

Optimal Information Dispersal for Reliable Communication in Computer Networks

Hung-Min Sun and Shiuh-Pyng Shieh

Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 30050

Abstract

In an (m, n) Information Dispersal Scheme (IDS), the sender node decomposes a message M of length L into n pieces S_i , $1 \leq i \leq n$, each of length L/m , such that any m pieces collected by the receiver node over different paths suffice for reconstructing M . Because of variations of network traffic, the number n of available vertex-disjoint paths for the transmission from the sender node to the receiver node may vary in time. It is very difficult to determine the best n and m such that give the highest communication reliability, when given the maximum number of available disjoint paths and an upper bound for the information expansion rate (n/m) . In this research, we discovered several interesting features of (m, n) IDSs which can help reduce the complexity for computing the highest communication reliability. From these findings, we propose a method for determining the optimal IDS.

1: Introduction

In point-to-point interconnected networks in which the nodes are connected by physical links, the sender node needs to transmit a message M to the receiver node. In general, the probability that a node or link will fail is small. However, the probability of a path failing is nonnegligible, since a path from the source node to the destination node may contain many nodes and links. Any broken node or link will lead to the loss of entire messages. An intuitive solution to this problem is to send a message along a path, request a confirmation, and retransmit it along a different path in case of failure. However, retransmission is time-consuming and thus undesirable for communication with time constraint.

*This research was supported by National Science Council of Republic of China under grant No. NSC-83-0404-E-009-106.

Asmuth and Blakley [1] proposed the concept of pooling, splitting, and restituting information. In the same sense, Rabin [13] proposed an information dispersal algorithm that breaks a file F into n pieces, such that any m pieces suffice for reconstructing F . Since then, information dispersal algorithm is applied to fault-tolerant communication in several types of networks, such as hypercube and Omega networks [8,12]. Later, Brickle and Stinson proposed a method of detecting illegal shadows in a threshold scheme [6]. This method can also be used to detect misconstructed pieces of a message. However, none of them study the influence of information dispersal degree (n) , information expansion rate (n/m) , and path success probabilities (P_s) on communication reliability, nor do they address ways to determine the optimal (m, n) IDS to achieve the highest communication reliability.

In this paper, we propose the (m, n) Information Dispersal Scheme (IDS) for fault-tolerant communication in unreliable networks. In an (m, n) IDS, the sender node decomposes a message M of length L into n pieces S_i , $1 \leq i \leq n$, each of length L/m , such that any m pieces collected by the receiver node over vertex-disjoint paths suffice for reconstructing M . We analyze the influence of the information dispersal degree, the information expansion rate, and the path successful probabilities on communication reliability and propose a method of dynamically determining (m, n) to achieve the optimal communication reliability.

It will be proven in Theorem 2 that a higher information expansion rate leads to higher communication reliability when the information dispersal degree is fixed. Therefore it is reasonable to transmit higher priority messages using a higher information expansion rate and lower priority messages using a lower information expansion rate. On the other hand, because of network topology and variations in network traffic, the number n

of available vertex-disjoint paths from the sender node to the receiver node may vary. Hence, given an upper bound for the information expansion rate (depending on the priority of the message) and the number of available vertex-disjoint paths from the sender node to the receiver node, we determine (m, n) so that the highest communication reliability can be achieved. In sections 2 and 3, we define the concept of an information dispersal scheme and propose several fundamental theorems that analyze the influence of n , n/m , and P_s on communication reliability. In section 4, we propose a method for dynamically selecting an (m, n) IDS to achieve optimal communication reliability. Finally, we conclude the paper in section 5.

2: (m, n) information dispersal scheme

In this section, we formally define the (m, n) information dispersal scheme.

Definition 1: An (m, n) *information dispersal scheme* (IDS) is the one which divides the message M of length $L = |M|$ into n pieces S_1, S_2, \dots, S_n , each of length $|S_i| = L/m$, such that M can be reconstructed from any m pieces, for $n \geq m \geq 1$.

The concept of an (m, n) IDS is similar to the concept of an (m, n) threshold scheme [2,3,4,5,10,11,14] in cryptography, in which a master key K is decomposed into n shadows, such that unless m shadows are collected, the master key 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.

Here, we define the information expansion rate of an (m, n) IDS to be the total length of pieces S_i divided by the length of the message M , i.e., $n \cdot \frac{L}{m} \div L = \frac{n}{m}$, and the degree of information dispersal of an (m, n) IDS to be n . The (m, n) information dispersal scheme (IDS) is able to tolerate up to $n-m$ path failures. If the sender node intends to send message M to the receiver node through an unreliable network, it must select n vertex-disjoint (except for the sender and the receiver nodes) paths (each may contain many nodes and links) from the sender node to the receiver node, and then route the S_i from the sender node to the receiver node along these n paths. Thus, the message can still be reconstructed by the receiver node even if up to $n-m$ paths are broken. In addition, with help of IDS, the network load can be balanced. In the next section, we will discuss the fundamental theorems which will lead to the

development of a method that can dynamically determine the optimal (m, n) IDS.

3: Fundamental theorems

In this section we will discuss the influence of n , m and path success probability on communication reliability. First, we study the communication reliability of two classes of IDSs to demonstrate the difficulty of selecting an optimal (m, n) IDS. Each class consists of IDSs with different information dispersal degrees and the same information expansion rate. For example, the $(1, 2)$ IDS and the $(2, 4)$ IDS are in the same class with information expansion rate 2. Next, we will discuss the communication reliability of IDSs with different information expansion rate. We assume that all paths from the sender node to the receiver node have an identical success probability. We define the following:

P_s is the probability that each path transmits the message correctly from the sender node to the receiver node, and

$P_d(m, n)$ is the probability that the receiver node correctly reconstructs M by using the (m, n) IDS, that

$$\text{is, } P_s(m, n) = \sum_{i=m}^n C_i^n \cdot (P_s)^i \cdot (1 - P_s)^{n-i}.$$

[Note that $P_d(m, n)$ increases as P_s increases for an (m, n) IDS.] Obviously, the conventional method uses a $(1, 1)$ IDS to transmit messages from the sender node to the receiver node. Its communication reliability $P_d(1, 1) = P_s$. Similarly, the communication reliabilities of the class of (m, m) IDSs which have the same information expansion rate 1 can be obtained as follows: $P_d(2, 2) = P_s^2$, $P_d(3, 3) = P_s^3$, ..., $P_d(m, m) = P_s^m$. It is clear that $P_d(m, m) - P_d(n, n) = P_s^m - P_s^n = P_s^m \cdot (1 - P_s^{n-m}) > 0$ if $m < n$ and $0 < P_s < 1$. The communication reliability curves for a $(1, 1)$ IDS, $(2, 2)$ IDS, and $(3, 3)$ IDS are shown in Figure 1.

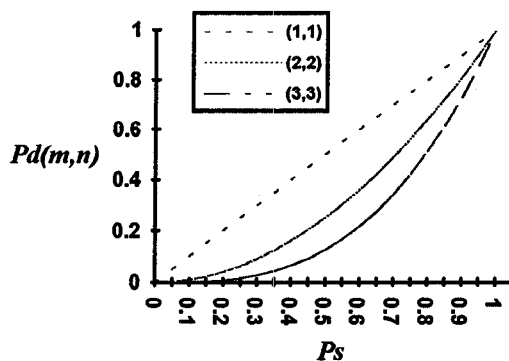


Figure 1: The communication reliability curves for a (1,1) IDS, (2,2) IDS, and (3,3) IDS.

It is clear that the communication reliability of an (m, m) IDS for a fixed P_s ($0 < P_s < 1$) decreases as m increases. It is also clear from the communication reliability curves in Figure 1 that the communication reliability cannot be improved as the degree of information dispersal increases under the information expansion rate 1.

The class of $(m, 2m)$ IDSs has the information expansion rate 2. The communication reliabilities of a (1, 2) IDS and (2, 4) IDS can be formulated as follows and the relationship between them is shown in Figure 2:

$$P_d(1, 2) = C_2^2 \cdot P_s^2 + C_1^2 \cdot P_s \cdot (1 - P_s),$$

$$P_d(2, 4) = C_4^4 \cdot P_s^4 + C_3^4 \cdot P_s^3 \cdot (1 - P_s) + C_2^4 \cdot P_s^2 \cdot (1 - P_s)^2,$$

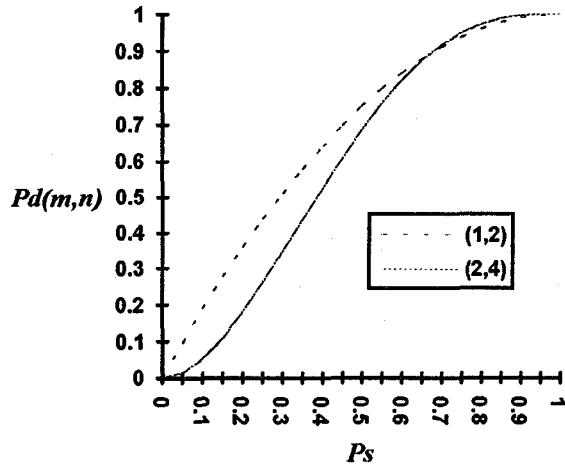


Figure 2: The communication reliability curves for a (1,2) IDS and (2,4) IDS.

It is interesting that

- if $P_s > 2/3$, then $P_d(1, 2) < P_d(2, 4)$,
- if $P_s = 2/3$, then $P_d(1, 2) = P_d(2, 4)$,
- if $P_s < 2/3$, then $P_d(1, 2) > P_d(2, 4)$.

This means that a (2,4) IDS is more reliable than a (1,2) IDS if the probability P_s of each path successfully transmitting a message from the sender node to the receiver node is larger than $2/3$, and a (1,2) IDS has better communication reliability than a (2,4) IDS if P_s is smaller than $2/3$. We will prove in Theorem 3 that for any two communication reliability curves of (k_1, m, k_1, n) IDS and (k_2, m, k_2, n) IDS, where n is greater than m ,

there exists one and only one intersection, and P_s of the intersection is less than 1 and greater than 0.

From observation of results, we have discovered several interesting properties of IDSs. We analyze these properties and propose three fundamental theorems that can help us to discover the optimal IDS. In Theorem 1, we show prove that the communication reliability of an $(m, n+k)$ IDS is higher than that of an (m, n) IDS. The theorem states that if more pieces of the message are sent, but the same number need to be received in order to recover the message, then communication reliability is improved.

Theorem 1: $P_d(m, n) < P_d(m, n+k)$ for $k \geq 1$ and $0 < P_s < 1$.

In Theorem 2, we show that the communication reliability when using an (m, n) IDS to transmit a message is higher than that when using an $(m+k, n)$ IDS. The theorem states that if the same number of pieces of the message are sent, but more number need to be received in order to recover the message, then communication reliability is decreased. Note that this does not imply that any IDS with a higher information expansion rate always has higher communication reliability than an IDS with a lower information expansion rate.

Theorem 2: $P_d(m, n) > P_d(m+k, n)$, for $k \geq 1$ and $0 < P_s < 1$.

In Theorem 3, we show that the communication reliability when using an (m, n) IDS to transmit a message is higher than that when using an $(m+k, n+k)$ IDS.

Theorem 3: $P_d(m, n) > P_d(m+k, n+k)$ for $k \geq 1$ and $0 < P_s < 1$.

In the next section, we will present a method that uses the properties described in the theorems above to reduce the complexity of finding the optimal (m, n) IDS constrained by $n \leq$ (number of available vertex-disjoint paths) and $\frac{n}{m} \leq$ (upper bound for information expansion rate).

4: Optimal (m, n) IDS

In this section, we will provide means for dynamically determining the optimal (m, n) IDS with the highest communication reliability constrained by $n \leq$ (number of available vertex-disjoint paths) and $\frac{n}{m} \leq$ (upper bound

for information expansion rate). From Theorem 2, it is clear that an (m_1, n) IDS has higher communication reliability than an (m_2, n) IDS if $m_1 < m_2$. So, it is reasonable to transmit higher priority messages at a higher information expansion rate and lower level messages at a lower information expansion rate (note that this doesn't imply that any IDS with a higher information expansion rate always has a higher communication reliability than an IDS with a lower information expansion rate). On the other hand, because of variations in network traffic, the number of available vertex-disjoint paths from the sender node to the receiver node may vary. We will propose methods for determining the optimal IDS when an upper bound on the information expansion rate (depending on the priority of the message) and the number of available vertex-disjoint paths are given.

When given an upper bound for the information expansion rate, u , and the number of available vertex-disjoint paths, v , the feasible IDS set is defined as the set of all possible IDSs that satisfy these conditions. It is clear that the optimal IDSs in each range of P_s are elements of the feasible IDS set.

Definition 2: A feasible IDS set, $F_{u,v}$, with an upper bound of information expansion rate, u , and the number of available vertex-disjoint paths, v , is $\{(m, n) \text{ IDS} \mid \text{for all } m, n \in \mathbb{N}, 1 \leq \frac{n}{m} \leq u, n \leq v, 1 \leq m \leq n\}$.

If $u = 1$, the feasible IDS set $F_{u,v} = \{(m, m) \text{ IDS} \mid 1 \leq m \leq v, m \in \mathbb{N}\}$.

If $u > 1$, the feasible IDS set $F_{u,v}$ can be described as the union of a number of partitions. Each partition consists of all (m, n) IDSs for which $n-m$ is a constant. That is,

$$F_{u,v} = \{ (m, m) \text{ IDS} \mid 1 \leq m \leq v, m \in \mathbb{N} \} \\ \cup \{ (m, m+1) \text{ IDS} \mid \lceil \frac{1}{u-1} \rceil \leq m \leq v-1, m \in \mathbb{N} \} \\ \vdots \\ \cup \{ (m, m+i) \text{ IDS} \mid \lceil \frac{i}{u-1} \rceil \leq m \leq v-i, m \in \mathbb{N} \} \\ \vdots \\ \cup \{ (m, m+t) \text{ IDS} \mid \lceil \frac{t}{u-1} \rceil \leq m \leq v-t, m \in \mathbb{N} \}$$

where t satisfies

$$\lceil \frac{t}{u-1} \rceil \leq v-t \text{ and } \lceil \frac{(t+1)}{u-1} \rceil > v-t-1 \\ (\lceil \lceil \rceil \text{ denotes the ceiling function}).$$

As Theorem 1, 2, and 3 state, many IDSs of a feasible IDS set are not optimal in any range of P_s . Therefore, a feasible IDS set can be reduced so that all optimal IDSs are still included in the reduced feasible IDS set. It is clear that the reduced feasible IDS set is a subset of the feasible IDS set. For any P_s , the optimal IDS of $F_{u,v}$ will be an element of the reduced $F_{u,v}$.

By Theorem 3, for each partition

$$\{(m, m+i) \text{ IDS} \mid \lceil \frac{i}{u-1} \rceil \leq m \leq v-i, m \in \mathbb{N}\},$$

$(\lceil \frac{i}{u-1} \rceil, \lceil \frac{i}{u-1} \rceil + i)$ IDS has the highest communication reliability among them. Therefore, $F_{u,v}$ can be reduced to

$\{(1, 1) \text{ IDS}\}$ if $u = 1$, and

$$\{(1, 1) \text{ IDS}\} \cup \{ (\lceil \frac{i}{u-1} \rceil, \lceil \frac{i}{u-1} \rceil + i) \text{ IDS} \mid 1 \leq i \leq t \}$$

if $u > 1$.

We compare the size of the feasible IDS set with that of the reduced feasible IDS set as follows.

If $u = 1$, it is clear that the size of the feasible IDS set is $O(v)$ and the size of the reduced feasible IDS set is $O(1)$.

If $u > 1$, then the size of the reduced feasible IDS set is $t+1$, where t satisfies $\lceil \frac{t}{u-1} \rceil \leq v-t$ and $\lceil \frac{(t+1)}{u-1} \rceil > v-t-1$. Hence, t must satisfy

$$\frac{t}{u-1} \leq v-t \text{ and } \frac{t+1}{u-1} + 1 > v-t-1. \text{ This implies that} \\ v \cdot \frac{u-1}{u} + \frac{1}{u} - 1 < t+1 \leq v \cdot \frac{u-1}{u} + 1. \text{ Therefore, the size of} \\ \text{the reduced feasible IDS set is } O(v).$$

The size of the feasible IDS set

$$= (v-1 - \lceil \frac{1}{u-1} \rceil + 1) + \dots + (v-t - \lceil \frac{t}{u-1} \rceil + 1) \\ \geq (v-1 - \frac{1}{u-1} - 1 + 1) + \dots + (v-t - \frac{t}{u-1} - 1 + 1) \\ = [(v-1) + (v-2) + \dots + (v-t)] - (1+2+\dots+t)/(u-1) \\ = \frac{t(2v-t-1)}{2} - \frac{t(t+1)}{2(u-1)} \\ = \frac{t(2v-t-1)(u-1) - t(t+1)}{2(u-1)} \\ = \frac{2vt(u-1) - t(t+1)u}{2(u-1)}$$

$$= vt - \frac{1}{2}t(t+1) \cdot \frac{u}{u-1}.$$

Because $v \cdot \frac{u-1}{u} + \frac{1}{u} - 2 < t \leq v \cdot \frac{u-1}{u}$, it is clear that $v \cdot \frac{u-1}{u} - 2 < t \leq v \cdot \frac{u-1}{u}$. Let $t = v \cdot \frac{u-1}{u} - c$, where $0 \leq c < 2$. Therefore, $vt - \frac{1}{2}t(t+1) \cdot \frac{u}{u-1} = \frac{1}{2}(v^2 \cdot \frac{u-1}{u} - v - c^2 \cdot \frac{u}{u-1} + \frac{u}{u-1})$. Because $u > 1$, the size of the feasible IDS set is $O(v^2)$, which is larger than the size of the reduced feasible IDS set $O(v)$.

As an example, let $u = 1.4$ and $v = 12$.

The feasible IDS set $F_{1.4, 12}$

$$= \{ (m, m) \text{ IDS} \mid 1 \leq m \leq 12, m \in \mathbb{N} \} \\ \cup \{ (m, m+1) \text{ IDS} \mid 3 \leq m \leq 11, m \in \mathbb{N} \} \\ \cup \{ (m, m+2) \text{ IDS} \mid 5 \leq m \leq 10, m \in \mathbb{N} \} \\ \cup \{ (m, m+3) \text{ IDS} \mid 8 \leq m \leq 9, m \in \mathbb{N} \}.$$

Thus, $F_{1.4, 12}$ can be reduced to be $\{ (1,1) \text{ IDS}, (3,4) \text{ IDS}, (5,7) \text{ IDS}, (8,11) \text{ IDS} \}$.

Every IDS in the reduced feasible IDS set may be the optimal IDS depending on the exact value of probability P_s . Therefore, we can determine the optimal (m, n) IDS by only comparing the communication reliabilities between the elements of the reduced feasible IDS set. The complexity for computing the highest communication reliability is reduced from $O(v^2)$ to $O(v)$ when the upper bound for the information expansion rate is larger than 1, or from $O(v)$ to $O(1)$ when the upper bound for the information expansion rate is equal to 1. Therefore, our method provides the advantage of reducing the complexity of finding the optimal IDS with the highest communication reliability.

5: Conclusions

In this paper, we propose a method for dynamically determining the optimal (m, n) IDS for message transmission in unreliable networks. In the course of our analysis, we discovered several novel features of (m, n) IDSs which can help reduce the complexity of finding the optimal IDS with the highest communication reliability. Based on the theorems given here, we have developed a method that reduces the complexity for computing the highest communication reliability from $O(v^2)$ to $O(v)$ when the upper bound for the information expansion rate is larger than 1, or from $O(v)$ to $O(1)$

when the upper bound for the information expansion rate is equal to 1.

References

- [1] Asmuth, C. A. and Blakley, G. R., "Pooling splitting and restituting information to overcome total failure of some channels of communication," IEEE Proceedings of the 1982 Symposium on Security and Privacy, New York, 1982, pp. 156-169.
- [2] Asmuth, C. and Bloom, J., "A Modular Approach to Key Safeguarding," IEEE Trans. on Inform. Theory, Vol. IT-29, No. 2, pp. 208-210, 1983.
- [3] Benaloh, J. C. and Leichter, J., "Generalized Secret Sharing and Monotone Functions," Proceeding of CRYPTO'88, Springer-Verlag.
- [4] Blakley, G. R., "Safeguarding Cryptographic Keys," Proc. NCC, Vol. 48, AFIPS Press, Montvale, N. J., pp. 313-317, 1979.
- [5] Blakley, G.R. and Meadows, C., "Security of Ramp Schemes," CRYPTO'84, Springer-Verlag, Berlin, 1985, pp. 411-431.
- [6] Brickle, E. F. and Stinson, D. R., "The Detection of Cheaters in Threshold Schemes," Proc. Crypto '88, Springer-Verlag, 1989, pp. 564-577.
- [7] Denning, D. E. R., Cryptography and Data Security, Addison-Wesley, Reading, MA, 1983.
- [8] Gargano, L., Rescigno, A. A. and Vaccaro, U., "Fault-Tolerant Hypercube Broadcasting via Information Dispersal," Networks, Vol. 23, pp. 271-282, 1993.
- [9] Hamming, R. W., Coding and Information Theory, Englewood Cliffs, Reading, NJ: Prentice-Hall, 1986.
- [10] Karnin, E. D., Greene, J. W. and Hellman, M. E., "On Secret Sharing Systems," IEEE Trans. on Inform. Theory, Vol. IT-29, pp. 35-41, 1983.
- [11] Kothari, S. C., "Generalized Linear Threshold Scheme," Proceeding of CRYPTO'84, Springer-Verlag, pp. 231-241.
- [12] Lyuu, Y.-D., "Fast Fault-Tolerant Parallel Communication for de Bruijn and Digit-Exchange Networks Using Information Dispersal," Networks, Vol. 23, pp. 365-378, 1993.
- [13] Rabin, M. O., "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance," J. of ACM, Vol. 36, No. 2, April 1989, pp. 335-348.
- [14] Shamir, A., "How to share a secret," Comm. ACM, Vol. 22, no. 11, pp. 612-613, 1979.