DVMRP に基づくマルチキャスト・トラヒック用パフォーマンス・アナライザ

植野誠史[†] 加藤聰彦[††] 鈴木健二[††]

近年インターネットにおいて，マルチキャストを用いたビデオや音声などの配信が広く行われるようになってきた．これにともない，マルチキャスト・トラヒックのトラヒック量の測定やその転送の要因の解析を行うマルチキャスト通信の性能評価が重要となると考えられる．しかし，これまでに提案されているマルチキャスト・トラヒックの性能評価ツールにおいては，転送されたデータグラムのトラヒック量などを収集する機能を有するのみで，そのデータグラムの転送がどのような理由で発生または停止したかなどの詳細な解析を行うことができない．マルチキャスト・トラヒックの転送に関して詳細な解析を行うためには，そのトラヒックの転送を制御するマルチキャスト・ルーチング・プロトコルの手順を解析することが必要となる．そこで筆者らは，主に JP-MBone で使用されているマルチキャスト・ルーチング・プロトコル DVMRP（Distance Vector Multicast Routing Protocol）に注目し，ルータ間で交換されている DVMRP メッセージと転送されたマルチキャスト・トラヒックを対応させることで，マルチキャスト通信の詳細な性能評価を行うアナライザの開発を行っている．本稿では，本アナライザの設計と実装，および本アナライザを用いたマルチキャスト・トラヒックの解析結果について述べる．

A Performance Analyzer for Multicast Traffic Based on DVMRP

Seiji Ueno,[†] Toshihiko Kato[††] and Kenji Suzuki[††]

Recently, audio and video delivery services are widely spread in the Internet. In order to deliver these data to multiple receivers at the same time, the multicast technologies are indispensable. In such a situation, the performance analysis of multicast traffic will be important in order to design and operate the Internet. Multicast traffic is controlled by its own routing protocol and the multicast routing protocol is more complex than conventional unicast routing protocols. In this paper, we propose a new multicast performance analyzer considering DVMRP routing protocols. It captures messages of a multicast routing protocol as well as multicast IP datagrams. It also analyzes DVMRP messages in order to investigate the behaviors of multicast IP datagrams and measures the statistics of multicast traffic in detail. This paper describes the detailed design and the implementation of our multicast performance analyzer and the results of analyzing multicast datagrams transmitted over networks.

1. はじめに

近年インターネットにおいて，ビデオや音声などの配信が広く行われるようになってきた．これらのデータを多数の受信者に同時に配信するためには，マルチキャスト技術[1)]の利用が必須となる．現在のインターネットにおいても，MBone（Multicast Backbone）[2)]などの上で各種の映像配信が行われており，今後インターネットの広帯域化にともない，より大容量のマルチキャスト・トラヒックが転送されることが考えられる．このような状況のもとでは，マルチキャスト・トラヒックの転送量の時間的変化，発信者・受信者の範囲，他のトラヒックに対する影響などを解析するマルチキャスト・トラヒックの性能評価が重要な課題となると考えられる．

マルチキャスト・トラヒックはユニキャスト・トラヒックとは異なるメカニズムで転送されている．たとえば，宛先 IP アドレスにはマルチキャスト・グループを示すクラス D アドレスが使用され，これは特定のホストを示すものではない．また，マルチキャスト・ルーチング・プロトコルは，マルチキャストの転送のためのツリー情報を交換するほかに，マルチキャスト・トラヒックの転送開始・停止を制御する機能を有する．このため，マルチキャスト・トラヒックの性能評価に

† 電気通信大学
The University of Electro-Communications
†† KDDI 研究所
KDDI R&D Laboratories

は独自に開発されたツールが必要となる．

現在までにいくつかのマルチキャスト用の解析ツールが開発されており，それらの多くはマルチキャスト・ネットワークのトポロジを解析するものである．たとえば米国 CAIDA（Cooperative Association for Internet Data Analysis）[3]の開発した MantaRay [4]がその代表例である．MantaRay はマルチキャスト・ルータの接続状態を各マルチキャスト・ルータに問い合わせることで，データグラムが配送される経路を表示する．また UCLA と Xerox PARC の Multicast Route Monitor [5]はマルチキャスト・ルータ間で交換されているルート更新情報を取得することで，ルーチング・テーブルを生成する．

これに対し，回線上を流れるマルチキャスト・データグラムをキャプチャし，マルチキャスト・トラヒックの統計情報を計測するツールも提案されている．例としては，カナダ CRC（Communications Research Centre）の開発した MultiMON がある[6]．MultiMON はインターネット上の回線に設置することで，その回線上を転送されたマルチキャスト・トラヒックのパケット数やバイト数を解析することが可能である．

しかし，既存のマルチキャスト用の解析ツールは，マルチキャスト・ルーチング・プロトコルの手順を考慮していないため，マルチキャスト・トラヒックの発生・停止などの原因の詳細を解析することができない．たとえば，国内の MBone である JP-Mbone で広く利用されている DVMRP（Distance Vector Multicast Routing Protocol）[7),8]は，マルチキャスト・ルータ間で Prune や Graft などの DVMRP メッセージを交換し，転送の開始・停止を制御しているが，これらのツールではその動作を考慮していない．このため，DVMRP の動作に基づくマルチキャスト・ツリーの動的な変更や，DVMRP に起因するマルチキャスト・トラヒックの転送開始・停止などが解析できない．

そこで筆者らは，DVMRP により制御されるマルチキャスト・トラヒックの性能評価を対象として，回線を流れるマルチキャスト・データグラムの統計情報を収集するとともに，DVMRP の手順に従ったトラヒックの発生・停止の原因などを詳細に解析するパフォーマンス・アナライザを開発している[9]．本稿ではその設計・実装の詳細および本アナライザを用いたマルチキャスト・トラヒックの解析結果について述べる．以下，2 章において DVMRP の概要について述べる．次に 3 章と 4 章において，本アナライザの設計方針と，アナライザの中心部分であるアナライジング・モジュールの詳細についてそれぞれ述べる．さらに，5 章で本アナライザを用いてマルチキャスト・トラヒックを解析した結果について述べる．

2. DVMRP の概要

2.1 DVMRP の機能

DVMRP はマルチキャスト・トラヒックの送信元へのメトリック（ディスタンス）の配列（ベクトル）を交換することを基本とするマルチキャスト・ルーチングプロトコルであり，以下の機能を有する．

2.1.1 隣接ルータの発見

DVMRP は直接接続されている物理リンクと，マルチキャスト・ルーチングをサポートしていないネットワークにマルチキャスト・データグラムを転送するための仮想リンクをサポートしている．仮想リンクとは，IP のカプセル化を用いてマルチキャスト・データグラムをユニキャスト・データグラムとしてルータ間を転送するためのリンクである．

DVMRP に基づくマルチキャスト・ルータ（以下 DVMRP ルータと呼ぶ）は，自分自身に接続されたすべての物理リンクおよび仮想リンクにに対して，Probe メッセージを定期的に送信することで隣接ルータの発見を行う．Probe メッセージには検出した隣接ルータのリストが含まれており，Probe メッセージを受信したルータは，リストに自分自身のアドレスが含まれているかを検査し，含まれていた場合は隣接ルータとの間でリンクを確立することができたと判断する．

2.1.2 配送木の構築

DVMRP ルータは，マルチキャスト・データグラムが転送される可能性がある配送木を構築する機能を提供する．

DVMRP は転送アルゴリズムに RPM（Reverse Path Multicasting）を使用する．RPM とは，送信元に対して通常の IP データグラムを転送する最短経路を逆にたどってマルチキャスト・データグラムを転送するというアルゴリズムであり，このため，送信元ネットワークごとに最短経路から構成される配送木を構築する．DVMRP ルータはインタフェースにデータグラムが到着すると，ルーチング・テーブルをチェックし，到着したインタフェースが送信元への最短経路上であるときのみ，下流に向かうインタフェースにデータグラムを転送する．

DVMRP は最短経路の計算を行うために，DVMRP 自身で経路情報を交換するメカニズムを持っている．ルータは Report メッセージを用いて，自分自身が持っている経路情報を隣接ルータに定期的に送信する．Report メッセージには，送信元ネットワーク・アドレス，

送信元ネットワークのサブネット・マスク，メトリック（Metric）が含まれている．メトリックは送信元ネットワークまでのホップ数を示している．

ルータは上流ルータに向けて，特定の送信元ネットワークからのデータグラムの転送要求を行う．これはReport メッセージを用いて経路情報を交換する際に，本来のメトリックに無限大（32）を加えた値を送信することで行う．これを Poison Reverse と呼ぶ．ルータは無限大の値よりも大きなメトリックを受信したときには，下流にデータグラムを転送する必要があるルータが存在することを検出することができる．

2.1.3 転送木の構築

DVMRP ルータは，マルチキャスト・トラヒックの受信要求の状況に応じて，配送木上で実際にデータグラムを転送する転送木を構築する機能を提供する．すなわち，マルチキャスト・グループのメンバが存在していないネットワークに対しては，データグラムの転送を停止することができる．下流にルータを持たない葉ルータは，IGMP（Internet Group Management Protocol）[10] メッセージの交換によって，ローカル・ネットワークにグループのメンバが存在していないことを検出すると，上流のルータに Prune メッセージを送信する．Prune メッセージには，マルチキャスト・グループ・アドレスと送信元ネットワーク・アドレスと Prune の有効時間（Prune Lifetime）が含まれており，Prune メッセージを受信したルータは対応するデータグラムの転送を Prune 有効時間だけ停止する．Prune メッセージを受信したルータは Prune 有効時間が経過した後に，再びデータグラムの転送を開始する．これを Broadcast&Prune と呼ぶ．Prune メッセージの有効時間中に新たにグループのメンバが出現したときには，Graft メッセージを送信することで先に送信した Prune メッセージを取り消し，データグラムの転送を開始することができる．

2.2 ルータの内部情報

DVMRP ルータは，到着したマルチキャスト・データグラムに対して，転送すべきインタフェースおよび実際に転送すべきかどうかを決定するために，ルーチング・テーブルと転送テーブルという 2 つのテーブルを保持している．

ルーチング・テーブルは送信元ネットワークへの最短経路を管理しているテーブルである．**図 1** にルーチング・テーブルの例を示す．このテーブルは，送信元ネットワークのネットワークアドレスとサブネットマスク，その送信元ネットワークへの最短系路上のルータ（上流ルータ）のアドレス，その送信元ネットワークへのメトリック（ホップ数），上流ルータへのリンクの状態（Up か Down），該当するエントリの有効時間（TTL）を保持している．図 1 の例では，2 つの送信元ネットワークがそれぞれの上流ルータを経由して，2 または 4 ホップで到達可能であることを保持している．

送信元ネットワーク	サブネットマスク	上流ルータ	メトリック	状態	TTL
192.168.1.0	255.255.255.0	192.168.1.1	2	Up	85
192.168.2.0	255.255.255.0	192.168.3.1	4	Up	85

図 1 ルーチング・テーブルの例
Fig. 1 Example of routing table.

送信元ネットワーク	グループ	TTL	受信インタフェース	出力インタフェース
192.168.1.0	224.1.1.1	150	1	2p 3
	224.2.2.2	200	1 Pr	2p 3p
	224.3.3.3	100	1	2 3
192.168.2.0	224.2.2.2	150	2 Pr	1p 3p

図 2 転送テーブルの例
Fig. 2 Example of forwarding table.

転送テーブルは，送信元ネットワークとマルチキャスト・グループのペアに対して，該当するデータグラムを受信した場合，下流のルータに転送するべきかどうかを管理しているテーブルである．**図 2** にその例を示す．このテーブルは，送信元ネットワークと宛先のマルチキャスト・グループ・アドレス，該当するエントリの有効時間（TTL），データグラムが到着すべき受信インタフェースと，データグラムを転送すべき出力インタフェースを保持している．ここで，受信インタフェースのフィールドの “Pr” は上流ルータに Prune メッセージを送信したことを，出力インタフェースのフィールドの “p” は，このインタフェースから Prune メッセージを受信したことを，それぞれ示している．図 2 の例では，送信元ネットワーク 192.168.1.0 はインタフェース 1 の先に存在し，3 種類のマルチキャスト・グループのデータグラムを送信しており，また送信元ネットワーク 192.168.2.0 はインタフェース 2 の先に存在し，1 つのグループのデータグラムを送信している．また，2 つの送信元ネットワークは，224.2.2.2 という 1 つのグループのデータグラムを送信しており，双方とも Prune メッセージにより転送を停止させられている．

3. アナライザの設計方針

3.1 概　　要

本稿で示すパフォーマンス・アナライザは，ネットワークを流れるデータグラムをオンラインで取得し，オフラインで性能評価を行う．本アナライザはネット

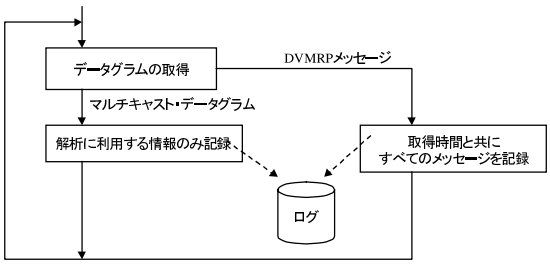

図 3 キャプチャリング・モジュールの処理の流れ
Fig. 3 Control flow of capturing module.

ワークを流れるマルチキャスト・データグラムとルータ間で交換されるメッセージを取得しログに記録するキャプチャリング・モジュールと，キャプチャリング・モジュールによって記録されたログを解析し，性能評価を行うアナライジング・モジュールにより構成する．

3.2 キャプチャリング・モジュール

キャプチャリング・モジュールは，以下の情報に，データグラムを取得した時間を表すタイムスタンプを付加して，ログに記録する．

- 宛先アドレスがクラス D アドレスのデータグラムの IP ヘッダ
- カプセル化されたデータグラムの宛先アドレスがクラス D アドレスのデータグラムの IP ヘッダと，オリジナルのデータグラムの IP ヘッダ
- プロトコル番号が 2（DVMRP）のデータグラムの IP ヘッダとメッセージ全体

なお，保存するログのサイズをできるだけ小さくするために，IP ヘッダに含まれる情報の中から解析に必要なデータグラム長，TTL，プロトコル番号，送信元アドレス，宛先アドレスのみを保存する．キャプチャリング・モジュールの処理の流れを**図 3** に示す．

3.3 アナライジング・モジュール

アナライジング・モジュールはキャプチャリング・モジュールによって記録された情報を解析し，その結果を GUI を用いて表示するモジュールである．本モジュール全体では以下の機能を実現する．

(1) トラヒックとメッセージの解析
(2) マルチキャスト・トラヒックの分割
(3) ルータの内部情報の推定
(4) トラヒックとルータの内部情報の関連付け
(5) 統計情報の解析

アナライジング・モジュールは複数のコンポーネントによって構成されており，**図 4** にこれらのコンポーネントを用いた処理の流れを示す．この図に示すように，DVMRP メッセージの種別およびマルチキャスト・データグラムのそれぞれに対して，処理するコンポーネントが異なる．

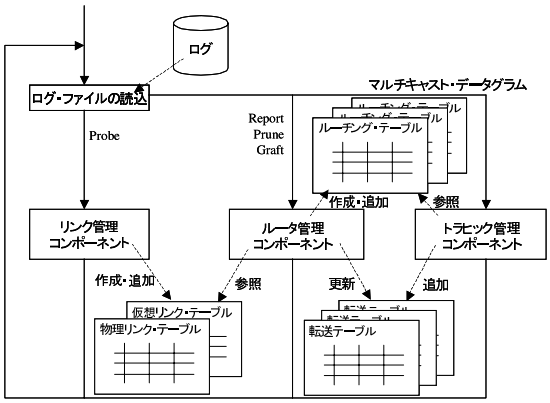

図 4 アナライジング・モジュールの処理の流れ
Fig. 4 Control flow of analyzing module.

4 章でアナライジング・モジュールの機能と処理手順の詳細について述べる．

4. アナライジング・モジュールの詳細

4.1 トラヒックとメッセージの解析

アナライジング・モジュールはキャプチャリング・モジュールによって記録されたログからパケット・データを読み込み，各コンポーネントでメッセージを処理する．Probe メッセージが検出されたときにはリンク管理コンポーネントへ渡し，Report，Probe，Graft の各メッセージが検出されたときにはルータ管理コンポーネントへ渡す．マルチキャスト・トラヒックが検出されたときには，トラヒック管理コンポーネントへ渡す．

各コンポーネント内では受け取ったメッセージとトラヒックを解析し，テーブルの作成やデータ管理を行う．GUI で解析結果を表示するときには，各コンポーネントによって解析された結果の時間的変化をグラフを用いて表示する．

4.2 リンクの検出

DVMRP は，前述のように，マルチキャスト・データグラムをカプセル化を用いて転送する仮想リンクと，直接転送する物理リンクの双方をサポートしているため，キャプチャリング・モジュールを設置しているネットワークには複数のリンクが設定されている場合がある．これらのリンクは同一の回線上を使用しているものの独立したリンクであるため，アナライジング・モジュールは，送信されたメッセージやトラヒックがどのリンクを流れているのかを検出する必要がある．

リンクの検出はリンク管理コンポーネントが行う．リンク管理コンポーネントの処理の流れは以下のよう

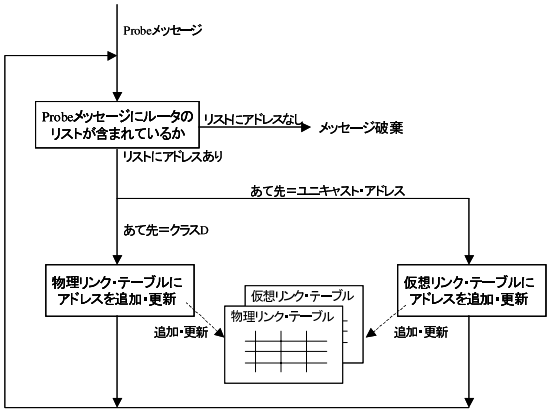

図 5 リンク管理コンポーネントの処理の流れ
Fig. 5 Control flow of link management component.

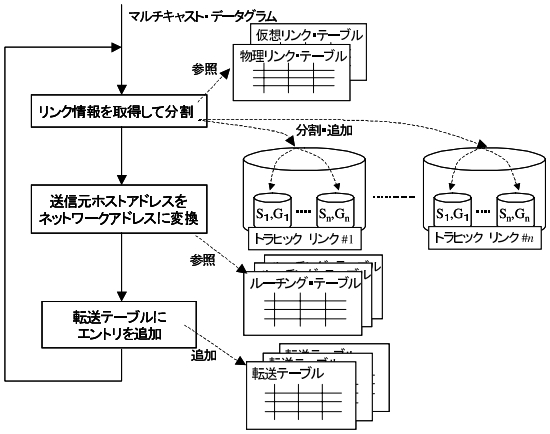

図 6 トラヒック管理コンポーネントの処理の流れ
Fig. 6 Control flow of traffic management component.

になる（**図 5** 参照）．

回線上に Probe メッセージが検出された場合に，リンク管理コンポーネントが呼ばれる．リンク管理コンポーネントはまず，Probe メッセージの中に隣接ルータのアドレスが含まれているかをチェックする．ルータのアドレスが含まれていないときには，リンクが確立していないものと見なしメッセージを破棄する．ルータのアドレスが含まれているときには，送信元ルータとリストに含まれているルータとの間にリンクが確立しているものと見なす．このとき，Probe メッセージのあて先アドレスがマルチキャスト・アドレスのときには，物理リンクに送信された Probe メッセージであると判断して，物理リンク・テーブルにエントリを追加する．また，Probe メッセージのあて先アドレスがユニキャスト・アドレスのときには，メッセージが仮想リンクに送信されたメッセージと判断して，仮想リンクのリンク・テーブルにエントリを追加する．ここで物理リンク・テーブルには，その物理回線に接続されている DVMRP ルータの IP アドレスが，仮想リンク・テーブルには，そのリンクの両端に存在する DVMRP ルータの IP アドレスが，それぞれ保持される．

4.3 マルチキャスト・トラヒックの分割

本アナライザは，マルチキャスト・トラヒックを，送信元のホストアドレスとマルチキャスト・グループのペアに分けて，そのパケット数やバイト数などの統計情報を収集する．そこで，トラヒック管理コンポーネントが，取得したトラヒックを送信元ホストアドレスとマルチキャスト・グループのペアに分割する（**図 6** 参照）．

トラヒック管理コンポーネントは，マルチキャスト・データグラムを受け取ると物理または仮想リンク・テーブルを参照し．どのリンクを転送されたトラヒックであるかを決定する．さらに，リンクごとのトラヒックに対して，送信元ホストアドレスとマルチキャスト・グループに分割して保持する．

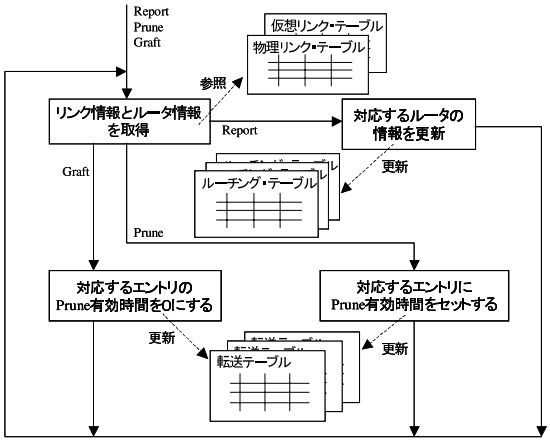

図 7 ルータ管理コンポーネントの処理の流れ
Fig. 7 Control flow of router management component.

さらに，トラヒック管理コンポーネントでは，新たなマルチキャスト・トラヒックを検出した場合に，転送テーブルへ登録する処理を行う．この処理が図 6 においてトラヒックの分割に引き続いて示されている．この処理については，4.5 節において述べる．

4.4 ルーチング・テーブルの推定

本アナライザでは，リンクの検出の結果検知された DVMRP ルータのそれぞれに対して，そのルータが管理するルーチング・テーブルを推定する．この処理は，**図 7** に示すような手順によりルータ管理コンポーネントで行われる．

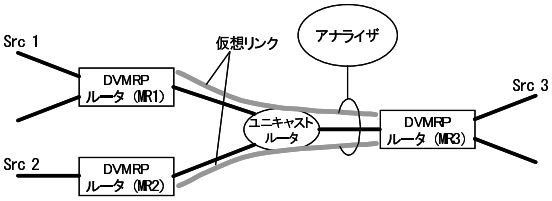

図 8 マルチキャスト・ネットワークの例
Fig. 8 Example of multicast network.

送信元ネットワーク	サブネット・マスク	上流ルータ	メトリック	有効時間 (sec)
Src1	255.255.255.0	MR1	5	70
Src2	255.255.255.0	MR2	5	70
Src3	255.255.255.0	Unknown	2	Unknown

図 9 推定したルーチング・テーブルの例
Fig. 9 Example of estimated routing table.

回線上に Report メッセージが検出されると，ルータ管理コンポーネントが呼ばれる．ルータ管理コンポーネントは，Report メッセージの送信元アドレスとあて先アドレスから物理または仮想リンク・テーブルを参照し，どのリンク上を転送されたメッセージをチェックする．このとき，リンク・テーブルに該当するエントリが存在しないときには，そのメッセージを破棄する．

次に，ルータ管理コンポーネントは Report メッセージの情報により，その送信元である DVMRP ルータのルーチング・テーブルの更新を行う．Report メッセージに含まれるエントリの中で，無限大（32）よりも小さいメトリックを持つルートについては，ルーチング・テーブルの送信元ネットワーク，サブネットマスク，メトリックの値を登録する．この場合は上流ルータのアドレスを推定できないため，上流ルータを “Unknown” とする．

一方，Report メッセージに含まれるエントリの中で，無限大よりも大きなメトリックを持つルート（Poison Reverse が行われたルート）は，送信元ルータが下流ルータであると判断し，その Report メッセージが流れたリンク上で最も小さなメトリックでルートを広告しているルータを，そのルータの上流ルータであると判断する．その結果をルーチング・テーブルに登録する．

図 8 の構成を持つネットワークを例にして，アナライザが DVMRP ルータ MR3 のルーチング・テーブルを推定した結果の例を**図 9** に示す．

ルータ MR1 経由で接続される Src1，MR2 経由で接続される Src2 のそれぞれのネットワークに対しては，上流ルータがそれぞれ MR1 と MR2 となる．また Src3 についてはアナライザが監視する範囲では上流ルータの情報が流れないため，上流ルータは “Unknown” のままとなる．

このように推定したルーチング・テーブルは，後述のように転送テーブルの更新において，ネットワーク・アドレスとホスト・アドレスを変換するために使用される．

4.5 転送テーブルの推定

転送テーブルの推定は，ルータ管理コンポーネントとトラヒック管理コンポーネントが行う．

トラヒック管理コンポーネントは，前述のように，マルチキャスト・データグラムを検出すると，送信元ホスト・アドレスとマルチキャスト・グループへの分割を行った後に，新たなマルチキャスト・トラヒックを検出した場合に，転送テーブルへ登録を行う．

しかし，DVMRP はマルチキャスト・トラヒックの転送を，送信元ネットワークとマルチキャスト・グループのペアによって管理している．そのため，マルチキャスト・データグラムから検出された送信元ホスト・アドレスから，対応するネットワーク・アドレスを求める必要がある．この処理はルーチング・テーブルを参照することにより行う．すなわち，図 6 に示すように，マルチキャスト・トラヒックの分割を行った後，そのトラヒックを受信するルータに対応するルーチング・テーブルを参照し，登録されている送信元ネットワークとサブネットマスクの値から，処理しているデータグラムの送信元アドレスに対応する送信元ネットワーク・アドレスを求める．その後，そのトラヒックを受信するルータに対応する転送テーブルを参照し，現在処理しているマルチキャスト・トラヒックが登録されていない場合は，エントリを追加する．

一方，Prune メッセージを検出すると，ルータ管理コンポーネントが呼ばれ，Prune メッセージを送信および受信したルータの転送テーブルの該当するエントリの Prune 有効時間を，メッセージ内で指定された時間にセットする．また Graft メッセージに対してもルータ管理コンポーネントが呼ばれ，転送テーブルの該当するエントリの Prune 有効時間を 0 にリセットする（図 7 参照）．

図 8 のネットワークにおいて，アナライザが DVMRP ルータ MR3 の転送テーブルを推定した結果の例を**図 10** に示す．この例においては，Src1 から 3 つのマルチキャスト・グループのトラヒックが転送され，Src3 から 1 種類のマルチキャスト・トラヒックが流れている状況を示している．また MR2 から 224.1.1.1 に対して Prune メッセージが転送され，さらに，上流

送信元ネットワーク	グループアドレス	上流ルータ		下流ルータ	
		IPアドレス	Prune有効時間	IPアドレス	Prune有効時間
Src1	224.1.1.1	MR1	200	MR2	200
	224.2.2.2	MR1	-	MR2	-
	224.3.3.3	MR1	-	MR2	-
Src3	224.2.2.2	Unknown		MR1, MR2	150, -

図 10 推定した転送テーブルの例
Fig. 10 Example of estimated forwarding table.

ルータである MR1 に対しても Prune メッセージが転送されたことになっている．

4.6 トラヒックとルータの内部情報の関連付け

前に述べた手法で推定したルーチング・テーブルと転送テーブルを用いて，マルチキャスト・トラヒックがリンク上を転送されたまたは転送されなくなった理由を解析する．

DVMRP においてマルチキャスト・トラヒックの転送が開始されるには，以下のような原因が考えられる．

(1) 送信元ホストが送信を開始した．
(2) Prune メッセージの有効時間が終了した．
(3) 新しいメンバが出現した．

これに対して，本アナライザでは，推定した転送テーブルにエントリがない場合「送信元ホストが送信を開始した」と判断する．推定した転送テーブルで保持している Prune メッセージの有効時間が終了するときにトラヒックが転送された場合には「Prune メッセージの有効時間が終了した」と判断する．また，Graft メッセージが送信された場合には「新しいメンバが出現した」と判断する．

同様に，マルチキャスト・トラヒックの転送が停止した場合に対しても，以下の 2 つの原因を推定する．

(1) 送信元ホストが送信を停止した．
(2) Prune メッセージが転送された．

4.7 統計情報の解析

DVMRP は RPM アルゴリズムによってデータグラムの転送を行っているため，定期的に Broadcast&Prune を繰り返しており，この間はグループのメンバが存在していないにもかかわらずデータグラムが転送される．この不要なトラヒックを評価するためにトラヒックの統計情報の解析を行う．

ここで下流にグループのメンバが存在している時間を有効時間，グループのメンバが存在していない時間を無効時間と呼ぶ．**図 11** に示すように，有効時間は Prune メッセージがまったく送信されていないグループの全時間と，Graft メッセージが送信された後の時間とし，無効時間は Prune メッセージが送信され，Graft メッセージが送信されるまでの時間とする．

各グループに対して，無効時間に転送されたトラヒックの転送量を評価する．

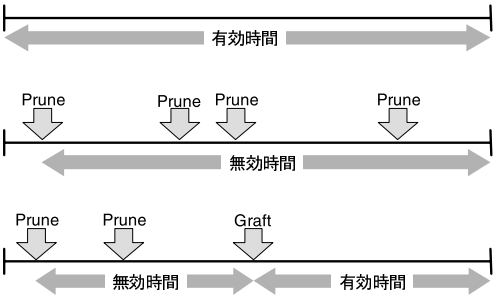

図 11 有効時間と無効時間
Fig. 11 Valid and invalid period.

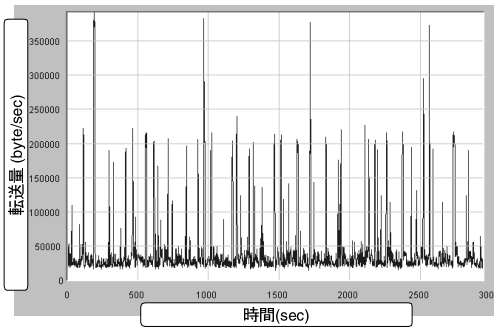

図 12 リンクを流れるトラヒック
Fig. 12 Total of transmitted traffic over monitored link.

5. 解 析 例

実装したシステムを用いて実際のネットワークにおけるマルチキャスト・トラヒックの解析を行った．**図 12** は監視したリンクを流れるマルチキャスト・トラヒック（バイト数）全体の時間的変化を表示したものである．このトラヒックを送信元ホスト・アドレス，マルチキャスト・グループごとに分割したトラヒックの例を図 13 から図 16 に示す．各図の上のグラフはトラヒックの転送量（バイト数）の時間的変化を示し，下のグラフは Prune メッセージの有効時間（Prune Lifetime）を示している．Prune メッセージの有効時間を示すグラフでは，値が増加している点で Prune メッセージが検出されたことを示し，値が 0 になった点で Prune メッセージの有効時間が終了したことを示している．また，Graft メッセージが検出されたときには，その時点で Prune メッセージの有効時間のグラフを 0 にリセットしている．

図 13 のトラヒックに対しては，対応する Prune メッセージが検出されなかった．したがってこのトラヒックは，監視したリンクよりも下流のネットワークにおいてマルチキャスト・グループのメンバを有し，

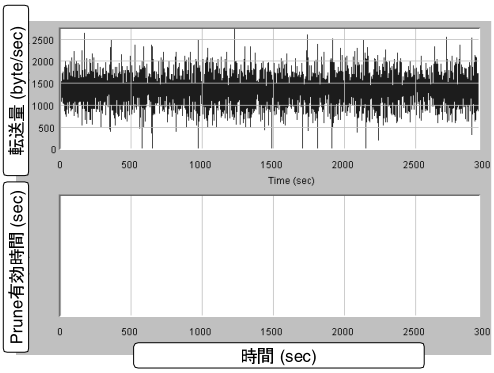

図 13 連続的に転送されるトラヒック
Fig. 13 Traffic transmitted continuously.

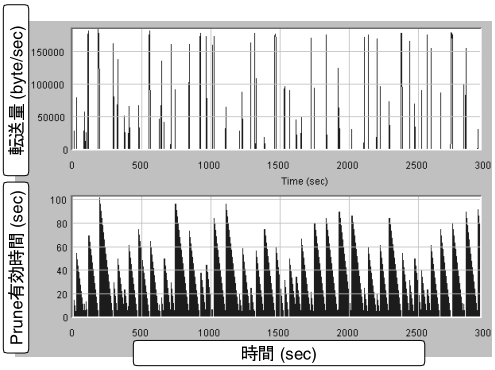

図 14 定期的に Prune メッセージが送信されるトラヒック
Fig. 14 Traffic with frequent prune messages.

このために連続的にトラヒックが転送されていると判断できる．

図 14 のトラヒックでは，対応する Prune メッセージが検出され，さらに Prune メッセージの有効時間が 0 になるとトラヒックの転送が再開され，それに対して再び Prune メッセージが送信されていることが分かる．このため，このトラヒックに対しては，下流にこのグループのメンバが存在しておらず，Broadcast&Prune が繰り返されていると判断できる．

図 15 のトラヒックは図 14 と似た形でトラヒックが転送されているが，対応する Prune メッセージが検出されなかった．したがって，このトラヒックは下流にグループのメンバを有しており，トラヒックの送信元が定期的にトラヒックの転送開始・停止を繰り返すようなパルス的なトラヒックを流していると判断できる．

図 16 のトラヒックは，最初は対応する Prune メッセージが検出されていたが，ある時点で Prune メッセージの有効時間が 0 となり，その後は Prune メッセージが検出されない．すなわち，最初は Broadcast&Prune

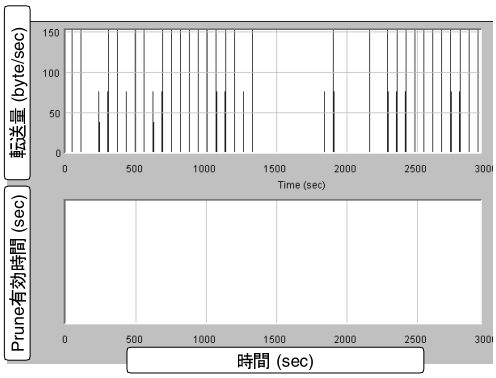

図 15 対応する Prune メッセージが送信されないトラヒック
Fig. 15 Pulse type traffic without associated prune messages.

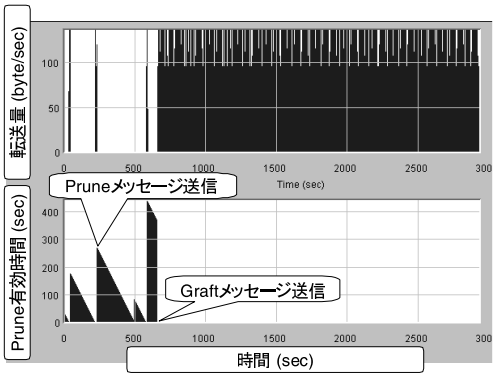

図 16 Prune と Graft が送信されるトラヒック
Fig. 16 Traffic with prune and graft messages.

を繰り返しているが，途中で新たにグループのメンバが出現したために Graft メッセージが送信され，連続的にトラヒックが転送されていたと判断できる．

このように，DVMRP のメッセージを解析することにより，個別のマルチキャスト・トラヒックの転送の開始・停止の原因を推定することが可能となった．特に，図 14 と図 15 の区別を行うためには，DVMRP の解析が不可欠であるといえる．

次に 4.7 節で述べた手法により統計情報の解析を行った．**表 1** はリンクを流れるマルチキャスト・トラヒックの統計情報を示している．この結果からリンクを転送されるトラヒックの中で，50.9% のトラヒックがマルチキャスト・グループのメンバが存在していないにもかかわらず転送されている無効なトラヒックであることが分かる．

6. む す び

本稿では DVMRP に基づくマルチキャスト・トラヒック用パフォーマンス・アナライザの実装とその解

表 1 マルチキャスト・トラヒックの統計情報
Table 1 Statistics of captured multicast traffic.

Item	Value
Number of Multicast Groups	52 groups
Transmitted Packet Counts	112,799 packets
Transmitted Bytes	52,602,947 byte
Average Throughput	17,874 byte/sec
Invalid Transmitted Packet Counts	37,185 packtes (33.0%)
Invalid Transmitted Bytes	26,781,609 (50.9%)
Average Throughput of Invalid Traffic	9,100 byte/sec

析例について述べた．本システムはネットワークを流れるデータグラムの統計情報だけでなく，マルチキャスト・ルータ間で交換されている DVMRP メッセージを取得し，ルータの内部情報を推定することで詳細な性能評価を行うことが可能である．

また，推定した内部情報とトラヒックの関連付けを行い，転送されたトラヒックの中で受信者が存在する有効なトラヒックと，受信者が存在していないにもかかわらず転送されている無効なトラヒックの評価を行うことができる．

参 考 文 献

1) Maufer, T. and Semeria, C.: Introduction to IP Multicast Routing, draft-ietf-mboned-intro-multicast-03.txt (Jul. 1997).
2) Kumar, V.（著），楠本博之（訳），インターネットマルチキャスト MBone，インプレス (Dec. 1996).
3) Cooperative Association for Internet Data Analysis. http://www.caida.org/
4) Manta Ray. http://www.caida.org/Tools/ Manta/
5) UCLA / Xerox PARC Multicat Route Monitor. http://www.ganef.cs.ucla.edu/ masseyd/ Route/
6) MultiMON — An IP Multicast Monitor. http://www.merci.crc.ca/mbone/MultiMON/
7) Waitzman, D., Partridge, C. and Deering, S.: Distance Vector Multicast Routing Protocol, RFC1075 (Nov. 1988).
8) Pusateri, T.: Distance Vector Multicast Routing Protocol, draft-ietf-idmr-dvmrp-v3-08.txt (Aug. 1999).
9) Ueno, S., et al.: Analysis of Internet Multicast Traffic Performance Considering Multicast Routing Protocol, *Proc.International Conference on Network Protocols 2000*, pp.95–104 (Nov. 2000).
10) Deering, S.: Host Extensions for IP Multicasting, RFC1112 (Aug. 1989).

(平成 13 年 6 月 8 日受付)
(平成 13 年 11 月 14 日採録)

植野 誠史（学生会員）
昭和 51 年生．平成 10 年千葉大学工学部電気電子工学科卒業．平成 12 年電気通信大学大学院情報システム学研究科情報ネットワーク学専攻博士前期課程修了．現在同研究科博士後期課程在学中．インターネットにおけるマルチキャスト通信とモバイル IP 等に関する研究に従事．

加藤 聰彦（正会員）
昭和 31 年生．昭和 53 年東京大学工学部電気工学科卒業．昭和 58 年同大学院博士課程修了．同年国際電信電話（株）入社．現在,（株）KDDI 研究所執行役員．工学博士．昭和 62 年から 63 年まで米国カーネギーメロン大学計算機科学科客員研究科学者．この間，OSI 通信プロトコルの実装，通信システムの試験技法，プロトコルの形式記述，分散処理，ATM，高速インターネット，モバイル IP 等の研究に従事．平成元年度元岡賞受賞．平成 5 年度より電気通信大学大学院情報システム学研究科客員助教授．電子情報通信学会会員．

鈴木 健二（正会員）
昭和 20 年生．昭和 44 年早稲田大学理工学部電気通信学科卒業．昭和 44 年から 45 年までオランダのフィリップス国際工科大学に招待留学．昭和 51 年早稲田大学大学院博士課程修了．同年国際電信電話（株）入社．同社研究所コンピュータ通信研究室長,（株）KDD 研究所代表取締役副所長等を歴任．現在,（株）アドバンスト・コミュニケーションズ取締役会長．工学博士．この間，磁気記録，パケット交換方式，ネットワークアーキテクチャ，高速・分散処理の研究開発に従事．昭和 62 年度前島賞，平成 4 年度電子情報通信学会業績賞，平成 7 年度科学技術庁長官賞を各受賞．平成 5 年度より電気通信大学大学院情報システム学研究科客員教授．電子情報通信学会，IEEE 各会員．