

氏名(本籍)	しょう むら ゆう すけ 正 村 雄 介 (東京都)
学位の種類	博 士 (工 学)
学位記番号	博 甲 第 5665 号
学位授与年月日	平成 23 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
審査研究科	システム情報工学研究科
学位論文題目	異なり数を用いた広帯域ネットワークのトラフィック解析技術に関する研究

主	査	筑波大学教授	博士(工学)	吉 田 健 一
副	査	筑波大学教授	工学博士	岡 本 栄 司
副	査	筑波大学教授	博士(工学)	津 田 和 彦
副	査	筑波大学准教授	工学博士	片 岸 一 起
副	査	筑波大学准教授	博士(システムズマネジメント)	倉 橋 節 也

論 文 の 内 容 の 要 旨

近年、アクセス回線のブロードバンド化に伴い、広帯域な常時接続環境が一般利用者に急速に普及し、ネットワークの利用形態が多様化している。従来の Best Effort 型のネットワークアプリケーションに加えて、IP 電話や IP テレビといった様々なサービスが同一ネットワークに統合される状況となっており、品質保証が重要となっている。経済性の観点から単純なオーバープロビジョニングによる品質の確保は難しく、トラフィックの優先度に応じ転送制御することが求められており、これを実現するためネットワーク機器に流れるトラフィックの分類技術が必要となっている。また一方で、不正なパケットを大量に送信しサーバやルータをサービス停止状態とする DoS 攻撃の発生、ウイルスや Worm による異常トラフィックの発生、及び、P2P ファイル交換による帯域占有が問題となっている。特に通信事業者の広域ネットワークでは、網管理者が、これらのトラフィックを判別し、QoS 処理やフィルタリング処理を実施し、ネットワークを管理する必要がある。このような網管理者の業務を支援するため、DDoS、Worm、P2P 過大トラフィック等の通信帯域を圧迫するフローの検出技術が求められている。このような背景に基づいて、本論文では、インターネットトラフィックをアプリケーションの挙動を元にリアルタイムで分類する解析技術の確立を目的とし、高速回線に対応可能なアルゴリズムを提案している。本提案は (1) トラフィック解析に必要な統計情報の計測手法に関する提案、(2) 10Gbps 回線フルパケット解析に対応する高速化手法の提案、(3) トラフィックの分類手法の提案からなり、筑波大学キャンパスネットワークに適用することで有効性を検証している。

本論文は 6 つの章から構成され、以下のような成果が得られている。まず、第 1 章は序論であり、本研究の背景と目的を説明し、研究の意義を明かにしている。第 2 章では、トラフィックモニタリングと解析技術の関連研究をレビューし、レビューに基づき本研究で解決すべき研究課題を明確化している。第 3 章では、流量の多いトラフィックの抽出に有効な頻出アイテムセット抽出技術に、異常トラフィックの解析に有効な異なり数情報の計測機能を追加したトラフィックモニタリング技術 Aggregated Flow Mining (AFM) を提案し、AFM は少ないメモリ量でリアルタイム処理可能なアルゴリズムである事を明らかにしている。第 4 章では、

AFM を通信事業者等の広帯域回線に適用するため、10Gbps のトラフィックをフルパケットで処理する高速化技術を提案している。第5章では、試作した AFM 装置を筑波キャンパスネットワークに適用し、有効性を検証すると共に、得られた統計情報の解析技術について述べている。最後に第6章で、本研究で得られた結果を総括している。

審査の結果の要旨

ネットワーク管理の上で、トラフィックの流量情報と異なり数情報の有用性は広く認識されている。しかしながら、これまでの研究では、流量情報と異なり数情報それぞれに特化し、別々の計測手法が提案されていた。即ち、既存の技術ではトラフィックを管理する際、トラフィック情報を流量の観点から見た情報と、異なり数の観点から見た情報と2つの情報を別々に扱わなければならなかった。ネットワーク運用管理者にとっては、これらの情報をつき合わせ判断する必要があり日常の運用管理に適用することは困難であり、10G の実ネットワークにおいて流量情報と異なり数情報を同時に計測できる手法を提案した本研究の有用性は極めて高い。またアルゴリズムの提案に止まらず、ハードを実装し、大学のキャンパスネットワークに持ち込み実用性の評価まで行った点も特筆に値する。

一方、異なり数の計測精度については実験的に示されているだけで、理論的な性能予測は試みられていない。示された実験結果によれば実運用上十分な精度の計測が期待されるが、理論的な計測精度が示せば、より価値ある研究になったと考えられる。しかし、異なり数の実時間計測に関する研究の歴史はまだ浅く、研究の初期として、様々な課題が残っている事自体は自然であり、逆に重要な研究分野の比較的初期に優れた研究成果をあげた事は、著者の見識の高さを示していると、捉える事もできる。

以上、一部に課題は残されているものの、本学位論文、及び、研究の内容は、博士（工学）を授与するに充分なものと判断する。