ソフトウェアによる視聴者限定型デジタル放送プラットホームに関する研究開発（0221042）

Research and Development of Limited Audience Type Digital Broadcast Platform by Software

山岡 克式
東京工業大学 大学院理工学研究科
Katsunori YAMAOKA
Graduate School of Science and Engineering, Tokyo Institute of Technology

上原 哲太郎† 佐藤 敬††
Tetsutaro UEHARA† Takashi SATOH††
†京都大学 大学院工学研究科 ††北九州市立大学 国際環境工学部
†Graduate School of Engineering, Kyoto University
††Faculty of Environmental Engineering, The University of Kitakyushu

研究期間 平成 14 年度～平成 16 年度

概要

専用認証ハードウエアなどのインフラストラクチャに依存しない、「ソフトウェアによる視聴者限定型デジタル放送プラットホーム」の実現を目指し、視聴者数に対してスケーラブルな視聴者限定型放送システムに必要な要素技術であるユーザ認証、鍵管理の研究開発、およびストリームメディアの時間特性に着目した電子指紋技術の研究開発を行う。さらに、これらのシステムをインターネット上で IP マルチキャストを利用して「インターネット放送システム」として実現する上で必要となる、ネットワークにおける様々なストリームメディア通信品質制御技術の研究開発を行う。最後に、試作システムによる実証実験を行い、提案手法の有効性を確認する。

Abstract

The objective of our research and development is to realize "limited audience type digital broadcast platform" by using only software. This system does not depend on particular authentication hardware or network or broadcast infrastructures. Toward the objective, we have researched and developed some elemental technologies such as user authentication, key management, digital watermark for stream media, QoS control for live streaming media, and so on. Finally, our prototype system has shown the effectiveness of our proposed technologies.

研究内容及び研究成果

本研究開発では、単一の同報ストリームに対するこれらの問題を同時に解決するために、各利用者に配布する情報を適切に符号化・暗号化することで、正当な利用者のみが視聴可能であり、かつ、このようにして配信されるコンテンツに各利用者毎に異なる電子指紋を埋め込むことで著作権保護を実現する、スケーラビリティを考慮したインフラストラクチャに依存しない「ソフトウェアによるコンテンツ視聴者限定型放送システム」の実現を目指した、セキュリティおよび通信品質の両面に関する様々な技術の研究開発を行った。さらに、これらの新規技術により実現される新しいセキュア放送プラットホームの一実装として、インターネットライブ放送実験システムを実現し、実証実験により提案手法の有効性を確認した。本研究で実現する放送システム全体の概念図を図 1 に示す。

まず、放送型暗号に Tracing Traitor 方式を用いた放送システムの実証実験のため、MPEG-1 LayerIII 方式による音声圧縮を予め行ったファイルを分割して IP マルチキャストを用いて転送し、再生させるシステム MusicCast/AS の設計・開発を行った。暗号化の鍵は、Naor らの提案による Tracing Traitor 方式で放送し、あらかじめ WEB クライアントを用いて各ユーザに個別配送しておいた認証用鍵で復号化させるようにした。この結果、システムを不正利用するための認証用鍵の偽造には複数のユーザがそれぞれの認証用鍵を持ち寄る「結託」が必要となるが、この結託の抑止パラメータとして、例えば 4 名までの結託が行われても不正ユーザの追跡が可能なシステムをユーザ数 10 万人に対し実現したとすると、Tracing Traitor 方式による鍵配布がトラヒックに与える影響は、MusicCast が対象とした MP3 のデータ量に対してはその約 10%しか必要とならず、十分実用的に運用可能であることが実証できた。また、データ配送には IP マルチキャストを用いたため、配送用インフラストラクチャはユーザ数に対し十分なスケーラビリティを持つことも実証された。なお、ユーザ数および結託人数に対する鍵配布に必要なトラヒックの関係も理論的に導出されており、システム運用側のセキュリティ要求およびネットワーク環境、ユーザ数に応じてセキュリティレベルを適切に変更可能であるとともに、インターネットの帯域が大きくなればなるほど、結託への耐性はさらに強化可能である。

次に、MusicCast/AS の開発成果をもとに、MPEG-1 による動画像をリアルタイムで生成し、分割して IP マルチキャストを用いて転送、再生させるシステム YouCanCast の設計・開発を行った。本システムでは、MPEG-1 の映像をフレームごとに分割し、全フレームに暗号化を施したものを RTP に基づく UDP データグラムに格納して、IP マルチキャストを用いて配送するシステムとした。その結果、MusicCast/AS に比べ、コンテンツそのもののデータ量が 1000 倍に大きくなったため、10 万ユーザへの対応、4 人までの結託といった条件での鍵配布配布がトラフィックに与える影響は 0.01%となり、本提案方式により生じるトラフィックはほとんど無視できるサイズとなったことを確認した。

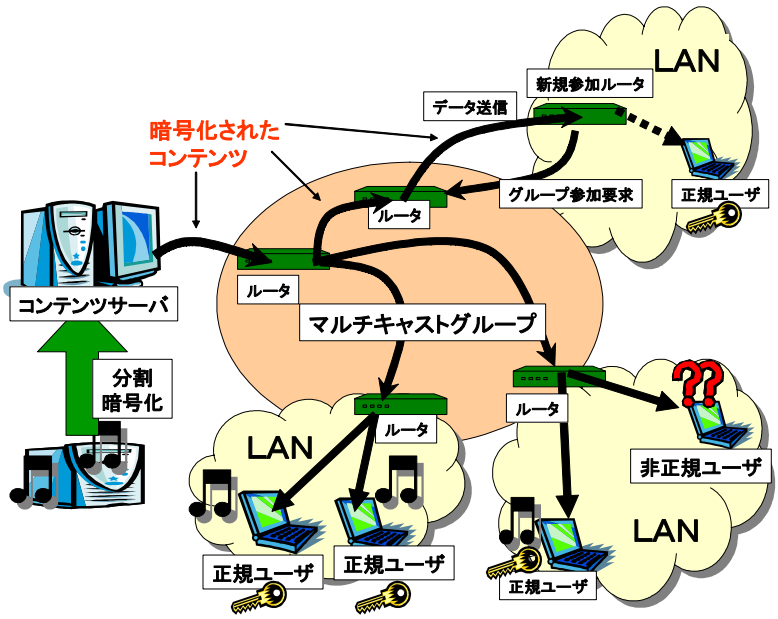

図 1　　実装放送システム概念図

さらに、復号化されたコンテンツの二次配布への抑制のため、ストリームメディアの特徴を利用した、MPEG 等の符号化方式によらない、汎用的な新しいストリームメディア用電子透かしの埋め込み方式、符号化方式を開発した。提案方式は、動画像がその価値を有するためには一定数以上のフレームが必要であるということを考慮し、透かし情報から各フレームに対する符号を生成して透かし情報を埋め込み、透かしが埋め込まれた動画像から一定数以上の符号を抽出して透かし情報を復元することを特徴としている。方式の安全性を理論的に検討するとともに、実際に動画像を利用して、透かしの埋め込みによる画質の劣化や、フレームデータの一部消失、破壊、編集に対する透かしの性能を実験により確認するために、DirectShow に基づいた MPEG1 圧縮コーデックを開発し、この中に圧縮時に同時に電子透かしを組み込むようにした。この結果、入力動画像データの各フレームに対して、MPEG エンコーダーが実装上正確に 1 対 1 対応でキャプチャリングすることができず、この段階で既に、入力動画像 1 フレームに対して重複や欠落などの発生が多数生じることがわかった。従来の動画像電子透かし技術では、攻撃者による意図的なフレームの重複や消失などの攻撃などについては検討されているが、キャプチャによる同期ずれについては考慮されていない。しかし、閾値法により秘密を時間方向に分散させる本提案方式は、当初よりこのようなフレーム消失や重複に対して耐性を有するため、本研究のようにビデオ信号のキャプチャリングに重複や欠落の生じる実システムを対象とする場合、従来方式に比べて優れた電子透かし検出能力を有する、実用的な方式であることが明らかになった。

以上のように本研究で開発した実験システムを、通常のインターネット環境で稼働させるために、既存アプリケーションに悪影響を及ぼさないようにストリーミングを共存させるためのストリーミング送信、制御技術の研究開発や、既存アプリケーションによりストリームに生じるパケットロスや遅延などを回避、回復し、良好な品質のライブ放送ストリーミングを実現する技術の研究開発を行った。ストリームと既存トラヒックが共存した場合の、ストリームから既存トラヒックへの影響度(耐性)、および、既存トラヒックからストリームへの影響度(親和性)を、実証システムによる実験により調べた結果、既存アプリケーションの到着頻度と保留時間、および既存アプリケーションの帯域要求性質、から、既存トラヒックを適切に分類し、親和性や耐性を考慮することにより、ストリーミングと既存アプリケーションのインターネット上での共存を実現した。また、本実証システムが将来多数運用される状況を想定した、ストリームメディアの再生品質に着目した、ストリーム送信帯域制御方式の研究を行い、帯域が不足する場合にも再生画質の劣化をおさえつつ各ストリームの帯域を削減する方式や、ストリームを効率的に伝送するためのネットワーク支援機構などを実現した。

誌上発表リスト

[1]　上原哲太郎, 川北良一, 辻義一, 佐藤敬, 山岡克式, 泉裕, 齋藤彰一, 國枝義敏, 結城皖曠, "IP マルチキャストを用いたユーザ認証つきインターネット放送システム", 情報処理学会論文誌, Vol.44 No.3, pp.610-624 (2003.3), 被引用度数：不明

[2]　Kenta Yasukawa, Ken-ichi Baba, Katsunori Yamaoka, "Dynamic Class Assignment for Stream Flows Considering Characteristics of Non-stream Flow Classes", IEICE Tramsactoins on Communications, Vol.E87-B, No.11, pp.3242-3254 (2004.11), 被引用度数：不明

[3]　Kentaro Ogawa, Aki Kobayashi, Katsunori Yamaoka, Yoshinori Sakai, "Distributed QoS Control Based on Fairness of Quality for Video Streaming", IEICE Transactions on Communications, Vol.E87-B, No.12, pp.3766-3773 (2004.12), 被引用度数：不明

他 8 編

申請特許リスト

[1]　佐藤敬, 山岡克式, 上原哲太郎, "動画像電子透かし埋込抽出装置及び方法", 日本, 2005.3.29