2004－DPS－118　(8)
2004／6／3

誤り訂正を用いた動画ストリーム認証情報分散方式

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

概要:
UDP を用いたリアルタイムストリームの認証では，パケットロスへの対応のために 1 パケットごとに認証する必要がある．また，動画像は差分を用いて圧縮を行っている方式が多いため，フレーム間に依存関係が存在し，フレーム毎に重要度が異なる．しかし，既存の認証技術ではこの動画像の構造を考慮していない．さらに，ロスした重要フレームを復元する機能も持っていない．そこで本稿では，誤り訂正技術の 1 つである IDA を利用することでフレームの重要度を考慮し，動画像に特化させたリアルタイムストリーム認証方式を提案し，これらの問題を解決する．また，本方式の有効性を示すために，シミュレーションによる評価を行う．

Authentication Information Distributed Scheme using Forward Error Correction for Moving Pictures

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

Abstract:
In real-time stream authentication over UDP, there is a need to authenticate each packet to correspond to packet loss. Furthermore, since moving pictures are usually compressed using the differences between frames, there are dependency relationship between frames thus the level of importance of frames differs. However, existing authentication schemes do not take these characteristics into consideration. In addition, they do not have restoration capabilities of important frames. In this paper, we propose a real-time stream authentication method specialized for moving pictures, that uses a FEC technique called IDA, to take the characteristics of moving pictures into consideration. We show the performance effectiveness of our method using the simulation results.

1. はじめに

近年，DSL や FTTH といったブロードバンド網の発展によりネットワークへの常時接続環境が整備され，回線速度も増加の一途を辿っている．このような状況に伴い，多くの一般ユーザ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，ネット会議システムやライブ配信といったリアルタイムストリームサービスが注目されている．しかし，このようなサービスはインターネットに代表される公開ネットワークにおいて利用されることが大半のため，データの改竄，成りすまし，事後否認などを問題として抱えている．これらの問題に対し，ディジタル署名を使用した認証技術を適用することによって，発信元の真正性やデータ改竄の有無を確認することが可能となるため，問題の解決に繋がる．

また，リアルタイムストリームサービスでは，リアルタイム性を重視するために UDP で通信されることが多く，パケットロスに対する耐性がない．そのため，リアルタイムストリームの認証では，パケットロスへの対応のために１パケットごとに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大きいディジタル署名を施すことは非効率である．また，MPEG に代表されるような動画像は予測差分を用いることでデータ量を圧縮している．予測元となるフレームをキーフレーム，予測差分演算により算出された画像をサブフレームと呼称する場合，キーフレームとサブフレームの間には依存関係がある．よって，通信の際にキーフレームをロスしてしまうとサブフレームは受信側で再生することができなくなり，フレーム毎に重要度が異なると考えられる．そこで本稿では，このフレームの重要度を考慮した動画ストリーム認証情報分散方式を提案する．本提案では，誤り訂正技術の 1 つである IDA を重要度の高いフレームに対して適用することにより，そのフレームをロスした場合でも復元することが可能である．

以下，本稿では，第 2 章で現在提案されているストリーム認証技術について述べ，第 3 章で提案方式について解説する．さらに，第 4 章では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 5 章で結論と今後の課題を述べる．

2. 関連研究

効率的なストリーム認証方式として，様々な方式が提案されている．

Gennaro らの Hash Chain 方式[1] では，各パケットが 1 つ後のパケットのハッシュを持ち，ブロックの先頭パケットのみに署名を施す．よって，この方式では，ブロック内の全てのパケットが揃わない限り送信側で署名演算が行う

† 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University

ことができない．また，一般にリアルタイムストリーム転送では，UDP を使って送信される．よって，この方式はパケットロスによって署名が連続しない部分が生じると認証が途切れてしまうため，パケットロスに対する耐性がないという欠点がある．しかし，この方式は欠点こそあるが，様々なストリーム認証方式の基礎となる方式である．

Wong らの WLtree 方式[2] では，各パケットのハッシュから tree 構造[3] を生成することで，複数のパケットを 1 度の署名認証演算で処理することができる．この方式は効率よく署名を行うことができ，パケットロスに対し高い耐性を持つ．

Park らによる SAIDA 方式[4] では，各パケットのハッシュを結合し，それに対して署名を行う．さらにハッシュの結合及び署名に対して，誤り訂正技術の 1 つである IDA[5] を利用して，これらのデータを分散する．この分散データを各パケットに持たせることで，パケットロスが起きても分散データの 1 部分が受信側で受信できれば，元のハッシュの結合及び署名を復元させることができるため，認証を行うことが可能となる．

これらの方式は効率的な認証が可能ではあるが，各パケットを同等のものとして扱っている．動画像においては，各パケットを同等のものとして扱うことは，各フレームを同等に扱うことと同義である．しかし，フレーム間には依存関係が存在しフレーム毎に重要度が異なるため，パケットに付加する認証情報の重みを変えた方がより効率的である．そこで，これらの方式の問題点を解決するための方式を第 3 章で提案する．

3. 提　　案

本章では，フレームの重要度を考慮した動画ストリーム認証情報分散方式を提案する．誤り訂正技術の 1 つである IDA を利用し，重要度の高いパケットのデータを他のパケットに分散させて持たせる．また，異なる 3 つの付加方式を示す．

3.1 IDA

本方式の中で使用している IDA とは，ある 1 つのデータを複数のデータに分散して送信し，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 IDA 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

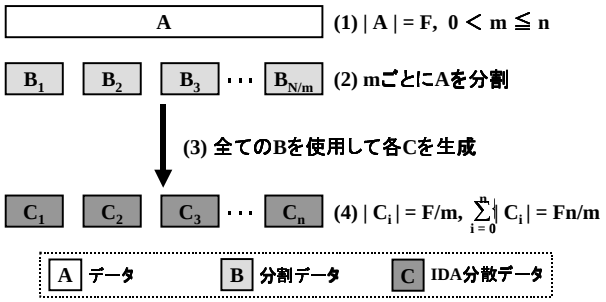


図 1　IDA

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率などを変化させることが可能となる．

3.2 前提条件と基本構成

本提案ではいくつかの前提条件が存在する．

- 動画の方式としては MPEG などの予測差分を用いた方式を想定
- 予測方式は順方向予測のみ想定
- 1 つのフレームを 1 つの UDP パケットに格納
- 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映像再生は不可能

ここで，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．

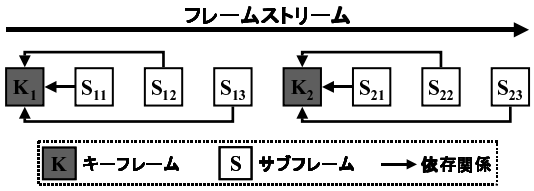


図 2　フレームの依存関係

この依存関係により，サブフレームに比べキーフレームの重要度が高くなるので，認証情報はキーフレームに付加すると効率的であると考えられる．ここで，本提案の基本パケット構成を図 3 に示す．

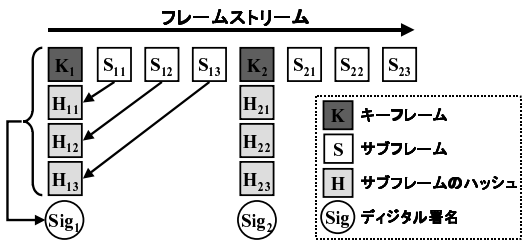


図 3　基本パケット構成

キーフレーム K にはサブフレーム S のハッシュH とディジタル署名 Sig が付加されている．図中の K_i は i 番目のキーフレームである．K_i と依存関係のある j 番目のサブフレームが S_{ij} であり，それらのハッシュが H_{ij} である．またここで，公開鍵暗号の秘密鍵を KEY_s，$DATA$ のハッシュを $Hash(DATA)$，$DATA$ を秘密鍵 KEY で暗号化したものを $Enc(KEY, DATA)$ で表すものとすると，Sig_i は以下の式で定義される．

$$Sig_i = Enc(KEY_s, Hash(K_i \parallel H_{i1} \parallel H_{i2} \parallel \cdots)$$

よってキーフレームが受信されれば，そのキーフレームと依存関係のあるサブフレームを認証することができる．また，キーフレームをロスすると依存関係のあるサブフレームを再生することができないので，認証する必要がない．しかし，キーフレームのロスは極力抑えるべきであると考えられる．そこで，キーフレームに IDA を使用して他のパケットに分散データを付加することで，キーフレームの復元を可能とする．この分散方式を 3 つ提案する．

3.3 順方向分散方式

順方向分散方式を図 4 に示す．図中の I は IDA 分散データを表している．この方式はキーフレームの分散データを，依存関係のあるサブフレームに付加する方式である．あるキーフレームの分散データを持つサブフレームをある閾値以上受信した場合，キーフレームをロスしていても復元することが可能であるので，サブフレームを認証することができる．

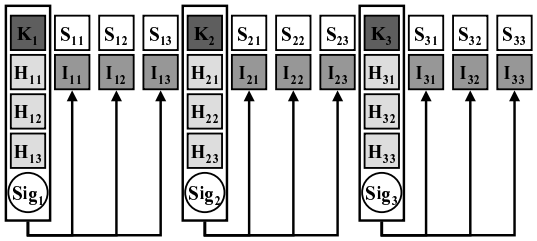


図 4 順方向分散方式

例えば，図 4 においてキーフレームを復元するための閾値が 2 である場合を考える．もし，K_1 をロスしたとしても S_{11}〜S_{13} の中で 2 つ以上受信されれば K_1 を復元することが可能となる．よって，受信されたサブフレームを認証することができ，再生することができる．

3.4 双方向分散方式

双方向分散方式を図 5 に示す．この方式はキーフレームの分散データを依存関係のあるサブフレーム，及び 1 つ前のキーフレームに依存しているサブフレームに付加する方式である．各サブフレームは前後のキーフレームの分散データを持つためオーバヘッドが大きくなってしまう．しかし，分散する領域が広がるため閾値を緩和することができ，キーフレームのロスに対する耐性を高めることができる．

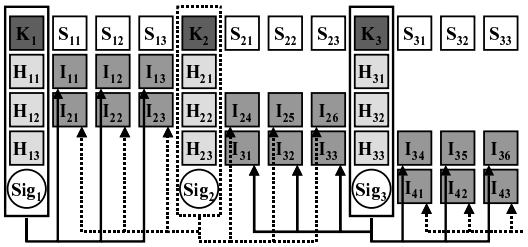


図 5 双方向分散方式

3.5 双方向隔キー分散方式

双方向隔キー分散方式を図 6 に示す．この方式は 1 つおきのキーフレームに対して IDA を使用する．そして，各キーフレームの分散データを依存関係のあるサブフレーム，1 つ前のキーフレーム，及び 1 つ前のキーフレームに依存するサブフレームに付加する方式である．

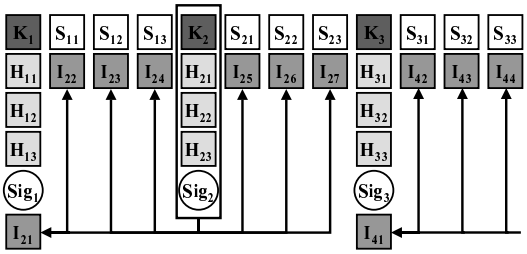


図 6 双方向隔キー分散方式

例えば，図 6 においては偶数番目のキーフレームのみに IDA を使用している．よって奇数番目のキーフレームをロスした場合，そのキーフレームを復元することはできない．ただし偶数番目のキーフレームに関しては，分散領域を広くとることができ，オーバヘッドを抑えることができる．また，動画像は連続してキーフレームをロスしなければ大きな画質の劣化が起きないので，1 つおきにキーフレームのロスに対する耐性を高めるこの方式は，極端な画質の劣化を防ぐことに特化した方式であると言える．

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．

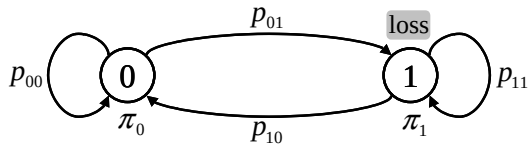
4.1 実 装 環 境

本シミュレーションの実装環境は以下の通りである．

- CPU：Pentium4 3.0GHz
- メインメモリ：2.0Gbyte
- OS：Windows XP
- 開発言語：JDK1.4.2
- ハッシュ関数：128bits MD5
- 公開鍵暗号方式：512bits RSA

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[6] を使用する．ある 1 つのパケットがロスする確率は，過去のパケットがロスしたか否かに依存し，過去のパケットがロスしていれば連続してそのパケットもロスする確率が高くなると考えることで，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，最も単純な場合である 1 次 Marcov 過程を使用する．1 次 Marcov 過程を使用することで，1 つ前のパケットをロスしていないか，ロスしているかという 2 つの状態で表すことができる．このように 2 つの状態で表せることから，特にこのモデルを 2-state Marcov Chain Loss Model（2-MC Loss Model）と呼ぶ．図 7 にこのモデルの状態遷移図を示す．



定常確率 ： π_0，π_1

遷移確率 ： p_{00}，p_{01}，p_{10}，p_{11}

図 7 2-MC Loss Model

図 7 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．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 1〜4 で表すことができる．

$$p_{00} = 1 - \frac{1}{\beta}\left(\frac{1}{\pi_0 - 1}\right) \tag{1}$$

$$p_{01} = \frac{\pi_1}{\beta\pi_0} \tag{2}$$

$$p_{10} = \frac{1}{\beta} \tag{3}$$

$$p_{11} = 1 - \frac{1}{\beta} \tag{4}$$

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，既存方式と本提案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：1 グループ中のサブフレームの数
- m：復元閾値
- N：総フレーム数
- π_1：パケットロス率
- β：期待バースト長

まず，n というのは，各グループにおけるサブフレームの数である．m は送信側において分散されたキーフレームの分散データのうち，受信側においてキーフレームを復元するために必要なデータ数を示している．N はシミュレーションを 1 度行った際の，送信した全フレーム数を表している．

π_1 は前述した 2-MC Loss Model の π_1 を百分率表示にしたものであり，パケットロス率とみなすことができる．β も 2-MC Loss Model の β と同様のものであり，平均的に起きるバースト長を表している．この π_1 と β をロスモデルに与えることにより，各遷移確率を求めることができる．

今回は $n = 5$，$m = 2, \ldots, 2n + 1$，$N \approx 10000$，$\pi_1 = 10, 20, \ldots, 50$，$\beta = 8$ という値を与えた場合の結果のみを例として示す．π_1 の値を上記のようにした理由は，実際のインターネットの平均パケットロス率が 20 %程度であるという研究結果があるからである．また，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 であるという検知が得られているためである[7)6)]．

さらに，シミュレーションの際のキーフレームのサイズは 80〜100byte でランダムに与えた．しかしこの値自体には特に意味を持たせていない．今回は認証方式の有効性を確かめることが主眼であり，パケットのサイズにそれほど意味はないからである．分散データによるオーバヘッドはパケットのサイズに対してほぼ相対的に大きくなることからも，パケットサイズ自体に意味はあまりないことがわかる．

4.4 評 価 項 目

評価項目は，パケットロス率と認証率の関係，オーバヘッドと認証率の関係という 2 項目で行った．認証率は認証パケット数を送信パケット数で割ったものとして定義している．今までの認証の研究において認証率とは，認証パケット数を受信パケット数で割ったものとして定義されてきた．しかし今回はその定義を変えている．この理由は，本稿における提案方式ではロスしたパケットを復元できるため，受信パケット数が実際に受信されたパケット数よりも大きくなるからである．したがって，パケット復元機能を持たない既存方式と比較する際に，分母の値が異なってしまうため，同一の軸で比較を行うことが不可能となる．そこで分母の値として，送信パケット数を使用することで，既存方式と比較することを可能としている．また，オーバヘッドは認証情報と分散データの合計をパケット数で割り，1 パケットあたりの平均オーバヘッドとして算出した．

本方式と比較する既存方式としては，Gennaro の Hash Chain 方式，Park の SAIDA 方式，及び認証情報を付加済みの同じキーフレームを 2 連続で送信する方式の 3 つである．3 つ目の方式は認証方式と呼べるものではないが，今回は仮に再送方式と呼称することにする．また，Hash Chain 方式と SAIDA 方式においても，キーフレームから

次のキーフレームまでを１つのグループと考えて方式を適用するものとする．

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 8，及び図 9 に示す．

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いほど受信されるパケット数が少なくなるので，認証されるパケット数も少なくなる．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．

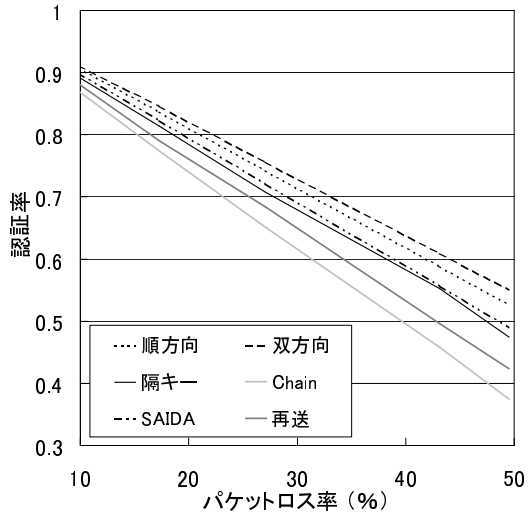


図 8 パケットロス率と認証率の関係 ($m = 2, n = 5$)

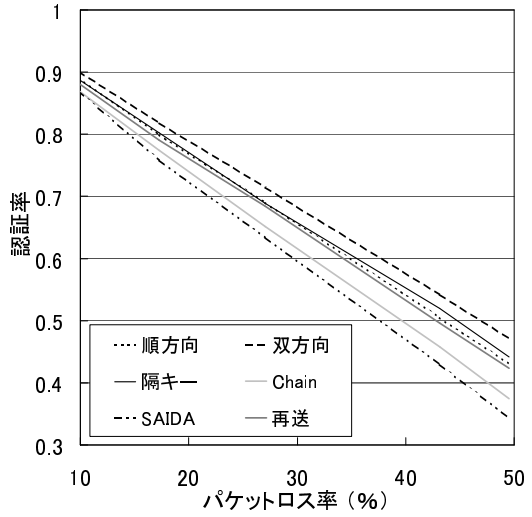


図 9 パケットロス率と認証率の関係 ($m = 5, n = 5$)

$m = 2$ の場合を見ると，双方向分散方式の認証率が最も高くなっている．双方向分散方式は優れたキーフレーム復元能力を有しているので，キーフレームロスに対する耐性が高い．キーフレームが復元できれば受信した同一グループのサブフレームも認証できるので，認証率が最も高くなっている．双方向分散方式に次いで高い認証率を示しているのが，順方向分散方式である．この方式は双方向分散方式ほどのキーフレーム復元能力を持たないが，m の値が小さければ十分な復元能力を有している．双方向隔キー分散方式の認証率は既存の SAIDA 方式と同等の性能であった．提案の 3 方式は m の値が小さいときは比較的容易にキーフレームを復元できるため，1 つおきでしか復元できない双方向隔キー分散方式は他の 2 方式に比べて性能が落ちてしまうと考えられる．

Hash Chain 方式と再送方式は m の値に依存しない．再送方式の場合は 2 つ送信されたキーフレームのうち 1 つでも受信できれば，同一グループのサブフレームを認証することが可能である．しかし，Hash Chain 方式はグループ中のフレームを一つでもロスしてしまうとそこでハッシュの連鎖が途切れてしまい，それ以降受信した同一グループのフレームを認証することができなくなってしまう．そのため，この 2 つを比較した場合，再送方式の認証率が高くなっている．それでも，$m = 2$ における 3 つの提案方式より認証率は低くなる．

$m = 5$ の場合においても，双方向分散方式は最も良い性能を示している．また，順方向分散方式と双方向隔キー分散方式の認証率はほぼ同じ値を示している．この場合，順方向分散方式はキーフレームをロスすると，同一グループ中の全てのサブフレームを受信しなければならない．それに対し双方向隔キー分散方式は IDA を施したキーフレームをロスしたとしても，分散領域が広いため比較的容易に復元可能であるが，IDA を施していないキーフレームは復元することができない．これら 2 つの事象の認証率に及ぼす影響がほぼ等しくなったため，両方式の認証率が近い値を示したのだと考えられる．SAIDA 方式は m の値が大きくなると性能が極端に悪化している．SAIDA 方式は各グループにおいて m 個以上のパケットを受信しなければ，グループ内の全てのパケットを認証することができなくなるので，認証率がそれに伴い低下したのだと考えられる．

以上の結果より，提案した 3 方式はある程度の m の値の増加においては，既存方式より高い認証率を保つことができるため，パケットロスに対する耐性が高くなる．

4.6 オーバヘッドと認証率の関係

オーバヘッドと認証率の関係を図 10 に示す．図中の上のクラスタが $\pi_1 = 20$ の場合，下のクラスタが $\pi_1 = 40$ の場合を示している．

オーバヘッドと認証率の関係は，オーバヘッドが大きくなると，認証率が高くなるという関係にある．オーバヘッドが大きいほど各パケットに付加される分散データが大きくなる，すなわち m の値が小さくなるので，ロスしたキーフレームを復元できる可能性が高くなり，認証率が高くなる．

π_1 の値に関わらず双方向分散方式の認証率の最大値が，

全方式の認証率の最大値を取っている．しかし，その際のオーバヘッドは非常に大きくなる．これは，双方向分散方式の各サブフレームには前後のキーフレームの分散データが付加されているためである．順方向分散方式は比較的オーバヘッドを抑えたまま，既存方式に比べ高い認証率を保っている．双方向隔キー分散方式も順方向分散方式には劣るが，オーバヘッドを抑えつつ認証率を高くすることが可能となる．順方向分散方式と双方向隔キー分散方式は，各サブフレームに 1 つの分散データしか付加していないので，オーバヘッドを抑えられている．SAIDA 方式はオーバヘッドが大きいときは良い性能を示しているが，オーバヘッドを小さくすると急激に性能が悪化する．オーバヘッドを小さくするということは，m の値を大きくすることと同義であるので，パケットロス率と認証率の関係の節で述べた通り，認証率が低くなってしまう．双方向分散方式と双方向隔キー分散方式はオーバヘッドに対する認証率の変化が小さいという点で，SAIDA 方式より優れていると言える．

Hash Chain 方式と再送方式は m の値の変化に関係のない方式であるので，当然オーバヘッドも変化しない．これらの方式はオーバヘッドを小さくすることができるが認証率の面では提案方式に劣る．

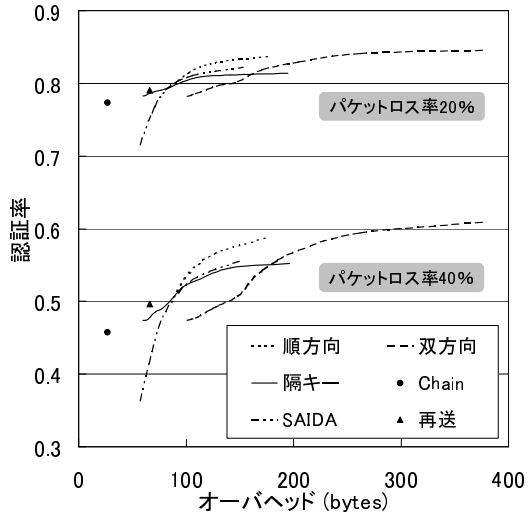


図 10 オーバヘッドと認証率の関係 ($n = 5$)

また，π_1 の値が大きくなるほど提案方式と既存方式の認証率の差が大きくなる．このことからも，提案した 3 方式のパケットロスに対する高い耐性を読み取ることができる．また，提案した 3 方式の認証率の幅も大きくなる．これは，π_1 の値が小さい時はロスするキーフレーム数が少なく，相対的に復元される可能性を持つキーフレーム数も少なくなるが，π_1 の値が大きくなると逆に復元される可能性を持つキーフレーム数が多くなるからであると考えられる．

以上の結果より，提案方式においてオーバヘッドと認証率はトレードオフであり，各方式を適用すべき状況が異なるということである．特に双方向分散方式においては，認証率は高くなるがオーバヘッドが大きくなるため，ネットワークの回線が太い場合にのみ適用可能であると言える．また，オーバヘッドは大きくなるものの既存方式より高い認証率を保つことが可能である．

5. おわりに

本稿では，誤り訂正技術の 1 種である IDA を用いることで，フレームにより重要度が異なるという動画像の構造を考慮した，ストリーム認証情報分散方式を提案した．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．

今後の課題としては以下のものが挙げられる．

- 1 つのピクチャが複数の UDP パケットにまたがる場合の対処
- 動画像の差分方式が双方向予測差分である場合の対処
- 音声認証との融合

これらの課題を解決することで初めて，現実のストリーミングサービスに本提案を適用することが可能となる．したがって早急に解決しなければならないと考えている．

参 考 文 献

1) R.Gennaro and P.Rohatgi. How to Sign Digital Streams. In *Proceedings of th Conference on Advances in Cryptology*, pages 180–197, 1997.
2) C.Wong and S.Lam. Digital Signatures for Flows and Multicasts. *IEEE/ACM Transactions on Networking*, 7(4):502–513, August 1999.
3) R.Merkle. A Certified Digital Signature. In *Proceedings of th Conference on Advances in Cryptology*, pages 218–238, 1989.
4) 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.
5) M.Rabin. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. *Journal of the ACM*, 2:335–348, 1989.
6) 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.
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.