M-002

マルチキャスト映像配信におけるスケーラブル映像暗号鍵管理
Management of scalable contents encrypting keys for multicast streaming

佐藤茜[1]　小尾高史[1]　鈴木裕之[2]　谷内田益義[2]　大山永昭[3]
Akane SATO[1] Takashi OBI[1] Hiroyuki SUZUKI[2] Masuyoshi YACHIDA[2] Nagaaki OHYAMA[3]

[1]東京工業大学大学院総合理工学研究科　[2]東京工業大学像情報工学研究施設　[3]東京工業大学フロンティア創造共同研究センター

1．はじめに

現在、IP 通信網を利用した通信ネットワーク利用放送の実現に向けた研究開発が進められている[1]。通信ネットワーク利用放送では、放送局が受信機器にデジタル化された映像データをリアルタイムにマルチキャスト配信することが想定されている。ここで、コンテンツの改変、通信路上での不正傍受を防ぐ必要があるが、マルチキャスト映像配信に適したコンテンツ暗号鍵管理方法は提案されていない。

我々は、現在までに機器登録、放送サービス利用登録を行い、放送サービスを受ける機器に対して利用可能な機能や情報の制御を可能としており[2]、本研究では、安全なマルチキャスト配信を実現するために、これら情報を利用して、スケーラブルコンテンツを暗号化し、配信するための暗号化鍵を安全に配送・管理する方法を提案する。

2．課題

マルチキャストでは、データをグループのマルチキャストアドレスに送信すると、ルータなどがデータを複製し、全メンバー（映像受信機器）に配信する。このため暗号化されたコンテンツを配信する場合、全メンバが同一の復号化鍵を持つ必要がある。IKE や SSL など従来一般的に用いられている共有鍵生成・配送技術は、1 対 1 通信（ユニキャスト）を基本としたプロトコルであり、お互いに乱数や ID などを交換し、それをもとに鍵を生成することから複数の受信機器に対して鍵を配送する場合、それぞれ異なる鍵が生成され、コンテンツ暗号化鍵として使用することができない。また、マルチキャスト配信においては、メンバの新規参加や、離脱が想定され、メンバの変化に対応した鍵配送方法が必要になる。

3. 鍵の種類とコンテンツ配信方法

受信機器は暗号鍵等の管理を行う多機能 IC チップを搭載した放送サービスを受ける機器であり、機器登録時に、機器固有の秘密鍵、放送許可書として用いられる公開鍵証明書が発行され、チップ内に保存されているものとする。コンテンツの配信には、セッション鍵、ワーク鍵、マスター鍵と呼ぶ 3 種類の鍵を使用する。セッション鍵はコンテンツの暗号化鍵で、一定時間おきに更新され、ワーク鍵はセッション鍵の暗号化鍵で、グループ内で共通の鍵とする。マスター鍵はメンバー固有の鍵とする。

コンテンツは、放送局でセッション鍵を用いて暗号化され、各エッジルータまで配信され、エッジルータから受信機器へはワーク鍵で暗号化したセッション鍵と共にマルチキャスト配信される。受信機器はワーク鍵を用いてセッション鍵を復号化し、セッション鍵でコンテンツを復号化する。ここで、エッジルータ以下が同じグループとなるため、新規メンバにマスター鍵、ワーク鍵を配送し、ワーク鍵を管理する機能を有する鍵サーバを、各グループに 1 つずつ設置する。

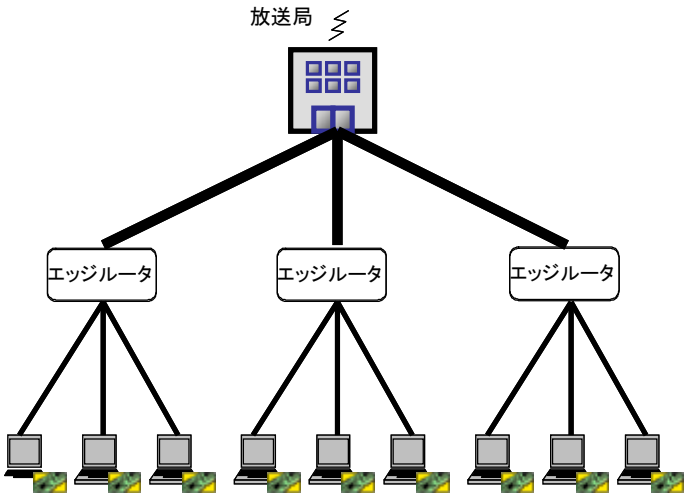


図 1　構成要素

4. マルチキャストメンバー変化への対応

- 参加 (join)

ユニキャスト通信を用い、鍵サーバと受信機器は、相互認証を行う。乱数などを交換し、マスター鍵を生成・共有する。鍵サーバはワーク鍵をマスター鍵で暗号化して配送する。

- 離脱 (leave)

離脱する受信機器が存在する場合、その機器においてその後コンテンツを閲覧できないようにするためグループ内のワーク鍵を一斉に更新する必要がある。本研究では、効率的に鍵更新を行うため、秘密分散共有法[1]を用いて、一斉更新する方法を提案する。提案手法では、各受信機器がマルチキャストグループ参加時に分散情報を得るものとし、新しいワーク鍵を秘密情報とする。ここで、分散情報を更新するための情報、さらに離脱する受信機器で生成される分散情報をマルチキャスト配信することにより、離脱する受信機器以外は分散情報を一定以上集め、ワーク鍵の更新が実現できる。

	機器 i	離脱する機器 j
生成される分散情報	Si	Sj
配信される分散情報	Sj	Sj
集められる分散情報の個数	一定以上	不足

表 1　分散情報

5. スケーラブルコンテンツへの応用

放送データは、複数ビットストリームによりスケーラブル化されてマルチキャスト配信される。そのため、各ストリームに対応したデータ暗号鍵を複数生成する必要があり、受信機器の性能に応じて鍵生成を行う必要がある。このとき、すべてのセッション鍵を異なるワーク鍵で暗号化して送信する方法があるが、ワーク鍵が複数存在するため、その管理・更新が複雑になってしまう。

本研究では、join 時に、受信機器の性能に合ったセッション鍵の種を受信機器に配送し、受信機器で、セッション鍵を生成できるようにした。すべての受信機器が受信する基本レイヤのセッション鍵のみマルチキャストにより配信する。最低画質のコンテンツを閲覧する機器では、配信されたセッション鍵をワーク鍵で復号化することになる。また、高画質のコンテンツを閲覧する機器では、配信されたセッション鍵とセッション鍵の種から、高画質のセッション鍵を生成する。

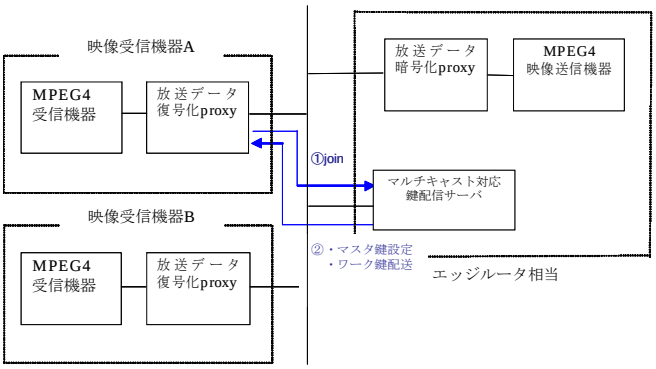
6. 鍵管理プロトタイプシステム

提案手法に基づきプロトタイプシステムを構築し、マルチキャスト配信を利用して放送データ暗号化のための鍵配送を行う実験を行った。プロトタイプシステムでは、映像受信機器の機器登録は終了しているものとし、機器には機能に応じた放送サービス利用秘密鍵及び放送利用許可証（公開鍵証明書）が設定されているものとする。

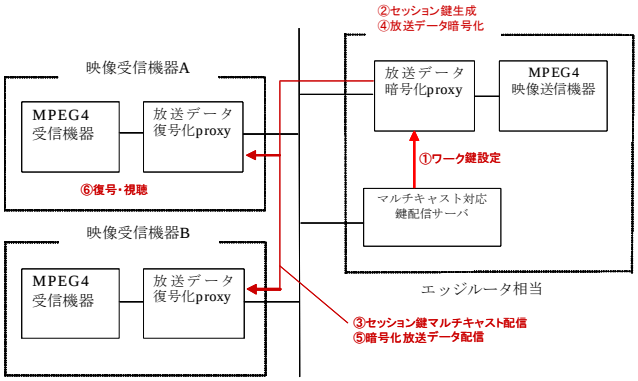
本実験システムはエッジルータ相当機器と映像受信機器により構築されている。エッジルータ相当機器は、マルチキャスト対応鍵配信サーバ、放送データ暗号化 Proxy、MPEG4 映像送信機器の 3 つから構成されている。映像受信機器は、放送データ復号化 Proxy、MPEG4 映像受信機器の 2 つから構成されている。

次に処理手順を示す。

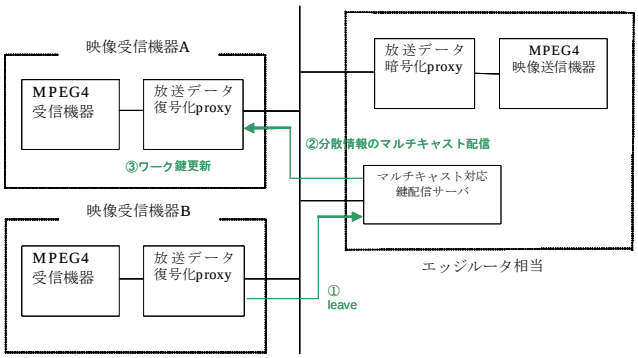
(ア) 映像受信機器のマルチキャストグループへの参加



(イ)放送受信時におけるセッション鍵配送



(ウ) 映像受信機器のマルチキャストグループからの離脱



7. まとめ

マルチキャスト配信に対応した鍵更新方法を実現し、スケーラブルコンテンツを暗号し、配信するための暗号鍵を安全に配送・管理する方法を提案した。プロトタイプシステムを用いて、映像受信機器がマルチキャストグループへの参加、放送受信時におけるセッション鍵のマルチキャスト配信、及び映像受信機器のマルチキャストグループからの脱退時におけるワーク鍵更新などを行い、提案手法が有効であることを確認した。

今後はセキュアチップを利用した実装方法を検討する予定である。

謝辞

本研究は，通信・放送機構の委託研究「通信ネットワーク利用放送技術の研究開発」により行われた。

参考文献

[1]　“通信ネットワーク利用放送技術に関する研究開発平成 15 年度報告書、”情報通信研究機構、平成 16 年 5 月

[2]　小尾、他：“通信ネットワーク利用放送における映像暗号鍵管理方法の提案”、FIT2004　第 3 回情報科学技術フォーラム、M-089

[3]　A. Shamir, “How to share a secret.” Communications of the ACM 22 (1979), pp. 612–613.