On the Availability of Information Dispersal Scheme for Distributed Storage Systems*

Sung Keun Song[1], Hee Yong Youn[1], Gyung-Leen Park[2], and Kang Soo Tae[3]

[1]School of Information and Communications Engineering, Sungkyunkwan University
Suwon, Korea
kskk103@skku.edu, youn@ece.skku.ac.kr

[2]Department of Computer Science and Statistics, Cheju National University,
Cheju, Korea
kstae@jeonju.ac.kr

[3]Dept. of Computer Engineering, Jeonju University, Korea
glpark@cheju.ac.kr

Abstract. For distributed storage systems the way how the data are replicated and distributed significantly affects availability, security, and performance. Here many factors such as the number of nodes and partitions, replications, node survivability, etc. are interrelated. This paper investigates the availability of Information Dispersal Scheme that can be used for distributed storage system. It will help construct a large distributed system allowing high availability.

1 Introduction

The survivable storage system [1-2] requires to encode and distribute data over multiple storage nodes to survive failures and malicious attacks. It also needs to replicate data to enhance availability. For distributed storage systems the way how the data are replicated and distributed significantly affects the availability, security, and performance.

There exist various data replication and distribution schemes such as replication, splitting, information dispersal, and secret sharing [3-8]. The schemes display different availability, security, and performance trade-off since many factors such as the number of nodes, storage space, operation speed, etc. affect each other. Therefore, finding an optimal scheme for a given condition is very difficult. In this paper we formally define a data replication and distribution scheme called information dispersal scheme (IDS), and investigate the availability of the IDS for deciding an optimal IDS with a given condition. It will help construct a large distributed system allowing

* This work was supported in part by 21C Frontier Ubiquitous Computing and Networking, Korea Research Foundation Grant (KRF - 2003 - 041 - D20421) and the Brain Korea 21 Project in 2003. Corresponding author: Hee Yong Youn

M. Bubak et al. (Eds.): ICCS 2004, LNCS 3036, pp. 453–457, 2004.

high availability. The rest of the paper is organized as follows. Section 2 investigates the availability of the IDS. We conclude the paper in Section 3.

2 The Availability of IDS

The basic properties of IDS are reported in [9]. This section focuses on the availability of IDS. The notations are as follows. The (m, n)-IDS is a data distribution scheme where m pieces of the original data are replicated into n pieces which are stored in n nodes respectively.

$k(=n/m)$	Information Expansion Ratio (IER); $k \geq 1$
P	node survivability; $0 < P < 1$
$P(m, n)$	availability of the (m, n)-IDS
$P^*((i, j), (m, n))$	critical node survivability which allows $P(i, j)=P(m, n)$
$Class_i$	all IDS's whose k is i
$(m, n)_{(i, j)}$-IDS	boundary IDS of $Class_{n/m}$; for example, if $m > s$ and $n > t$, (i, j)-IDS and (s, t)-IDS of $Class_{n/m}$ do not have a critical node survivability. However, if $m \leq s$ and $n \leq t$, there exists a critical node survivability.

Availability of (m, n)-IDS is as follows [9-10].

$$P(m, n) = \left(\sum_{i=1}^{k} \binom{k}{i} P^i (1-P)^{k-i} \right)^m, \quad k = \frac{n}{m} \text{ (In what follows } k \text{ is assumed to be an integer)} \tag{1}$$

Some important properties of IDS based on this availability formula are as follows.

Theorem 1: If m and n increase by the same ratio, the availability decreases. Say,

$$P(k_1 m, k_1 n) > P(k_2 m, k_2 n) \text{ if } k_1 < k_2 \tag{2}$$

Proof: $(k_1 m, k_1 n)$-IDS and $(k_2 m, k_2 n)$-IDS have the same IER and belong to the same class. Then,

$$P(m, n) > P(m+i, n+j) \text{ if } k=n/m=(n+j)/(m+i),\ i, j \geq 1$$

Therefore, $P(k_1 m, k_1 n) > P(k_2 m, k_2 n)$. ■

Theorem 2: For two IDS's, A and B, if the number of partitions of A is smaller than that of B while the k value of A is larger, then the availability of A is larger than that of B. Say,

$$P(i, j) > P(m, n) \text{ if } i < m \text{ and } j/i \geq n/m \tag{3}$$

Proof: If $j/i = n/m$, then this is the following case.

$$P(m, n) > P(m+i, n+j) \text{ if } k=n/m=(n+j)/(m+i),\ i, j \geq 1$$

If $j/i > n/m$, then $j > (ni)/m$. Since $P(m, n) < P(m, n+mi)$ for $i > 1$, $P(i, j) > P(i, (ni)/m)$. $P(i, (ni)/m) > P(m, n)$ due to Theorem 1 since $((ni)/m)/i = n/m$. As a result, $P(i, j) > P(m, n)$. ■

Theorem 2 reveals that availability increases if the number of partitions decreases and the number of replications increases.

Theorem 3: Given $Class_a$ and $Class_b$ of different IER values, if $a < b$, an $(m, n)_{(i, j)}$-IDS of $Class_b$ always exists, where $m > i$ and $n > j$. If $a > b$, an $(m, n)_{(i, j)}$-IDS exists, where $m < i$ and $n < j$.

Proof: In the case of $a < b$, if m and n are smaller than i and j respectively, for all P ranges, (m, n)-IDS is more available than (i, j)-IDS by Theorem 2. That is, critical node survivability does not exists. Note that if $l \to \infty$, $P(l, bl) \to 0$ by Theorem 1. Therefore, a boundary IDS, $(m, n)_{(i, j)}$-IDS exists, where $m > i$ and $n > j$. Similarly, in the case of $a > b$, if m and n are larger than i and j respectively, for all P ranges, (i, j)-IDS is more available than (m, n)-IDS by Theorem 2. If $l \to 0$, $P(l, bl) \to 1$ by Theorem 1. Therefore, a boundary IDS, $(m, n)_{(i, j)}$-IDS exists, where $m < i$ and $n < j$. ■

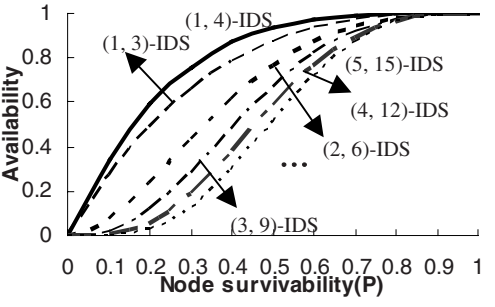
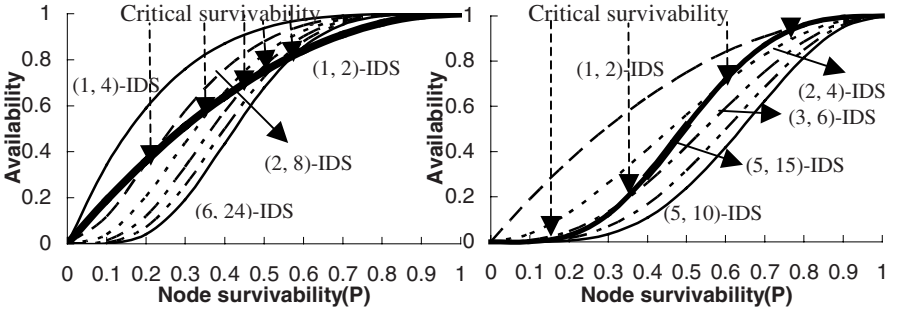


Fig. 1. The availabilities for (1, 4)-IDS and IDS's of $Class_3$

We know that if (m, n)-IDS and $Class_a$ do not have a boundary IDS and the IER of the (m, n)-IDS is larger than a, the (m, n)-IDS is more available than all IDS's of $Class_a$ for entire P range. Fig. 1 shows an example of Theorem 3. Generally, the IDS of (1, 1), (1, 2), (1, 3), ⋯, (1, n) and the classes that have smaller IER's than (m, n)-IDS do not have a boundary IDS.



(a) (b)

Fig. 2. The availabilities for (1, 2)-IDS and the IDS's of $Class_4$ and the availabilities for (5, 15)-IDS and the IDS's of $Class_2$

Theorem 4: Suppose that an (i, j)-IDS of $Class_a$ and $Class_b$ have $(m, n)_{(i, j)}$-IDS of $Class_b$ and $a < b$. If m and n increase, critical node survivability converges to 1. On the contrary, suppose that an (i, j)-IDS of $Class_a$ and $Class_b$ have $(m, n)_{(i, j)}$-IDS and $a > b$. If m and n increase, critical node survivability converges to 0.

$$P^*((i, j), (m, n)) \rightarrow 1 \text{ if } j/i < n/m \text{ and } m,n \rightarrow \infty$$
$$P^*((i, j), (m, n)) \rightarrow 0 \text{ if } j/i > n/m \text{ and } m,n \rightarrow \infty \quad (4)$$

Proof: The IDS of the largest availability in the $Class_b$ is $(1, b)$-IDS by Theorem 1. Here, if $l \rightarrow \infty$, $P(l, bl) \rightarrow 0$. Therefore, when m and n increase, while $a < b$, critical node survivability of (i, j)-IDS of $Class_a$ and $(m, n)_{(i, j)}$-IDS converges to 1. If $a > b$, it converges to 0. ■

Fig. 2 shows an example that critical node survivability converges to 1 or 0, respectively. In Fig. 2(a), the $(m, n)_{(1, 2)}$-IDS is (2, 8)-IDS. Also, the (1, 4)-IDS and (1, 2)-IDS do not have critical node survivability. In Fig. 2(b), the $(m, n)_{(5, 15)}$-IDS is (4, 8)-IDS. Also the (5, 10)-IDS and (5, 15)-IDS do not have critical node survivability. Using these properties, an IDS allowing the highest availability can be determined for a given condition.

3 Conclusion

In this paper we have studied the availability of information dispersal schemes that can be used for survivable storage systems. It will help construct a large distributed system allowing high availability. In the study, we made some assumptions in deriving the models. We will develop a more vigorous model without such assumptions which allows the best IDS in real environment. We will also investigate the properties of IDS in terms of both security and availability with which secure and highly available IDS can be obtained.

References

1. Wylie, J.J., Bigrigg, M.W., Strunk, J.D., Ganger, G.R., Kiliccote, H., Khosla, P.K.: Survivable information storage systems. IEEE Computer. (2000) 61-68
2. Wylie, J.J, Bakkaloglu, M., Pandurangan, V., Bigrigg, M.W., Oguz, S., Tew, K., Williams, C., Ganger, G.R., Khosla, P.K.: Selecting the Right Data Distribution Scheme for a Survivable Storage System. Technical Report CMU-CS-01-120 Carnegie Mel-lon University. (2001)
3. Choi, S.J., Youn, H.Y., Choi, J.S.: An Efficient Dispersal and Encryp-tion Scheme for Secure Distributed formation Storage, International Conference on Computational Science, Springer-Verlag, (2003) 958-967
4. Rabin, M.O.: Efficient Dispersal of Information for Security. Load Balancing and Fault Tolerance. ACM (1989) 335-348

5. Shamir, A.: How to Share a Secret: Comm. ACM. (1979) 612-613
6. Blakley, G.R., Catherine Meadows: Security of ramp scheme: Advances in Cryptol-ogy, Springer-Verlag, (1985) 242-268
7. Karnin, E., Greene, J., Hellman, M.: On Secret Sharing Systems: IEEE Trans. Informa-tion Theory (1983) 35-41
8. A. De Santis and B. Masucci: Multiple Ramp Schemes: IEEE Trans. Information Theory (1999) 1720-1728
9. Song, S.K., Youn, H.Y., Park, J.K.: Deciding Optimal Information Dispersal for Parallel Computing with Failures: International Conference on Parallel Computing Technologies, Springer-Verlag, (2003) 332-335
10. Hung-Min Sun., Shiuh-Pyng Shieh.: Optimal Information Dispersal for Increasing the Reliability of a Distributed Service. IEEE Trans. Vol. 46. (1997) 462-472