数理解析研究所講究録
1093 巻 1999 年 182-187

ハイパーキューブ上の安全な情報伝達

中村 雅子 (Noriko Nakamura), 酒井 秀晃 (Hideaki Sakai),
西谷 泰昭 (Yasuaki Nishitani), 五十嵐 善英 (Yoshihide Igarashi)

群馬大学工学部情報工学科
〒 376-8515 桐生市天神町 1-5-1
tel: 0277 30 1829
email: igarashi@comp.cs.gunma-u.ac.jp

本論文では，n 次元ハイパーキューブにおいて，メッセージが完全に安全である確率，すなわち盗聴者にメッセージについての情報が全く洩れない確率がある定数 β $(0 < \beta < 1)$ 以上であるという条件を満たす通信量の少ない情報伝達法を提案する。我々の提案する方法は，大きく分けて，送信者から受信者への内素なパスを用いる方法と，リレーによる方法である。そのそれぞれにおいて，メッセージをピースに分割する方法として，しきい値法を用いる方法と情報伝播アルゴリズム (Information Dispersal Algorithm, IDA) を拡張した方法を用いる方法を提案する。計算機実験の結果，送信者から受信者への内素なパスによって情報伝達を行なう場合，しきい値法を用いる場合の通信量に比べて，拡張 IDA を用いる場合の通信量が少なくなるのは，β が大きく，かつ n がある範囲である場合に限られていることがわかった。しかし，リレーによって情報伝達を行なう場合，n が大きいときには常にしきい値法を用いる場合の通信量に比べて，拡張 IDA を用いる場合の通信量が少ないことがわかった。また，n が大きいときには，すべての方法の中でも拡張 IDA を用いてリレーによって情報伝達を行なう場合の通信量が一番少ないことがわかった。

1 はじめに

安全でないネットワーク上での送信者から受信者への安全な情報伝達について考える。これまで，安全な情報伝達のための方法はいくつも提案されている [1, 3]。本稿では，ハイパーキューブ上で情報伝達を行なった時の安全性と通信量を考察する。我々が考える情報伝達では，メッセージをピースに分割して，それぞれのピースをハイパーキューブ上のパスを使って伝達する。メッセージを分割する方法としては，しきい値法と IDA を拡張した方法を用いる。

2節において，準備として IDA を拡張した方法について説明する。次に，3節において，ハイパーキューブ上においての安全な情報伝達について考える。ここで，各辺において，ピースが盗聴されない確率を定数 α $(0 < \alpha < 1)$ であるとする。このモデルにおいて安全性について議論するために，β- 安全という概念を定義する。ある情報伝達法が β- 安全であるというのは，盗聴者が送信されたメッセージについての情報を得ることができない確率が β $(0 < \beta < 1)$ 以上であるということを意味する。β が 1 に近いほど安全であるということを意味する。我々の目標は，ハイパーキューブ上で β- 安全であり，かつ通信量の少ない情報伝達法を提案することである。

2 IDA の拡張

最初に Information Dispersal Algorithm (IDA) について簡単に説明する。m, n を $m < n$ である正整数とする。IDA は集合 S の要素であるメッセージ (大きさは $\log|S|$) を n 個のピースに分割し，そのピースを伝達し，これらのピースのうち任意の m 個のピースを獲得できれば，元のメッセージを復元できるという方法である。このとき各ピースの大きさは $\frac{1}{m}\log|S|$ である。

次に IDA の安全性について述べる。伝達された n 個のうち m 個のピースを獲得することでメッセージを復元できるということは，$n-m$ 個のピースを紛失してもかまわないということであり，この意味で IDA は安全であるといえる。しかし，獲得したピースの個数が m より小さい場合にも可能なメッセージの個数をしぼることができるという意味で IDA の安全性は高いとは言えない。つまり，盗聴者の獲得したピースの個数が r $(r < m)$ であれば，メッセージを完全に復元することはできないが，その候補は $|S|^{\frac{m-r}{m}}$ 個となり，ピースを全く獲得しないときの候補数 $|S|$ より減ずることができる。このように，メッセージ解読の可能性が増加するために IDA の安全性は低いと考えられる。そこで，解読の可能性を減らすために解読に必要とされるピースの個数を増やす方法が考えられる。具体的には，S の要素であるメッセージに対して，S を拡張した集合 S' の要素を複数対応付ける。ここで，$|S'| = |S|^{\frac{m+k}{m}}$ である。この対応付けされた S' の要素から 1 個をランダムに選び，それを通常の IDA によって n 個のピースに分割して伝達する。

このような拡張 IDA について次のような性質をもつ情報伝達法が示されている [7]。

$$H(S|r) = \begin{cases} \log|S| & \text{if } r \le k \\ \left(1 - \frac{r-k}{m}\right)\log|S| & \text{if } k \le r \le m+k \\ 0 & \text{if } m+k \le r \end{cases}$$

ここで，r は盗聴者が獲得したピースの個数，$H(S|r)$ は盗聴者がピースを r 個獲得した場合にメッセージを特定するために必要な情報量 (エントロピー) を示す。この結果より $r \leq k$ の場合には $H(S|r) = \log|S|$ であるので，k 個のピースを盗聴されても盗聴者はメッセージに関して何も情報を得ることになる。また，$k \leq r \leq m+k$ の場合には，メッセージが復元されてしまうわけではないが，盗聴者に $\frac{r-k}{m}\log|S|$ だけ情報が洩れていることがわかる。

また送信者から受信者への長さ 1 の n 本のパスを用いた場合の通信量は，ピース 1 個あたりの大きさが $\frac{1}{m}\log|S|$ であることから $\frac{n}{m}\log|S|$ となる。一方，しきい値法を用いた場合の通信量は $n\log|S|$ であるため，IDA を拡張した方法の通信量はしきい値法を用いた場合の $\frac{1}{m}$ になっている。

上で示した方法を用いて，我々は，ピース n 個中 k 個からは元のメッセージに関して何も情報を得ることができず，w 個からは完全にメッセージを復元できるようなピースにメッセージを分割することができる。以後，この方法を (k,w,n)-IDA と呼ぶことにする。

3 ハイパーキューブにおける安全な情報伝達と通信量

n 次元ハイパーキューブは連結度が n であるため，任意の頂点から別の任意の頂点の間には，内素な n 本のパスが存在する。したがって，しきい値法 や 2節において説明した IDA を拡張した方法を用いてメッセージを n 個に分割して，それぞれを内素なパスを用いて送信するという方法が考えられる。ここでしきい値法とは，一般には (k,n)- しきい値法と呼ばれる，もとの情報を任意の k 個から復元できるように n 個のピースに分割するものである。このとき，各ピースの大きさはもとのメッセージと同じである。

長さ n のパスが n 本存在するようなネットワークがあるとき，k 個のピースが盗聴されても，盗聴者が，送信されたメッセージに関する情報を得ることができないように，かつなるべく情報量を少なくするという問題を考える。このとき，しきい値法を用いる場合には，$(k+1,k+1)$- しきい値法を用いればよい。また，IDA を拡張した方法を用いる場合には $(k,m+k,m+k)$-IDA を用いればよい。2 つの場合の通信量を比べると，しきい値法を用いた場合には，ひとつのピースの大きさは $\log|S|$ であるので通信量は $(k+1)n\log|S|$ であり，IDA を拡張した方法を用いた場合には，ひとつのピースの大きさは $\frac{1}{m}|S|$ であるので通信量は $\frac{k+m}{m}n|S|$ である。$1 \leq m \leq n-k$ であるので，IDA を拡張した方法の場合の通信量は $m=1$ の場合にはしきい値法を用いた場合と等しく，m が大きくなるにしたがってしきい値法を用いた場合よりも少なくなっていく。したがって，この場合にはしきい値法を用いるよりも IDA を拡張した方法を用いた方が明らかに優れていることがわかる。

しかし k 個のピースが盗聴されたとしても，送信されたメッセージに関する情報を，盗聴者が何も得ることができないようにするという要求があるとは考えにくい。むしろ，盗聴者がメッセージについての情報を得ることができない確率をある定数 β $(0<\beta<1)$ 以上にしたい，という要求の方が自然である。

そこで我々は，ハイパーキューブ上で，しきい値法と IDA を拡張した方法を用いて，盗聴者がメッセージについての情報を得ることができない確率がある定数 β $(0<\beta<1)$ 以上であって，かつ通信量の少ない情報伝達法を提案する。

3.1 モデル

我々が考えるモデルは n- 次元ハイパーキューブ n-HC である。送信者はノード $00\ldots0$ であり，受信者はノード $11\ldots1$ であるとする。各辺において盗聴されない確率を α $(0<\alpha<1)$ とする。このようなハイパーキューブを以後 n-HC(α) と呼ぶ。

送るメッセージの集合を S と表す。したがって，メッセージの大きさは $\log|S|$ である。盗聴者はピースがどのような方法で作成されたものか知っていて，各辺で盗聴に成功したピースを集めてメッセージに関する情報を得ようと務めるものとする。

情報伝達法の安全性を議論する為に次の定義をする。

定義 1 ある情報伝達法を用いてメッセージを送信した時，盗聴者にメッセージについての情報が全く洩れない確率が定数 β $(0<\beta<1)$ 以上であるならば，その情報伝達法は β- 安全 (β-*secure*) であるという。

各方法の評価に用いる通信量は，(情報伝達に用いた辺の数) × (ピースの大きさ) で求める。

また，この節で確率を計算する時に，次の Chernoff bound の式を用いる。

Chernoff Bound X を成功確率が p であるベルヌーイ試行を N 回行なったときの成功回数であるとする。$0<\epsilon<1$ である任意の定数 ϵ に対して，成功回数が ϵpN 回以下である確率 $Prob\{X \leq \epsilon pN\}$ は次の不等式を満たす。

$$Prob\{X \leq \epsilon pN\} \leq e^{-(1-\epsilon)^2 pN/2} \tag{1}$$

3.2 送信者から受信者への内素なパスを用いる方法

n-HC には送信者から受信者へ n 本の内素なパスが存在し，それぞれのパスの長さは n である。それぞれのパスを用いて，ピースをひとつずつ送信した場合を考える。

各パスは n 個の辺からなっているので，各パスの盗聴されない確率は α^n である。表記を簡単にする為，$\gamma = \alpha^n$ とおく。

しきい値法を用いた場合について次の定理を得る。証明は省略する。

定理 1 $\beta \leq 1-(1-\gamma)^n$ ならば，n-HC(α) において，

$$\lceil \frac{\ln(1-\beta)}{\ln(1-\gamma)} \rceil \leq t$$

である t に対して，(t,t)- しきい値法を用いた情報伝達は β- 安全である。但し，$\gamma = \alpha^n$。

通信量については，定理 1より，次の定理が得られる。

定理 2 n-HC(α) における，定理 1で構成された (t,t)- しきい値法を用いた情報伝達の通信量を $C_{TS}(t)$ とすると，

$$C_{TS}(t) = tn \log |S|$$

である。$C_{TS}(t)$ は $t = \lceil \frac{\ln(1-\beta)}{\ln(1-\gamma)} \rceil$ のとき最小であり，その値は

$$\lceil \frac{\ln(1-\beta)}{\ln(1-\gamma)} \rceil n \log |S|$$

である。但し，$\gamma = \alpha^n$。

(k,w,w)-IDA を用いた場合の情報伝達について次の定理を得る。

定理 3 n-HC(α) において，$\beta < 1-e^{-\frac{1}{2}\gamma n}$ であれば，

$$w \geq \lfloor \frac{-2\ln(1-\beta)}{\gamma} \rfloor + 1$$

$$k+1 = \lceil w(1-\gamma) + \sqrt{-2\gamma w \ln(1-\beta)} \rceil$$

である w と k に対して (k,w,w)-*IDA* は β- 安全な情報伝達法である。但し，$\gamma = \alpha^n$。

(証明) $\beta < 1-e^{-\frac{1}{2}\gamma n}$ より，$\frac{-2\ln(1-\beta)}{\gamma} < n$ であるので $\lfloor \frac{-2\ln(1-\beta)}{\gamma} \rfloor + 1 \leq n$ が成り立つ。したがって，条件を満たす w が存在する。また，$1 \leq k+1 < w$ であるから，このような w,k に対して (k,w,w)-IDA が存在する。次に β- 安全であることを示す。$P(X)$ を w 個のピースのうち X 個のピースの盗聴に失敗する確率とする。盗聴者がメッセージについての情報を得るためには $k+1$ 個以上のピースを盗聴しなければならない。すなわち，盗聴に失敗するピースの個数が $w-(k+1)$ 以下でなければならない。したがって，$1-P(X \leq w-(k+1)) \geq \beta$ であれば β- 安全であることがわかる。ここで $\epsilon = 1-\sqrt{\frac{-2\ln(1-\beta)}{\gamma w}}$ とおくと，

$$\begin{aligned} \epsilon\gamma w &= \gamma w - \sqrt{-2\gamma w \ln(1-\beta)} \\ &= w - \{w(1-\gamma) + \sqrt{-2\gamma w \ln(1-\beta)}\} \\ &\geq w-(k+1) \end{aligned}$$

である。また，$\frac{-2\ln(1-\beta)}{\gamma} < w$ より $0 < \epsilon < 1$ である。したがって Chernoff Bound の式を用いることができ，

$$\begin{aligned} P(X \leq w-(k+1)) &\leq P(X \leq \epsilon\gamma w) \\ &\leq \exp\{-\frac{(1-\epsilon)^2\gamma w}{2}\} \\ &= \exp(\ln(1-\beta)) \\ &= 1-\beta \end{aligned}$$

を得る。よって $1-P(X \leq w-(k+1)) \geq \beta$ であるから，β- 安全である。 □

通信量については，定理 3より次の定理を得る。

定理 4 定理3で構成される (k,w,w)-*IDA* の通信量を $C_{IDA}(w)$ とすると，次の式が成り立つ。

$$\frac{1}{\gamma(1-\delta)+\frac{1}{w}}n\log|S| \leq C_{IDA}(w) < \frac{1}{\gamma(1-\delta)}n\log|S|$$

但し，$\delta=\sqrt{\frac{-2\ln(1-\beta)}{\gamma w}}$，$\gamma=\alpha^n$。

3.3 リレーによる方法

リレーによる方法は，図1にあるように，送信者から受信者へメッセージを送信する途中で，メッセージの復元と分割を何度も行なうものである。

送信者から受信者へのひとつのパスを考え (図1では 00000, 00001, 00011, 00111, 01111, 11111)，そのパスに含まれるノードをリレーノードと呼ぶことにする。任意のリレーノードから隣接するリレーノードへは，図1のように，長さ 3 の $n-1$ 本の内素なパスが存在する。

あるリレーノードから隣接するリレーノードへは，内素なパスを用いる方法と同様の方法を用いてメッセージを送信する。

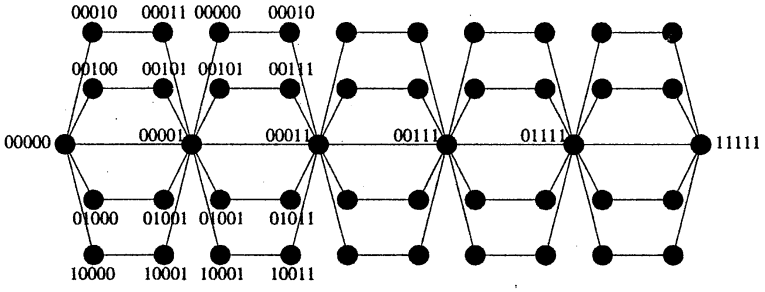

図 1: Relaying in 5-dimensional hypercube 5-HC.

各リレーにおける各パスは 3 個の辺からなっているので，各パスの盗聴されない確率は α^3 である。表記を簡単にする為，$\gamma'=\alpha^3$ および $\beta'=\beta^{\frac{1}{n}}$ とおくと，内素なパスを用いる方法と同様の結果を得ることができる。証明は省略する。

定理 5 $\beta' \leq 1-(1-\gamma')^{n-1}$ ならば，n-HC(α) において，

$$\lceil\frac{\ln(1-\beta')}{\ln(1-\gamma')}\rceil \leq t$$

である t に対して，(t,t)- しきい値法を用いた情報伝達は β- 安全である。但し，$\gamma'=\alpha^3$，$\beta'=\beta^{\frac{1}{n}}$。

定理 6 n-HC(α) における，定理5で構成された (t,t)- しきい値法を用いた情報伝達の通信量を $C'_{TS}(t)$ とすると，

$$C'_{TS}(t)=3tn\log|S|$$

である。$C'_{TS}(t)$ は $t=\lceil\frac{\ln(1-\beta')}{\ln(1-\gamma')}\rceil$ のとき最小であり，その値は

$$3\lceil\frac{\ln(1-\beta')}{\ln(1-\gamma')}\rceil n\log|S|$$

である。但し，$\gamma'=\alpha^3$，$\beta'=\beta^{\frac{1}{n}}$。

定理 7 n-HC(α) において，$\beta' < 1-e^{-\frac{1}{2}\gamma'(n-1)}$ であれば，

$$w \geq \lfloor\frac{-2\ln(1-\beta')}{\gamma'}\rfloor+1$$

$$k+1=\lceil w(1-\gamma')+\sqrt{-2\gamma' w\ln(1-\beta')}\rceil$$

である w と k に対して (k,w,w)-*IDA* は β- 安全な情報伝達法である。但し，$\gamma'=\alpha^3$，$\beta'=\beta^{\frac{1}{n}}$。

定理 8 定理7で構成される (k,w,w)-*IDA* の通信量を $C'_{IDA}(w)$ とすると，次の式が成り立つ。

$$\frac{3}{\gamma'(1-\delta')+\frac{1}{w}}n\log|s| \leq C'_{IDA}(w) < \frac{3}{\gamma'(1-\delta')}n\log|s|$$

但し，$\delta' = \sqrt{\frac{-2\ln(1-\beta')}{\gamma' w}}$，$\beta' = \beta^{\frac{1}{n}}$。

3.4 比較

$\alpha = 0.99$，$\beta = 0.9$ としたときの，n と通信量 $(C_{TS}, C_{IDA}, C'_{TS}, C'_{IDA})$ の関係を図2，3に示す。図中，内素なパス(しきい値法)とあるのが C_{TS} を表し，内素なパス((k,w,w)-IDA)とあるのが C_{IDA} を表し，リレー(しきい値法)とあるのが C'_{TS} を表し，リレー((k,w,w)-IDA)とあるのが C'_{IDA} を表す。図2は n が 200 まで，図3は n が 1000 まで計算したものである。

まず，C_{TS} と C_{IDA} を比較する。図2では，n が 40 以上のとき，C_{TS} よりも C_{IDA} の方が小さくなっている。しかし，図3では，n が 350 以上のとき，C_{IDA} よりも C_{TS} の方が小さくなっている。

いくつかの α, β に対して計算した結果，β が大きくて，かつ n がある範囲にある場合には C_{TS} よりも C_{IDA} の方が小さいが，全体的に見ると C_{TS} (しきい値法を用いた情報伝達の通信量) の方が小さいことがわかった。

次に，C'_{TS} と C'_{IDA} を比較する。図2では，n が 60 以上のとき，C'_{TS} よりも C'_{IDA} の方が小さくなっている。また，図3では，C'_{TS}, C'_{IDA} ともにあまり増減しない。

いくつかの α, β に対して計算した結果，常に，n がある値よりも大きくなると，C'_{TS} よりも C'_{IDA} ((k,w,w)-IDA を用いた情報伝達の通信量) の方が小さいことがわかった。

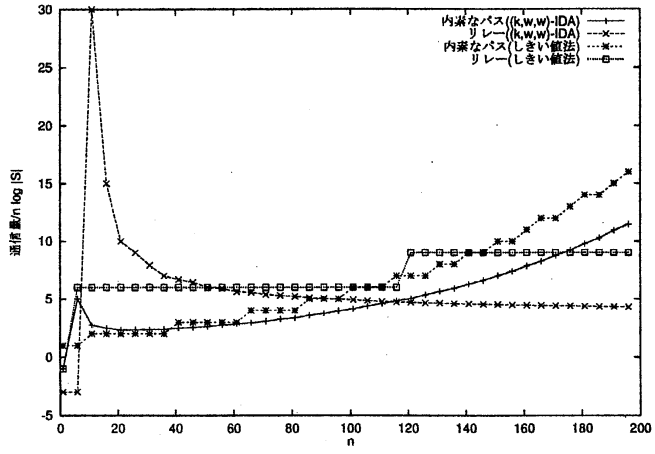

図 2: n と通信量の関係 $(1 \leq n \leq 200)$

4 まとめ

我々は β-安全という概念を定義し，ハイパーキューブ上で β-安全である情報伝達を提案した。その各情報伝達法に対して，n と通信量 $(C_{TS}, C_{IDA}, C'_{TS}, C'_{IDA})$ の関係を調べ，それぞれの方法の通信量が少なくなる条件を実験により調べた。その結果，送信者から受信者への内素なパスによって情報伝達を行なう場合，しきい値法を用いる場合の通信量に比べて，(k,w,w)-IDA を用いる場合の通信量が少なくなるのは，β が大きく，かつ n がある範囲である場合に限られている。しかし，リレーによって情報伝達を行なう場合，n が大きいときにはしきい値法を用いる場合の通信量に比べて，(k,w,w)-IDA を用いる場合の常に通信量が少ないこと。また，n が大きいときには，すべての方法の中で (k,w,w)-IDA を用いてリレーによって情報伝達を行なう場合に通信量が少ないことがわかった。しきい値法を用いる場合の通信量に比べて，(k,w,w)-IDA を用いる場合の通信量が少なくなる一般的な条件を導くのは今後の課題である。

また，我々の解析は，すべてのパスの長さが等しい状況を考えたため，すべてのパスの盗聴確率が等しい場合であった。用いるパスの盗聴確率が等しくない場合の解析は今後の課題である。

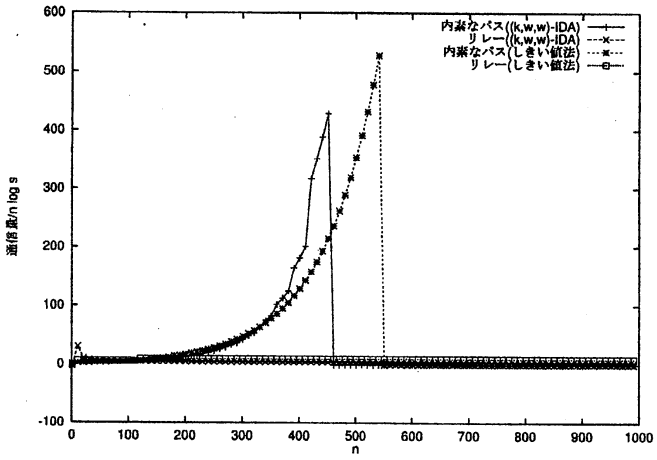

図 3: n と通信量の関係 $(1 \leq n \leq 1000)$

参考文献

[1] F. Bao, Y. Funyu, Y. Hamada, and Y. Igarashi, "Reliable broadcasting and secure distribution in channel networks", *IEICE Trans. on Fundamentals.*, vol. E81-A, pp. 796–806, 1998.

[2] M. Carpentieri, A. De Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold schemes", *Eurocrypt'93, Lecture Notes in Computer Science*, vol. 765, Springer-Verlag, Berlin, pp. 118-125, 1994.

[3] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission", *J. of ACM*, vol. 40, pp. 17–47, 1993.

[4] M. O. Rabin, "Efficient dispersal of information for security, load balance, and fault tolerance", *J. of ACM*, vol. 36, pp. 335–348, 1989.

[5] A. Shamir, "How to share a secret", *CACM*, vol. 22, pp. 612–613, 1979.

[6] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, Florida, 1995.

[7] H. Sakai, N. Nakamura, Y. Nishitani and Y. Igarashi, "Secure Message Transmissions by the Information Dispersal Algorithm", 電子情報通信学会技術研究報告, COMP98-47, pp. 73–80, 1998 年 10 月.

[8] F. Bao, *Reliable and Secure Message Transmissions in Distributed Systems*, Ph.D. Thesis, Gunma University, 1996.