社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（37）
2005－CSEC－28（37）
2005／3／23

動画像の構造を考慮したリアルタイムストリーム認証方式の提案

金子 伸一郎 †　上田 真太郎 †　川口 信隆 †　荻野 剛 †　重野 寛 †　岡田 謙一 †

概要:
動画像では差分を用いて圧縮している方式が多いため，フレーム間に依存関係が存在し，フレームごとに重要度が異なる．動画像において重要度の高いフレームがパケットロスにより失われた場合，そのフレームに依存する他のフレームを受信しても再生できない問題が生じる．よって重要度の高いフレームをよりパケットロスに耐性を持たせる必要がある．しかし，既存のストリーム認証方式は動画像におけるフレーム間の依存関係を考慮しておらず全てのフレームを同等のものとして扱っているため効率が悪い．そこで本提案ではフレームを格納するパケットの依存関係を考慮しパケットごとに認証情報の多重度を変えて付与する，動画像の構造を考慮したリアルタイムストリーム認証方式を提案する．

Proposal of Real-time Stream Authentication Scheme for Motion Pictures

Shin-ichiro KANEKO†, Shintaro UEDA†, Nobutaka KAWAGUCHI†, Takeshi OGINO†, Hiroshi SHIGENO†, and Ken-ichi OKADA†

Abstract:
Motion pictures are compressed by removing spatial and temporal redundancies between frames. Therefore there are dependencies between frames and the importance of a frame differs from one another. If a high priority frame is lost due to packet loss, all frames dependent to the lost frame is unplayable even if received on the receiver side. Therefore high priority frames must be made robust to packet loss. However previously proposed authentication schemes do not take the characteristics specific to motion pictures into consideration and thus all frames are handled at the same level. Therefore in our scheme, the amount of redundancy distributed to each frame is adjusted according to the importance of each frame.

1. はじめに

近年ブロードバンドアクセス網の普及に伴って，多くの利用者がネットワークにおける様々なサービスを利用できるようになってきた．その中でも IP 電話やネット会議などのリアルタイムストリーミングサービスが注目されている．しかしこれらのサービスは未だにデータの改ざん，成りすまし，事後否認といった問題を抱えている．よって，今後これらのサービスが重要な場面で用いられることを想定した場合，対策を講じる必要がある．

一般的にリアルタイムストリーミングサービスではリアルタイム性を重視するため再送を行わない UDP が用いられるが，それによりパケットロスが起こりやすくなるという問題を生じてしまう．ストリーム認証を考える際には継続的な認証を行う必要があるという観点から，このパケットロスによる影響を考慮しなければならない．そのため，リアルタイムストリーミングの認証ではパケットロスへの対応のため 1 パケットごと認証する必要がある．しかし，全てのパケットに対し演算負荷の高いディジタル署名を施すのは効率が悪い．

また，動画像は予測差分を用いることでデータを圧縮している．したがって，フレーム間に依存関係が存在し，フレーム毎の重要度が異なる．ここで，重要度の高いフレームがパケットロスにより失われた場合，依存する他のフレームを受信しても動画として再生できない問題が生じる．よって重要度の高いフレームほどパケットロスへの耐性を高める必要がある．しかし，既存のストリーム認証方式は動画像におけるフレーム間の依存関係を考慮しておらず全てのフレームを同等のものとして扱っているため効率が悪い．そこでフレームを格納するパケットの依存関係を考慮し，パケットごとに認証情報の多重度を変えて付与する，動画像の構造を考慮したリアルタイムストリーム認証方式を提案する．本方式は，重要度の高いフレームを格納したパケットが失われたとしても，Information Dispersal Algorithm という技術を用いて復元し，効率的な認証を可能としている．

以下，本稿では，第 2 章において関連研究について述べる．次に，第 3 章において提案方式について解説する．さらに，第 4 章においてシミュレーションによる提案方式の評価について解説し，最後に第 5 章で結論を述べる．

2. 関連研究

本章では，提案方式において使用する IDA，及び既存のストリーム認証方式について解説する．

2.1 Information Dispersal Algorithm

提案方式で使用する Information Dispersal Algorithm (IDA)[1] について解説する．IDA とは誤り訂正技術の 1 つであり，ある 1 つのデータを複数のデータに分散して送

† 慶應義塾大学理工学部
Faculty of Science and Engineering, Keio University

信し，その 1 部分が受信されれば元データを復元することができるという技術である．ここで，IDA を適用するデータ A のサイズを F，分散するデータ数を n，A を復元するために受信する必要のある分散データ数を m とした場合の，送信側の処理の流れを以下に示す．また，その概念図を図 1 に示す．

(1) m と n の関係は $0 < m \leq n$
(2) A を長さ m ごとに分割し，F/m 個の分割データ B を生成
(3) この B を全て使用して演算を行い，n 個の分散データ C を生成
(4) 各 C のサイズは F/m，n 個の C の合計サイズは Fn/m

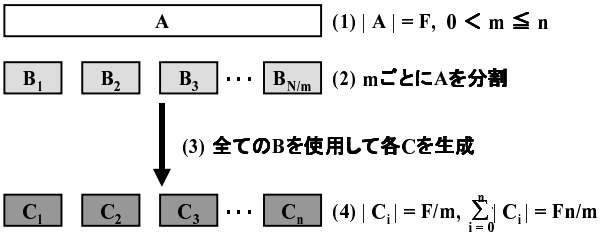

図 1 Information Dispersal Algorithm（IDA）

また，受信側において m 個以上の C が受信されれば，その内の m 個を使用して演算を行うことにより A を復元することができる．よって，m と n の値を変化させることにより，分散データサイズや復元確率などを変化させることが可能となる．

2.2 既存のストリーム認証方式

ストリーミングメディアの認証を効率化する技術がいくつか提案されている．以下では，それらの技術について述べる．

ストリーム認証に関しては，Gennaro らの研究が早くから行われており，Hash Chain 方式[2] が提案されている．この方式は，各パケットが 1 つ後ろのパケットのハッシュ値を持つというハッシュ連鎖の考えを用い，先頭のパケットにのみディジタル署名を施す方式である．この方式では，受信側における即時認証，及び署名演算回数の抑制を実現している．しかし，送信側において全てのパケットが揃わない限り署名演算が行えないため，リアルタイム送信をする際には一定の範囲でパケットを区切って署名を行う必要がある．また，Hash Chain 方式は，パケットロスによってハッシュ連鎖が切れてしまうと，認証が続かなくなってしまうという欠点を持つ．

Wong らは，Merkle のハッシュツリー[3][4] を用いてツリー型のハッシュ連鎖をとり，ルートハッシュにディジタル署名を施す WLtree 方式[5] を提案している．この方式は各パケットにルートハッシュまでの道程の兄弟ノードハッシュとディジタル署名を付与することで，パケットロスに対する高い耐性を持たせ，さらに受信側での即時認証を可能としている．しかし，送信側におけるバッファリングの遅延と，各パケットのオーバヘッドの増加という問題点を持つ．

Park らは，IDA を利用した Signature Amortization using IDA（SAIDA）方式[6] を提案している．この方式はまず，各パケットのハッシュ値を結合したもののハッシュ値をとることでグループハッシュを生成し，グループハッシュに対してのみ署名を施す．この後，グループハッシュと署名に対してそれぞれ IDA の処理を施すことにより，これらのデータに分散する．各パケットには分散後のそれぞれのデータが付与される．この方式は IDA を利用することで，パケットロスに対する耐性を持たせると共に，各パケットのオーバヘッドを抑えている．しかし，送信側，受信側の双方においてバッファリングが大きくなってしまい，遅延が発生する問題点を含んでいる．

これらの方式に共通することは，数パケットを 1 つのグループとし，グループ中のパケットを全て同等のものとして扱っていることである．しかし，本稿では差分演算を用いた動画像のストリームを想定しているため，差分元となるフレームと演算により生成されるフレームとでは，重要度が異なってくる．それに伴い各パケットの重要度も異なり，パケット間に依存関係が存在することになる．したがって，各パケットに付与する認証情報も重みを変えて付与したほうが効率的である．そこで次章において，動画像の構造を考慮した効率的な認証方式を提案する．

3. 提　　案

本章では，提案方式について解説する．本提案ではディジタル署名，ハッシュ，及び IDA を用いることによって，動画像の構造を考慮したストリーム認証を実現している．すなわち，重要度の高いパケットに認証情報を付与し，重要度の低いパケットに重要度の高いパケットの復元情報を分散させて持たせることにより，効率的な認証を可能とする．

3.1 前 提 条 件

本提案における前提条件を以下に示す．

- 動画の方式としては予測差分を用いた方式を想定
- 予測差分方式は順方向予測と双方向予測を想定
- キーフレームをロスすると，それに依存しているサブフレームの動画再生は不可能
- 1 つのフレームを 1 つ以上の UDP パケットに格納

ここで，キーフレームとは差分の元となるフレーム，サブフレームとはキーフレームからの差分により生成されたフレームと定義する．

次に，本提案で想定しているキーフレームとサブフレームの依存関係を図 2 に示す．

図中の K はキーフレーム，F は順方向予測差分によって生成される順方向予測サブフレーム，B は双方向予測差分によって生成される双方向予測サブフレーム，矢印は依存関係を表す．この依存関係により，受信側で動画再生を

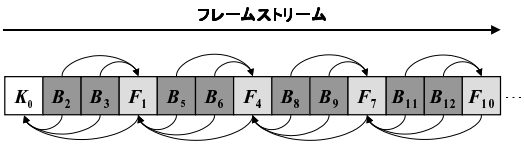

図 2 フレームの依存関係

行う際，K フレームが最も重要度が高く，B フレームが最も低いと設定することが出来る．

また，本提案では，複数のフレームを 1 グループにしたものをフレームグループと定義する．フレームグループの内容を以下に示す．

- 1 つのフレームグループは約 13 フレームを有する
- フレームグループは K フレームで開始する
- 2〜3 フレームごとに F フレームが存在する

ここで，今回扱う各フレームのフレームサイズを，F フレームは K フレームの約 40〜50%，B フレームは K フレームの約 20〜30%と想定している．例として，K フレームが 10 個の UDP パケットに格納される場合を考えると，F フレームは 5 個の UDP パケットに，B フレームは 3 個の UDP パケットに格納されることになる．

最後に，各フレームが送信側で生成される順番と受信側で再生される順番の様子を図 3 に示す．フレームの生成順番と再生順番が異なることがわかる．例えば送信側で K_0 の次に生成された F_1 が受信側では B_2，B_3 の後に再生されている．これは B_2，B_3 が K_0 と F_1 の間の双方向予測によって生成されたサブフレームであるため，再生の順序が入れ替わる．

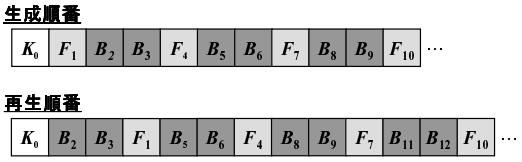

図 3 フレームの生成順番と再生順番の関係

3.2 署 名 方 法

本提案のリアルタイムストリーム認証方式では，重要度の高い K フレームの復元情報を K フレームより重要度の低い F と B フレームに付与する．また，F フレームの復元情報を B フレームに付与する．このように階層的に復元情報を付与することで，K フレームのパケットロスに対する耐性を強固にすると共に，効率的な認証を行うことができる．実際にはフレーム単位ではなくパケット単位での処理を行い，以下にその詳細を記す．

3.2.1 K パケットの署名方法

K フレームのデータが格納されている，K パケットの署名方法について述べる．K，F，B フレームのデータが図 4 で示されるように，それぞれ 10 個，5 個，3 個のパケットに格納される場合を例として解説する．また，これから解説する流れを図 5 に示す．図 5 の矢印が交わる部分はデータの連結を表すものとする．

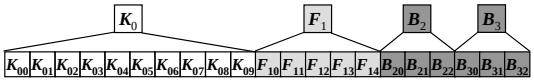

図 4 各フレームとパケット数

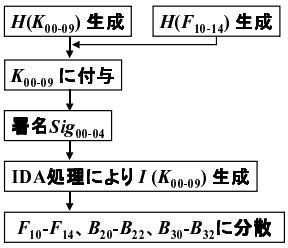

図 5 K パケットの署名方法

まず，K_0 フレームのデータを格納する K_{00},...,K_{09} の各パケットのハッシュ値を連結した値のハッシュ値を $H(K_{00-09})$ とする．

同様に F_1 フレームのデータを格納する F_{10},...,F_{14} の各パケットのハッシュ値を連結した値のハッシュ値 $H(F_{10-14})$ を生成する．ここで，認証においてフレーム間の連鎖を持たせるために $H(F_{10-14})$ を先に生成した $H(K_{00-09})$ と連結し K_{00-09} に付与する．K_{00-09} とは K_{00},...,K_{09} パケットのことを示している．これに対しディジタル署名 Sig_{00-09} を生成し付与する．このディジタル署名を付与したものに対して IDA 処理を行うことによって生成される復元情報 $I(K_{00-09})$ を F_{10},...,F_{14}，B_{20},...,B_{22}，B_{30},...,B_{32} パケットに分散する．ここで，$I(K_{00-09})$ を持つ F_{10},...,F_{14}，B_{20},...,B_{22}，B_{30},...,B_{32} をそれぞれ F'_{10},...,F'_{14}，B'_{20},...,B'_{22}，B'_{30},...,B'_{32} とする．

$I(K_{00-09})$ を分散させる F と B のパケット数を K 多重パケット数と呼び，n_k とする．また，K パケットの一部もしくは全てがパケットロスによって失われた際に復元を行うのに必要な F と B のパケット数を K 復元閾値と呼び，m_k とする．

3.2.2 F パケットの署名方法

F パケットの署名方法について述べる．これから解説する流れを図 7 に示す．また，用いられるフレームとパケット数の関係を図 6 に示す．

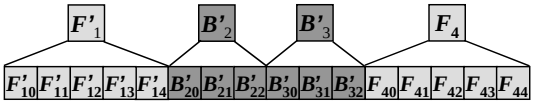

図 6 各フレームとパケット数

まず $H(F'_{10-14})$，$H(B'_{20-22})$，$H(B'_{30-32})$ と次の F フレームの $H(F_{40-44})$ を生成する．これらを連結し F'_{10-14} に付与する．これに対しディジタル署名 Sig_{10-14} を生成し付与する．このディジタル署名を付与したものに対して IDA 処理を行うことによって生成される復元情報 $I(F'_{10-14})$ を B'_{20},...,B'_{22} と B'_{30},...,B'_{32} に分散させる．

ここで，$I(F_{10-14})$ を分散させる B' のパケット数を F 多重パケット数と呼び，n_f とする．また，F フレームを格納する F パケットの一部もしくは全てがパケットロス

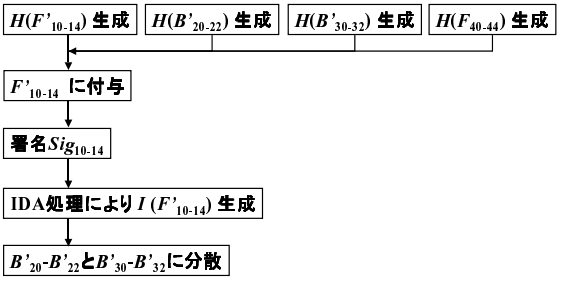

図 7 F パケットの署名方法

によって失われた際に復元を行うのに必要な B' のパケット数を F 復元閾値と呼び，m_f とする．

フレームグループの 2 つ目の F フレーム以降のフレームを格納するパケット，つまり $F_{40},\ldots,F_{44}$ 以降のパケットについても同様の処理を繰り返し行う．これにより，フレームグループ内のフレーム間には連鎖的な認証を行うことが可能となる．

3.3 検 証 方 法

本方式の検証ついて，パケットロスがない場合とある場合の二つに分けて述べる．また例として，K_{00-09} からの検証について述べる．

3.3.1 パケットロスがない場合の検証

本方式では，パケットロスがない場合は受信したパケットと認証情報を用いて，通常のディジタル署名を用いた検証を行う．受信側において K_{00-09} を受信した場合，付与されている認証情報を使用して K_{00-09} の検証を行う．公開鍵暗号の公開鍵 KEY_p を用いて Sig_{00-09} を復号化し，同時に K_{00-09} と付与された $H(F_{10-14})$ を連結したもののハッシュ値を生成し，両者が等しければ K_{00-09} が認証される．それと同時に F_{10-14} も認証される．

3.3.2 パケットロスがある場合の検証

本方式では，パケットロスがある場合は送信側で IDA 処理により生成し分散された復元情報を受信側で用いる必要がある．

ここで，受信側で再生を行う際に最も重要度の高いキーフレームを格納する K パケットが任意の数失われた場合を例に検証方法について述べる．この検証方法を解説する上で，さらにこの例を，K パケットの復元情報を持つ F や B パケットをある閾値以上受信した場合としていない場合に分けて，具体例をあげて説明する．

$K_{00},\ldots,K_{09}$ のパケットが失われた場合，$K_{00},\ldots,K_{09}$ の復元情報である $I(K_{00-09})$ を持つ $F_{10},\ldots,F_{14}$，$B_{20},\ldots,B_{22}$，$B_{30},\ldots,B_{32}$ のうち，受信側で m_k 以上受信できればパケットロスが生じた際にも K_0 の復元が可能である．また，ここで復元されたデータには認証情報も含まれるため，受信側で継続的な署名の検証が可能になる．署名の検証は復元された認証情報を用いて 3.3.1 と同様に行う．

次に m_k 以上受信していない場合，$K_{00},\ldots,K_{09}$ を直接復元することが不可能である．したがって，まず先に $K_{00},\ldots,K_{09}$ の復元情報を持つ $F_{10},\ldots,F_{14}$ を復元する必要がある．F の復元情報 $I(F_{10-14})$ を持つ $B'_{20},\ldots,B'_{22}$ と $B'_{30},\ldots,B'_{32}$ が m_f 個以上受信されていれば，$F_{10},\ldots,F_{14}$ の復元と検証が可能になる．ここで復元されたデータに K の復元情報も含まれているため，最終的には $K_{00},\ldots,K_{09}$ も復元・検証することができる．

この節で示されたように，本方式では重要度の高いキーフレームを格納するパケットの復元情報を，重要度の低いサブフレームを格納するパケットに階層的に分散させることにより，パケットロス時にも重要度の高いパケットの復元確率を高めている．

4. 評　　価

提案方式の有効性を確かめるため，シミュレーションを行った．実際のネットワークではパケットロス率が時間とともに変動するため，評価を取ることが困難である．そこでパケットロスモデルを作成し，それを仮想的なネットワークとみなしたシミュレーションを行った．

4.1 実 装 環 境

本シミュレーションの実装環境について述べる．シミュレーションは CPU が Pentium4 3.2GHz，メインメモリが 2.0Gbyte のマシンを使用した．また，OS は Windows XP を用いた．シミュレーションの開発言語には JDK1.4.2 を使用した．さらに，提案方式はハッシュ関数と公開鍵暗号方式に依存しないものであるが，今回はハッシュ関数に 160bits SHA-1，公開鍵暗号方式に 1024bits RSA を用いた．

4.2 パケットロスモデル

一般的なネットワークにおけるパケットロスは，ランダムロスではなくバーストロスである．そこで，より現実的なシミュレーションを行うために，バーストロスモデルの 1 つである，Marcov Chain Loss Model を使用する．パケットロスを連続した過去のパケットロスに依存していると捉えることで，バーストロスを表現することが可能となる．本シミュレーションにおいては 1 次 Marcov 過程を用いた 2-state Marcov Chain Loss Model（2-MC Loss Model）を使用する．2 つの状態をパケットロスの有無に対応付けている．図 8 にこのモデルの状態遷移図を示す．

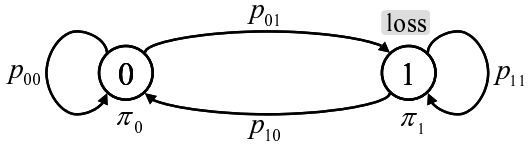

図 8 2-MC Loss Model

図 8 では 2 つの状態を 0 及び 1 で表し，それぞれロスなし及びロスありに対応している．遷移確率は p_{00}，p_{01}，p_{10}，p_{11} という 4 つの確率が存在する．定常確率は π_0，π_1 が存在し，$\pi_1 = 1 - \pi_0$ という関係が成立する．この π_1 がパケットロス率となる．また，期待するバースト長を β と

する．遷移確率は定常確率と β を使用して，以下に示す式で表すことができる．

$$p_{00} = 1 - \frac{1}{\beta}(\frac{1}{\pi_0 - 1}), \quad p_{01} = \frac{\pi_1}{\beta\pi_0}$$
$$p_{10} = \frac{1}{\beta}, \quad p_{11} = 1 - \frac{1}{\beta}$$

4.3 シミュレーションパラメータ

前述したパケットロスモデルを用いたシミュレーションにより，本提案方式と既存方式との比較評価を行った．シミュレーションに入力するパラメータを以下に示す．

- N：総パケット数
- n_k：K 多重パケット数
- m_k：K 復元閾値
- n_f：F 多重パケット数
- m_f：F 復元閾値
- π_1：パケットロス率（%）
- β：期待バースト長
- S_k：K フレームのサイズ ($KBytes$)
- S_f：F フレームのサイズ ($KBytes$)
- S_b：B フレームのサイズ ($Bytes$)

今回は $N \approx 10000$，$n_k = 16$，$m_k = 11, 15$，$n_f = 10$，$m_f = 4, 9$，$\pi_1 = 0, \ldots, 40$，$\beta = 8$，$S_k = 2.5$，$S_f = 1.25$，$S_b = 625$ という値を与えた場合の結果のみを例として示す．

S_k，S_f，S_b の値をそれぞれ 2.5，1.25，625 に設定したのは，今回利用を想定している Windows の NetMeeting で用いられる約 120 × 160 のサイズの画像と同等サイズの MPEG 画像の各フレームサイズがこの程度のサイズを有しているためである．本来は差分演算によりサブフレームサイズが求まるため各フレームのサイズは画像によって異なるが，今回は仮想パケットを用いるため実測した画像の代表的な値を用いた．n_k，n_f は各フレームサイズに対応付けて設定した．m_k，m_f は復元条件に応じて変化するが，復元条件が易しい場合と厳しい場合の 2 通りの代表値としている．

π_1 の最大値が 40 となっているのは，インターネットにおいて，それ以上のパケットロスが起こる場合というのは考えにくいからである．実際のインターネットでは平均して，パケットロスが 20 %程度であるという研究結果[7)8)]もあることから，40 を最大値とした．β の値が 8 となっているのも，インターネットにおいて平均的に起きるバースト長が 8 パケットであるという知見が得られているからである．

4.4 評 価 項 目

評価項目は，認証率と動画再生率という 2 項目にした．認証率と動画再生率は以下に示す式と定義する．

$$\text{認証率} = \frac{\text{受信側認証パケット数}}{\text{送信パケット数}}$$
$$\text{動画再生率} = \frac{\text{受信側動画再生パケット数}}{\text{送信パケット数}}$$

動画再生率とは，実際に認証され，かつ動画再生されたフレームの割合を表している．既存方式においては認証されても動画再生されないフレームというものが存在するので，それと比較して提案方式の優位性を知るための項目である．また，本提案方式と比較する既存方式として，既存方式の中で誤り訂正技術を使用している Park らの SAIDA 方式を用いる．

4.5 パケットロス率と認証率の関係

パケットロス率と認証率の関係を図 9 に示す．図中の凡例の表記は「認証方式名-n_k，m_k，n_f，m_f」となっている．

パケットロス率と認証率の関係は，パケットロス率が高くなると認証率が低くなるという関係にある．パケットロス率が高ければ高いほど受信されるパケット数が少なくなるので，それにつれて認証されるパケット数も少なくなってしまう．そのため，認証率も低下する．しかし，各方式によりその認証率の低下の傾きが異なってくる．

図 9 から提案方式の認証率が SAIDA の認証率とほぼ同等の値をとっていることがわかる．m_k の値を変えることで復元条件が易しい場合と厳しい場合に分けて解説をする．m_k と復元条件の関係は，m_k の値が大きくなると復元条件が厳しくなるという関係にある．

まずは，$m_k = 11$ と復元条件が易しい場合，SAIDA 方式の認証率が提案方式の認証率に比べて若干良い認証率となっていることがわかる．これは SAIDA 方式はグループ内の全てのパケットを同等として扱っているため，全てのパケットに対しての認証情報の復元情報を分散しているのに対して，提案方式ではパケットの重要度に応じて分散させる復元情報の多重度を変えているため，重要度の低いパケットがパケットロスで失われた際，そのパケットの認証情報の復元率は低く，認証率が低くなるためである．

次に，$m_k = 15$ と復元条件が厳しい場合，提案方式の認証率が SAIDA 方式に比べて高い値となっている．これは提案方式が厳しい復元条件において有効性を発揮することを表している．この理由として，パケットロスによって K パケットが失われた場合，SAIDA に比べて提案方式では K パケットの復元を容易にしているためである．これは K パケットは階層的な復元が可能であるためである．

提案方式内の比較として，m_k のみならず m_f の値を変化させた場合の認証率を測定した．ここで，m_f が小さい値のほうが認証率が高いことがわかる．これは，階層的な K パケットの復元を可能にしている本方式の特性を表している．図 9 の m_k を変えた認証率の変化に比べ，m_f を変化させた認証率の変化が大きいことからもわかる．

以上の結果から本提案の認証方式は SAIDA 方式と認証率に関して，パケットロスに対しての耐性が同等であると言える．

4.6 パケットロス率と動画再生率の関係

パケットロス率と動画再生率の関係を図 10 に示す．図中の凡例の表記は先ほどと同様に「認証方式名-n_k，m_k，

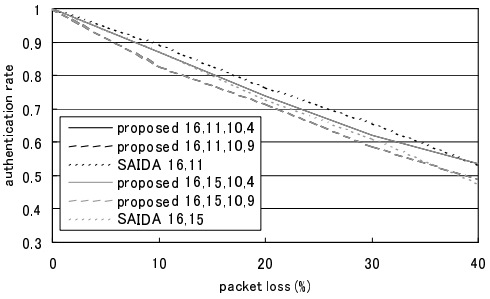

図 9 パケットロス率と認証率の関係

n_f, m_f」となっている．

パケットロス率と動画再生率の関係は，パケットロス率と認証率の関係と同様にパケットロス率が高くなれば，動画再生率も低くなる．この理由はパケットロス率と認証率との関係と同じである．しかし，図 10 からわかるように，提案方式の動画再生率は SAIDA 方式に比べ高い値を保っている．例えば，パケットロス率が 20%の場合，提案方式の動画再生率は約 0.65，SAIDA 方式の動画再生率は約 0.45 である．これは，提案方式が SAIDA 方式に比べて約 50%も向上していることを表している．また，パケットロス率 20% の提案方式の動画再生率がパケットロス率 10%の SAIDA 方式の動画再生率と同等の値となってることがわかる．

提案方式では，再生を行う際に最も重要であるキーフレームの K フレームの復元情報をより多くの重要度の低いフレームに分散させていることで，パケットロスが起きた際にも K フレームの復元を容易にしている．これにより，受信されたサブフレームの F と B フレームが無駄になることが少なくなる．ここで言う無駄になるとは受信されてもキーフレームがないため動画再生できないサブフレームが存在することを示す．提案方式の動画再生率は認証率に比べ若干低下しているが，それに対して SAIDA 方式は動画再生率が認証率に比べ大幅に低下している．SAIDA 方式はグループ内のパケットが m_k 個以上受信されればグループ内の受信されたパケットは全て認証される．したがって，キーフレームをロスしている場合でも，そのグループのサブフレームのみで認証が可能である．そのため，認証されても動画再生されないサブフレームが存在するので，動画再生可能なパケット数が認証可能なパケット数より少なくなり，動画再生率が認証率より低くなる．

5. おわりに

本稿では，動画像の構造を考慮した，リアルタイムストリーム認証方式を提案した．またシミュレーションによる既存方式との比較評価を行い，提案方式の優位性を示した．以上より，本提案方式は，動画像リアルタイムストリーミングの効率的な認証を実現することを可能とし，今後のリアルタイムストリーミングサービスの普及，及び発展に大

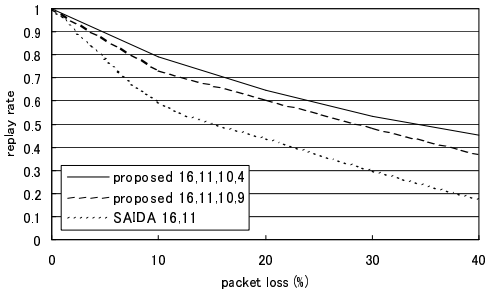

図 10 パケットロス率と動画再生率の関係

きく寄与するものであるという結論が導き出される．

参 考 文 献

1) M.Rabin. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. *Journal of the ACM*, 2:335–348, 1989.
2) R.Gennaro and P.Rohatgi. How to Sign Digital Streams. In *Proceedings of th Conference on Advances in Cryptology*, pages 180–197, 1997.
3) R.Merkle. A Certified Digital Signature. In *Proceedings of th Conference on Advances in Cryptology*, pages 218–238, 1989.
4) R.Merkle. A Digital Signature Based on a Conventional Encryption Function. In *Proceedings of th Conference on Advances in Cryptology*, pages 369–378, 1987.
5) C.Wong and S.Lam. Digital Signatures for Flows and Multicasts. *IEEE/ACM Transactions on Networking*, 7(4):502–513, August 1999.
6) J.Park, E.Chong, and H.Siegel. Efficient Multicast Stream Authentication Using Erasure Codes. *ACM Transactions on Information and System Security*, 6(2):258–285, May 2003.
7) M.Yajnik, J.Kurose, and D.Towsley. Packet Loss Correlation in the Mbone Multicast Network. In *Proceedings of the IEEE Global Internet Conference*, 1996.
8) M.Yajnik, S.Moon, J.Kurose, and D.Towsley. Measurement and Mmodeling of the Temporal Dependence in Packet Loss. In *Proceedings of the IEEE Conference on Computer Communications*, pages 345–352, 1999.