

L-11

大規模ライブ配信アーキテクチャの提案

A proposal of Large-Scale live broadcast

流 一秀†
Kazuhide Nagare

近藤 栄一†
Eiichi Kondou

1. はじめに

ブロードバンドの出現によって、エンドユーザへの高品質なストリーミングが実用化されてきている。現在、インターネット上で行われているストリーミング配信は、ライブ配信とオンデマンド配信に分類される。

ストリーミング配信の大部分は、キャストによって行われているが、キャストではネットワーク帯域を圧迫するため、大規模なライブ配信を行うのに現実的ではない。これを解決する技術としてIPマルチキャストがある。IPマルチキャストは、ルータでパケットをコピーし、データ転送を行うため、特定のネットワーク部分へ大きな負荷をかけずに、大規模なライブ配信ができる。しかし、IPマルチキャストによる大規模ライブ配信を実現するためには課題が残されている。

本稿ではこれらの課題を解決し、大規模なライブ配信を実現するアーキテクチャを提案する。

2. IP マルチキャストとその課題

2.1 課題の分類

IPマルチキャストは、宛先アドレスにグループアドレスを用いて配信を行うため、通常のキャストと異なり、グループへ参加しているメンバーを管理することによって、配信を行う。しかし、グローバルネットワーク上に多数存在している多くのルータはIPマルチキャストに対応しておらず、IPマルチキャストを使用することによって配信先のネットワークや、端末が限られてしまう。従って、視聴可能ユーザ数が少なく、大規模配信として成立が難しい。

一方、アプリケーションレベルでのマルチキャストが存在する。しかし、ソフト処理であるため、ネットワーク内での遅延のばらつきが大きく大規模なライブ配信を行うのには適さない。

また、IPマルチキャストでのライブ配信事業は、インターネットでの配信であるため、既存の放送事業の様に多くの視聴者を得ることが困難であり、広告費のみで運営を行うビジネスモデルの成立が難しく、コンテンツへの課金が必要である。しかし、IPマルチキャストにはユーザ認証や課金等の基本的な管理を行う機能が考慮されておらず、事業への活用が難しい。

2.2 大規模配信実現への課題

(1) グループアドレスの扱い

NATはIPv4アドレスの枯渇問題の解決を目的とする技術であるが、NATの存在もIPマルチキャストの普及を妨げている。NATはグローバルアドレスとプライベートアドレスを対応づける技術であり、入力パケット、及び出力パケットの宛先アドレスとソースアドレスを、テーブルに従って書き換えを行う。一方、グローバルアドレス空間より送られてくるグループアドレスは一意であり、単にテーブルを使用するだけでは、アドレスを確認できないため、変換することができない。従って、IPマルチキャストに対応していないNATを通過して配信を行うことができない。

現在、NATは広く使用されているが、IPマルチキャストに対応しているNATは少なく、多数の視聴者へ配信を行うことができない。

(2) ライブ配信に要求される機能

配信にあたって、コンテンツの配信側は何らかの形で収益を得る必要がある。そのために、コンテンツの配信を行う相手を選択し、特定の相手へのみ配信を行うユーザ認証機能が必要である。また、放送モデルを考えた場合、ユーザ認証によって得た情報を元に、視聴率や視聴時間といった視聴情報を収集し、課金を行うシステム、視聴情報を収集し、今後のコンテンツやサービス等の事業へ生かす仕組みが必要である。

しかし、IETFによって定められているIPマルチキャストプロトコルには、認証を行う機能が含まれていない。そのため、ライブ配信を提供する側は、単にIPマルチキャスト配信を行うだけではユーザ認証を行えず、配信先を選択することができない。従って、視聴状況の収集や課金のための情報を取得することが困難である。

2.3 関連方式

IPマルチキャストによるユーザ認証は、様々な議論がなされているが、大規模な配信を考えた場合、これらの方式には課題が残っている。

(1) IGMP 拡張方式

IGMPv2を拡張し、認証を行う方式が提案されている[1]。この方式は、配信ホストの認証を行うために送信開始をネットワークの入口ルータに通知するメッセージと、ユーザ認証時のセキュリティ確保のためのメッセージを、IGMPに追加する。これを用い、ネットワークの入口と出口のルータにてRADIUSサーバを使用し、配信ホスト及び受信ホストの認証を行う。このモデルを図1に示す。ユーザデータベースをネットワーク内のRADIUSサーバで、一括管理することで、メンテナンスが容易になり、大規模ネットワークへの適用が可能である。しかし、この方式では、IPマルチキャストプロトコルを拡張するため、ルータ及び端末のソフトウェア変更を伴う。従って、大規模に配信を行うことを想定した場合、多くの視聴者を得ることは難しい。また、NATを越えた配信を行えない問題も依然残されている。

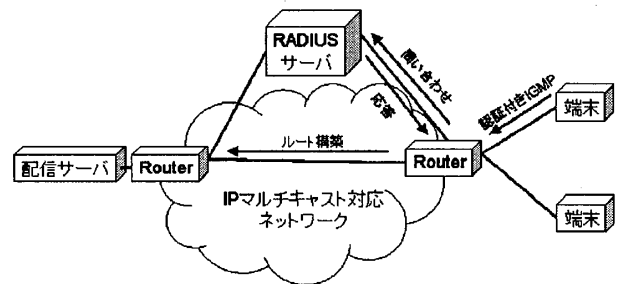


図1 IGMP 拡張方式におけるネットワークモデル

(2) IP マルチキャストに対応するファイアウォール

セキュリティを確保しつつファイアウォールを通過するためのアトライバルが提案されている[2]。グループアドレスでは配信サーバ-受信端末間で互いの認証を行うことができず、従来のキャストの手法ではセキュリティを確保することが困難である。この中の提案方式の1つとして、ファイアウォールがIGMP要求を認識し、グループメンバーを管理する手法が提案されている。しかし、この手法では、ファイアウォールを変更しなくてはならず、それらの変更は

† (株) NEC ネットワークス IP ネットワーク事業本部 IP ソフトウェア技術本部

個々のネットワーク管理者に頼らなくてはならない。

3. 提案方式

3.1 提案モデル

IP マルチキャストプロトコルから独立した認証機構を提案する。このとき、IP マルチキャストルーティングプロトコルから独立した IP マルチキャスト対応ネットワーク、非対応ネットワークに関わらず、同一の機構でユーザ認証を行う。そのため、定期的に行うユーザ認証を基に、視聴状況情報を収集し、それらの情報を元に課、視聴状況の分析などを行うことが可能な方式を提案する。

また、本提案はスケーラビリティに富んでおり、既存の設備をそのまま利用できるため、初期コストを抑えることで、小規模なライブ配信からの実現も可能である。

これらのネットワークモデルを図2に示す。

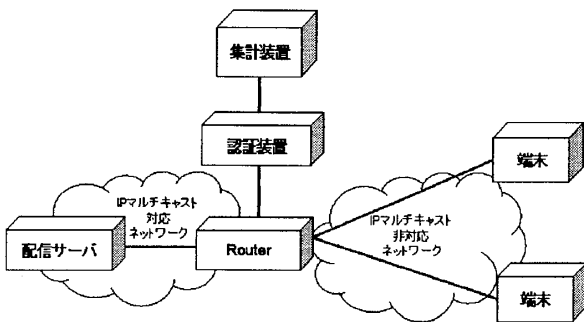


図2 ネットワークモデル

3.2 提案アーキテクチャ

3.2.1 IP マルチキャストの適応

IP マルチキャスト非対応ネットワークを配信データが通過する手法として、配信された IP マルチキャストデータを配信先数コピーし、個々のエキストアドレスに変換して送信することで、IP マルチキャスト非対応ネットワーク内のデータ転送を可能にする。

遅延に対し、十分な変換性能を得るためにハードウェアによるパケットコピーを行うルータ[3]を応用するものとする。また、ルータは、IP マルチキャストネットワークとエキストネットワークの境界において変換を行うことができる。

グループへの参加をエキスト通信にて可能な構成を構築する。端末はマルチキャスト対応ネットワーク、マルチキャスト非対応ネットワークに関わらず、認証装置にグループへの参加を要求する。認証装置は、ユーザ認証を行った後、IP マルチキャストに対応している各ルータへ、マルチキャストデータをエキストデータに変換し、要求のあった各端末へデータ配信を開始するメッセージを送信する。

3.2.2 認証・視聴状況監視方式

認証装置、集計装置を用いることによって、ユーザ認証、視聴情報収集を行う。ユーザ認証によって、配信先を選択した配信を実現する。また、配信開始時のみならず配信中も、定期的にユーザ認証を行うことによって、なりすまし等の不正な視聴を防ぐ仕組みを構成する。

図3に認証のシーケンス図を示す。

まず、マルチキャスト非対応端末は、ポート叩くなどへアクセスし、受信コンテンツを定める。ポート叩くでは、ユーザのアクセスに対し、配信を行っても良いかどうかを認証装置へと問い合わせる。このとき、端末が受信要求を行ってからデータ配信が終了するまでの間、通信メッセージなどを暗号化しセキュリティを確保する必要がある。

認証装置は、ユーザ認証によって得られた情報から、視聴に関する情報を集計装置へと送信する。

集計装置は、複数の認証装置より、ユーザ情報、配信開始時刻、配信終了時刻、視聴時間帯、配信内容等の情報を受信し集計を行う。集計されたデータから視聴時間、視聴コンテンツといった課金情報や、コンテンツごとの視聴率といった視聴情報の集計をし、視聴者の趣向や視聴率の調査、主要視聴時間帯等の調査を行い、今後の事業へフィードバックし、サービスの充実を図ることができる。

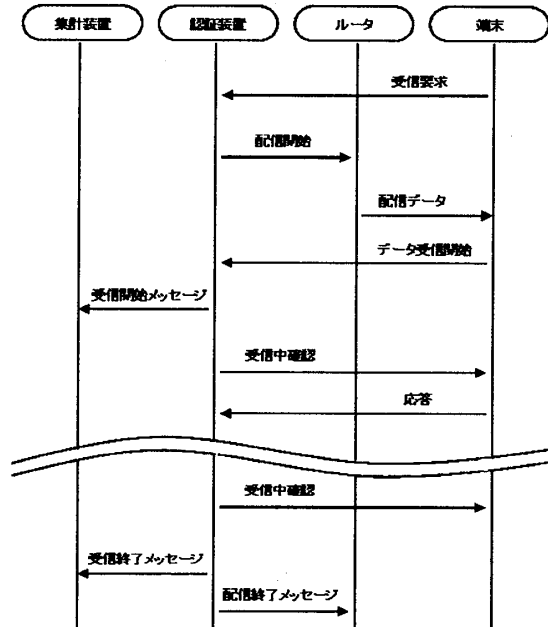


図3 認証シーケンス図

4. おわりに

IP マルチキャスト技術を活用しつつ、大規模ライブ配信に対応する方式を提案した。

本提案では、IP マルチキャストデータをエキストデータに変換し転送を行うことで、宛先アドレスがマルチキャストアドレスから、エキストアドレスへと変換されるため、多くの NAT が宛先アドレスを認識できない問題を解決でき、ファイアウォールの外側で変換を行えば、IP マルチキャストに対応していないファイアウォールを通過し配信できる。従って、配信可能ネットワークを広げ、多くのユーザへ配信を行える。

また、本稿では、ルーティングなどの経路選択には触れていない。その理由は、大規模なライブ配信を想定した場合、IP マルチキャストルーティングプロトコルは標準化されており、ルータ同士の相互接続性を保つために、IP マルチキャスト対応部分では IP マルチキャストルーティングプロトコルで経路の決定を行うべきである。

今後、実験環境を構築し、配信データのセキュリティ確保について調査・検討する。

参考文献

- [1] 石川憲洋他, IP マルチキャスト通信のユーザ認証機能の提案と実装, 情報処理学会論文誌, vol40, No10, 1999
- [2] Ross. Finlayson, IP Multicast and Firewalls, RFC 2588 (1999)
- [3] http://ccsd.biglobe.ne.jp/dio/new_site/products/middl_e_router/ix5000/ix5000.html