2F-5

FECと暗号化を融合させた高速アルゴリズムの開発

稲生　智久　佐藤　雅史　平岡　冠二　新谷　義弘
沖電気工業株式会社

はじめに

ブロードバンドネットワークが発展し、映像によるサービスが出現してきている。ＩＰ放送やＶＯＤ（ビデオオンデマンド）などである。

映像サービスを実現させるためには、様々な技術が必要となるが、その中でも、映像データを暗号化する情報秘匿が不可欠と考えられている。また、ネットワーク中でのパケットロスなどの品質を補うために FEC(Forward-Error-Correction)が注目をあびている。

2つの技術とも転送する全てのデータを元にデータを変換や計算を行って処理されるものであるが、現状は、独自に実現されている。これらの２つの処理を実行することは、配信側、受像機側とも負荷となっており、処理負荷の低減が望まれている。

これら FEC と暗号化を融合させることで負荷を下げるアルゴリズムを開発したので成果を発表する。

１．概要

映像サービスとして、衛星などで放送されている番組をそのままＩＰ上に再配信を行うＩＰ放送を例にして述べる。

ＩＰ放送の１例のしくみを述べると、配信側は、番組を放送している衛星の電波を受信しチューナで一度アナログ映像にした後、ＭＰＥＧ２に再エンコードし、その後、暗号化を行い、そしてＦＥＣによる冗長データを付加して、データをパケットに分割してマルチキャストで配信する。一方受信側は、マルチキャストアドレスからパケットを受信し、欠損がある場合ＦＥＣの冗長データで欠損データの復元を行った後、暗号を復号化し、ＭＰＥＧ２データをデコードし、映像をＴＶに出力する。

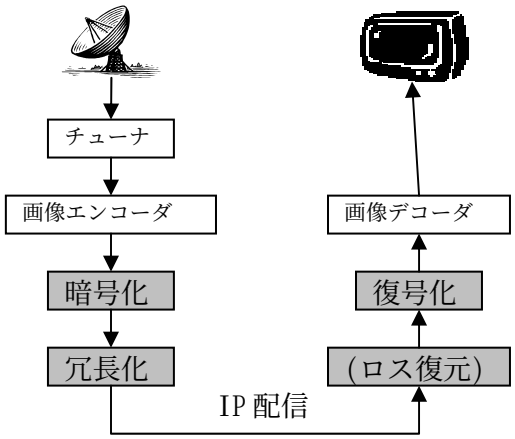

図１：ＩＰ放送概要

本論文では、暗号化処理とＦＥＣによる冗長化処理に注目をする。暗号化処理は、ネットワーク中の不正な行為を防止するため、許可された受信端末でしか映像を見えなくするものである。本例はマルチキャストでデータを配信しており、アドレスが判明していれば、ネットワーク中のどの場所からでもデータの取得ができることになる。暗号処理により不正取得を行っても、解読しないと実際の映像データを取り出せないようにするものである。一方、冗長化はＦＥＣ技術を利用し、あらかじめ冗長データを送付し、データ欠損が生じても端末側で、再度データを転送しなくても復元ができるしくみである。ＦＥＣの冗長方式には２種類あり、元データをそのままにして冗長データのみを付加する組織符号化方式と、元データを冗長データ付のまったく別のデータに変換する非組織符号方式とがある。非組織符号は全データの復元が必要になるため処理は組織符号に比較して多くなるが、冗長部分を含めた全体のデータ量の削減が期待できる。

暗号化と冗長化の２つの処理は、いずれも全データを対象に演算を行うが、別個に処理をしているため、効率が悪い処理となっている。今回２つの処理を融合し処理の高速化と負荷の低減を試みた。

The high efficient complex algorithm of cipher and FEC
Tomohisa Inao, Masashi Sato,
Kanji Hiraoka, Yoshihiro Shintani,
Oki Electric Industry Co., Ltd.

２．新融合方式

アルゴリズムは、以下の２方式を検討し、FECと暗号化を別々に実施した場合と比較して評価を行うものとした。評価は、処理負荷の低減と安全の低下について行う。

(1) 非組織符号ＦＥＣを流用した方式

非組織符号方式のＦＥＣは、もともと、データを別体系に変更するため暗号化と似た処理を行っているといえる。従って、復元するための管理データを暗号化してしまえば、パケットがどの位置のデータなのか不明となり、データを復元するのは困難となる。パケットの順番を入れ替えれば、より効果的である。

受信側では、ＦＥＣヘッダの暗号を解読した後、欠損したパケットの復元を行い、元データを取得する。

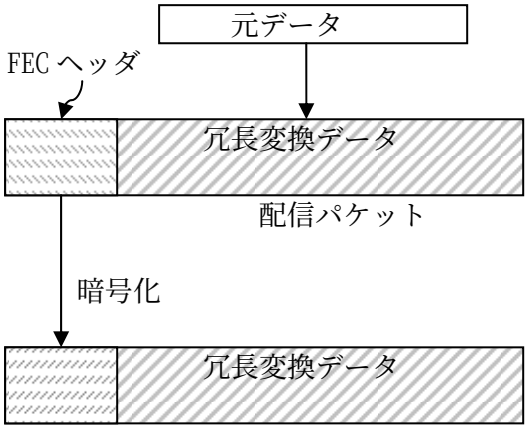

図２：非組織符号ＦＥＣを利用した方式

本方式は暗号化の処理量がかなり削減されるため処理速度が大幅にアップする。ただし、暗号部分が少ないことで解読が全体を暗号化するのに比べて容易になる。

(2) 並列処理方式

もう１つの方式は、全てのデータに対して処理を行う暗号処理と冗長処理を同時に行う方式である。冗長処理は、組織符号ＦＥＣを使用し、元データに対して行う。この場合冗長データは暗号化せずに送ることになるが、冗長データのみでは元データは復元できないため、安全性は保たれる。

受信側では、暗号を解読した後、欠損したパケットの復元を行い、元データを取得する。

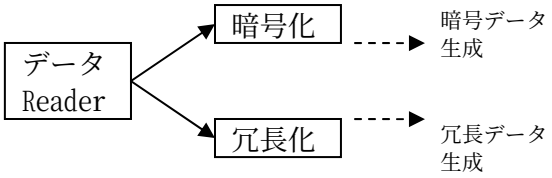

図３：並行処理方式

本処理は、データ処理部の読込みを１回にすること、および欠損時の復元パケットを暗号解読後のデータにすることで処理を削減している。

３．評価

以下の方式に対して、評価を行った。

(0) 暗号化＋組織符号冗長化

現行の方式である、暗号化を行い、その後冗長化を行う方式

(1) 非組織符号ＦＥＣを流用した方式

非組織符号ＦＥＣを行った後、ヘッダ部分にのみ暗号化を行う方式

(2) 並列処理方式

暗号化と冗長化を同時に行う方式

評価結果は以下のとおりである。

表１：評価結果

方式	高速性	安全性
暗号化＋組織符号冗長化	×	○
非組織符号ＦＥＣを流用した方式	○	×
並列処理方式	△	△

４．おわりに

ＦＥＣと暗号化の融合を図った新しいアルゴリズムの提案をした。本研究は、情報通信研究機構の委託研究開発にて行ったものである。

参考文献

[1]平岡ら、”OKI MediaServer V5 におけるIPv6 の取り組み～ IPv4/IPv6 デュアルスタックビデオサーバ～”, 沖テクニカルレビュー, 197号 Vol.71 No.1 (2004. 1)
[2]佐藤ら、” MPEGストリーミングのためのブロック暗号処理方式”, 電子情報通信学会, FIT2002, M-94