확률 추상 시간 기계를 이용한 시스템의 동적 실행 예측

이철*0, 박지연*, 이문근**
전북대학교 컴퓨터과학과*
전북대학교 전자정보공학부**
{chlee, jypark, mklee}@cs.chonbuk.ac.kr

Estimation of Real-Time Systems' Dynamic Execution Using Probabilistic Abstract Timed Machine

Chol Lee, Ji-Yeon Park, Moon-kun Lee
Dept. Computer Science, Chonbuk National University

요 약

정형 기법으로 명세된 시스템이 구현되어 실제 물리적 환경에서 실행될 때는 시스템 행위들의 성공과 실패가 다양한 환경 요인에 의해 영향을 받는다. 본 논문에서는 PATM(Probabilistic ATM)을 이용하여 시스템의 행위에 영향을 주는 요인의 정도를 확률로써 명세하고, 명세 단계에서 시스템의 실행을 예측할 수 있는 방법을 제시한다. PATM은 실행시간에 변화하는 요인을 가변 확률로 명세하여 실행 시 발생할 수 있는 상황에 대한 능동적인 분석과 예측을 가능하도록 한다.

1. 서론

실시간 시스템은 정적 명세 환경과는 달리 실제 환경에서 통신의 프로토콜이나 상태 또는 하드웨어 성능과 같은 다양한 물리적 요인에 의해 영향을 받으며 실행된다. 이에 따른 불확실성을 명세하기 위해 기존 정형 기법들에 확률을 적용하는 연구가 진행되고 있다[1,2,3]. 그러나 기존의 확률 정형 기법들은 많은 실행 영향 요인들 중 특정한 요소만을 고려하여 확률을 명세하고 분석하거나 혹은 확률이 무엇에 의해 결정되는지에 대한 기술이 부족하다.

본 논문에서는 기존 확률 명세 연구들이 가진 단점을 보완하여, 실행에 영향을 주는 많은 환경 요소를 고려, 동적으로 변화하는 실행 환경을 예측하기 위한 PATM을 기술한다. PATM은 실시간 시스템을 위한 정형 기법인 ATM[4]을 확률 속성에 의해 확장한 정형 기법이다. PATM에서 확률은 실행 도중 변경 가능한 환경 요인의 가변 확률과 불가능한 고정 확률로 구분하였으며 가변 확률 변경을 통해 확률의 동적 변화를 제공하여 시스템 동작의 동적인 예측을 가능하게 한다. 확률에 따른 시스템의 예측에는 도달성 그래프를 사용한다.

본 논문의 구성은 다음과 같다. 2절에서는 본 시스템의 확률과 PATM을 정의하며, 3절에서는 PATM을 통해 얻어지는 실행 모델인 도달성 그래프와, 확률적 특성 추출 방법을, 4절에서는 PATM을 통한 분석을 소개한다. 5절에서는 결론 및 향후 연구 과제에 대해 기술한다.

본 연구는 한국과학재단 특정기초연구(1999-2-303-003-3) 지원으로 수행되었음

2. PATM

2.1 확률

PATM에서의 확률은 명세 단계에서 정의한 시스템이 동작할 때, 실제 구현된 물리적 환경이 가진 요소에 의해 영향을 받게 되는 정도를 의미한다. 명세가 정적인 형태로 시스템을 표현하였다면 확률은 동적으로 물리적 환경을 정적인 명세에 반영할 수 있도록 한다. 시스템의 실행에 영향을 주는 환경 요인으로는 CPU의 성능, 네트웍의 신뢰도 및 대역폭, 프로토콜, 채널의 상태, 자원의 경쟁 상태 등이 있으며 이러한 요인은 실행 과정에서 확률 값이 변경되는 가변 확률 요인과 확률 값이 변경되지 않는 고정 확률 요인으로 구분할 수 있다.

정의 1: 전이의 발생에 영향을 주는 물리적 환경 요인의 집합을 S라 했을 때, 확률 p는 집합 S에 대한 다음을 만족하는 확률 함수 P의 값이다.
$S = \{x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m\}$, $x_i \in S$, $1 \le i \le n$,는 고정 확률 요인, $y_j \in S$, $1 \le j \le m$,은 가변 확률 요인일 때,
$p = P[S] = f(P_{x_1}[x_1],\ldots,P_{x_n}[x_n],P_{y_1}[y_1],\ldots,P_{y_m}[y_m])$, 여기에서 f는 환경 요인들이 가진 확률에 대한 단일 확률 값을 구하는 함수이며, $P_i[i]$, $i \in S$,는 각 확률 요인에 대한 확률을 구하는 함수이다. □

2.2 PATM의 정의

ATM은 활성화되었을 때 내부의 흐름을 스스로 제어할 수 있는 태스크, 프로시져와 같은 독립적 프로그램 블록인 머신 단위로 시스템을 명세한다. PATM M은 ATM을 확률로 확장하여 다음과 같이 정의 한다.

정의 2 : PATM M은 $M = <\Sigma, S, T, q_0, F, C>$의 6-튜플로 정의 되며 여기에서

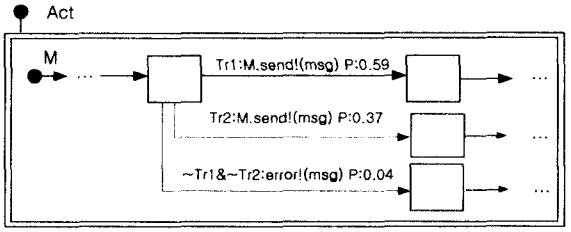
- Σ 는 포트의 집합, S는 모드의 집합,
- 전이 $T=\{S \cup M\} \times \{S \cup M\}$로 전이가 가지는 레이블의 구성 요소에 확률이 포함된 $L = <C_o, E, R, P>$로 정의한다. C_o는 조건(*condition*), E는 이벤트(*event*), R은 전이의 제약 시간(*real time*)을 나타낸다. P가 해당 전이가 가지는 전이 확률이며 정의 1에서 정의한 확률 함수 P에 의한 값을 가진다.
- q_0는 머신의 시작점, F 종료점들의 집합, C는 머신의 지역시계이다. □

ATM에 정의된 다양한 명세 속성은 PATM에 상속된다. 정의 3 PATM의 확률 명세에 대한 정의를 보인다.

정의 3 : 한 모드에서 발생 전이 $t_1, t_2, \cdots, t_n \in T$(정의2)($n$은 유한수)에 대해, 확률 p는 전이가 발생할 때 전이의 실행에 영향을 주는 환경 요인에 의한 확률 함수 P에 의한 값이고, $Pv(t_i)=p$, $0 \le p \le 1$, 는 전이의 확률 값을 구하는 함수라고 할 때 다음을 만족한다.

- 전이에 확률 p가 명시되지 않은 경우 $p=1$이다.
- 전이 t_i, $1 \le i \le n$,가 확률 $\sum_{i=1}^{n} pv(t_i) < 1$인 경우는 환경 요인에 의한 성공 확률이며, 실패 확률 $1-\sum_{i=1}^{n} pv(t_i)$을 갖는 전이 $\sim t$ 가 존재하며 이에 대한 명세가 없는 경우 실행 모델 생성 시 고려한다.
- 한 모드에서 발생되는 전이에 대한 확률의 합은 1이다. □

<그림 1>은 ATM머신이 확률을 가지고 M의 채널 *send*를 통하여 메시지 *msg*를 보내는 상태를 나타낸다. 실패할 경우에는 error 채널을 통해 msg를 전송하고 다른 모드로 전이한다. 만약 한 전이에 쌍이 되는 전이가 표현 되어 있지 않다고 해도 PATM에서는 암시적으로 임의의 에러로의 전이를 내포한다. '&'(∧)나 '|'(∨) 기호를 이용하여 여러 개의 전이를 통합하여 표현할 수 있다.



<그림 1> 확률 ATM 전이 레이블 예제

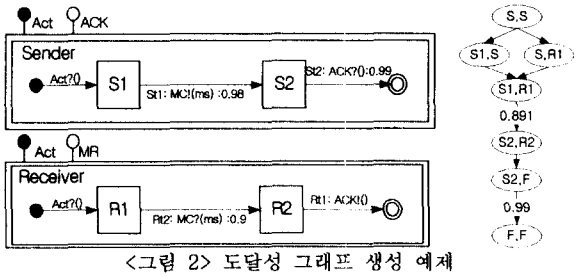
3. PATM의 실행 모델

PATM에서 머신과 그들의 전이로 된 명세는 시스템의 구조적인 측면을 나타낸다. 실행 시간에 동적인 측면을 명세하기 위해서 시스템의 실행을 도달성 그래프로 모델링 한다. PATM의 도달성 그래프는 시스템의 도달 가능한 상태와 그에 관련된 확률을 노드와 에지로 표현하여 시스템을 검증, 분석하기 위한 모델로 사용한다. ATM의 도달성 그래프와 생성 알고리즘은 [5]에서 연구되었으며, 확률로 확장한 PATM의 도달성 그래프는 다음과 같이 정의한다.

정의 4 : 주어진 일련의 PATM 머신의 집합 $M=\{M_1, M_2, \cdots M_n\}$ (n은 $n \ge 1$인 유한 수)의 도달성 그래프는 $G=<N, n_0, E>$의 3-튜플로 정의한다.

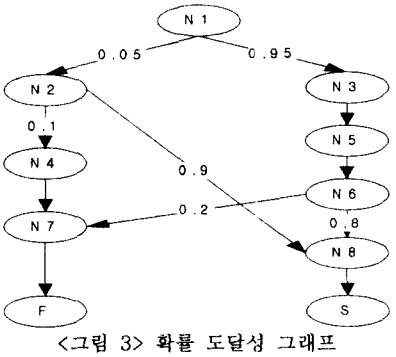
- N은 도달성 그래프의 유한한 노드의 집합으로 $N=<S, V, C>$의 세가지 구성 원소로 정의한다.
  - S은 관련된 PATM의 모드의 유한집합,
  - V는 전이와 관련된 변수 값의 집합,
  - T는 전이와 관련된 시간 값의 집합이다.
- $n_0 \in N$는 각 PATM 머신의 초기 모드의 조합과 각 머신의 전이 관련 변수와 시간의 초기 값을 갖는 그래프의 시작 노드이다.
- $E=N \times N$는 유한한 에지의 집합으로 에지를 생성하는 PATM 전이들이 가진 조건, 이벤트, 시간, 확률을 레이블로 갖는다. 확률이 1일 경우 확률의 표현은 생략 가능하다. □

실행시간에는 여러 머신이 병렬적으로 동기화 되거나 비동기화 되어서 실행 되기 때문에 다중의 전이가 동시에 발생 할 수 있다. <그림 2>에서 St1과 Rt2가 채널 MC를 통해 동기적 통신을 할 경우 도달성 그래프에서 <S1,R1>→<S2,R2>의 에지는 확률 값이 두 전이의 확률 곱인 0.891을 갖게 된다. St2와 Rt1의 통신이 비동기적일 경우 <S2,F>→<F,F>의 에지에 전이 St2의 확률 값인 0.99를 갖게 된다.



<그림 2> 도달성 그래프 생성 예제

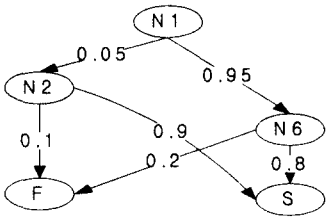
PATM의 실행 모델을 통해 확률에 의한 시스템을 분석하기에는 실행 모델이 가진 복잡도가 높다. 확률 분석을 위해 실행 모델을 단순한 확률 그래프로 변형하여 시스템의 분석을 위한 복잡도를 낮추었다. 예를 들어 <그림 3>에 제시한 도달성 그래프는 확률 전이를 일으키는 일부 에지에 확률 값을 가지고 있다. 이 그래프의 노드 중 확률 전이가 발생하지 않는 N3, N4, N5, N7, N8은 확률적인 실행 경로에 영향을 주지 않으므로 생략 하여 단순화 시켜 <그림 4>와 같은 그래프를 생성한다.



<그림 3> 확률 도달성 그래프

확률 트리의 시작 노드로부터 단말 노드나 또는 분석을 필요로 하는 임의의 노드에서 특정 노드까지의 경로에 존재하는

확률을 곱하여 전이 가능 확률을 구할 수 있다. 노드 A에서 노드 B까지 가는 경로가 m개 존재하고, 각 경로상에 존재하는 에지 중 확률을 가지는 에지가 n_m 개가 있다고 하면 임의의 경로를 통해 성공할 수 있는 확률은 $\prod_{i=1}^{n} p_i$ 가 되고, 모든 경로를 통해 전이가 성공할 수 있는 확률은 $\sum_{j=1}^{m} \prod_{i=1}^{n_j} p_i$ 가 된다.



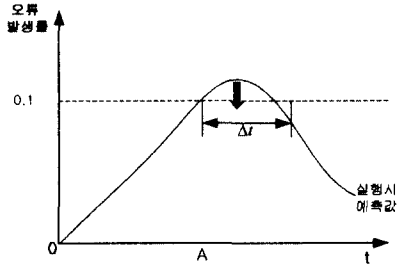
<그림 4> 단순화된 확률 도달성 그래프

<그림 4>을 통해서 이 시스템은 성공한 확률은 N1→N6→S, N1→N2→S의 경로의 확률 곱의 합인 0.805라 볼 수 있고 실패할 확률은 N1→N6→F, N1→N2→F의 경로의 확률 곱의 합인 0.195라고 분석 할 수 있다.

4. 분석

시스템의 안전성(*Safety*), 신뢰도(*Reliability*), 응답시간(*Response Time*) 등은 시스템의 성능을 평가하는 기준이 되는 성질들이다. 사용자가 "신뢰도 90% 유지되는 시스템"을 요구한다면 시스템을 명세, 분석하는 단계에서 그 요구사항을 만족시킬 수 있는 근거가 되는 구체적인 결과를 제시해야 한다. 본 논문에서 제시하고 있는 확률적인 측면을 통해서 구해지는 특성들은 시스템이 실행 시 물리적인 환경에 어떻게 영향을 받는지 명세 단계에서 예측할 수 있도록 한다.

환경 요인이 시스템에 미치는 정도는 확률을 통해 명세하고 도달성 그래프를 생성, 분석함으로써 확인할 수 있다. 확률 분석을 통해 구해진 시스템의 값이 기준치 이상을 만족해야 한다고 할 때, 시스템의 동적 실행 시간에 다양한 환경 요인을 반영한 분석을 제공할 수 있어야 한다. PATM은 이를 위해 가변적인 확률 요인을 추출하고, 이들에 대한 확률을 동적으로 변경함으로써 시스템의 동적 실행 분석을 제공 한다.



<그림 5> 신뢰도 분석 값과 요구사항 만족도

<그림 5>은 요구사항이 "오류 발생률을 0.1미만으로 유지하되 0.1을 초과할 경우 Δt 시간 안에 오류 발생률을 변경하라."일 경우에 대한 확률분석 도표이다. 만약 오류 발생률이 A라는 시점에 0.1을 넘게 되는 분석이 나왔다면 이 시스템의 요구사항을 만족하기 위해서는 Δt 시간 안에 자원에 대한 프로세스의 우선순위와 같은 가변 확률 요인들의 상태를 변경함으로써 오류 발생률을 0.1 미만으로 낮추어 요구사항을 만족시켜줄 수 있다. 또한 실행 전에 고정 확률 요인에 대한 변경을 미리 해서 조건을 만족시킬 수도 있다.

5 결론 및 향후 연구

본 연구에서는 명세된 시스템이 구현되어 물리적 환경에 배치되어 실행되었을 때의 시스템에 대한 분석과 환경 요인의 변화에 따른 시스템의 예측을 제공할 수 있도록 확률 개념을 통하여 ATM을 확장한 확률 추상 시간 기계를 정의 하였다. 또한 시스템의 동적 실행에서 발생할 수 있는 상황을 예측하고 대비할 수 있도록 확률에 대한 정의와 분석 방법 및 실행결과 예측에 대해 기술하였다.

실행에 대한 분석은 PATM에 대한 실행 모델을 생성하고 확률에만 관계된 단순화된 도달성 그래프를 통해 이루어 진다. 또한, 시스템이 가진 여러 환경 요인에 대한 확률 함수를 통해 환경 요인이 변경될 경우 발생하는 확률 값의 변동을 PATM에 반영함으로써 능동적인 시스템 예측이 가능함을 재시했다.

본 연구에서는 확률에 대한 정의와 분석 방법을 기술함으로써 발생되는 복잡도나 확률에 의해 추가된 속성에 대한 검증 방법에 대한 연구가 지속되어야 한다. 또한, 확률 변경에 따른 물리적 환경 요소가 어떻게 변경되어야 하는 가에 대한 절차, 방법, 적용 예제에 대한 향후 연구가 지속되어야 할 것이다.

참고문헌

[1] Anna Philippou, Oleg Slkosky, Insup Lee, Rance Cleaveland, Scott Smolka. Specifying Failures and Recoveries in PACSR. *Proceeding of Workshop on Probabilistic Methods in Verification*, June 1998.

[2] Hans A. Hansson. Time and Probability in Formal Design of Distributed Systems. *ELSEVIER*. pp.37~93. 1994.

[3] Marta Kwiatkowska, Gethin Norman, Roberto Segala, Jeremy Sproston. Automatic Verification of Real-time Systems with Discrete Probability Distribution. *Technical Report CSR-00-2, University of Birmingham*, 2000.

[4] 노경주, 박지연, 이문근. 추상 시간 기계를 이용한 순환 공학 정형 기법. *한국정보과학회 소프트웨어공학회지*. 제 13권 제1호. pp. 32-49. 2000.

[5] 박지연, 이문근. 추상 시간 기계를 이용한 실시간 시스템의 도달성에 대한 검증 방법. *정보과학회논문지*. Vol.28, No.2, pp. 224~238. Mar 2001.

[6] Hou Jianmin, Dang Van Hung. Verifying Linear Duration Properties of Probabilistic Real-Time System. *UNU/IIST report No.155*, February 1999.

[7] Costas Courcoubeties, Stavros Tripakis. Verification of Digital and Hybrid Systems. *NATO ASI Series*. pp. 83~219.

[8] Vijay K. Garg, Ratnesh Kumar and Steven I. Marcus. A Probabilistic Language Formalism for Stochastic Discrete-Event Systems. *IEEE Transactions on Automatic Control*, Vol. 44, No. 2, February 1999. pp.280~293.