Optimal Information-Dispersal for Increasing the Reliability of a Distributed Service

Hung-Min Sun
Chaoyang Univ. of Technology, Taichung

Shiuh-Pyng Shieh, *Member IEEE*
National Chiao Tung University, Hsinchu

Key Words — Fault tolerance, Security, Threshold scheme, Distributed server, Data storage.

Summary & Conclusions — This paper investigates the (m, n) information dispersal scheme (IDS) used to support fault-tolerant distributed servers in a distributed system. In an (m, n)-IDS, a file M is broken into n pieces such that any m pieces collected suffice for reconstructing M. The reliability of an (m, n)-IDS is primarily determined by 3 important factors:

- n = information dispersal degree (IDD),
- n/m = information expansion ratio (IER),
- P_s = success-probability of acquiring a correct piece.

It is difficult to determine the optimal IDS with the highest reliability from very many choices. Our analysis shows:

- several novel features of (m, n)-IDS which can help reduce the complexity of finding the optimal IDS with the highest reliability;
- that an IDS with a higher IER might not have a higher reliability, even when $P_s \to 1$.

Based on the theorems given herein, we have developed a method that reduces the complexity for computing the highest reliability from,

- $O(v)$ [v = number of servers] to $O(1)$ when the 'upper bound of the IER' = 1, or
- $O(v^2)$ to $O(1)$ when the 'upper bound of the IER' > 1.

1. INTRODUCTION

Acronyms[1]

ID	information dispersal
IDD	ID degree
IDS	ID scheme
IER	information expansion ratio

Notation

n	the IDD
m	[see (m, n)-IDS]
n/m	the IER; $n/m \geq 1$
(m, n)-IDS	an IDS which breaks a file into n pieces such that any m pieces collected suffice for reconstructing the file; $1 \leq m \leq n$
v	number of available servers
u	upper bound of IER
P_s	Pr{a server can provide the correct information piece}; $0 < P_s < 1$
$P_d(m, n)$	binfc$(m; P_s, n)$: Pr{the file can be correctly constructed using the (m, n)-IDS}
$P_s^*\left((i,j),(k,l)\right)$	critical probability: the P_s such that $P_d(i,j) = P_d(k,l)$
P_s^*	$P_s^*\left((i,j),(k,l)\right)$
S_i	piece #i of (m, n)-IDS, $1 \leq i \leq n$
$F_{u,v}$	$\{(m, n)$-IDS; for all $m, n, u \in N$, $1 \leq (n/m) \leq u$, $n \leq v\}$: feasible IDS set.

Other, standard notation is given in "Information for Readers & Authors" at the rear of each issue.

Many desirable services (*eg*, file service, authentication service) in a distributed system should be both highly fault-tolerant and secure [13, 16]. Therefore, it is desirable to increase the reliability & security of a service by distributing the responsibility of providing the service among many servers. There are many ways to increase the fault tolerance of a service in a distributed system. A common approach is to replicate the service so that any one of them can perform the service. However, this approach considerably increases the storage cost for maintaining the replication of files, as well as reduces the level of security (if one server is compromised, security is compromised). Another approach is to use (m, n)-IDS [1, 16] wherein a file M is broken into n pieces, $S_i, 1 \leq i \leq n$, such that any m pieces collected do suffice for reconstructing M. These n pieces can be stored on n different servers (or systems) to improve total reliability. The (m, n)-IDS is able to tolerate up to $n - m$ server failures. With the (m, n)-IDS, not only the reliability & security can be increased, but also the work load can be shared & balanced among servers. Many applications using the (m, n)-ID algorithm were proposed [3, 5 - 7, 12 - 15]. With a limited number of servers and storage resources, it is important to determine the m, n that give the optimal fault-tolerant capability.

This paper:

- analyzes the influence of IDD, IER, and P_s,

[1] The singular & plural of an acronym are always spelled the same.

0018-9529/97/$10.00 ©1997 IEEE

- proposes a method to determine the optimal (m, n)-IDS with the highest reliability, when given the number of servers and an upper bound on IER.

The method reduces the complexity of determining the highest reliability from:

- $O(v)$ to $O(1)$: if the 'upper bound of IER' = 1;
- $O(v^2)$ to $O(1)$, otherwise.

Assumptions

1. The (m, n)-IDS is used to tolerate the server failures in a distributed system. These n pieces of information are stored on n different servers to improve total reliability.
2. All servers have the same success probability. ◀

2. INFORMATION DISPERSAL SCHEME

The concept of an (m, n)-IDS is similar to the concept of an (m, n) threshold scheme [2, 4, 17] in cryptography, in which a master key K is transformed into n shares, such that unless m shares are collected, the K cannot be reclaimed. The main difference between an IDS and a threshold scheme is that the latter provides security while the former provides reliability.

An example is an (m, n)-IDS based on Shamir's threshold scheme [17], as follows. A file is regarded as a binary string which can be divided into m blocks of equal size, where each block is represented as a number: $M = (a_0, \ldots, a_{m-1})$. Select a prime p such that,

$0 \leq a_i \leq p - 1$, for $i = 0, \ldots, m - 1$. Let,

$$f(x) \equiv \left[\sum_{i=0}^{m-1} a_i \cdot x^i\right] \bmod p$$

be a polynomial of degree $m - 1$ over the finite field GF(p). The n pieces are computed from $f(x)$ by:

$[S_i = f(i)] \bmod p, \; i = 1, \ldots, n.$

Given any m pieces S_{i_j}, for $j = 1, \ldots, m$, and $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$, then $f(x)$ can be reconstructed from the Lagrange interpolating polynomial [9]:

$$f(x) = \sum_{k=1}^{m} \left[S_{i_k} \cdot \prod_{j=1, j \neq k}^{m} \frac{x - i_j}{i_k - i_j}\right] \bmod p.$$

Thus, the file M can be obtained. ◀

3. FUNDAMENTAL THEOREMS

This section discusses the influence of n, m, P_s on the total reliability. Section 3.1 studies the reliability of two classes of IDS to demonstrate the difficulty of selecting an optimal (m, n)-IDS. Each class consists of IDS with the same IER but different IDD. For example, the (1,2)-IDS and the (2,4)-IDS are in the same class with the IER=2. Section 3.2 discusses the reliability of IDS with various IER.

3.1 IDS Reliability

Conventional network services use a (1,1)-IDS:

$P_d(1, 1) = P_s$.

Similarly, the reliabilities of the class (m, m)-IDS which have the same IER=1 can be obtained as follows:

$P_d(i, i) = P_s^i, i = 2, \ldots, m$. Thus:

$$P_d(m, m) - P_d(n, n) = P_s^m - P_s^n$$
$$= P_s^m \cdot (1 - P_s^{n-m}) > 0 \text{ if } m < n.$$

The reliability of an (m, m)-IDS for a fixed P_s decreases as m increases. Figure 1 has reliability curves for a (1,1)-IDS, (2,2)-IDS, and (3,3)-IDS, and shows that the total reliability cannot be improved as the degree of ID increases under 'IER=1'.

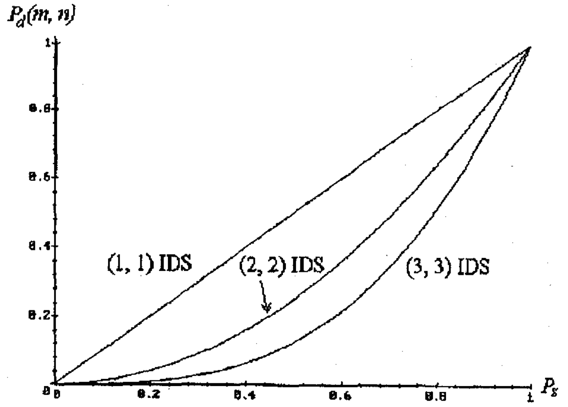


Figure 1. Reliability Curves for (1,1)-IDS, (2,2)-IDS, (3,3)-IDS

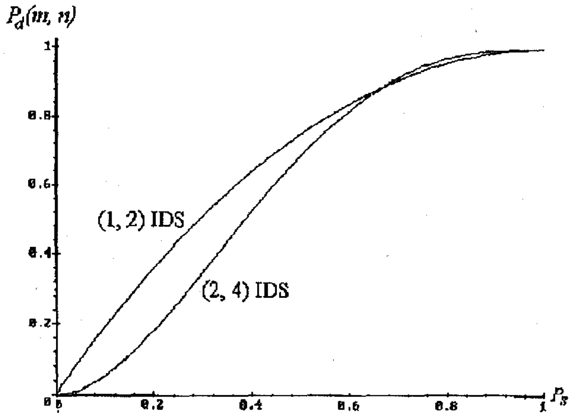


Figure 2. Reliability Curves for (1,2)-IDS, (2,4)-IDS

The class of $(m, 2m)$-IDS has IER=2. The reliabilities of a (1,2)-IDS and (2,4)-IDS can be formulated as follows; figure 2 shows their relationship:

$P_d(1,2) = \text{binfc}(1; P_s, 2)$; $P_d(2,4) = \text{binfc}(2; P_s, 4)$.

$$\begin{aligned} P_d(1,2) &< P_d(2,4), \text{ if } P_s > 2/3 \\ P_d(1,2) &= P_d(2,4), \text{ if } P_s = 2/3 \\ P_d(1,2) &> P_d(2,4), \text{ if } P_s < 2/3 \end{aligned}$$

That is, a (2,4)-IDS is more reliable than a (1,2)-IDS if $P_s > 2/3$, and a (1,2)-IDS is more reliable than a (2,4)-IDS if $P_s < 2/3$. Thus in different P_s ranges, the IDS that gives the optimal reliability can be different. Corollary 1 proves that for any two reliability curves of $(k_1 \cdot m, k_1 \cdot n)$-IDS and $(k_2 \cdot m, k_2 \cdot n)$-IDS, there exists exactly one intersection; and, at the intersection, $0 < P_s < 1$. These intersections can partition probabilities into ranges in which the optimal IDS can be determined.

3.2 Important Properties of IDS

Theorems 3.1 - 3.9 can help find the optimal IDS.

- Theorem 3.1

$P_d(m, n) < P_d(m, n+k)$, for $k \geq 1$.

Proof: [Omitted].

Theorem 3.1 suggests that a designer use as many servers as possible to distribute the data-pieces of a file, where each server keeps a data-piece. The data-pieces of $(m, n+k)$-IDS class are all of the same size, and a collection of m pieces suffices for reconstructing the file. The $(m, n+k)$-IDS class can tolerate $n+k-m$ server failures. Since the members of $(m, n+k)$-IDS class all need the same number of data-pieces to recover the file, an $(m, n+k)$-IDS with larger k can tolerate more server failures and give better total reliability of the file service. For the $(m, n+k)$-IDS class, the data-piece stored in each server need not be changed when new servers join the distributed service – simply distribute a data-piece to each new server. However, the advantage of using larger k is acquired at the expense of higher IER which increases from n/m to $(n+k)/m$. A higher IER also indicates an increase of storage cost.

- Theorem 3.2

$P_d(m, n) > P_d(m+k, n)$, for $k \geq 1$.

Proof: See appendix A.1.

Theorem 3.2 does not imply that any IDS with a higher IER always has higher reliability than an IDS with a lower IER. It does suggest that a designer store a larger data-piece on each server if the total number of participated servers is fixed. In the $(m+k, n)$-IDS class, an IDS with smaller k can give better total reliability at the expense of higher IER. That is, a larger data-piece must be stored on each one of the n servers. Hence, the IER (which is a measure of storage cost) increases. In the $(m+k, n)$-IDS class, the data-piece stored on each server must be updated when the system configuration (the IDS being used) is changed.

- Theorem 3.3

$P_d(m, n) > P_d(m+k, n+k)$ for $k \geq 1$.

Proof: See appendix A.2.

Theorem 3.3 suggests that a designer use fewer servers in the $(m+k, n+k)$-IDS class of which each IDS member can tolerate the same number of server failures. Although, in the class, each $(m+k, n+k)$-IDS has the same fault-tolerance capability, the one with smaller k gives better reliability, but needs larger IER; *ie*, the IER decreases as the number of participating servers increases. Among all $(m+k, n+k)$-IDS, the (m, n)-IDS gives the best reliability, but needs the highest IER.

- Theorem 3.4

$P_d(i, j) \leq P_d(k, l)$ if $l \geq j$ and $k \leq i$,
with equality only when $l = j$ and $k = i$.

Proof: See appendix A.3.

Theorem 3.4 suggests giving larger data-pieces to as many servers as possible, where each server holds a single data-piece. In this way, fewer data-pieces need be collected to recover the file, and at the same time the total reliability increases. The advantage is achieved at the expense of higher IER.

- Theorem 3.5

$P_d(i, j) > P_d(k, l)$ if $l \geq j$, $k > i$, and $l - k \leq j - i$.

Proof: See appendix A.4.

Theorem 3.5 shows that the total reliability increases if:

- fewer servers participate ($l \geq j$);
- each server keeps a larger data-piece ($k > i$);
- more server failures can be tolerated ($l - k \leq j - i$).

In the IDS class, the advantage is acquired at the expense of higher IER, where fewer servers are involved but each server keeps a larger data-piece.

- Theorem 3.6

Given two different IDS, (i, j)-IDS and (k, l)-IDS for $l \geq j, k > i$, and $l - k > j - i$, there exists exactly one $P_s^*((i,j),(k,l))$ such that:

$$\begin{aligned} P_d(i,j) &> P_d(k,l) \text{ if } 0 < P_s < P_s^*((i,j),(k,l)), \\ P_d(i,j) &= P_d(k,l) \text{ if } P_s = P_s^*((i,j),(k,l)), \\ P_d(i,j) &< P_d(k,l) \text{ if } P_s^*((i,j),(k,l)) < P_s < 1, \\ &\text{for } l \geq j, \quad k > i, \quad l - k > j - i. \end{aligned}$$

Proof: See appendix A.5.

Theorem 3.6 indicates that for any two IDS in the IDS class, an IDS can have better reliability in a range of P_s, but worse reliability in the other range. Thus, a particular IDS does not always give better reliability than another. This suggests that a designer must determine the range of P_s first, and then choose the right IDS in the class.

- Discussion

Theorems 3.4 - 3.6 show that for any two different IDS, (i,j)-IDS and (k,l)-IDS (let $l \geq j$, without loss of generality):

if $k \leq i$ then $P_d(i,j) \leq P_d(k,l)$ for all P_s,

if $k > i$ and $l-k \leq j-i$ then $P_d(i,j) > P_d(k,l)$ for all P_s

if $k > i$ and $l-k > j-i$ then there exists a $P_d^*\,((i,j),(k,l))$, where:

$P_d(i,j) > P_d(k,l)$ if $P_s < P_s^*\,((i,j),(k,l))$,

$P_d(i,j) = P_d(k,l)$ if $P_s = P_s^*\,((i,j),(k,l))$,

$P_d(i,j) < P_d(k,l)$ if $P_s > P_s^*\,((i,j),(k,l))$.

Theorem 3.6 implies corollary 1.

- Corollary 1

There exists exactly one P_s^* for $(k_1 \cdot m, k_1 \cdot n)$-IDS and $(k_2 \cdot m, k_2 \cdot n)$-IDS, for $m < n$ and $k_1 < k_2$.

Proof: See appendix A.6.

- Lemma 1

Let p, q be real non-negative numbers such that $p+q = 1$, then:

$$\exp\left[(n'-m') \cdot \log\left(\tfrac{n' \cdot q}{n'-m'}\right) + m' \cdot \log\left(\tfrac{n' \cdot p}{m'}\right)\right]$$

$$\geq \begin{cases} \text{binfc}(m'; n', p), & \text{for } m' \geq p \cdot n' \\ \text{binf}(m'; n', p), & \text{for } m' \leq p \cdot n'. \end{cases}$$

Proof: See [8] or [10].

- Lemma 2

$P_d(k \cdot m, k \cdot n) \to 0$ as $k \to \infty$, for $P_s < m/n$ and $k \geq 1$.

Proof: See appendix A.7.

- Lemma 3

$P_d(k \cdot m, k \cdot n) \to 1$ as $k \to \infty$, for $m/n < P_s$.

Proof: See appendix A.8.

- Theorem 3.7

As $k \to \infty$:

$P_d(k \cdot m, k \cdot n) \to 0$, for $P_s < m/n$; $P_d(k \cdot m, k \cdot n) \to 1$, for $P_s > m/n$.

Proof: This follows from lemmas 2 & 3.

Theorem 3.7 demonstrates a principle to determine the lower bound of IER such that the IDS with the lower bound of IER has better reliability. Given the success probability of each P_s, we should select those IDS whose IER $> 1/P_s$; *ie*, for the class of $(k \cdot m, k \cdot n)$-IDS, the reliability $\to 1$ if IER $(= n/m) > 1/P_s$. From a design perspective, theorem 3.7 indicates that if more servers are provided, but the same IER $(> 1/P_s)$ is provided, then the total reliability of the distributed servers increases.

- Lemma 4

If every infinite subsequence of $< x_n >$ has an infinite subsequence that converges to x, then the sequence $< x_n >$ converges to x.

Proof: Omitted.

- Theorem 3.8

Let $A_k = P_s^*\,[(m,n),(k \cdot m, k \cdot n)]$, the critical probability of (m,n)-IDS and $(k \cdot m, k \cdot n)$-IDS.

Then the sequence $< A_k >$ converges to m/n.

Proof: See appendix A.9.

Theorem 3.8 shows that the critical probability of (m,n)-IDS and $(k \cdot m, k \cdot n)$-IDS, $P_s^*\,[(m,n),(k \cdot m, k \cdot n)]$, converges to m/n as k increases. Because the reliability curves of $(k \cdot m, k \cdot n)$-IDS vary consistently, the critical probability of (m,n)-IDS and $(k \cdot m, k \cdot n)$-IDS, either strictly decreases to m/n or strictly increases to m/n as k increases.

- Discussion

Use a Gaussian approximation of $P_d(k \cdot m, k \cdot n)$, evaluated at $P_s = m/n$ [11]:

$$P_d(k \cdot m, k \cdot n) \approx \text{gaufc}(-0.5\zeta), \text{ for } P_s = m/n;$$

$$\zeta \equiv \left[k \cdot n \cdot \frac{m}{n} \cdot \frac{n-m}{n}\right]^{-\frac{1}{2}}.$$

Because gauf(-0.5ζ) strictly increases to 0.5 as k increases, the value of $P_d(k \cdot m, k \cdot n)$ evaluated at $P_s = m/n$ strictly decreases to 0.5 as k increases. From theorem 3.6, the critical probability of (m,n)-IDS and $(k \cdot m, k \cdot n)$-IDS (for all $k > 1$) is larger than m/n. Therefore, the critical probability of (m,n)-IDS and $(k \cdot m, k \cdot n)$-IDS strictly decreases to m/n as k increases. That is, the sequence:

$< A_k > = P_s^*\,[(m,n),(k \cdot m, k \cdot n)]$

strictly decreases to m/n. The result has been confirmed by examining the sequence for $n \leq 100$. As an example, figure 3 shows the reliabilities of $(k,2k)$-IDS $(1 \leq k \leq 4)$. Figure 4 augments a subregion in figure 3.

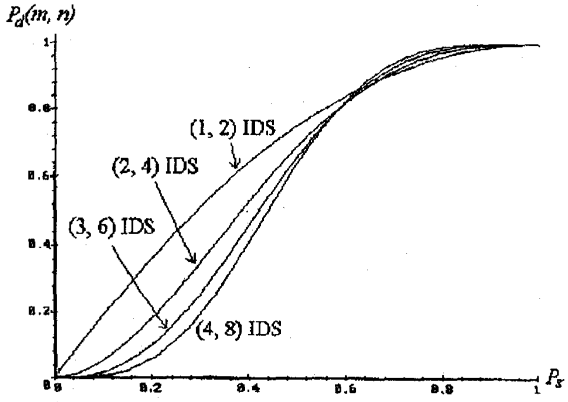


Figure 3. Reliability Curves for (1,2)-IDS, (2,4)-IDS, (3,6)-IDS, (4,8)-IDS

The critical probability $P_s^*[(1,2),(k,2k)]$ for $2 \leq k \leq 4$ is computed as:

$$\begin{aligned} P_s^*[(1,2),(2,4)] &\approx 0.6667, \\ P_s^*[(1,2),(3,6)] &\approx 0.6377, \\ P_s^*[(1,2),(4,8)] &\approx 0.6198. \end{aligned}$$

This shows that $P_s^*[(1,2),(k,2k)]$ is strictly decreasing, for $2 \leq k \leq 4$.

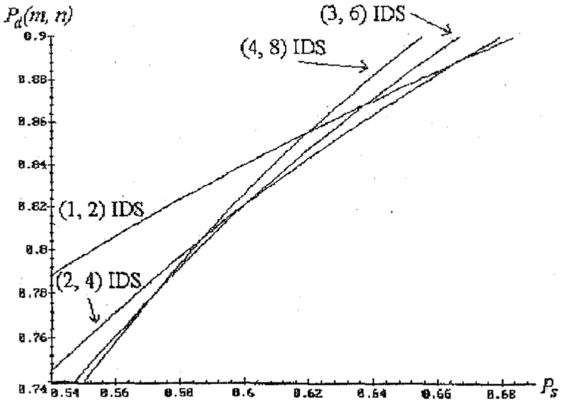


Figure 4. Augmentation of the Subregion in Figure 3

- Theorem 3.9

The following conditions hold for any $P_d(t \cdot m, t \cdot n)$, $1 < t < k$:
$P_d(t \cdot m, t \cdot n) < P_d(m,n)$, if $P_s \leq P_s^*[(m,n),(k \cdot m, k \cdot n)]$,
$P_d(t{\cdot}m, t{\cdot}n) < P_d(k{\cdot}m, k{\cdot}n)$, if $P_s^*[(m,n),(k{\cdot}m,k{\cdot}n)] \leq P_s$.

Proof: See appendix A.10.

From a design perspective, theorem 3.9 shows that we can choose the most reliable IDS from the class of $(t \cdot m, t \cdot n)$-IDS for $1 \leq t \leq k$. The best choice is:

(m,n)-IDS iff $P_s \in (0, P_s^*[(m,n),(k \cdot m, k \cdot n)])$,
$(k \cdot m, k \cdot n)$-IDS iff $P_s \in (P_s^*[(m,n),(k \cdot m, k \cdot n)], 1)$.

Notation (for an (m,n)-IDS)

n	total number of participating servers
m	number of servers involved to recover a file
$n-m$	fault-tolerant capability
n/m	IER

These factors (in the Notation) determine the cost & performance of a distributed service. For example:
· a larger n implies that the service needs more participating servers,
· a larger m implies that the time to recover a file is longer,
· a larger $n-m$ implies that the service can tolerate more server failures,
· a larger n/m implies that storage cost of the service is higher.

According to the resource & performance constraints, the designer has many possible choices for (m,n)-IDS. Given these IDS, then determine the optimal IDS with the highest reliability. From theorem 3.6, every pair of IDS has at most one critical probability. The optimal IDS for the two ranges ($P_s > P_s^*$, and $P_s < P_s^*$) are usually different. Given a set of IDS, one of them might be not optimal in all ranges of P_s. Therefore, finding optimal IDS is quite complicated. Based on the theorems 3-1 – 3-9, we give a pseudo-algorithm for finding the possible optimal systems. The input of the algorithm is a set of IDS which the designer can choose according to the resource & performance constraints. The output is the reduced IDS set indicating a possible optimal IDS.

```
• Algorithm: Search_the_Possible_Optimal_Systems
     Input:  $S$ [set of IDS with different parameters]
     Output: $S'$ [reduced set of IDS indicating possible
                optimal IDS]

  1. Let $S' = S$.

 2a. Search $S'$ to find the IDS which belong to the same
     class of $(m, n+k)$-IDS. Let this IDS be
     $\{(m, n+k_g)\text{-IDS}\}_{g=1}^{t}$, where $k_g < k_{g+1}$.
 2b. Reduce $S'$ by deleting $\{(m, n+k_g)\text{-IDS}\}_{g=1}^{t-1}$.
     (by theorem 3.1)
 2c. Repeat this step 2 until no IDS belongs to the same
     class of $(m, n+k)$-IDS.

 3a. Search $S'$ to find the IDS which belong to the same
     class of $(m+k, n)$-IDS. Let this IDS be
     $\{(m+k_g, n)\text{-IDS}\}_{g=1}^{t}$, where $k_g < k_{g+1}$.
 3b. Reduce $S'$ by deleting $\{(m+k_g, n)\text{-IDS}\}_{g=2}^{t}$.
     (by theorem 3.2)
 3c. Repeat this step 3 until no IDS belongs to the same
     class of $(m+k, n)$-IDS.

 4a. Search $S'$ to find the IDS which belong to the same
     class of $(m+k, n+k)$-IDS. Let this IDS be
     $\{(m+k_g, n+k_g)\text{-IDS}\}_{g=1}^{t}$, where $k_g < k_{g+1}$.
 4b. Reduce $S'$ by deleting $\{(m+k_g, n+k_g)\text{-IDS}\}_{g=2}^{t}$.
     (by theorem 3.3)
 4c. Repeat this step 4 until no IDS belongs to the same
     class of $(m+k, n+k)$-IDS.

 5a. Search $S'$ to find the IDS which belong to the same
     class of $(m \cdot k, n \cdot k)$-IDS. Let this IDS be
     $\{(m \cdot k_g, n \cdot k_g)\text{-IDS}\}_{g=1}^{t}$, where $k_g < k_{g+1}$.
 5b. Reduce $S'$ by deleting $\{(m \cdot k_g, n \cdot k_g)\text{-IDS}\}_{g=2}^{t-1}$.
     (by theorem 3.9)
 5c. Repeat this step 5 until no IDS belongs to the same
     class of $(m \cdot k, n \cdot k)$-IDS.
```

6. For every pair of IDS in S', say (i,j)-IDS & (k,l)-IDS, execute the process:

   a. if $l > j$, and $k < i$, then delete (i,j)-IDS from S'; (by theorem 3.4)

   b. if $l > j$, $k > i$, and $l - k < j - i$, then delete (k,l)-IDS from S'; (by theorem 3.5)

   c. if $l < j$, and $k > i$, then delete (k,l)-IDS from S'; (by theorem 3.4)

   d. if $l < j$, $k < i$, and $l - k > j - i$, then delete (i,j)-IDS from S'; (by theorem 3.5)

7. Output S'.

End_Algorithm

Once the reduced IDS set S' is determined and the success probability of each P_s is known, the designer can compute & compare the reliabilities of these possible optimal IDS to find the optimal IDS.

Section 4 considers a special case when an upper-bound of the IER and the number of available servers are given. The method uses the properties in theorems 3.1 – 3.9 to reduce the complexity of finding the optimal IDS.

4. OPTIMAL INFORMATION DISPERSAL

Theorem 3.2 shows that an (m_1,n)-IDS has higher reliability than an (m_2,n)-IDS if $m_1 < m_2$. So, it is reasonable to store higher priority files in the distributed servers at a higher IER and lower level files at a lower IER; this does not imply that any IDS with a higher IER always has a higher reliability than an IDS with a lower IER. On the other hand, the number of available servers in a distributed system can change. Based on the analysis in section 3, we propose a method for determining the optimal IDS when an upper-bound of the IER (depending on the priority of the file) and the number of available servers are given.

Notation

u	upper bound of the IER
v	number of available servers
k	$\lfloor v/u \rfloor$

Given u & v, the feasible IDS set is the set of all possible IDS that satisfy these conditions. The optimal IDS in each range of P_s are elements of the feasible IDS set. Theorems 3.4 & 3.5 show that many IDS of a feasible IDS set are not optimal in any range of P_s. Theorem 3.6 shows that an IDS can be optimal in some range, but not in all ranges. Therefore, a feasible IDS set can be reduced so that all optimal IDS are still included in the reduced feasible IDS set. The reduced feasible IDS set is a subset of the feasible IDS set. For any P_s, the optimal IDS of $F_{u,v}$ is an element of the reduced $F_{u,v}$.

The feasible IDS set is the union of several partitions. Each partition consists of all (m,n)-IDS for which m is a constant:

$$F_{u,v} = \left[\bigcup_{g=1}^{k} (g,t)\text{-IDS};\ g \le t \le g \cdot u\right] \cup \left[\bigcup_{g=k+1}^{v} (g,t)\text{-IDS};\ g \le t \le v\right]. \tag{1}$$

By theorem 3.1, in each partition:

$[(i,t)\text{-IDS};\ i \le t \le i \cdot u]$,

the $(i, i \cdot u)$-IDS has the highest reliability. Similarly, in each partition:

$[(k+j,t)\text{-IDS};\ k+j \le t \le v]$,

the $(k+j,v)$-IDS has the highest reliability. Thus, (1) reduces to:

$$F_{u,v} = [(i, i \cdot u)\text{-IDS};\ 1 \le i \le k] \cup [(k+j,v)\text{-IDS};\ 1 \le j \le v-k]. \tag{2}$$

By theorem 3.9, the IDS set:

$[(i, i \cdot u)\text{-IDS};\ 1 \le i \le k]$

can be reduced to:

$[(1,u)\text{-IDS},\ (k, u \cdot k)\text{-IDS}]$.

By theorem 3.2, in the IDS set:

$[(k+j,v)\text{-IDS};\ 1 \le j \le v-k]$,

the $(k+1,v)$-IDS has the highest reliability. Therefore, (2) can be reduced to:

$$[(1,u)\text{-IDS},\ (k, u \cdot k)\text{-IDS},\ (k+1,v)\text{-IDS}]. \tag{3}$$

If $k = v/u$, then (3) reduces to: $[(1,u)\text{-IDS},\ (k,v)\text{-IDS},\ (k+1,v)\text{-IDS}]$.

By theorem 3.2, $P_d(k,v) > P_d(k+1,v)$. Thus, (3) reduces to:

$$[(1,u) - IDS, (k,v)\text{-IDS}]. \tag{4}$$

Compare the number of feasible IDS sets with the number of reduced feasible IDS set as follows. The reduced feasible IDS set contains 3 elements (2 elements if $k = v/u$), *ie*, the number of elements in the reduced feasible IDS set is $O(1)$.

Without much loss of generality, let $k = v/u$. Then, the number of the feasible IDS sets is:

$$\left[\sum_{g=1}^{k} (g \cdot u - g + 1)\right] + \left[\sum_{g=k+1}^{v} (v - g + 1)\right] = \frac{u \cdot v^2 + 2u \cdot v - v^2}{2u}. \tag{5}$$

Thus, the number of elements in the feasible IDS set is: $O(v^2)$, if $u > 1$, $\quad O(v)$, if $u = 1$.

Hence, we can reduce the complexity for computing the highest reliability:

from $O(v)$ to $O(1)$ when the upper bound of the IER is 1 from $O(v^2)$ to $O(1)$ when the upper bound of the IER is larger than 1.

Example

Let $u = 3$, $v = 11$.

The feasible IDS set:

$$F_{3,11} = \left[\bigcup_{g=1}^{11} [(g,t)\text{-IDS};\ g \le t \le \min(3g, 11)] \right].$$

Thus, $F_{3,11}$ reduces to:
[(1,3)-IDS, (3,9)-IDS, (4,11)-IDS],
and the number of feasible IDS sets is reduced from 51 to 3. Figure 5 shows the reliability curves of these 3 IDS; figure 6 shows the subregion in figure 5.

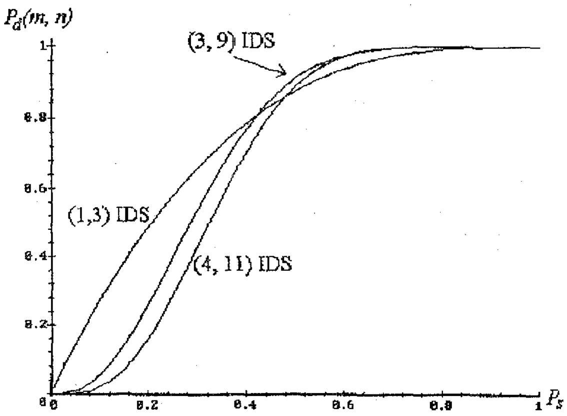


Figure 5. Reliability Curves of (1,3)-IDS, (3,9)-IDS, (4,11)-IDS

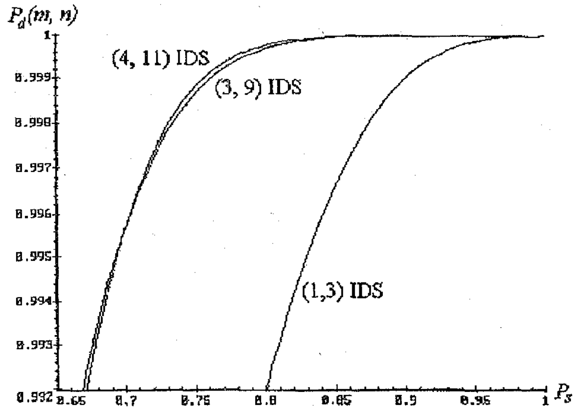


Figure 6. Augmentation of the Subregion in Figure 5

From figures 5 & 6 the optimal selection is:

- (1,3)-IDS, when $P_s \in [0, P_s^*[(1,3),(3,9)]]$;
- (3,9)-IDS, when $P_s \in [P_s^*[(1,3),(3,9)], P_s^*[(3,9),(4,11)]]$;
- (4,11)-IDS, $P_s \in [P_s^*[(3,9),(4,11)], 1]$;

where:

- P_s^*[(1,3), (3,9)] ≈ 0.42138,
- P_s^*[(3,9), (4,11)] $= 0.7$;
- IER of (1,3)-IDS is 3,
- IER of (3,9)-IDS is 3,
- IER of (4,11)-IDS is 2.75.

Thus an IDS with a higher IER need not have a higher reliability, even though the probability → 1.

ACKNOWLEDGMENT

This work was supported in part by the National Science Council of Taiwan, under contract NSC-86-2213-E-324-002. We appreciate the constructive inputs of the referees, the Associate Editor, and the Managing Editor during the review process.

APPENDIX

Notation

$Q_s \quad 1 - P_s$

A.1 Proof of Theorem 3.2

$P_d(m,n) = P_d(m+k,n) + \sum_{g=m}^{m+k-1} \text{binm}(g; n, P_s)$.
So, $P_d(m,n) > P_d(m+k,n)$. *Q.E.D.*

A.2 Proof of Theorem 3.3

Use mathematical induction.

A.2.1 For $k = 1$

The total reliability of $(m+1, n+1)$-IDS is:

$$P_d(m+1, n+1) = \text{binfc}(m+1; n+1, P_s)$$
$$\equiv \sum_{g=m+1}^{n+1} \binom{n+1}{g} \cdot P_s^g \cdot Q_s^{n-g}$$
$$= \sum_{g=m}^{n} \left(\binom{n}{g+1} + \binom{n}{g} \right) \cdot P_s^{g+1} \cdot Q_s^{n-g}$$
$$= \sum_{g=m+1}^{n} \binom{n}{g} \cdot P_s^g \cdot Q_s^{n-g+1}.$$

The total reliability of (m,n)-IDS is:

$$P_d(m,n) = \sum_{g=m}^{n} \binom{n}{g} \cdot P_s^g \cdot Q_s^{n-g}.$$

Therefore,

$$P_d(m+1, n+1)$$
$$= Q_s \cdot P_d(m,n) - \binom{n}{m} \cdot P_s^m \cdot Q_s^{n-m+1} + P_s \cdot P_d(m,n)$$
$$= P_d(m,n) - \binom{n}{m} \cdot P_s^m \cdot Q_s^{n-m+1}.$$

Thus, $P_d(m,n) > P_d(m+1,n+1)$, and the theorem holds for $k = 1$.

A.2.2 For $k > 1$

Assume the theorem holds when $k = t$:

$P_d(m,n) > P_d(m+t,n+t)$.

Let $m' = m+t$ and $n' = n+t$; then from A.2.1,

$P_d(\mathrm{m,n}) > P_d(m+t,n+t)$

$= P_d(m',n') > P_d(m'+1,n'+1)$.

Therefore,

$P_d(m,n) > P_d(m+t+1,n+t+1)$,

and the theorem holds also when $k = t+1$. *Q.E.D.*

A.3 Proof of Theorem 3.4

By theorem 3.1,

$P_d(k,j) \leq P_d(k,l)$ for $l \geq j$,

with equality when $l = j$. By theorem 3.2,

$P_d(i,j) \leq P_d(k,j)$ for $k \leq i$,

with equality when $k = i$.

Therefore,

$P_d(i,j) \leq P_d(k,j) \leq P_d(k,l)$ for $l \geq j$ and $k \leq i$,

with equality when $l = j$ and $k = i$. *Q.E.D.*

A.4. Proof of Theorem 3.5

Let $t = l - j$. By theorem 3.3,

$P_d(i,j) \geq P_d(i+t,j+t) = P_d(i+l-j,l)$,

with equality when $l = j$. Because $l - k \leq j - i$, then $k \geq i + l - j$. By theorem 3.2,

$P_d(i+l-j,l) \geq P_d(k,l)$,

with equality when $i + l - j = k$. So,

$P_d(i,j) \geq P_d(k,l)$,

with equality when $l = j$ and $i + l - j = k$, or equivalently $l = j$ and $i = k$. However, $k > i$. Thus,

$P_d(i,j) > P_d(k,l)$ if $l \geq j,\ \ k > i,$ and $l - k \leq j - i$.

Q.E.D.

A.5 Proof of Theorem 3.6

Notation

$\delta(P_s)$ $\quad P_d(i,j) - P_d(k,l)$

$\delta'(P_s)$ $\quad P'_d(i,j) - P'_d(k,l)$

A.5.1 Prove:

$\delta(P_s) > 0$, when $P_s \to 0^+$,

$\delta(P_s) < 0$, when $P_s \to 1^-$.

$$P_d(i,j) = \sum_{g=i}^{j} \binom{j}{g} \cdot P_s^g \cdot Q_s^{j-g},$$

$$P_d(k,l) = \sum_{g=k}^{l} \binom{l}{g} \cdot P_s^g \cdot Q_s^{l-g}.$$

$$\lim_{P_s \to 0^+} \left[\frac{\delta(P_s)}{P_s^i}\right] = \lim_{P_s \to 0^+} [\Psi_{s:1} - \Psi_{s:2}]$$

$$= \binom{j}{i} > 0,$$

$$\Psi_{s:1} \equiv \left[\sum_{g=i}^{j} \binom{j}{g} \cdot P_s^{g-i} \cdot Q_s^{j-g}\right]$$

$$\Psi_{s:2} \equiv \left[\sum_{g=k}^{l} \binom{l}{g} \cdot P_s^{g-i} \cdot Q_s^{l-g}\right]$$

thus $P_d(i,j) > P_d(k,l)$ when $P_s \to 0^+$.

$$P_d(i,j) = 1 - \sum_{g=j-i+1}^{j} \binom{j}{g} \cdot P_s^{j-g} \cdot Q_s^g,$$

$$P_d(k,l) = 1 - \sum_{g=l-k+1}^{l} \binom{l}{g} \cdot P_s^{l-g} \cdot Q_s^g.$$

$$\lim_{P_s \to 1^-} \left[\frac{\delta(P_s)}{Q_s^{j-i+1}}\right] = \lim_{P_s \to 1^-} [\Phi_{s:1} - \Phi_{s:2}]$$

$$= -\binom{j}{j-i+1} < 0,$$

$$\Phi_{s:1} \equiv \left[\sum_{g=l-k+1}^{l} \binom{l}{g} \cdot P_s^{l-g} \cdot Q_s^{g-j+i-1}\right]$$

$$\Phi_{s:2} \equiv \left[\sum_{g=j-i+1}^{j} \binom{j}{g} \cdot P_s^{j-g} \cdot Q_s^{g-j+i-1}\right]$$

thus $P_d(i,j) < P_d(k,l)$ when $P_s \to 1^-$.

These equations show:

$\delta(P_s) > 0$ when $P_s \to 0^+$,

$\delta(P_s) < 0$ when $P_s \to 1^-$.

A.5.2 Prove (Based on A.5.1)

There exists exactly 1 critical P_s^* such that:

$P_d(i,j) = P_d(k,l)$,

$P_d(i,j) > P_d(k,l)$ if $P_s < P_s^*$,

$P_d(i,j) < P_d(k,l)$ if $P_s^* < P_s$.

Because:

$$P_d(m,n) = \sum_{g=m}^{n} \binom{n}{g} \cdot P_s^g \cdot Q_s^{g-m},$$

then the first derivative of $P_d(m,n)$ is:

$$P'_d(m,n) = m \cdot \binom{n}{m} \cdot P_s^{m-1} \cdot Q_s^{n-m}.$$

Therefore,

$$\frac{\delta'(P_s)}{P_s^{i-1}} = i \cdot \binom{j}{i} \cdot Q_s^{j-i} - k \cdot \binom{l}{k} \cdot P_s^{k-i} \cdot Q_s^{l-k};$$

$$\lim_{P_s \to 0^+} \left[\frac{\delta'(P_s)}{P_s^{i-1}}\right] = i \cdot \binom{j}{i} > 0;$$

$\delta'(P_s) > 0$ when $P_s \to 0^+$.

Similarly,

$$\frac{\delta'(P_s)}{Q_s^{j-i}} = i \cdot \binom{j}{i} \cdot P_s^{i-1} - k \cdot \binom{l}{k} \cdot P_s^{k-1} \cdot Q_s^{(l-k)-(j-i)};$$

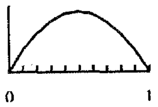
$$\lim_{P_s \to 1^-} \left[\frac{\delta'(P_s)}{Q_s^{i-1}}\right] = i \cdot \binom{j}{i} > 0;$$

$\delta'(P_s) > 0$ when $P_s \to 1^-$.

Let $\delta'(P_s) = 0$. Then, $P_s = 0$, or $P_s = 1$, or

$$P_s^{k-i} \cdot Q_s^{(l-k)-(j-i)} = \frac{i \cdot \binom{j}{i}}{k \cdot \binom{l}{k}}. \qquad (6)$$

Let $a = k - i$, $b = (l - k) - (j - i)$.
The graph of $P_s^a \cdot Q_s^b$ is:



So, there are at most two solutions in (0,1) for (6). If there is no solution or one solution in (0,1) for (6) then $\delta'(P_s) \geq 0$ for all P_s. [There is at most one P_s such that $\delta'(P_s) = 0$.] This implies that $\delta(P_s)$ is a monotonic increasing function.
$\delta(P_s) > 0$ as $P_s \to 1^-$, because $\delta(P_s) > 0$ when $P_s \to 0^+$. This contradicts the claim that $\delta(P_s) < 0$ when $P_s \to 1^-$ in A.5.1. Therefore, there are exactly 2 solutions in (0,1) for (6); and there are 3 stationary points for $\delta(P_s)$ when $P_s \in (0, 1)$. However,
$\delta(P_s)$ is a polynomial of P_s, and
$P_d(i, j) > P_d(k, l)$ when $P_s \to 0^+$,
$P_d(i, j) < P_d(k, l)$ when $P_s \to 1^-$.
So, there exists exactly 1 P_s^* such that:
$P_d(i, j) = P_d(k, l)$,
$P_d(i, j) > P_d(k, l)$ if $P_s < P_s^*$,
$P_d(i, j) < P_d(k, l)$ if $P_s^* < P_s$. *Q.E.D.*

A.6 Proof of Corollary 1

Because:
$k_2 \cdot n > k_1 \cdot n$,
$k_2 \cdot m > k_1 \cdot m$,
$k_2 \cdot n - k_2 \cdot m = k_2 \cdot (n - m) > k_1 \cdot (n - m) = k_1 \cdot n - k_1 \cdot m$
then theorem 3.6 shows that there exists exactly 1 critical probability in (0,1) for $(k_1 \cdot m, k_1 \cdot n)$-IDS and $(k_2 \cdot m, k_2 \cdot n)$-IDS. *Q.E.D.*

A.7 Proof of Lemma 2

Let $P_s < m/n$.
Lemma 1 shows that:

$$\sum_{t=k\cdot m}^{k\cdot n} \binom{k \cdot n}{t} \cdot P_s^t \cdot Q_s^{k\cdot n - t} \leq \exp\left[\Theta_{s:1} + \Theta_{s:2}\right]$$

$$\Theta_{s:1} \equiv (k \cdot n - k \cdot m) \cdot \log\left(\frac{k \cdot n \cdot Q_s}{k \cdot n - k \cdot m}\right)$$

$$\Theta_{s:2} \equiv k \cdot m \cdot \log\left(\frac{k \cdot n \cdot P_s}{k \cdot m}\right).$$

Hence,

$$P_d(k \cdot m, k \cdot n) \leq \exp\left[\Theta_{s:1} + \Theta_{s:2}\right]$$

Let:

$$\begin{aligned} g(P_s) &\equiv (\frac{n \cdot Q_s}{n - m})^{n-m} \cdot (\frac{n \cdot P_s}{m})^m, \\ f(P_s) &\equiv \log(g(P_s)). \end{aligned}$$

Calculate where the maximum of $g(P_s)$ is.

$$\begin{aligned} g'(P_s) = &-n \cdot (\frac{n \cdot Q_s}{n - m})^{n-m-1} \cdot (\frac{n \cdot P_s}{m})^m \\ &+ (\frac{n \cdot Q_s}{n - m})^{n-m} \cdot n \cdot (\frac{n \cdot P_s}{m})^{m-1} = 0; \\ &-(n - m) \cdot P_s + m \cdot Q_s = 0; \end{aligned}$$

$P_s = m/n$; and the maximum value of $g(P_s)$ is $g(m/n) = 1$. Since $P_s < m/n$, then,
$0 < g(P_s) < 1$ when $0 < P_s < m/n$.
Because $0 < g(P_s) < 1$, then $f(P_s) < 0$.

Therefore,
$\exp\left[k \cdot f(P_s)\right] \to 0$ as $k \to \infty$.
Because,

$$\sum_{t=k\cdot m}^{k\cdot n} \binom{k \cdot n}{t} \cdot P_s^t \cdot Q_s^{k\cdot n - t} \leq \exp\left[(k \cdot f(P_s)\right],$$

then,
$P_d(k \cdot m, k \cdot n) \to 0$ as $k \to \infty$, for $0 < P_s < m/n$. *Q.E.D.*

A.8 Proof of Lemma 3

Let $\frac{m}{n} < P_s$.
Lemma 1 shows that:

$$\sum_{t=0}^{k\cdot m} \binom{k \cdot n}{t} \cdot P_s^t \cdot Q_s^{k\cdot n - t} \leq \exp\left[\Omega_{s:1} + \Omega_{s:2}\right]$$

$$\Omega_{s:1} \equiv (k \cdot n - k \cdot m) \cdot \log\left(\frac{k \cdot n \cdot Q_s}{k \cdot n - k \cdot m}\right)$$

$$\Omega_{s:2} \equiv k \cdot m \cdot \log\left(\frac{k \cdot n \cdot P_s}{k \cdot m}\right).$$

Let:

$$g(P_s) \equiv (\frac{n\cdot Q_s}{n-m})^{n-m}\cdot(\frac{n\cdot P_s}{m})^{m},$$
$$f(P_s) \equiv \log(g(P_s)).$$

Because $0 < P_s < 1$ and $n \ge m$, then $g(P_s) > 0$.
Calculate where the maximum of $g(P_s)$ is.

$$g'(P_s) = -n\cdot(\frac{n\cdot Q_s}{n-m})^{n-m-1}\cdot\left(\frac{n\cdot P_s}{m}\right)^{m} + \left(\frac{n\cdot Q_s}{n-m}\right)^{n-m}\cdot n\cdot\left(\frac{n\cdot P_s}{m}\right)^{m-1} = 0;$$
$$-(n-m)\cdot P_s + m\cdot Q_s = 0;$$
$$P_s = m/n;$$

the maximum value of $g(P_s)$ is $g(m/n) = 1$.
Hence,
$0 < g(P_s) < 1$ when $m/n < P_s$.
Because $0 < g(P_s) < 1$, then $f(P_s) < 0$.
Therefore, $\exp[k\cdot f(P_s)] \to 0$ as $k \to \infty$.
Because,

$$\sum_{t=0}^{k\cdot m}\binom{k\cdot n}{t}\cdot P_s^t\cdot Q_s^{k\cdot n-t} \le \exp[k\cdot f(P_s)],$$

then,

$$P_d(k\cdot m, k\cdot n) = 1 - \left[\sum_{t=0}^{k\cdot m}\binom{k\cdot n}{t}\cdot P_s^t\cdot Q_s^{k\cdot n-t}\right] + \binom{k\cdot n}{k\cdot m}\cdot P_s^{k\cdot m}\cdot Q_s^{k\cdot n-k\cdot m}$$
$$\ge 1 - \exp[k\cdot f(P_s)] + \binom{k\cdot n}{k\cdot m}\cdot P_s^{k\cdot m}\cdot Q_s^{k\cdot n-k\cdot m}$$
$$\ge 1 - \exp[k\cdot f(P_s)]$$

Hence, $P_d(k\cdot m, k\cdot n) \to 1$ as $k \to \infty$. *Q.E.D.*

A.9 Proof of Theorem 3.8

Let $< A_{s_k} >$ be any subsequence of $< A_k >$. If we can construct a subsequence $< A_{t_k} >$ of $< A_{s_k} >$ such that $< A_{t_k} > \rightarrow m/n$, then, by lemma 4, the theorem is proved.

Corollary 1 asserts the existence & uniqueness of A_k, *ie*, A_k is unique in (0,1) such that $P_d(m,n)$ and $P_d(k\cdot m, k\cdot n)$ are equal at A_k. By assumption, $< A_{s_k} >$ is a subsequence of $< A_k >$, so it corresponds to the subsequence,

$< P_d(s_k\cdot m, s_k\cdot n) >$ of $P_d(k\cdot m, k\cdot n)$.

Construct $< A_{t_k} >$ such that,

$$A_{t_k} \in \left[\frac{m}{n} - \frac{m}{n\cdot k}, \frac{m}{n} + \frac{n-m}{n\cdot k}\right]$$

for all k. Consequently,
$< A_{t_k} > \rightarrow m/n$ as $k \to \infty$.

To begin with, choose $t_1 = 2$; then $A_2 \in [0,1]$. Define t_k inductively. Let t_k be defined for $k = 1, 2, \ldots, i-1$. The following discussion is needed before t_i is defined. Let,

$L = P_d(m,n)$ and $L_{s_k} = P_d(s_k\cdot m, s_k\cdot n)$,
at $P_s = \frac{m}{n} - \frac{m}{n\cdot i}$;

$R = P_d(m,n)$ and $R_{s_k} = P_d(s_k\cdot m, s_k\cdot n)$,
at $P_s = \frac{m}{n} - \frac{n-m}{n\cdot i}$.

$\lim_{k\to\infty}(L_{s_k}) = 0$ by theorem 3.7.

Therefore we can choose a subsequence $< u_k >$ of $< s_k >$ such that:

$L_{u_k} < L$, for all k,

$< L_{u_k} >$ is strictly decreasing to 0.

On the other hand,
$\lim_{k\to\infty}(R_{u_k}) = 1$, by theorem 3.7.

Therefore we can choose a subsequence $< v_k >$ of $< u_k >$ such that $R_{v_k} > R$ for all k, and $< R_{v_k} >$ is strictly increasing to 1.

Now consider v_k:

$L_{v_k} < L$, and $R_{v_k} > R$, for all k.

Therefore,

$$A_{v_k} \in \left[\frac{m}{n} - \frac{m}{n\cdot i}, \frac{m}{n} + \frac{n-m}{n\cdot i}\right], \text{ for all } k.$$

Geometrically, this can be understood easily; the Intermediate Value Theorem in calculus applies here. Let,
$t_i \equiv \min_k\{v_k; v_k > t_{i-1}\}$.

By induction, construct a subsequence $< A_{t_k} >$ of $< A_k >$ such that,

$< A_{t_k} > \rightarrow m/n$.

Hence, by lemma 4,

$< A_k > \rightarrow m/n$. *Q.E.D.*

A.10 Proof of Theorem 3.9

As explained in section 3, just before theorem 3.9,
$P_s^*[(m,n),(k\cdot m,k\cdot n)] < P_s^*[(m,n),(t\cdot m,t\cdot n)]$,
if $k > t$.

The Cdf, $P_d(m',n')$ of an (m',n')-IDS, is strictly monotonic increasing for $P_s \in (0,1)$; therefore,

$P_s^*[(t\cdot m,t\cdot n),(k\cdot m,k\cdot n)] < P_s^*[(m,n),(k\cdot m,k\cdot n)]$
$< P_s^*[(m,n),(t\cdot m,t\cdot n)]$.

Let,

$p_a \equiv P_s^*[(t\cdot m,t\cdot n),(k\cdot m,k\cdot n)]$,
$p_b \equiv P_s^*[(\mathrm{m,n}),(k\cdot m,k\cdot n)]$,
$p_c \equiv P_s^*[(\mathrm{m,n}),(t\cdot m,t\cdot n)]$.

According to the definition of the critical probability:

$P_d(t\cdot m,t\cdot n) < P_d(m,n)$ if $P_s < p_c$,
$P_d(t\cdot m,t\cdot n) < P_d(k\cdot m,k\cdot n)$, if $p_a < P_s$.

Because $p_a < p_c$,

$P_d(t \cdot m, t \cdot n) < P_d(m, n)$, if $P_s \leq p_b$.

Because $p_a < p_b$,

$P_d(t \cdot m, t \cdot n) < P_d(k \cdot m, k \cdot n)$, if $p_b \leq P_s$. *Q.E.D.*

REFERENCES

[1] C. Asmuth, G.R. Blakley, "Pooling splitting and restituting information to overcome total failure of some channels of communication", *IEEE Proc. 1982 Symp. Security & Privacy*, 1982, pp 156-169.

[2] C. Asmuth, J. Bloom, "A modular approach to key safeguarding", *IEEE Trans. Information Theory*, vol IT-29, num 2, 1983, pp 208-210.

[3] A. Bestavros, "IDA-based redundant arrays of inexpensive disks", *Proc. First Int'l Conf. Parallel & Distributed Information Systems*, 1991 Dec.

[4] G.R. Blakley, "Safeguarding cryptographic keys", *Proc. NCC*, vol 48, 1979, pp 313-317; AFIPS Press.

[5] W.A. Burkhard, K.C. Claffy, T.J.E. Schwarz, "Performance of balanced disk array schemes", 11th *IEEE Symp. Mass Storage Systems*, 1991, pp 45-50.

[6] W.A. Burkhard, J. Menon, "Disk array storage system reliability", *Proc* 23rd *IEEE Int'l Symp. Fault-Tolerant Computing*, 1993, pp 432-441.

[7] P. Chen, E. Lee, G. Gibson, *et al*, "RAID: High-performance, reliable secondary storage", *ACM Computing Surveys*, vol 26, num 2, 1994 Jun, pp 145-185.

[8] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations", *Annals Mathematical Statistics*, vol 23, 1952, pp 493-507.

[9] D.E.R. Denning, *Cryptography and Data Security*, 1983; Addison-Wesley.

[10] P. Erdö s, J. Spencer, *Probabilistic Methods in Combinatorics*, 1974, pp 18; Academic Press.

[11] R. G. Gallager, *Information Theory and Reliable Communication*, 1968; John Wiley & Sons.

[12] L. Gargano, A.A. Rescigno, U. Vaccaro, "Fault-tolerant hypercube broadcasting via information dispersal", *Networks*, vol 23, 1993, pp 271-282.

[13] L. Gong, "Increasing availability and security of an authentication service", *IEEE J. Selected Areas in Communications*, vol 11, 1993 Jun, pp 657-662.

[14] Y.D. Lyuu, "Fast fault-tolerant parallel communication and online maintenance for hypercube using information dispersal", *Mathematical Systems Theory*, vol 24, num 4, 1991, pp 273-294.

[15] Y.D. Lyuu, "Fast fault-tolerant parallel communication for de Bruijn and digit-exchange networks using information dispersal", *Networks*, vol 23, 1993, pp 365-378.

[16] M.O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance", *J. ACM*, vol 36, 1989 Apr, pp 335-348.

[17] A. Shamir, "How to share a secret", *Comm. ACM*, vol 22, 1979 Nov, pp 612-613.

AUTHORS

Dr. Hung-Min Sun; Dep't of Information Management; Chaoyang Univ. of Technology; Wufeng, Taichung, 413 TAIWAN - R.O.C.

Internet (e-mail): hmsun@dscs.csie.nctu.edu.tw

Hung-Min Sun received his BS (1988) in Applied Mathematics from National Chung-Hsing University, MS (1990) in Applied Mathematics from National Cheng-Kung University, and PhD (1995) in Computer Science and Information Engineering from National Chiao-Tung University. Since 1995 he has been with the Department of Information Management, Chaoyang University of Technology. His research interests include reliability theory, computer security, cryptography, and information theory.

Dr. Shiuh-Pyng Shieh; Dep't of Computer Science and Information Engineering; National Chiao Tung Univ; Hsinchu 30010 TAIWAN - R.O.C.

Internet (e-mail): ssp@csie.nctu.edu.tw

Shiuh-Pyng Shieh received the MS (1986) and PhD (1991) in Electrical Engineering from the University of Maryland, College Park. He is an Associate Professor with the Department of Computer Science and Information Engineering, National Chiao Tung University. From 1988 to 1991 he participated in the design & implementation of the B2 Secure XENIX for IBM, Federal Sector Division, Gaithersburg, Maryland, USA. He is the designer of the SNP (Secure Network Protocols). Since 1994 he has been a consultant for Computer & Communications Laboratory, Industrial Technology Research Institute, TAIWAN - R.O.C. in network security and distributed operating systems. He is also a consultant for the National Security Bureau, TAIWAN - R.O.C. Dr. Shieh was on the organizing committees of several conferences, such as Int'l Computer Symp, and Int'l Conf. Parallel & Distributed Systems. He was the program chair'n of the Information Security Conf. (INFOSEC'97) and a program-committee member of the ACM Conf. Computer & Communications Security (CCCS'96). His research interests include distributed operating systems, computer networks, and computer security.

Manuscript TR96-063 received 1996 May 6;
revised 1997 March 13, 1997 July 14, 1997 September 17.
Responsible editor: J.B. Dugan
Publisher Item Identifier S 0018-9529(97)09382-2