L-013

モバイルIPネットワークにおけるフロー挙動に基づくトラフィック分類手法
Flow Behavior based Traffic Classification in Mobile IP Network

佐藤 彰洋† 長田 俊明† 北形 元† 阿部 亨† 白鳥 則郎† 木下 哲男†
Akihiro Satoh Toshiaki Osada Gen Kitagata Toru Abe Norio Shiratori Tetsuo Kinoshita

1. はじめに

近年，モバイルIPネットワークの必要性と共に，その管理の重要性が高まってきている．そこで本稿では，モバイルIPネットワークにおいて，トラフィックの分類を実現するため「部分フロー選択手法」を提案し，実験を通じて，その効果を示す．

2. 関連研究

モバイルIPネットワーク，およびフロー挙動に基づくトラフィックの分類手法について述べる．それらを踏まえ，本研究で対象とする問題点を明らかにする．

2.1 モバイルIPネットワーク

モバイルIPネットワークとは，IPモビリティを考慮した移動要素により構成されるネットワークである．モバイルIPネットワークを実現するための基礎技術として，Mobile IPv6 [1]，およびNetwork Mobility [2]が注目されている．移動要素は，その要素が属するネットワークで付与されるホームアドレスと，移動先ネットワークで一時的に付与される気付けアドレスを持つ．これら2つのアドレスの対応関係を，ホームエージェントで管理し，常にホームエージェント経由で通信することで，移動要素は通信を切断することなく，管理領域の異なるネットワーク間を移動することができる．

2.2 フロー挙動に基づくトラフィックの分類

ネットワークの適切な管理を実現するため，トラフィックの分類は必要不可欠である．その目的は，管理者が，ポリシーに基づいたトラフィックの処理を実現するため，対象とするアプリケーションごとにトラフィックを分類することである．

近年，トラフィックの分類の有効な手段として，フロー挙動に基づくトラフィックの分類手法が提案されている[3]．フロー挙動とは，フローを構成するパケットのデータサイズや到着時間間隔などの統計的特徴である．この手法は，管理ネットワークにおいて計測されたトラフィックをフロー単位に分割し，そのフローの先頭Nパケット，すなわち先頭部分フローの挙動から，機械学習を用いてトラフィックの分類を行う．

2.3 既存手法の問題点

既存のフロー挙動に基づくトラフィックの分類手法では，先頭部分フローの計測が必要不可欠である．しかしながら，モバイルIPネットワークでは，要素の移動により，その通信経路が頻繁に変化する．そのため，移動要素に接続を提供するネットワークの管理において，移動要素が通信の途中で管理ネットワークに接続した場合，管理ネットワークにおいて先頭部分フローを計測することができない（図1）．これにより，フロー挙動に基づくトラフィックの分類が困難となる．すなわち，モバイルIPネットワークにも対応するためには，先頭部分フローに依存しないトラフィックの分類手法の確立が必要である．

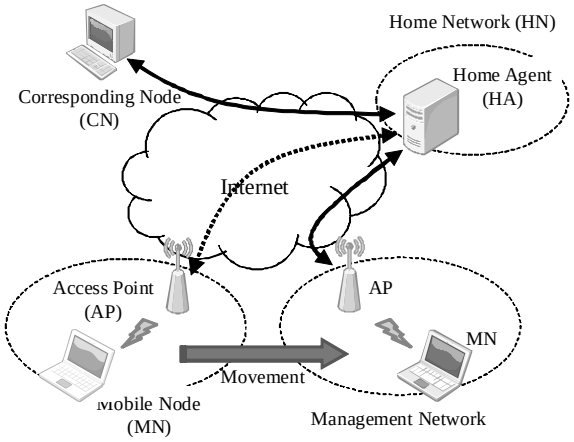

図 1: モバイルIPネットワークでのフロー計測

3. 提案

フロー挙動を分析し，それらの特徴を明らかにし，その分析結果を活用した部分フローの選択手法を提案する．

3.1 フローの分析

先頭部分フローに依存しないトラフィックの分類を可能とするためには，(1) フローの途中に存在する分類に有効な部分フローの有無と，その特徴を明らかにすること，(2) その分類に有効な部分フローの選択方法の検討，が必要不可欠である．そのため，フロー挙動を分析することで，上述の2点について明らかにした．

文献[4]に基づいて，HTTPの1フローにおいて，その通信の内容を可視化したものを図2に示す．ここで，x軸はパケットのシーケンス番号，y軸はパケットのデータサイズを表している．また，データサイズが正の場合はアップリンク，負の場合はダウンリンクの通信を意味する．HTTPのフローは，その通信の内容から，制御フェーズ，およびデータ転送フェーズの2種類に分類される．ここで，制御フェーズは，リクエストメソッドやレスポンスコードなどの送受信を行っている箇所であり，データ転送フェーズは，ファイルなどのデータの送受信を行っている箇所である．

まず，(1) に関する分析により，既存研究で用いられていた先頭部分フローは制御フェーズであること，これら制御フェーズの挙動が各アプリケーション固有であることに加え，新たに制御フェーズがフローの途中にも存在

†東北大学 Tohoku University

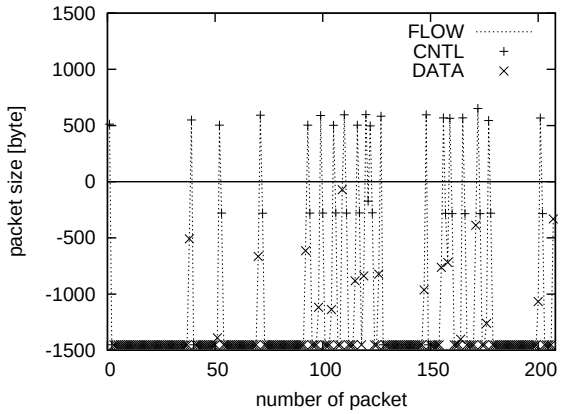

図 2: HTTP フローにおける通信の内容

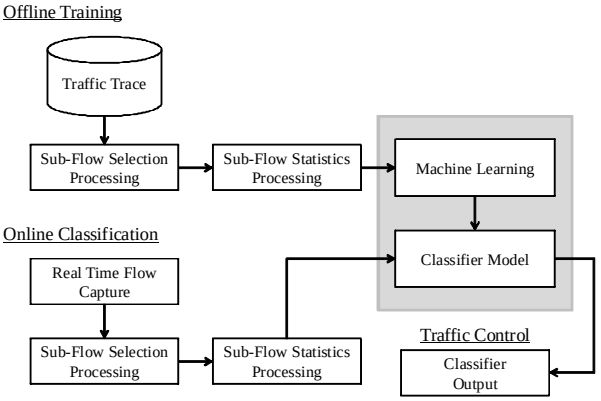

図 3: 提案手法に基づくトラフィック分類システムの概要

することが明かになった．以上の結果から，先頭フローに依存しない分類を行うためには，通信の途中に存在する制御パケットを含む部分フローを用いることが効果的であるという知見を得た．

また，(2) に関する分析の結果，各フェーズは通信方向やそのデータサイズに特徴があることが明かになった．具体的には，データ転送フェーズは，データサイズの大きいパケットによる片方向の通信であり，制御フェーズは，データサイズの小さいパケットによる双方向の通信であるという特徴が見てとれた．すなわち，これらの特徴を用いることにより，各フェーズを識別し，選択することが可能となる．

3.2 部分フロー選択手法

本稿では，モバイル IP ネットワークにおけるフロー挙動に基づくトラフィックの分類を実現するために,「部分フロー選択手法」を提案する．本手法では，上述の分析により明らかとなった特徴を活かし，フローの先頭および途中に存在する，トラフィックの分類に有効な部分フローを選択する．本手法の利点は，部分フローの学習と分類に既存の手法を用いることができることである．

4. 設計

図 3 に，提案手法に基づくトラフィック分類システムの概要を示す．本システムは，(i) オフライン学習部，(ii) オンライン分類部，および (iii) フロー制御部により構成される．これらの機能を，文献 [3] を参考に設計した．各機能の役割と，その処理内容は次の通りである．

オフライン学習部では，学習用トラフィックから分類モデルを導出する．はじめに，学習用トラフィックから，対象とするアプリケーションのトラフィックを 5-tuple を用いてフロー単位に分割する．次に，提案手法により学習に用いる部分フローを選択し，そのフロー挙動を導出する．最後に，クラスタリングにより，類似したフロー挙動を集約する．この結果，各クラスタには，同一アプリケーションのフロー挙動が集約されるため，分類モデルとして，(1) クラスタの重心と (2) クラスタに対応するアプリケーションラベル，を出力する．

オンライン分類部では，管理ネットワーク内で計測したフローから，提案手法を用いて部分フローを選択する．そのフロー挙動と分類モデルを比較することで，各フローをアプリケーションラベルに基づいて分類する．また，その結果をフロー制御部に通知する．

フロー制御部では，通知された結果および管理ポリシーに基づき，それらのフローを適切に処理する．

5. 評価

本提案手法により，モバイル IP ネットワークにおけるトラフィックの分類が実現可能であることを示すため，前章で設計したシステムを用いて，実験を行った．本実験では，対象とするアプリケーションを HTTP のみとする．複数のアプリケーション (HTTP, SMTP, IMAP, SSH) が混在している分類用トラフィックの中から，HTTP のトラフィックを分類し，その精度について評価する．実験に用いたデータは，実運用ネットワークで計測したトラフィックから，学習用として対象アプリケーションを 1000 フロー，分類用として各アプリケーションごとに 1000 フローを抽出し，それらを基に生成した．

実験の結果，提案手法で選択された部分フローを用いることで，対象とするアプリケーションである HTTP のトラフィックを 85%の精度で分類できることを確認した．

6. おわりに

本稿では，モバイル IP ネットワークにおいて，トラフィックの分類を実現するため「部分フロー選択手法」を提案した．また，実験を通じて，その効果を示した．

今後は，多種多様なアプリケーションに対して，本手法の有効性を検証する予定である．

参考文献

[1] D. Johnson, et al., “Mobility Support in IPv6”, Internet RFC 3775, 2004.
[2] V. Devarapalli, et al., “Network Mobility (NEMO) Basic Support Protocol”, Internet RFC 3963, 2005.
[3] L. Bernaille, et al., “Early Application Identification”, proc. of CoNEXT, 2006.
[4] C.V. Wright, et al., “Using Visual Motifs to Classify Encrypted Traffic”, proc. of VizSEC, pp.41-50, 2006.