효율적인 결함허용 시스템 설계를 위한 탐색기법*

이효순○ 신현식
서 울 대 학 교 컴 퓨 터 공 학 과
{fanta, shinhs}@cselab.snu.ac.kr

Search Technique for the Design of Cost Effective Fault Tolerant Systems

Hyosoon Lee○ Heonshik Shin
Dept. of Computer Engineering, Seoul National University

요 약

결함허용 시스템은 다양한 형태의 중복을 사용하여 신뢰도를 향상시킬 수 있는 반면, 시스템의 비용을 크게 증가시킨다. 본 논문은 만족스러운 신뢰도를 갖추면서 추가 비용을 적게 요구하는 결함허용 컴퓨터 시스템의 구조를 결정하기 위한 설계 문제를 정의하고 탐색에 기반을 둔 해결법을 제안한다. 이 때, 탐색 기법이 방문하는 탐색 공간의 크기를 줄이기 위하여 사용되는 세 가지의 유용한 사실을 설명한다. 이를 바탕으로 삼중 모듈 중복(TMR: Triple-Modular-Redundancy), 백업 예비(backup sparing), 그리고 혼합 중복(hybrid redundancy) 기법과 같은 결함허용 기법들이 시스템 구조에 적용되었을 때, 탐색 공간을 줄이는 용도로 사용될 수 있는 신뢰도 제약조건을 유도해낸다.

1. 서론

신뢰도는 비행시스템과 우주선 제어, 원격 통신, 그리고 OLTP와 같은 시스템에서 아주 중요한 척도이다. 이들 의존적인 컴퓨터 시스템들은 기능성뿐만 아니라 동작 수행 중에 결함이 발생했을 경우에도 올바르게 동작을 지속할 수 있도록 중복성을 채택하고 있다([1], [2], [3]). 어느 자원에 어떤 중복기법을 적용하여야 하는가의 문제는 시스템의 요구사항에 따라 좌우된다. 앞으로 중복기법이 적용되는 시스템내의 부분을 **부시스템**이라고 부르기로 하자. 부시스템은 프로세서 모듈, 메모리 모듈 등과 같이 기능의 종류에 의해 나뉘어 질 수 있다. 각 부시스템에 얼마나 많은 중복성을 부여하여야 하는가는 감내되어야 할 결함의 수/양에 의해서 결정된다. 적용 가능한 중복기법의 종류는 부시스템의 종류와 결함 모델에 따라서 다르다. 예를 들면, 메모리 부시스템의 경우 다중 모듈 중복(NMR: N-Modular-Redundancy) 기법보다는 ECC(Error Correction Coding) 기법을 적용하는 것이 훨씬 더 저렴하면서도 충분한 신뢰도 향상을 가져올 수 있지만, NMR이 ECC기법보다 더 많은 종류의 결함을 감내할 수 있다. 중복기법이 적용된 부시스템은 일련의 **구성요소**로 구성된다. TMR 기법이 적용된 경우, 부시스템은 세 개의 기능 모듈과 하나의 투표기(voter)를 구성요소로 가진다고 볼 수 있다.

시스템 설계자들은 결함의 종류와 양에 대한 요구사항을 검토하고 이 요구 사항을 만족하는 시스템을 설계한다. 그러나, 각 부시스템에 적용할 수 있는 중복기법은 여러 가지이므로, 시스템의 비용, 성능, 신뢰도를 비롯한 여러 척도들을 바탕으로 각 중복기법들의 장·단점을 비교 평가하여야 한다. 만약 초기 설계된 시스템이 충분한 신뢰도를 가지지 못할 경우, 설계자는 신뢰도를 향상시키기 위해서 어떤 구성요소들의 신뢰도를 향상시켜야 하는지 살피거나 부시스템에 적용할 중복기법을 변경함으로써 시스템의 구조를 바꾸어야 한다. 그러나, 컴퓨터 시스템에 중복성을 도입하는 것은 추가 비용을 요구하는 일이다. 이 비용은 중복기법의 종류와 중복의 정도에 따라서 증가하게 되므로, 설계자는 전체 비용을 최소화하도록 중복기법을 취사선택하여야 한다. 높은 신뢰성을 요구하는 시스템 설계에 있어서 신뢰도와 비용사이의 체계적인 비교 분석이 필요함에도 불구하고 설계자들은 이제까지 다소 경험과 직관에 의존해왔다. 본 논문에서는 이러한 시스템 설계의 문제를 형식화하고 비용을 최소화하는 시스템 구조를 탐색하는 방법을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 만족할 만한 신뢰도를 가지면서 최소의 비용을 가지는 시스템의 구조를 찾기 위한 문제를 설명한다. 3장에서는 2장에서 설명하는 문제에 대한 탐색 방법과 탐색공간의 크기를 줄일 수 있는 방법을 제안한다. 아울러, 이 방법들을 대표적인 중복기법인 TMR, 백업 예비 기법, 그리고 혼합 중복 기법에 적용한 결과를 보인다. 마지막으로, 4장에서는 본 논문의 결과를 요약한다.

*본 연구는 국방과학연구소 및 서울대 자동제어특화연구센터의 연구비 지원에 의한 연구결과입니다.

2. 문제 정의

이 장에서는 비용을 최소화하면서 시스템 신뢰도의 목표를 만족시키기 위하여 각 부시스템의 신뢰도를 탐색하는 문제를 정의한다. 시스템 설계자가 초기에 n개의 부시스템으로 구성되는 초기 시스템의 구성과 신뢰도 요구값을 입력으로 준다고 가정하자. 이 때, COTS(Commercial Off-The-Shelf) 구성요소들이 기본단위가 되고, 이들의 신뢰도와 비용은 미리 알려져 있다고 하자. 만약 초기 시스템의 신뢰도가 요구값을 만족시키지 못한다면 부시스템에 결함허용 기법을 적용하여 신뢰도가 요구값 이상으로 향상되도록 시스템의 구조를 수정하여야 한다. 결함허용 기법 FT가 부시스템 S_i에 적용되었을 때, 부시스템 S_i를 구성하는 m개의 구성요소를 $\{C_{1,i,r}, C_{2,i,r}, ..., C_{m_i,r}\}$이라고 하자. 시스템의 신뢰도 목표 값을 ρ, R_i와 $R_{k,i,r}$를 부시스템 S_i와 구성요소 $C_{k,i,r}$의 신뢰도라고 하자. $C_T(R_1, R_2, ..., R_n)$와 $R_T(R_1, R_2, ..., R_n)$는 각각 부시스템 S_i가 신뢰도 R_i를 가질 때의 총 비용과 시스템의 신뢰도를 나타낸다고 하자. 모듈간의 상호 연결에 대한 비용을 무시하면, C_T는 각 부시스템들의 비용을 합한 것과 같다. $R_1, R_2, ..., R_n$의 값을 동시에 얻기 위한 탐색 문제는 다음과 같이 정의할 수 있다.

목표:모든 FT에 대해서 $C_T(R_1, R_2, ..., R_n)$의 최소값 탐색
제약: $\rho \le R_T(R_1, R_2, ..., R_n)$

부시스템이 여러 개의 낮은 수준 부시스템으로 구성된 경우에는 위의 문제를 재귀적으로 확장함으로써 간단하게 수용할 수 있다. 여기서는 부시스템의 수준이 하나라고 가정하자. 이 문제는 다중변수, 비선형 최적화 문제이며 일반적으로 분석적인 방법으로는 해결할 수 없다[4]. 그러나, 부시스템과 구성요소들의 비용과 신뢰도가 유한한 이산 값들을 가진다고 가정하면 알고리즘으로 문제를 풀 수 있다.

3. 탐색 기법

시스템 구조는 통상 조합모델이나 상태공간모델로 표현될 수 있다[5, 6, 7]. 조합모델로는 보통 결함나무(fault tree)를, 그리고 상태공간모델로는 마르코프 체인(Markov chain)이 사용된다. 이들 모델을 사용하여 결함나무의 경우는 종단 노드에, 마르코프 체인의 경우에는 전이 확률과 각 상태에 값을 할당하여 전체 시스템의 비용과 신뢰도를 산출할 수 있다. 따라서, 이들 모델을 사용하여 모든 시스템 대안에 대한 비용과 신뢰도를 산출할 수 있고, 이를 근거로 가장 저렴한 구조를 탐색할 수 있다. 하지만, 이 방법은 복잡도가 크기 때문에 실용성이 부족하다. 따라서, 가능한 탐색 공간을 최소화하여야 한다.

우리는 시스템 신뢰도의 목표 값을 만족시키는 부시스템과 구성요소들의 신뢰도 범위를 줄이기 위하여 사용할 수 있는 추가의 제약조건들을 고안하였다. 시스템의 신뢰도는 부시스템들의 신뢰도에 대한 함수로 표현된다. 마찬가지로 부시스템의 신뢰도는 각 구성요소들의 신뢰도를 통하여 산출된다. 그러므로, 시스템이 가져야 하는 신뢰도 목표 값은 각 부시스템과 구성요소들이 가져야 하는 신뢰도에 대해 제약성을 가지게 된다. 우리는 각 구성요소들의 탐색 대상이 되는 신뢰도의 범위를 감소시키고 구성요소들과의 관계를 유도하는데 유용하게 사용할 수 있는 아래의 몇 가지 사실을 관찰하였다.

(C-1) 한 부시스템/구성요소는 다른 모든 부시스템/구성요소들이 완벽한 신뢰도를 가질 때, 가장 작은 신뢰도 요구값을 가진다. 즉,

$$R_T(1, 1, ..., R_i, ..., 1) \le \rho.$$

$$R_S(1, 1, ..., R_{k,i,r}, ..., 1) \le \rho_i$$

(C-2) 결함허용기법 FT는 부시스템의 신뢰도를 향상시킬 수 있는 경우에만 적용되어야 한다. 즉,

$$\frac{R(R_{1,i,r}, R_{2,i,r}, ..., R_{m_i,r})}{FT \text{ 적용 전의 부시스템 } S_i\text{의 신뢰도}} > 1$$

(C-3) 구성요소의 신뢰도 요구값의 범위는 다른 구성요소들의 범위가 주어졌을 때 개선될 수 있다.

첫 번째 사실은 시스템의 전체 신뢰도가 모든 부시스템과 구성요소들의 신뢰도에 따라 단조 증가한다는 점에 근거를 두고 있다. 두 번째는 시스템 설계자가 시스템의 신뢰도 향상 이득을 얻을 수 있는 경우에 한해서 결함허용 기법을 적용한다는 사실로부터 기인한다. 마지막 사실은 각 구성요소들의 필요 신뢰도 값의 범위는 다른 것들의 신뢰도에 영향을 받는다는 점에 기인한다. 다시 말하면, 한 구성요소가 충분히 높은 신뢰도를 가진다면 다른 구성요소는 그만큼 낮은 신뢰도를 가져도 된다는 것이다. 이제 이러한 관찰들을 이용하여 널리 사용되는 하드웨어 중복 기법들에 대하여 2장에서 정의한 문제에 새로운 제약조건들을 추가한다.

3.1 중복 기법에의 적용

본 장에서는 대표적인 중복 기법인 TMR, 백업 예비 기법, 그리고 혼합기법에 대하여 탐색 공간을 줄이기 위하여 추가할 수 있는 제약조건들을 유도한다. R_{var}, R_v, R_a를 각각 기능모듈, 투표기(voter), 수용성 검사기(acceptance tester)의 신뢰도라 하고, ρ_i를 시스템의 목표 신뢰도 값 ρ를 만족시키기 위한 부시스템 S_i의 목표 신뢰도 값이라고 하자.

TMR 기법의 경우, 기법이 적용되는 부시스템의 신뢰도는 $(3R_{var}^2 - 2R_{var}^3)R_v$이다. (C-1)에 의해서 다음과 같은 제약조건을 추가할 수 있다.

$$R_v \geq \rho_i$$
$$R_{var} \geq 3R_{var}^2 - 2R_{var}^3 - \rho_i = 0 \text{ 의 해}$$

(C-2)에 의해서는 다음 조건이 만족되어야 한다.

$$1 \leq \frac{(3R_{var}^2 - 2R_{var}^3)R_v}{R_{var}} \leq \frac{9}{8}R_v$$

R_{var}의 신뢰도가 고정되었다고 할 때, (C-3)에 의하여, 다음과 같은 추가의 제약조건을 이용하여 탐색공간을 줄일 수 있다.

$$R_v \geq \max\left(\rho_i, \frac{8}{9}, \frac{\rho_i}{3R_{var}^2 - 2R_{var}^3}\right)$$

능동 예비 모듈(active spare)을 가지는 백업 예비 기법의 경우, 부시스템의 신뢰도 함수는 $(1-(1-R_{var})^N)R_a$이다. 하나의 여분을 가지는 경우라고 가정하면, 신뢰도 함수는 $(2-R_{var})R_{var}R_a$이 된다. (C-1)에 의해서 다음 제약조건을 얻을 수 있다.

$$R_a \geq \rho_i$$
$$R_{var} \geq 1-\sqrt{1-\rho_i}$$

(C-2)에 의해서는 다음 조건을 추가할 수 있다.

$$R_a \geq \max\left(\rho_i, \frac{1}{2-R_{var}}\right)$$

(C-3)에 의해서는 다음을 얻을 수 있다.

$$R_a \geq \max\left(\rho_i, \frac{1}{2-R_{var}}, \frac{\rho_i}{(2-R_{var})R_{var}}\right)$$
$$R_{var} \geq \max\left(1-\sqrt{1-\rho_i}, 1-\sqrt{\frac{(R_a-\rho_i)}{R_a}}\right)$$

다음으로, 하나의 수동 예비 모듈(inactive spare)을 가지는 백업 예비 기법에 대해서 적용해 보았다. $R_{var}(t)$와 $F_{var}(t)$를 각각 시간 t까지의 신뢰도와 고장확률이라고 하자. 부시스템의 신뢰도 함수는 다음과 같다.

$$R_{var}(t) + F(t_1)R(t-t_1)$$

만약, $R_{var}(t) = e^{-\lambda t}$라고 하면 신뢰도는 다음과 같다.

$$R_{var}(t)(1-\ln(R_{var}(t)))R_a(t)$$

(C-1)을 이용하면 다음과 같은 제약조건을 유도할 수 있다.

$$R_a(t) \geq \rho_i$$
$$R_{var}(t) \geq (R_{var}(t)(1-\ln(R_{var}(t))) = \rho_i) \text{의 해}$$

(C-2)에 의해서는 아래 조건을 추가할 수 있다.

$$R_a(t) \geq \max\left(\rho_i, \frac{1}{1-\ln(R_{var}(t))}\right)$$

(C-3)에 의해서는 다음 식을 유도할 수 있다.

$$R_a(t) \geq \max\left(\rho_i, \frac{1}{1-\ln(R_{var}(t))}, \frac{\rho_i}{R_{var}(t)(1-\ln(R_{var}(t)))}\right)$$

이번에는 세 개의 주(primary) 모듈과 하나의 예비 모듈로 구성되는 혼합 중복 기법에 대해서 적용해보자. 부시스템의 신뢰도 함수는 $R_{var}^2(6-8R_{var}+3R_{var}^2)R_v$이다. (C-1)에 의해서 다음의 제약조건을 도출할 수 있다.

$$R_v \geq \rho_i$$
$$R_{var} \geq 6R_{var}^2 - 8R_{var}^3 + 3R_{var}^4 = \rho_i \text{ 의 해}$$

(C-2)에 의해서는,

$$R_v \geq \max\left(\rho_i, \frac{1}{R_{var}(6-8R_{var}+3R_{var}^2)}\right)$$
$$R_{var} \geq \max\left(\frac{5-\sqrt{13}}{6}, 6R_{var}^2 - 8R_{var}^3 + 3R_{var}^4 = \rho_i \text{ 의 해}\right)$$

(C-3)에 의해서는 다음 제약조건을 추가할 수 있다.

$$R_v \geq \frac{\rho_i}{R_{var}^2(6-8R_{var}+3R_{var}^2)}$$

4. 결론

본 논문에서는 만족스러운 신뢰도를 갖추면서 비용을 적게 요구되는 결함허용 컴퓨터 시스템의 구조를 결정하기 위한 탐색 문제를 정의하였다. 시스템의 신뢰도 함수는 일반적인 형태를 가지며 부시스템의 신뢰도와는 비선형적인 관계를 가지므로 분석적인 방법으로는 해결하기가 어렵다. 탐색 방법은 적용 가능한 결함 허용 기법의 수와 부시스템 그리고 구성요소들의 수에 따라서 탐색공간이 크게 증가한다. 우리는 탐색공간의 크기를 줄이는데 사용할 수 있는 세 가지 관찰을 제시하고, 이를 바탕으로 대표적인 중복기법들인 TMR, 백업 예비 기법, 그리고 혼합 기법이 시스템 구조에 적용되었을 때의 탐색 공간을 줄이는 신뢰도 범위를 도출하였다.

5. 참고 문헌

[1] D. P. Siewiorek and R. S. Swarz, *Reliable Computer Systems: Design and Evaluation*. Digital Press, 1992.

[2] D. K. Pradhan, *Fault-Tolerant Computer System Design*. Prentice-Hall, 1995

[3] F. P. Mathur, "On reliability modeling and analysis of ultra-reliable fault-tolerant digital systems," *IEEE Transactions on Computers*, vol. 20, pp.1376-1382, Nov. 1971.

[4] F. S. Hillier and G. J. Lieberman, *Introduction to Operations Research*. McGraw-Hill Publishing Company, 1990.

[5] R. A. Sahner, K. S. Trivedi, and A. Puliafito, *Performance and Reliability Analysis of Computer Systems: An Example-Based Approach Using the SHARPE Software package*. Kluwer Academic Publishers, 1996.

[6] A. L. Reibman and M. Veeraraghavan, "Reliability modeling: An overview for system designers," *IEEE Computer*, vol.24, pp.49-57, Apr. 1991.

[7] J. Dugan, K. Venkataraman, and R. Culati, "DIFtree: A software package for the analysis of dynamic fault tree models," Proc. 1997 Reliability and Maintainability Symposium, Jan. 1997.