マルチメディア通信と分散処理　101－22
コンピュータセキュリティ　12－22
（２００１．２．２１）

マルチキャスト認証機構を付加したMusicCast/ASの構築

†川北良一　††泉裕　‡齋藤彰一　‡上原哲太郎　‡國枝義敏
†：和歌山大学大学院システム工学研究科　††：和歌山大学システム情報学センター
‡：和歌山大学システム工学部

内容梗概

現状のインターネットの映像・音楽配信は、ユニキャストによるビデオ・オン・デマンドシステム等がほとんどであり、放送システムに転用されているものでもスケーラビリティに欠ける。そこでマルチキャストを通信に利用する。しかし課金制放送システムの実現のためには、暗号化とユーザ認証が不可欠であるが、マルチキャストでは固有の困難がある。

本研究では、インターネット上での課金制放送システムの実装手法について考察する。特に、暗号化の手法、鍵管理の手法およびユーザ認証の手法について考察する。さらに、マルチキャストによる音楽放送システムMusicCast/ASを設計、実装を行う。

The implementation of a subscriber music-broadcasting system on IP multicasting : "MusicCast/AS".

Ryoichi Kawakita†　Yutaka Izumi††
Shoichi Saito‡　Tetsutaro Uehara‡　Yoshitoshi Kunieda‡

†Graduate School of Systems Engineering, Wakayama University
††Center for Information Science, Wakayama University
‡Faculty of Systems Engineering, Wakayama University

Abstract

Currently, most of the video/audio distribution systems on the Internet are basically unicasting video/audio-on-demand systems. Some of them are diverted as broadcasting systems, but they lack scalability by nature. To obtain their scalability, multicasting is indispensable. Encryption and user-authentication are also indispensable to realize subscriber-broadcasting system, but there are specific difficulties to realize them on multicasting system.

This research discusses the implementation of subscriber-broadcasting systems on the Internet. In particular, the methods to realize encryption security, key-management security and user-authentication techniques on those systems are argued. Furthermore, this paper describes the design and implementation of a music-broadcasting system on IP multicasting named "MusicCast/AS".

1. 背景

研究機関や大学を中心に発展してきたインターネットは、近年になって急速に社会の隅々に浸透しつつある。IMT-2000 による携帯電話サービスや、Fiber To The Home といった計画は、今後数年の間に個人・家庭に向けた高帯域で安価なデジタル通信回線が次々と提供されることを示している。近い将来インターネットは、あらゆる個人や団体に対し、あらゆる場所において提供される社会的インフラストラクチャとしての地位を得るのは確実である。

また、近年のマルチメディア通信技術の発達により、インターネットを用いてあらゆる形態の情報が伝達可能になった。その結果、既存のあらゆるメディア（手紙・新聞・電話・テレビ・ラジオなど）の機能はインターネットで技術的には代替可能になってきた。既に電子メールが手紙を置き換えつつあるように、他のメディアも、帯域と経済性の問題が解決され得るものは、次第にインターネットでの置き換えが進むと考えられる。

本研究では、テレビ・ラジオといった従来の放送メディアのインターネットへの置き換えが今後進むと予想して、その技術的問題点を考察した。

現在インターネットでの放送システムとして多く使われているもの（Real Networks, Windows Media, QuickTime など）は通信にユニキャストを用いており、「ビデオ・オン・デマンド」や「ミュージック・オン・デマンド」を単に同報的にしたシステムである。従って放送システムではデータ転送量がユーザ数に比例して増大し、スケーラビリティに欠ける。しかし将来はインターネット上でもマルチキャスト通信が一般化し、スケーラビリティの確保が可能になると思われる。

人々の嗜好の多様化により、現在テレビ・ラジオは多チャンネル化が進んでいるが、これにより１チャンネルあたりの視聴者数は低下し、広告収入に頼る無料放送が難しくなっている。従来の地上波・衛星波やケーブルを用いた放送に比べてより低いコストでの放送が可能と思われるインターネットテレビ・ラジオにおいては、さらに多チャンネル化が進行し、比較的少人数のコミュニティに対する放送の提供が中心になると思われる。このため、現在、衛星放送やケーブルテレビ放送において実現しているのと同様の有料放送が主流になると思われる。しかし、サービスを有料化にするためには、サービスを受けることが可能なユーザを制限する何らかのセキュリティシステムを導入する必要がある。

本研究では、以上の「セキュリティ」「スケーラビリティ」を兼ね備えたインターネット課金制放送システムについて考察する。さらに、マルチキャスト認証機構を付加したプロトタイプである MusicCast/AS の設計と試作、検証を行う。

2. システムのモデル

スケーラビリティとセキュリティを兼ね備えたインターネット放送システムを実装するため、以下のようなシステムのモデルを考察した。

まず、インターネットでの放送を可能にするために、放送局となるサーバが必要である。この放送局となるサーバからのデータ転送は、スケーラビリティ確保のため、コネクションレス型のマルチキャストを使用する。マルチ

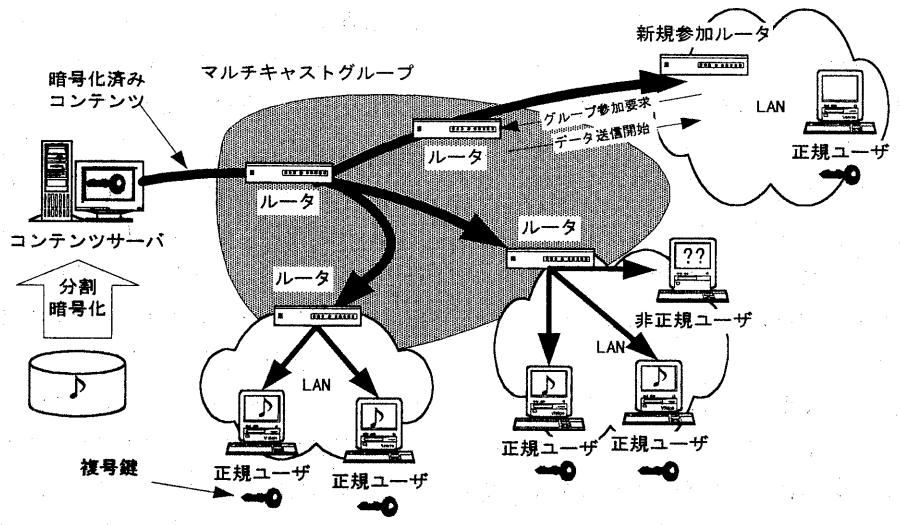

図 1 システムのモデル図

キャストは、IPv4 においては現在実験運用段階にあり、IPv6 への移行の際にはより実用化が進むと期待される。マルチキャストでは、サーバはネットワークに対してデータをクライアント数に関係なく一定量しか送信しないため、クライアント数に対するスケーラビリティの確保が容易である。その反面、本質的にコネクションレスの通信が前提となり、双方向性は限られる。

本システムは有料サービスを前提としているために、サービスを受けることが可能であるユーザを制限する必要がある。そのため、マルチキャストにおけるデータ送受信の際のユーザ認証システムを構築する必要がある。IPv4 におけるマルチキャストデータの配送は、現状ではマルチキャストグループと呼ばれる単位で管理され、IGMP[1]によってデータの受信要求を処理しているが、ここには個別のホストやユーザの認証機構は存在しない。また、IGMP は LAN 単位で管理されるため、同一 LAN 内に放送の受信権限のあるユーザ（正規ユーザ）と、ないユーザ（非正規ユーザ）が混在する場合、非正規ユーザにもデータの受信自体は可能になってしまう。さらに、IGMP の拡張などによってユーザ認証機構を実現することは、現状のマルチキャストシステム全体に波及する。よってこれを避けるため、コンテンツデータ自体への共通鍵による暗号化によって正規ユーザ以外へのデータ配信を抑止し、鍵の管理によって正規ユーザと非正規ユーザを区別することにした。

これらにより、システムのモデルは図 1 のようになる。放送されるコンテンツのデータはコネクションレス通信のためにパケット単位に分割され、暗号化されてから送信される。送信自体は現状のマルチキャスト通信のスキームがそのまま利用される。送信されたデータはクライアントプログラム内で再結合され、複号化されてから再生される。この際、データの欠落などへの対処も必要となる。

なお、このシステムで想定したのは有料サービスであるが、システムのモデル自体は、有料ではないが秘匿性の必要な放送などにも適用可能である。

3. マルチキャスト認証

このようなモデルに基づくインターネット有料放送システムの運用上の最も重要な課題は、マルチキャスト向けの認証をいかにおこなうかという問題である。具体的には、暗号化と鍵の管理に関する問題であり、

- どのような形式で暗号化するか
- 復号用の鍵をいかにして正規ユーザに分配するか
- 復号用の鍵が、正規ユーザから非正規ユーザに漏洩するのをいかに抑止するか（故意に漏洩するほか、料金未納などにより正規ユーザが非正規ユーザになる場合も含む）

この３点が課題となる。

暗号化の方式に関しては、放送コンテンツの性質によっては、全てのデータを暗号化せずともよいという場合がある。例えば音声や画像の場合、一部をノイズにするだけでも質が低下し、内容の概要が漏れても良い場合にはこれで十分な暗号化となっている。これを利用することにより、暗号化・復号化のコストが低く押さえられる他、鍵のサイズを小さくすることも可能である

暗号化の形式であるが、マルチキャストによるデータ配送を前提とする以上、全ユーザに同一の暗号化データが届くことを仮定せざるを得ない。よって最も単純な実装では、通常の秘密鍵による暗号化をおこない、全ユーザに同一の複合化用鍵を配布することになる。これはまた、鍵そのものはユーザIDとなる情報を持ち得ないことを意味する。

この鍵の配布方法と鍵の漏洩抑止は密接な関係にある。最も安全性の高い方法は、現在衛星放送などで行われているように、ハードウェアで作成した、ユーザに簡単に解析できない機器に鍵を実装する方法であるが、これはコスト等の問題が発生する。ソフトウェアにより実現する方法を考えると、全ユーザが同じ復号化用鍵を使い続けるという前提の場合、料金未納のユーザが不正に視聴し続けるのを防止するため、一定時間ごとに鍵を再配布することが必要になる。この再配布の際に各ユーザの視聴権を確認することになるが、ここでスケーラビリティが制限される。スケーラビリティを確保するためには鍵の再配布の時間間隔を広げることになるが、これは鍵が漏洩する危険性を増すことになる。

実装時には、これら点を考慮した上で、暗号化と鍵の配布方式を決定する必要がある。

4. 実装

前節までの考察に基づき様々な実装を試みるためのプロトタイプとして、インターネットでの課金制音楽配信システムMusicCast/AS を試作した。配送するコンテンツは、MP3（MPEG I layerIII）方式で符号化された音楽に限定し、PC 上でソフトウェアのみを用いて放送・再生するソフトウェアを作成した。OS として、サーバ・クライアントとも Linux を用いている。

4.1 放送局サーバ側

放送局となるサーバ側の主な処理は、以下のようになっている。

- MP3 ファイルの読み込み
- 共通鍵暗号方式を用いた暗号化
- マルチキャストでデータの配信 [2]

サーバ側処理では、まず配信するために登録してある MP３ファイルを読み込む。読み込んだデータをいったんバッファに溜め込み、暗号化を行う。暗号化の手法としては、ここ

では単純な共通鍵暗号方式を用いた。 [3]

MP3 のファイルは、フレームと呼ばれる小さなデータ群で構成されている。このフレームは、MP3 のファイルのビットレートや圧縮法などによって、このフレームの大きさはさまざまであるが、一般的には約 418Byte の大きさである。それぞれのフレームは、ヘッダ部・サイド情報部・メインデータ部から構成されているが、1 つ 1 つが完全に独立している。よって、途中 1 つのフレームが欠落しても、音楽ファイルとしては、再生することが可能である。

このファイル構造を利用し、サーバ側では、MP 3 ファイルをフレーム単位に分解し、メインデータ部に暗号化を行う。

暗号化は、数フレームごとに 1 つずつ、データ部分のいくつかのビットを反転させることによって行う。この反転パターンが暗号化・復号化の鍵となる。反転させるデータは MP3 によるエンコード後のものであるので、全体の 5%以下のデータのビット反転でも十分にデータは破壊され、品質は劣化する。これにより、正規の復号化鍵を持つユーザはもちろん、持たないユーザもどの曲がかかっているか推測できる程度の音質で視聴することができる。現在の実装では、暗号化を行ったフレームに対しては、ヘッダの中のエクステンション（通常、MP3 ファイルでは値は 0）を 1 にすることにより暗号化フレームが受信クライアントプログラムで選別できるようにしている。

このように暗号化を行ったデータを、サーバ側では、フレームごとに UDP でマルチキャストアドレスに向けて配信する。現在の実装では配信データには簡単のため何も特殊なヘッダを設けていないが、将来の実装では

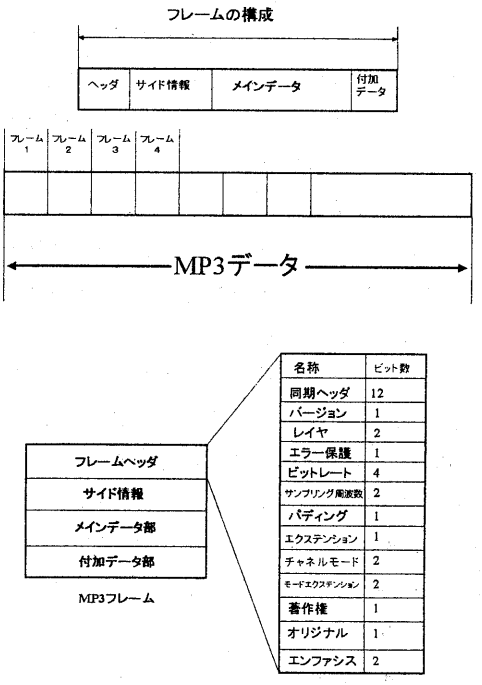

図 2 MP3 データのフレーム構造

RTP[4]に準拠したヘッダを設けて順序制御を行うことを検討している。

4.2 受信クライアント側

受信するクライアント側の主な処理は、以下のようになっている。

- 複合化鍵の受信
- データの受信
- データの復号
- HTTP データとして再構成して送出

クライアント側のプログラムではまず、認証用サーバにユーザ ID とパスワードを送信し、復号化用の鍵を受信する。この操作は通常の TCP である。現状では一度決定した鍵を時間ごとに変更する部分は未実装である。

次にクライアントは、サーバから送信されてくる UDP パケットを受信し、バッファリ

ングしながら単純に結合してゆく。その際、エクステンションビットを調べ、暗号化されているフレームがあれば鍵を用いて復号化する。また、バッファの大きさには限りがあるため、受信中に再生されなかったデータは古いものから破棄される。

こうしてバッファ上に構成した元の MP3 データの再生は、汎用の MP3 プレイヤーで行う。そのため、クライアントプログラムは、HTTP サーバとして動作し、HTTP 接続要求に応じて、バッファ上のデータに適切な HTTP ヘッダを付加してからデータストリームとして送出する。サービスを受けるユーザは、HTTP ストリーミング再生が可能であるプレイヤーを利用してクライアントマシン自身に HTTP アクセスすることにより、ストリーミング再生が可能である。

プレイヤーでアクセスしない間も、プログラムが動作していると、データを受信しつづけ、古いものから破棄されるようになっている。

以上のようにして、サービスを受けるクライアントは、サーバから届いた最新の音楽を聴くことが可能になる。

5. おわりに

本システムの実装により、音楽データのマルチキャスト配信の基本的な枠組みは作成できた。特に、復号化鍵を持たない場合には質の低い状態での試聴が可能であり、鍵を持つ場合に正しい品質で聴取が可能になるという初期の実装目標は達成した。しかし、システムはまだ実装の初期段階にあり、現時点ではわれわれが目指している機能の多くを備えていない。特に現時点では欠落したデータがあった場合に生じるフレーム間の不整合を最低限しか修正していないため、ノイズが生じる。この部分は RTP の導入・実装時に同時に解決する予定であるが、RTP はユーザ認証機構に対する考慮がなされていないため、ユーザ認証機能の実装方法とあわせて現在議論中である。これらの実装は今後の課題として残っている。

今後は、特にユーザ鍵の管理部分について検討する予定である。特に、鍵の漏洩があった場合に、鍵を漏らしたユーザが特定できるよう、鍵に ID 情報を含めることのできるような手法の確立のため各種調査を続けている。また、他のマルチメディアファイル(動画像・音声ファイルなど) を扱えるようなシステムを構築することにより、インターネットでの課金制放送システム一般についても考察を広げてゆきたい。

謝辞

いつも御議論いただく、和歌山大学システム工学部情報通信システム学科國枝・上原研究室の各位に感謝の意を表します。

参考文献

[1] W.Fennner: *Internet Group Management Protocol, Version 2*, RFC2236 (1997)

[2] Thomas A.Maufer : bit 別冊 IP マルチキャスト入門、共立出版(2000)

[3] 菅野　政孝：ネットワークセキュリティと暗号化,カットシステム (1997)

[4] Audio-Video Transport Working Group : *RTP: A Transport Protocol for Real-Time Applications*, RFC1889 (1996)