では、ルール数に依存せず一定時間でフィルタリングが可能な方法を構築し、この遅延の問題を解決することを目指した。その際、プレフィックスルールなどの限定されたルールだけではなく、任意のビットマスクを含むルールセットに対して有効な方法を目指した。これは、近年複雑化しつつある様々な攻撃手法に対処するために、アドレスやポート番号といったL2やL3でのパケット属性だけではなく、ペイロードの一部を条件として含むようなフィルタリングを意図したことによる。一定時間でのフィルタリングは近年増加しつつある動画や通話といったサービスや、リアルタイム系のサービスの品質安定に寄与する。我々は最終的に現実的なサイズのフィルタで提案手法の有効性を実験的に検証することを目的とした。

３．研究の方法

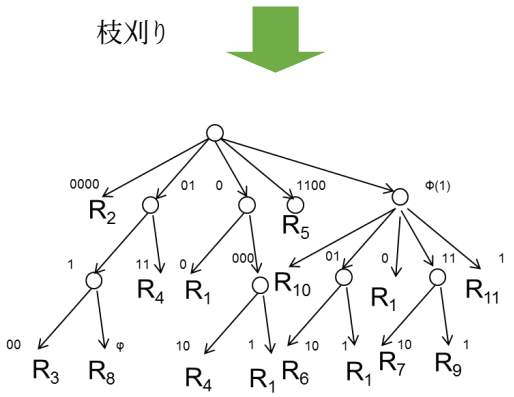
初年度は、探索木の領域計算量について理論、実装の両面から検討を行った。理論面から必要なことは、ルールのビット数とそれに含まれるビットマスクの数が木のサイズにどのように影響するかを検討することである。これにより、よりタイトな計算量を導くことが出来た。

実装面では理論的な成果を実際の木を構築することで確認した。様々なビット数のルール集合に対し、マスクの数や位置が構築にメモリサイズにどのように影響するかを検証した。これにより、マスクの数や位置が、木のサイズに大きく影響することが明らかとなり、木の構築に先立ちビット入れ替えによりメモリサイズを大幅に削減できる予想を得た。

２６年度からは実証実験の基礎となる木の構築とその枝刈り法を検討した。エッジルータに記述される数百～数千のルールを扱えるパケットフィルタの実装を中心に実験に必要な各種ツールの作成を行った。最終年度は、パケットフィルタリングの標準ベンチマークである ClassBench を用いて本手法の有効性を検証した。

ルール集合

R_1　*0*1
R_2　0000
R_3　0*00
R_4　0*1*
R_5　1100
R_6　*001



ナイーブに構築すると巨大な木になるが、枝刈りを行うことで実用的なサイズにまで縮小可能！！

図２：決定木の枝刈り法

４．研究成果

本研究では、ClassBench で最大 4000 個のルールからなるフィルタを生成しパケットフィルタリング実験を行った。また、ネットワークシミュレータ上で同様の実験を行いネットワーク上でキャプチャしたパケットに対して同様の実験を行いその有効性を確認した。これらの結果より、本研究では数千ルール規模の実用的なフィルタにおいてルール数に依存しないパケットフィルタを構築できることが確認できたといえる。

本研究の成果は今後様々な問題に適用していくことができる。近年、様々なマルウェアの蔓延や標的型メールのような新たな攻撃手法の登場により、ネットワークそのものを仮想化する SDN(Software Defined Network)が注目されている。SDN を実現するにあたっての課題は、従来分散的に実現されてきたネットワーク機器上のパケット転送やパケット分類を集中的に、かつ動的に行うことである。これを実現するためには、ソフトウェアベースで動作する極めて高速なパケット分類手法が不可欠だが、本研究で提案した手法はそのような要求にそのまま合致する。パケットの属性に基づく転送の許可、拒否という二値への判断を、サービスなどのポリシに応じた経路の選択などの多値への分類に一般化することができる。今後は、そのような問題への適用を検討していく必要がある。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　8 件）

（１）疎なルールのもとでの RBT からの決定木構築法，原田崇司，田中賢，三河賢治，信学技報，Vol.117，No.28，　pp.9-15，2017 年 05 月（査読無）

（２）単一の連からなる Run-Based Trie によるルール探索の高速化，原田崇司，田中賢，三河賢治，情報処理学会研究報告，Vol.2017-AL-162，No.2，　pp.1-7，2017 年 03 月（査読無）

（３）Linear-time generation of uniform random derangements encoded in cycle notation，K. Mikawa，K. Tanaka，Discrete Applied Math.，Vol.217，　pp.722-728，2017 年 01 月（査読有）

（４）ポインタ付与による Run-Based Trie 探索の高速化，原田崇司，田中賢，三河賢治，信学技報，Vol.116，No.315，　pp.13-18，2016 年 11 月（査読無）

（５）ビットの照合順序を考慮したトライに基づくパケット分類手法，小林由人，高橋俊彦，三河賢治，田中賢，信学技報，Vol.115，No.315，　pp.65-70，2015 年 11 月（査読無）

（６）Run-Based Trie から構成される決定木の枝刈り法，原田崇司，田中賢，三河賢治，信学技報，Vol.115，No.294，　pp.11-17，2015 年 10 月（査読無）

（７）Run-Based Trie Involving the Structure of Arbitrary Bitmask Rules，K. Mikawa，K. Tanaka，IEICE Trans. Inf. & Syst.，Vol.E98-D，No.6，　pp.1206-1212，2015 年 06 月（査読有）

（８）決定木を用いた Run-Based Trie の探索法，原田崇司，田中賢，三河賢治，電子情報通信学会ソサイエティ大会，　p.84，2014 年 09 月（査読無）

〔学会発表〕（計　4 件）

（１）撹乱順列の高速なランキングとアンランキング，三河賢治，田中賢，第 15 回情報科学技術フォーラム，　pp.87-88，2016 年 09 月（査読無）

（２）ビットの照合順序を考慮したトライによるパケット分類法の高速化，小林由人，高橋俊彦，三河賢治，田中賢，電子情報通信学会総合大会，　p.160，2016 年 03 月（査読無）

（３）トライを用いた高速パケット分類法の提案，小林由人，高橋俊彦，三河賢治，田中賢，電子情報通信学会総合大会，　p.198，2015 年 03 月（査読無）

（４）パケットフィルタリング最適化のためのルール集合分割法，池本泰斗，田中賢，三河賢治，第 13 回情報科学技術フォーラム，pp.181-182，2014 年 09 月（査読無）

〔図書〕（計　0 件）

〔産業財産権〕

○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
該当なし

６．研究組織
(1)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

(2)研究分担者
三河賢治（MIKAWA,kenji）
新潟大学・学術情報基盤機構・準教授
研究者番号： 00344838

(3)連携研究者
（　　）

研究者番号：

(4)研究協力者
（　　）