내고장 실시간 시스템의 신뢰도 향상을 위한 확률 명세 및 실행 예측 분석 방법

(An Analysis Methodology for Probabilistic Specification and Execution Prediction for Improving of Reliability of Fault-Tolerant Real-Time Systems)

이 철 † 이 문 근 ††
(Chol Lee) (Moon-Kun Lee)

요 약 시스템이 실행 중 다양한 환경 요인에 의해 발생할 수 있는 불확실성을 명세하기 위해 확률의 개념을 적용한 명세 방법이 요구되고 있다. 본 논문에서는 실행에 영향을 주는 많은 환경 요인들을 고려하여, 변화하는 실행 환경에서 시스템의 행위를 예측, 분석하기 위한 확률 정형 기법인 확률 추상 시간 기계(PATM : *Probabilistic Abstract Timed Machine*)를 제안한다. PATM에서는 확률에 영향을 주는 환경요인을 실행 도중 변경이 가능한 가변 확률 요인과 변경이 불가능한 고정 확률 요인으로 분류하고 있다. 시스템의 행위에 대한 분석은 PATM의 동적 실행모델인 확률 도달성 그래프를 통해서 이루어진다. 분석 결과를 토대로 시스템의 동작 실패 가능성을 예측하고, 이에 영향을 미치는 가변 환경 요인을 변경하여 궁극적으로 시스템의 신뢰도를 향상할 수 있도록 한다.

키워드 : 정형기법, 확률, 확률추상시간기계(PATM), 도달성, 예측

Abstract *The formal specification methods with probability have been demanded in the area of fault real-time systems, in order to specify the uncertainty that the systems can encounter during their execution due to various environmental factors. This paper presents a new formal method with probability, namely Probabilistic Abstract Timed Machine (PATM), in order to analyze and predict system's behavior in dynamical environmental changes. This method classifies the factors into two classes: the variable and the constant. The analysis of system's behavior is performed on the probabilistic reachability graph generated from the ATM specification for the system. The analysis can predict any possibility that the behavior may not satisfy some safety requirements of the system, indicate which variable factors cause such satisfaction, and further recover from this unsatisfying fault state by fixing the variable factors. Consequently the reliability to the fault real-time systems can be improved.*

Key words : Formal Method, Probability, PATM, reachability, prediction

1. 서 론

실시간 시스템의 정형적인 개발을 위한 많은 연구가 진행되고 있으며, 이들은 "10 단위시간 안에 패킷을 전송할 확률이 99.9%이상"과 같은 확률적 요구사항을 명세하고, 분석, 검증하기위해 기존 명세 기법에 확률적 속성을 추가한 연구를 지속적으로 수행하고 있다[1,2,3,4]. 정형 기법을 사용하여 명세된 시스템은 실제 환경에서 통신 프로토콜이나 불확실한 지연 길이, 미디어 동기화 프로토콜, 네트워크 대역폭, 시스템 성능과 같은 다양한 물리적 요인에 의해 영향을 받으며 실행되기 때문에 이에 대한 시스템의 실행을 예측하기 위해서 실시간 시스템을 확률적으로 정형 명세할 필요성이 있다.

그러나 이러한 확률 정형 기법들은 시스템의 확률적

· 본 연구는 한국과학재단 특정기초연구(1999-2-303-003-3)지원으로 수행되었음
† 학생회원 : 전북대학교 대학원 컴퓨터통계정보
chlee@cs.chonbuk.ac.kr
†† 종신회원 : 전북대학교 전자정보공학부 교수
mklee@cs.chonbuk.ac.kr
논문접수 : 2002년 3월 26일
심사완료 : 2002년 9월 25일

행동의 원인이 되는 환경 요인들에 대한 명세 방법이 정의되어 있지 않기 때문에 이를 위해서는 추가적인 작업이 필요하게 된다. 또한 처음 명세할 때 제시한 확률을 통해 시스템의 실행을 예측, 분석 및 검증하기 때문에 시스템이 실행할 때 변경될 수 있는 환경을 고려할 수 없다는 단점을 가지고 있다.

본 논문은 이와 같은 연구들이 가진 문제점을 보완하여, 실행에 영향을 주는 많은 환경 요소를 고려, 동적으로 변화하는 실행 환경에서 시스템의 행위를 예측하기 위한 PATM(*Probabilistic Abstract Timed Machine*)을 제안하고, 이를 통한 분석 기법에 대하여 기술한다.

PATM은 실시간 시스템의 정형 명세를 위하여 고안된 ATM(*Abstract Timed Machine*)[5]을 확률 속성에 의해 확장한 정형 기법이다. PATM에서의 확률은 시스템에 영향을 미치는 모든 물리적 환경요인을 고려한 시스템의 실행 가능성을 의미한다. 환경 요인은 실행 도중 변경이 가능한 가변 확률 요인과 변경이 불가능한 고정 확률 요인으로 구분하였으며, 가변 확률 요인의 임의 변경을 통해 시스템이 실행 할 때 확률의 동적 변화를 제공할 수 있다.

PATM을 이용해서 시스템을 명세하고 분석하는 과정은 <그림 1>과 같다. PATM에 프로세스의 구성이나 모듈단위 구조 등 시스템의 구조적, 정적인 측면을 확률과 함께 명세하고, 실제 실행시 가질 수 있는 상태들을 나타내는 실행모델인 도달성 그래프를 통해 시스템의 동적 측면인 실행을 명세 및 분석하게 된다. 확률에 따른 시스템의 실행 예측은 확률 도달성 그래프에 대한 분석을 기반으로 이루어진다.

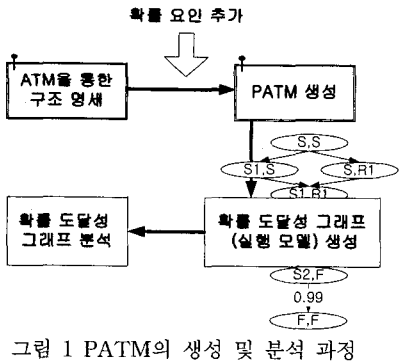

그림 1 PATM의 생성 및 분석 과정

PATM은 그 근본이 되는 ATM이 상태 기반, 그래픽 기반 명세 언어이기 때문에 명세와 분석 측면에서 사용자의 이해도를 더욱 높일 수 있다.

PATM은 다양한 물리적 환경 요소를 고려하여 보다 구체적인 확률 분석을 수행 할 수 있다. 또한, 실행 중 시스템의 상태 분석을 통해 동적인 확률 제어 환경을 제공하는 장점을 가지고 있다.

그러나 PATM을 통해 실행 중 수시로 변하는 환경에 따른 분석을 수행하기 위해서 여러 가지 속성들을 처리하기 위한 작업들로 시간, 공간적 복잡도가 증가되는 문제점을 가지고 있다. 이러한 문제점들은 PATM의 명세를 통해 발생한 실행 모델의 단순화를 통해 해결하고 있으며, 좀더 근본적으로는 PATM의 명세 단계에서 머신의 우선순위를 명세하는 방법 등을 통해 이루어져야 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 통해 다른 연구에서 제시한 확률과 PATM이 가진 확률의 차이 및 장, 단점을 기술하고, 3장에서는 PATM과 PATM의 확률을 정의한다. 4장에서는 PATM을 통해 얻어지는 시스템의 실행 모델과 그 생성 규칙을 기술하며, 5장에서는 PATM과 실행 모델을 통한 확률적 분석 기법을 소개한다. 6장은 PATM을 적용한 예제를 기술하고, 마지막으로 7장에서는 결론 및 향후 연구 과제에 대해 기술한다.

2. 관련 연구

다양한 정형 기법들이 시스템에 대한 확률을 명세하는 방법을 제공하고 있다. 이러한 확률 명세 기법들은 시스템에 대한 행위나 상태 등에 확률을 부여하여 표현하고, 시스템의 행위에 대한 예측, 분석, 검증하는 방법을 제시한다.

관련 연구 [1]의 PTA(*Probabilistic TA*)에서는 시스템을 분석하기 위한 상태에 대한 표현을 위해 TA(*Timed Automata*)[6]를 확률적으로 확장한 PTA (*Probabilistic TA*)[1]를 사용하였다. PTA의 구조(Structure)를 정의하고, PTA로 표현된 시스템을 통해 다시 각 상태에 영향을 주는 변수들로 구성된 영역 그래프(*Region Graph*)를 구성한다. 이것을 기반으로 시스템을 검증하기 위해 CTL(*Computation Tree Logic*)을 확률과 시간 속성으로 확장한 TPCTL(*Timed Probabilistic Computation Tree Logic*)[1,3]을 사용하고, 그 표현은 도달성 그래프를 이용한다.

ACSR(*Algebra of Communication Shared Resources*)[7]을 확장한 PACSR(*Probabilistic ACSR*)에서 확률은 각 자원(resource)에 대한 사용 가능성을 나타낸다. PACSR에서 시스템은 지속적으로 사용 가능한 자원의 집합을 가지며 또한 사용 실패 자원

(failed resource)의 집합 을 가진다. PACSR의 동작은 시간을 소비하는 동작(timed action)과 소비하지 않는 이벤트, 확률에 관한 동작(probabilistic action)으로 구분되어 이에 따른 전이 규칙을 정의한다. 확률에 따른 전이 규칙을 바탕으로 PACSR은 자원 사용 가능성을 예측, 분석한다. ACSR은 공유 자원을 통하여 통신이 이루어지므로, 자원 사용 가능성에 대한 확률 분석을 통하여 통신의 성공 가능성도 분석할 수 있다.

관련연구 [3]의 TPCCS는 프로세스 알지브라인 CCS(*Calculus of Communicating systems*)[8]를 시간의 개념으로 확장한 TCCS(*Timed CCS*)[3]와 확률 개념으로 확장한 PCCS(*Probabilistic CCS*)[3]를 조합한 정형 기법이다. TPCCS는 시간과 확률 개념이 조합된 전이 규칙을 제공하며 TPCCS를 통해 정의된 확률 프로세스들에 대한 확률적 동치(probabilistic equivalence)와 bisimulation을 정의하여 다르게 표현된 확률 프로세스가 동일하게 취급되어 간단하게 시스템의 확률 분석을 수행할 수 있도록 한다.

앞에서 소개된 PTA&TPCTL, PACSR, TPCCS 등의 확률 정형기법을 통한 연구들은 시스템의 확률적인 측면을 분석, 검증하는 방법을 제공하고 있으나 이들 연구에서 목표로 하는 확률에 대한 명확하고 근본적인 정의가 되어 있지 않다. 즉, 확률을 가진 시스템을 명세하고 검증할 수 있으나 확률을 만들어내는 어떤 요인에 대한 정의나 표현은 하지 못하고 있다. 따라서 이 정형기법을 이용하려는 사용자는 확률의 의미와 내용을 추가적으로 정의해야 한다는 단점을 가지고 있다.

또한, 이들 확률 명세를 제공하는 정형 기법들에서는 확률이 고정적이다. 즉, 확률이 의미하는 바가 일단 정해지면 시스템의 동작 시 다변하는 환경에 대처하지 못한다.

이에 비해 본 연구에서는 확률을 정의하고, 확률에 영향을 주는 요인들을 표현함으로써 불확실성을 가진 실시간 시스템을 위한 확률 명세를 보다 구체적으로 명세할 수 있도록 하고 있다. 또한 확률에 영향을 주는 환경 요인을 고정적인 환경 요인과 가변적인 환경 요인으로 구분함으로써 시스템의 정적, 구조적인 명세 뿐 아니라 실행 중 변화하는 환경에 능동적으로 시스템을 분석할 수 있는 방법을 제시하고 있다. 더 나아가 실제 실행 환경에서 확률적 요구사항에 위배되는 상태가 발생할 경우 분석을 통해 변경해야 할 환경 요인들을 제시할 수 있다.

3. PATM

3.1 확률

확률[確率]의 사전적 의미는 "실현될 수 있는 가능성의 정도, 또는 그것을 나타내는 수치"[9]이다. 즉, 어떤 일의 발생 가능성을 말하게 된다. 명세하고자 하는 대상 시스템에 표현될 수 있는 확률은 그 시스템이 어떤 일을 수행할 수 있는지의 가능성으로 말할 수 있다. 따라서 확률은 그 시스템의 행위에 결부되어 명세 되며, 시스템의 행위에 연관된 여러 요인들이 확률을 결정하게 된다.

PATM에서 정의하는 확률은 명세 단계에서 정의한 시스템이 구현되어 실행될 때, 실제 물리적 환경에서 여러 가지 요인에 의하여 영향을 받게 되는 정도를 의미한다. 시스템의 실행에 영향을 주는 환경 요인으로는 CPU의 성능, 네트워크의 신뢰도 및 대역폭, 프로토콜, 채널의 상태, 자원의 경쟁 상태, 하드웨어의 상태 등이 있으며, 이러한 요인들은 시스템이 동작하는 과정에서 요인 자체의 변경이 가능해 확률 값을 변경시킬 수 있는 가변 확률 요인과 변경시키지 못하는 고정 확률 요인으로 구분할 수 있다. 특정 전이가 몇 가지의 환경 요인에 의해 실행이 좌우된다면 그 전이가 수행 될 확률은 관련된 환경 요인들의 연관성을 고려한 다음 <정의 1>의 확률함수를 통해 나타낼 수 있다.

정의 1 : 확률함수

시스템의 행위 t의 성공에 영향을 주는 물리적 환경 요인의 집합을 E라 했을 때, $P_t[E]$는 집합 E에 포함된 환경 요인들에 의한 확률을 구하는 확률 함수이다.

- $E=x_1, x_2, \cdots, x_n, y_1, y_2 \cdots, y_m$는 전이 t의 성공에 영향을 주는 환경 요인의 집합, $x_i \in E$, $(1 \le i \le n)$는 고정 확률 요인, $y_j \in E$, $(1 \le j \le m)$은 가변 확률 요인일 때,
- $P_t[E] = F(P_{x_1}[x_1], \cdots, P_{x_n}[x_n], P_{y_1}[y_1], \cdots, P_{y_m}[y_m])$,

여기에서 F는 각각의 환경 요인들에 의한 확률을 통합하여 단일 확률 값을 구하는 함수이며, $P_{e_i}[e_i]$, $e_i \in E$,는 각 확률 요인에 대한 확률을 구하는 함수이다. □

3.2 ATM의 정의

ATM은 RTS(*Real Time Systems*)를 순공학과정에서 정형적으로 명세하거나 역공학과정에서 역명세하기 위하여 고안된 정형기법이며, FSM(*Finite State Machine*)에 기반을 둔 LTS(*Labeled Transition System*)으로 분류할 수 있다. ATM은 RTS을 구성하는 병렬 프로세스나 태스크를 의미한다.

정의 2 : ATM

ATM M은 $<\Sigma, N, n_0, F, T, V, H, C, p>$의 9-튜플로 정의된다. 여기에서 Σ는 포트의 유한 집합, N은 모드(mode)의 유한 집합, $n_0 \in N$은 시작모드(시작점), $F \subseteq N$는 최종 모드(정상/비정상 종료점)의 유한 집합, T는 조건과 시간제약을 가진 다른 ATM과의 선택적 상호작용에 기반을 둔 모드 간의 전이들의 유한 집합, V는 데이타 변수의 유한 집합, H는 실행된 모드와 전이의 실행 경로를 기록하고 있는 history, C는 지역시계(local clock), p는 우선순위를 나타낸다.□

3.3 PATM의 정의

PATM M은 ATM을 확률로 확장하였으므로 ATM에 정의된 다양한 명세 속성은 PATM에 상속되며, ATM 구성 원소를 모두 포함한다. PATM은 동작을 나타내는 전이의 구성 요소에 확률이 추가된다.

정의 3 : PATM

PATM M은 M = $<\Sigma, N, n_0, F, T', V, H, C, p>$의 9-튜플로 정의 되며 T'를 제외한 각 구성 원소는 <정의 2>와 같다.

- 전이 $T' = S \cup M \times S \cup M$는 $<n_s, g, e, b_t, p, n_t>$의 튜플로 정의된다. 여기에서 n_s와 n_t는 전이의 시작과 종료 모드들을 나타내며, g는 전이가 발생되기 위한 조건, e는 외부와의 제어나 메시지 송/수신을 나타내는 상호작용, 즉 이벤트, b_t는 전이가 발생되어 완료되어야 하는 시간 제약 또는 소모 시간을 각각 의미한다. p는 전이가 성공할 확률을 나타낸다. 이들 중 g, e, b_t, p는 전이의 레이블로 표현된다. □

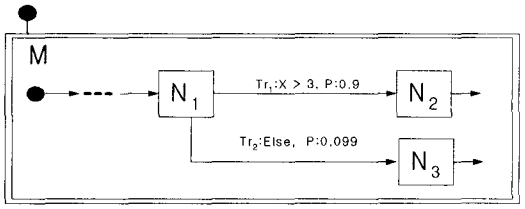

그림 2 조건에 의한 다중 분기

<그림 2>은 PATM에서 노드간의 전이를 표현한 예이다. N_1노드에서 N_2로 이어지는 전이 Tr의 성공 확률은 0.9가 된다. 한 모드에서 발생하는 전이의 다중 분기에는 두 가지 종류가 있다. 하나는 조건에 의한 다중 분기이고, 다른 하나는 예외처리와 같은 경우에 따른 다중 분기가 된다. <그림 2>은 모드의 전이가 변수 x의 값에 의해서 선택되는 경우를 나타내고 있다. 이와 같은 경우는 모드 안에서 전이가 결정 된다. 즉 전이가 한번 선택되어 실행되면 어떤 일이 있어도 다른 전이를 다시 선택 할 수 없다. 따라서 두 전이는 전이의 성공 여부를 나타내는 각각의 확률을 가지게 된다.

그러나 <그림 3>의 경우 모드 N_2에서 M.send!(msg)을 통한 전이가 실패할 경우 N_1으로 전이하게 하는 PATM을 나타내고 있다. 이런 경우는 Tr_1에는 전이가 성공할 확률을 표현하고 ~Tr_1에는 Tr_1이 실패할 확률을 표현한다. 그리고 이 두 전이는 점선을 통해서 그룹화 시킨다.

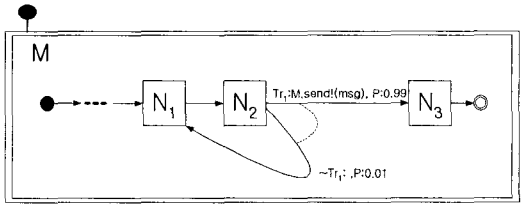

그림 3 예외 처리에 의한 다중 분기

<정의 4>는 PATM의 확률 명세를 대한 정의한다.

정의 4 : 확률 명세

한 모드에서 발생하는 전이 $t_1, t_2, \ldots, t_n \in T$(정의 3)(n은 유한 수)에 대해:

- 확률 p_i는 전이 t_i의 확률 함수 P에 의한 확률 값,
- $P_t(t_i) = p_i, 1 \le i \le n$,는 전이에 대한 확률 함수,
- G_N : 모드 N에서 발생하는 전이 그룹의 집합이라 할 때 다음을 만족한다:
  - i. 전이에 확률 p가 명세되지 않은 경우 $p=1$이다.
  - ii. 한 그룹에 포함된 전이들의 확률 합은 1 이하이다.
  - iii. 한 모드에서 발생할 수 있는 모든 전이의 확률 합은 '그룹의 수' 이하이다. 즉,

$$0 \le \sum_{i=1}^{n} p_t(t_i) \le n(G_N).$$

  - iv. 전이 $t_i, 1 \le i \le n$,가 확률 $p(p<1)$를 가진 경우는 환경 요인에 의한 성공 확률이고, 실패 확률 $(1-p)$를 갖는 $\sim t_i$와 쌍을 이룰 수 있다. 이 두 전이는 PATM상에서 그룹화 되어 표시된다. 즉, $P_t(t_i) + P_t(\sim t_i) = 1$.
  - v. '&'(AND,∧)와 '|'(OR,∨), '~'(NOT,¬)을 조합하여 둘 이상의 전이관계를 표현 할 수 있다. 즉 t_i와 t_j가 AND 관계로 전이를 한다면 통합된 확률은 확률 곱으로 표현하고, OR관계로 전이하면

확률 합으로 표현 할 수 있다. □

<정의 4>의 4항에 제시한 바와 같이 '&'나 '|' 기호를 이용하여 에러에 대한 전이 또는 다중 전이의 조합을 표현할 수 있다. <그림 4>는 전이 Tr_1과 Tr_2가 모두 실패한 경우를 $\sim Tr_1 \& \sim Tr_2$로 표현한 예이다.

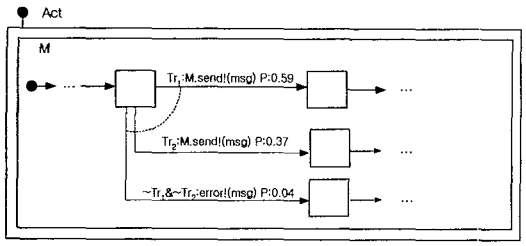

그림 4 확률 ATM 전이 레이블 예제

4. PATM 실행 모델

PATM으로 명세된 시스템의 실행 상태 및 확률 분석은 PATM의 실행 모델인 도달성 그래프를 통해 이루어진다. 본장에서는 PATM에서 도달성 그래프를 생성할 때 확률을 결정하는 전이 규칙 및 생성된 도달성 그래프의 복잡도를 낮추고 가독성을 높이기 위한 방법에 대해서 기술한다.

4.1 PATM 전이 규칙

PATM으로 명세된 시스템의 실제 실행시간에는 여러 머신이 병렬적으로 동기화 되거나 비동기화 되어서 실행된다. 따라서 시스템의 상태가 매우 다양해지게 된다. 시스템의 실행 상태는 4.2절에서 정의하는 확률 도달성 그래프(PRG : *Probabilistic Reachability Graph*)를 통해 나타내게 되는데, 이절에서는 독립적 또는 병렬적으로 수행되는 PATM 머신과 모드들 사이의 관계 및 시간, 확률 등을 고려하여, PRG의 현재 상태에서 전이 가능한 상태를 결정짓는 PRG 생성을 위한 전이 규칙을 정의한다.(전이 발생에 영향을 주는 이벤트는 고려하지 않는다.).

전이 규칙은 한 머신 안에 있는 모드간의 단순한 전이나, 병렬적으로 동작하는 머신들의 상태 전이가 발생할 때 전이가 성공할 수 있는 확률 및 발생하는 모든 경우를 따지게 된다.

전이 규칙의 용어 설명:

(1) 전이규칙의 구조는 다음과 같다.

$$\frac{PATM}{PRG(Condition)}$$

(a) *PATM* : 구조적 명세에서 표현되는 모드와 전이 및 확률 표현

(b) *PRG* : 실행시간에 실제 발생할 수 있는 모드 집합과 전이들

(c) *Condition* : *PATM*의 전이의 발생 조건

(2) *PATM*과 *PRG*의 형식은 다음과 같다:

(a) $m \xrightarrow{Cond,[a,C,b],p} m'$

(b) m : PATM의 머신 또는 모드.

(c) *Cond* : 전이 발생을 위한 조건

(d) p : PATM의 전이가 성공할 확률.

(e) $[a,b]$: 전이의 시간적 제약사항.

① a : 대기시간, 전이 발생 조건이 만족되더라도 대기시간까지 전이가 발생하지 않음.

② b : 데드라인, 전이가 완료해야 할 시간.

(f) C : 전이에 소모되는 시간

(3) $\vee$: OR.

(4) + : 머신, 모드의 병렬 동작.

(5) *ERR* : 시스템의 올바르지 못한 상태.

(6) PRG의 상태에 있어서 [ ]안은 생략 가능.

(7) 예외 처리와 관련된 PATM의 분기는 "()"를 사용해서 표현한다.

$$\frac{M_1 : \{(m \xrightarrow{p} m', m \xrightarrow{1-p} m'')\}}{m \xrightarrow{p} m' \vee m \xrightarrow{1-p} m''}$$

정의 5 : 확률의 결정

PRG의 상태 전이가 결정 될 때 그 전이에 따른 확률을 다음과 같이 결정한다:

1) PRG의 전이가 PATM의 한 머신의 전이에 의해 결정될 경우:

$$\frac{M_1 : \{m \xrightarrow{p} m'\}}{m \xrightarrow{p} m'}$$

2) PRG의 전이가 PATM의 2개 이상의 머신의 2개 이상의 전이에 의해 결정될 경우(확률 곱) :

$$\frac{M_1 : \{m \xrightarrow{p} m'\} \quad M_2 : \{n \xrightarrow{q} n'\}}{m + n \xrightarrow{p \times q} m' + n'}$$ □

정의 6 : 단일 PATM 전이 규칙

시스템의 상태 전이가 하나의 모드에서 발생하는 특정 그룹의 전이에 의해 결정되는 경우 전이 규칙을 다음과 같이 정의한다:

1) 실패와 성공의 확률을 명시적으로 가진 전이의 경우(두 전이는 하나의 그룹에 포함된다.) :

$$\frac{m \xrightarrow{p} m',\ m \xrightarrow{1-p} m''}{m \xrightarrow{p} m' \vee m \xrightarrow{1-p} m''}$$

2) 성공에 대한 확률만을 가진 경우 :

$$\frac{m \xrightarrow{p} m'}{m \xrightarrow{p} m' \vee [m \xrightarrow{1-p} ERR]}$$

3) 확률이 명세되지 않은 전이의 경우 :

$$\frac{m \longrightarrow m'}{m \xrightarrow{p=1} m'}$$

4) 시간 속성 포함(제약 사항만 포함-전이는 즉각적으로 발생) :

$$\frac{M_1 : \{A \xrightarrow{[a,b]} B\},}{A \xrightarrow{t} B(a \le t \le b) \vee A \xrightarrow{x} ERR(t < a \text{ OR } b < a)}$$

(a) a ≤ b,

(b) n : 머신의 경과시간

(c) t : 모드 A의 완료 이후 전이 발생시점,

5) 전이의 소모시간만 포함된 경우 :

$$\frac{M_1 : \{A \xrightarrow{C} B\},}{A \xrightarrow{C} B}$$

(a) C : 전이의 소모 시간(Consuming Time), 전이 발생 시점은 모드 A가 완료하는 시점에 발생함을 가정.

3) 제약 사항, 소모 시간 모두 포함된 경우 :

$$\frac{M_1 : \{A \xrightarrow{[a,C,b]} B\},}{A \xrightarrow{t+C} B(a \le t \le b - C) \vee A \xrightarrow{x} ERR}$$

□

<정의 6>에 제시하는 단일 전이 규칙은 시스템의 상태 결정이 한 머신에 의해서 이루어지는 경우이다. 여러 머신이 병렬적으로 실행하는 시스템에서도 다른 머신들의 상태가 고정되고 한 머신의 전이에 의해서 상태 변화가 발생 할 경우에도 동일한 전이 규칙을 적용할 수 있다.

다음은 여러 머신이 동시에 동작하는 시스템의 전이 규칙을 기술한다. 여러 머신이 동시에 동작하는 방법은 프로세서가 하나인 단일 컴퓨터에서 병렬 프로세스로 동작하거나, 다중 프로세서 또는 분산 환경에서 병렬적으로 동작하는 방법이 있다. 또한 이들은 특정 머신, 모드간의 통신을 통해 두개 이상의 전이가 연관되어 발생하는 전이와, 머신들의 통신 관계가 없어 무작위로 동작하는 전이가 있다.

도달성 그래프를 생성하기 위해서는, 각각의 머신 중 어느 머신이 먼저 수행 될 것인지에 대한 결정이 선행 되어야 한다. 머신들이 통신 관계가 없이 무작위로 동작하거나, 비동기적인 통신 관계로 동작한다면, 여러 머신 중 먼저 상태 전이가 이루어지는 머신은 운영체제에서 주어지는 프로세스의 스케쥴링 방식과 머신의 우선순위, 그리고 전이에 소모되는 시간 등을 고려해서 가장 먼저 전이 작업이 완료되는 머신이 된다. 전이 작업이 완료되는 시간이 동일한 머신의 경우 동시에 전이가 이루어진다.

<정의 7>에서는 통신 관계가 없이 동작하는 PATM의 전이 규칙을 정의하고 있다.

정의 7 : 통신 관계가 없는 PATM 전이규칙

통신 관계가 없이 동작하는 2개의 병렬 머신의 전이 규칙을 다음과 같이 정의 한다:

1) 제약 사항만 포함된 경우

$$\frac{M_1 : \{M \xrightarrow{[a,b]} M'\},\ M_2 : \{N \xrightarrow{[c,d]} N'\},}{\begin{array}{l} M+N \xrightarrow{t_1} M'+N(t_1 < t_2, a \le t_1 \le b) \\ \vee M+N \xrightarrow{t_2} M+N'(t_2 < t_1, c \le t_2 \le d) \\ \vee M+N \xrightarrow{t_1 \text{ or } t_2} M'+N'(t_2 = t_1, a \le t_1 \le b \text{ AND } a \le t_1 \le b) \\ \vee M+N \xrightarrow{t_1} ERR+N((t_1 < a, t_1 < t_2) OR (b < t_1, t_1 < t_2)) \\ \vee M+N \xrightarrow{t_2} M+ERR((t_2 < c, t_2 < t_1) OR (d < t_2, t_2 < t_1)) \\ \vee M+N \xrightarrow{t_1 \text{ or } t_2} ERR+ERR \\ \quad ((t_2 = t_1) AND (\neg(a \le t_1 \le b) AND \neg(c \le t_2 \le d))) \end{array}}$$

2) 소모시간 까지 포함된 경우

$$\frac{M_1 : \{M \xrightarrow{[a,C_1,b]} M'\},\ M_2 : \{N \xrightarrow{[c,C_2,d]} N'\},}{\begin{array}{l} M+N \xrightarrow{t_1+C_1} M'+N_{t_1+C_1}(t_1+C_1 < t_2+C_2, a \le t_1 \le b-C_1) \\ \vee M+N \xrightarrow{t_2+C_2} M_{t_2+C_2}+N'(t_2+C_2 < t_1+C_1, c \le t_2 \le d-C_2) \\ \vee M+N \xrightarrow{t_1+C_1 \text{ or } t_2+C_2} M'+N' \\ \quad (t_2+C_2 = t_1+C_1, a \le t_1 \le b-C_1, c \le t_2 \le d-C_2) \\ \vee M+N \xrightarrow{b} ERR+N_b \\ \quad (b < t_1+C_1, t_1+C_1 < t_2+C_2) \\ \vee M+N \xrightarrow{d} M_d+ERR \\ \quad (d < t_2+C_2, t_2+C_2 < t_1+C_1) \\ \vee M+N \xrightarrow{b \text{ or } d} ERR+ERR(t_2 = t_1, b = d, b < t_1+C_1, d < t_2+C_2) \end{array}}$$

□

다음은 동기적으로 전이하는 머신의 도달성 그래프 생성에 관한 전이 규칙을 정의한 것이다.

정의 8 : 통신 관계가 있는 PATM 전이 규칙

동기적으로 동작하는 2개의 병렬 머신의 전이 규칙을 다음과 같이 정의한다. 비동기적으로 동작하는 머신의 경우 <정의 6>의 전이규칙을 따른다.

1) 실패와 성공의 확률이 명시적으로 표현된 경우

$$\frac{m \xrightarrow{p} m', m \xrightarrow{1-p} m'', \quad n \xrightarrow{q} n', n \xrightarrow{1-q} n''}{m+n \xrightarrow{p\times q} m'+n' \vee m+n \xrightarrow{1-p\times q} m''+n''}$$

2) 성공에 대한 확률만 가진 경우

$$\frac{m \xrightarrow{p} m', n \xrightarrow{q} n'}{m+n \xrightarrow{p\times q} m'+n' \vee [m+n \xrightarrow{1-p\times q} ERR]}$$

3) 시간의 제약 사항만 포함된 경우

$$\frac{M_1 : \{M \xrightarrow{[a,b]!} M'\}, \quad M_2 : \{N \xrightarrow{[c,d]?} N'\},}{M+N \xrightarrow{t_1 \text{ or } t_2} M'+N' ((a \le t_1 \le b \text{ AND } c \le t_2 \le d), t_2 = t_1) \vee M+N \xrightarrow{t_2} ERR+ERR(ELSE)}$$

2) 소모시간도 포함된 경우

$$\frac{M_1 : \{M \xrightarrow{[a,C_1,b]!} M'\}, \quad M_2 : \{N \xrightarrow{[c,C_2,d]?} N'\},}{M+N \xrightarrow{t_1 \text{ or } t_2} M'+N' ((a \le t_1 \le b - C_1 \text{ AND } c \le t_2 \le d - C_2), t_2 = t_1, C_1 = C_2) \vee M+N \xrightarrow{t_2} ERR+ERR(ELSE)}$$

□

이와 같은 전의 규칙에 의해 4.2절에서 정의하는 실행 모델인 도달성 그래프가 생성된다.

4.2 PATM 도달성 그래프

도달성 그래프는 시스템의 실행에 따라 변하는 상태에 대해 가능한 모든 동작을 모델링하는, 즉 시스템의 실제 동작을 표현하는 실행 모델이다. ATM으로 명세된 시스템의 실행을 모델링 함으로써 실제 실행 시 발생할 수 있는 시스템의 행위와 결과에 대한 각종 분석을 수행할 수 있다. 도달성 그래프는 병렬로 실행되거나 혹은 순차적으로 실행되는 시스템의 도달 가능한 상태를 파악, 노드(node)와 에지(edge)로써 표현한다. 노드는 시스템이 위치한 현재 모드나 머신에 대한 상태 정보가 포함 되며, 에지에는 ATM의 모드나 머신간의 전이에 관련된 정보가 포함된다. 노드와 에지의 값을 분석함으로써 시스템의 분석 및 검증을 수행할 수 있다. PATM의 실행은 도달성 그래프로 모델링되며 ATM의 도달성 그래프와 생성 알고리즘은 [10]에서 연구되었다.

PATM의 도달성 그래프는 ATM의 도달성 그래프에 확률속성이 추가된 상태가 된다. 그래프의 확률 및 시간 속성들을 분석하여 시스템의 확률적 실행과 결과를 예측할 수 있다. <정의 7>은 PATM의 도달성 그래프를 정의한다.

정의 7 : PATM의 도달성 그래프

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:

(1) N은 도달성 그래프의 유한한 노드의 집합으로 $N=<S, V, C>$의 세 가지 구성 원소로 정의한다.
  (a) S는 관련된 PATM의 모드의 유한집합,
  (b) V는 전이와 관련된 변수 값의 집합,
  (c) C는 전이와 관련된 시간 값의 집합이다.

(2) $n_0 \in N$는 각 PATM 머신의 초기 모드의 조합과 각 머신의 전이 관련 변수와 시간의 초기 값을 갖는 그래프의 시작 노드이다.

(3) $E=N \times N$는 유한한 에지의 집합으로 에지를 생성하는 PATM 전이들이 가진 조건, 이벤트, 시간, 확률을 레이블로 갖는다. 이 때 주어지는 확률의 값은 4.2절의 PATM의 도달성 그래프 전이 규칙에 따라 결정된다. 확률 p=1인 에지를 *일반 에지*, $0<p<1$인 에지를 *확률 에지*라 한다. □

본 논문에서는 시스템의 PATM의 실행 모델을 확률 및 시간적 측면에서 분석한다. 가독성을 높이기 위해서 본 논문에서 예로 제시하는 도달성 그래프에는 표현되는 정보를 확률 및 시간 위주로 단순화해서 나타내도록 한다. 즉 노드의 내용에는 노드의 이름과 시간의 속성만을, 에지의 레이블에는 시간과 확률만을 표현한다. 또한 시간적 측면만을 고려할 경우 레이블의 확률을 생략하며 확률만을 고려하는 경우 시간 요소는 생략하도록 한다. 또한 에지에 주어지는 확률이 1인 경우 그 표현을 생략할 수 있다.

<그림 5>의 PATM의 예제에서는 전이 St_1과 Rt_1이 채널 MC를 통해 동기적 통신을 하게 되고, 전이 St_2와 Rt_2는 비동기적 통신을 한다고 가정한다. 또한 Receiver가 Sender보다 높은 우선순위를 가지고 있다고 가정한다. 4.1절의 전이규칙을 통해 생성되는 도달성 그래프는 <그림 6>와 같다.

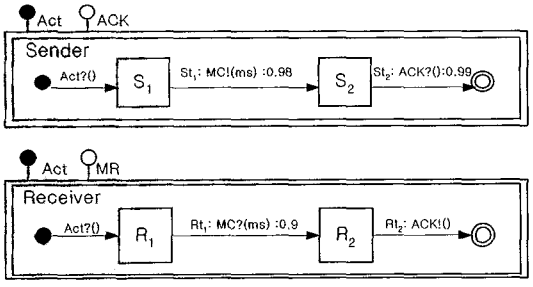

그림 5 병렬 실행하는 PATM

노드 <S_1,R_1>, <S_2,R_2>간의 에지는 확률 값이 두 전이의 확률 곱인 0.891을 갖게 된다. St_2와 Rt_2의 통신이 비동기적이고 R_2에서 즉각적 종료 상태를 나타내는 ◎로 먼저 전이가 일어나게 되므로 상태 <S_2,◎>와 <◎,◎>의 에지에는 전이 St_2의 확률 값인 0.99를 갖게 된다.

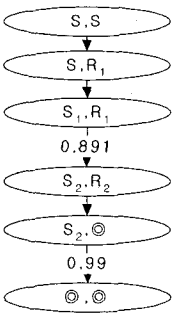

그림 6 <그림 5>에 대한 도달성 그래프

4.3 PATM 도달성 그래프의 복잡도 감소

PATM의 실행 모델은 확률, 시간 등의 세부적 특성들을 분석하거나 사용자가 이해하기에는 너무 복잡하다. 이러한 그래프의 복잡도를 줄이기 위해서 분석하고자 하는 확률 또는 시간 등의 속성과 관계가 없는 노드와 에지를 생략하거나 다른 노드나 에지에 포함시킴으로써 보다 간결한 그래프를 생성할 수 있다. 다음 <정의 8>는 도달성 그래프를 단순화 시키는 감소 규칙을 정의한다.

정의 8 : 도달성 그래프 감소 규칙

도달성 그래프 G의 감소 규칙을 다음과 같이 정의한다.

- N : G의 노드의 집합
- n_i, $n_{i-1} \in N$ ($1 \le i \le k$, k는 집합 N의 원소 수)

1) 확률적 속성만 있는 경우

$$\frac{\{n_i\} \xrightarrow{p:1} \{n_{i+1}\}}{\{n_i > n_{i+1}\}}$$

- 노드 n_i에서 다음 노드인 n_{i-1}로의 에지가 결정적이고, 그 확률이 1인 경우 노드 n_{i-1}& n_i에 merge한다.
- 합쳐진 노드들의 순서를 지정하기 위해서 '>' 기호를 사용하여 표현한다.

2) 시간적 속성이 포함된 경우

$$\frac{\{n_i\} \xrightarrow{p:1,t:a} \{n_{i+1}, t:b\}}{\{n_i : a > b : n_{i+1}[, t : a+b]\}}$$

- 에지에 표현되는 시간 a는 에지가 발생하는 노드 n_i의 뒤에 서술한다. 노드 n_{i-1}에서 소모되는 시간 b는 단축된 노드에서 노드 n_{i-1}의 앞에 서술한다. 단축 노드의 총 소모 시간인 $a+b$를 포함 할 수 있다. □

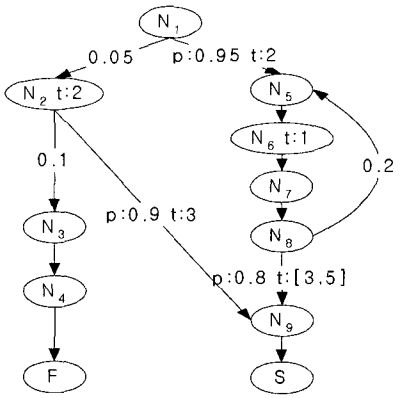

그림 7 도달성 그래프 예제

<그림 7>에 제시한 도달성 그래프에는 확률 전이를 일으키는 일부 에지에만 확률 값을 표현하고 있다. 이 그래프의 노드 중 N_4와 N_6, N_7, N_8의 노드로의 전이는 결정적이며 그 확률이 1이다. 이렇게 노드로의 전입이 유일하고 그 확률이 1인 노드들은 <정의 7>의 감소 규칙에 따라 선행되는 노드에 포함시켜서 <그림 8>와 같이 단순화된 그래프로 변경할 수 있다. 그룹을 표현하기 위해 노드 이름을 합쳐진 노드들의 이름으로 구성한다. 그룹화 된 노드들의 도달 확률은 그룹 내에서는 모두 동일하다.

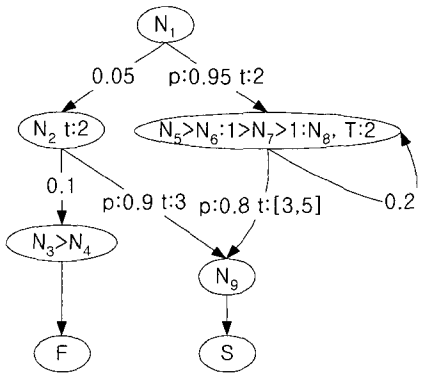

그림 8 <그림 7>을 단순화한 도달성 그래프

```
input : a reachability graph;
output : a reduced reachability graph;

reduce_reachability_graph()
begin;
      n0=initial node ;
      reduce(n0);
end;

reduce(node N)
begin;
   if visited = true then return;
   else visited = true;
   // 이미 방문한 노드이면 종료한다.
   precedence = find_precedence(N);
   // N의 선행되는 노드리스트를 구한다.
   successor = find_successor(N);
   // N의 후행하는 노드리스트를 구한다.

   if (( count(precedence) = 1 ) and
       (probability of precedence to N = 1))
   then
   // 선행되는 노드의 개수가 1이고,
   // 그 노드로부터 현재 노드로
   // 전이 확률이 1일 경우
   // 선행 노드와 현재 노드를 합치게 된다.
      merge_node( find_precedence(N), N);
   end if
   while (not end of list of successor )
      make_short(successor);
   // 후행하는 노드들 전체에 대해서 수행한다.
   end while;

   return;
end;
```

그림 9 단축 도달성 그래프 생성 알고리즘

<그림 9>는 도달성 그래프의 확률에 관련한 단축 도달성 그래프 생성 알고리즘을 기술한 의사코드(pseudo code)이다. 이 알고리즘은 노드의 전이관계를 나타내는 에지를 따라 함수를 수행하게 된다. 현재 노드에서 발생하는 모든 에지에 관계된 노드에 대해서 수행을 한 후 실행을 함수의 실행을 종료하게 된다. 노드를 단축시키는 함수의 실행 회수는 노드에서 노드로 전이하는 수의 총 합과 동일하며, 이미 평가된 노드는 다시 평가 되지 않으므로 노드에 부속된 에지 역시 한번만 평가가 된다. 즉 복잡도를 따져보면 노드의 수를 n이라 하고, 각 노드에서 발생하는 에지 수의 평균을 k라 하면 그 복잡도는 $O(kn)$이 된다. 확률 도달성 그래프의 한 노드에서 발생할 수 있는 에지의 수는 PATM에서 병렬적으로 동작하는 머신의 수보다 많을 수 없다. 따라서 한 노드에서 발생하는 평균 에지 수 k는 복잡도에 큰 영향을 주지 않는 상수의 의미를 갖게 되므로 알고리즘의 실질적인 복잡도는 $O(n)$이라 할 수 있다.

5. 분 석

5.1 PATM의 확률 속성 분석

이 절에서는 PATM의 도달성 그래프를 이용해서 시스템의 확률적인 분석을 위한 방법을 기술한다. 도달성 그래프에서 시작 노드에서 종료 상태를 나타내는 노드까지의 전이 가능성이나 또는 분석을 필요로 하는 임의의 노드에서 특정 노드까지의 경로에 존재하는 확률들을 통해 시스템의 동작 가능성을 분석할 수 있다. 이를 위해서 일반적인 특성을 통해 다음의 몇 가지 사항을 정의하였다.

정의 9 : 경로

확률 도달성 그래프에서 주어진 일련의 노드 S_1, S_2, ..., S_n (n은 n>1인 유한 수)이 순차적으로 전이가 가능할 때 즉 $S_1 \rightarrow S_2 \rightarrow \cdots \rightarrow S_n$의 순서로 전이할 때 이를 S_1에서 S_n으로의 경로라 말하며 $R_{S_1 \sim S_n}$로 표현한다. □

경로는 <정리 1>과 같은 특성을 가진다.

정리 1 : 경로의 수 (증명 생략)

(1) 임의의 그래프에 루프가 형성 될 경우 루프를 경유하는 경로의 수는 무한개이다.

(2) 두 노드 사이의 경로의 수는 0개 이상이다. □

<정의 9>에서 정의한 경로의 각 에지에는 확률이 주어져 있다. 이 확률들을 통해 시스템이 그 경로를 거쳐 작동될 때 성공할 수 있는 확률을 계산하는 확률 함수를 다음과 같이 정의한다.

정의 10 : 경로 확률 함수

상태 $S_1 \rightarrow S_2 \rightarrow \cdots \rightarrow S_n$($n$은 n>1인 유한 수)의 전이를 나타내는 경로(Route) R에 대해 경로 확률 함수 P_R를 다음과 같이 정의한다:

$$P_R = \prod_{i=1}^{n-1} P_E(E_i)$$

(1) E_i : 상태 $S_i \rightarrow S_{i+1}$로 전이를 나타내는 에지

(2) $P_E()$: 에지의 확률을 구하는 함수 □

<정의 10>에서 제시한 경로 확률 함수를 통해 두 노드 사이에 도달 가능 확률을 계산 할 수 있다. 두 노드 사이에 존재하는 경로는 여러 개 일 수 있으므로 존재하는 모든 경로의 합을 통해 한 노드에서 다른 노드로 전이할 수 있는 확률을 계산한다. <정의 11>은 두 노드간의 전이 확률을 구하는 함수를 정의하고 있다.

정의 11 : 도달 확률 함수

상태 S_n에서 S_m으로 도달 가능한 확률을 나타내는

함수 $P_{S_n \sim S_m}$를 다음과 같이 정의한다.

$$- P_{S_n \sim S_m} = \sum_{i=1}^{k} P_{R_i}$$

· $P_{R_i}(1 \le i \le k)$: 상태 S_n에서 S_m으로 도달 가능한 k개의 경로에 대한 확률 함수. □

이상의 정의를 이용해서 분석할 수 있는 시스템의 확률 속성은 다음과 같은 것들이 있다.

1) ATM의 도달성 그래프를 통해서 시스템이 어떤 상태로 전이하는지에 대한 상태 분석에 대한 연구는 [10]에 기술되어 있다. 특정 상태가 시스템의 안전한 종료를 나타내는지, 또는 Deadlock 같은 상태를 나타내는지 분석이 이루어 져 있다면, 이상에서 정의한 경로 함수, 경로 확률 함수, 도달 확률 함수 등을 이용해서 상태에 전이하게 될 확률을 분석할 수 있다.
2) 도달성 그래프의 에지는 한쪽으로만 방향을 가지게 된다. 만약 요구사항이 특정 상태들을 지나 시스템이 수행할 확률을 분석하는 것이라면 PATM의 도달성 그래프에서는 각 지점간의 도달 가능 확률을 조합해서 분석 할 수 있다. 예를 들어 노드 시작노드 A에서 임의의 노드 B를 거쳐서 목적노드인 C까지 갈 수 있는 확률은 <정의 11>의 도달 확률 함수를 이용해서 구하면 $P_{A \sim B} \times P_{B \sim C}$ 이다.

<정의 11>에 제시한 도달 확률 함수를 통해 <그림 8>의 시스템의 성공 가능성을 분석해 보도록 한다. <그림 8>의 초기 노드 N1에서 성공을 나타내는 노드 S로 전이할 수 있는 경로는 N1→N2→N9→S의 경로 R_1과 N1→(N5>N6>N7>N8)*→N9→S의 경로 $R_{(2,\infty)}$가 있다 (*는 0회 이상 반복을 의미함). 도달 확률 함수를 이용해서 계산을 하면 이 시스템이 모든 경로를 고려해서 성공할 확률은 $0.05 \times 0.9 + 0.95 \times \sum_{i=0}^{\infty} 0.2^i \times 0.8$임을 알 수 있다. <그림 8>에 제시된 도달성 그래프에서는 성공으로 전이하기 위한 경로에 루프가 존재하고 있다. 반복실행에 대한 제한회수나 시간적인 제약이 없기 때문에 이 도달성 그래프에서는 시스템이 성공하게 될 확률을 구하기 위해 반복 횟수를 무한하게 지정 하였다. 그러나 일반적인 실시간 시스템에서는 시간적인 제약이 주어진다. 다음 절은 시간적인 제약을 받는 시스템의 도달성 그래프를 분석하기 위한 방법을 기술한다.

5.2 PATM의 시간 속성 분석

실시간 시스템을 대상으로 하는 정형 명세에는 시간에 대한 명세가 필수적이다. ATM의 도달성 그래프에서 표현되는 시간은 시스템이 특정 노드의 상태나 에지가 나타내는 전이가 소모하는 시간 또는 시작과 데드라인 등의 제약을 나타내는 시간이다. ATM에서는 이산적인 시간을 표현하고 있다. PATM에서도 동일한 시간 값들을 가지게 되는데 그래프를 단순화 하는 단계에서는 노드들이 융합될 때 합쳐지게 되는 노드의 이름에 시간을 표시하도록 한다.

PATM의 도달성 그래프에서 두 노드간의 전이를 나타내는 실행에 주어지는 시간과 확률을 동시에 분석하기 위해서 다음의 시간과 관련된 함수를 정의한다.

정의 12 : 경로 시간 함수

상태 $S_1 \rightarrow S_2 \rightarrow \cdots \rightarrow S_n$의 전이를 나타내는 경로 $R_{S_1 \sim S_n}$(n은 $n>1$인 유한 수)에 대해 경로 시간 함수 T_R를 다음과 같이 정의한다.

$$- T_R = \sum_{i=1}^{n-1} T_E(E_i) + \sum_{i=1}^{n} T_S(S_i)$$

(1) E_i : 상태 $S_i \rightarrow S_{i+1}$로의 전이를 나타내는 에지
(2) $T_E()$: 에지의 소요 시간을 구하는 함수
(3) $T_S()$: 각 상태의 시간을 구하는 함수 □

시간에 관련된 PATM의 특정 전이는 실행 시간에 제약을 가질 경우가 있다. 예를 들어 전이에 관련된 A라는 작업이 3초 대기후 7초 안에 작업이 완료 되어야 하는 경우는 PATM의 전이에 시간 제약이 "[8,11]"로 표현이 된다. 경로 상에 이런 시간 제약이 있을 경우 경로 시간 함수를 통해지는 시간의 합도 최소 값과 최대 값으로 구분되어서 "[X,Y]"의 형태가 된다.

<정의 11>에 제시한 도달 확률 함수를 통해 얻어지는 확률은 도달 가능한 모든 경로들이 수행될 수 있는 시간에 관계된다. 특정 시간에 해당 노드로 전이할 수 있는 확률은 그 시간 이전에 전이를 마치는 경로들에 의해서 결정된다. 즉 모든 경로들이 만족할 수 있는 시간은 경로들의 소요시간 중 최대 시간이 되고, 그 확률은<정의 11>에서 제시한 확률 값이 된다.

<그림 7>의 예제를 살펴보면 노드 N_2와 N_6에 시간이 각각 2, 1씩 소모되고 있고, 주어지고 에지 $N_1 \rightarrow N_5$에 2, $N_7 \rightarrow N_8$은 1, $N_2 \rightarrow N_9$에서는 3, $N_8 \rightarrow N_9$에서는 최소 시간이 3에서 최대 5까지 소모될 수 있다.

<그림 7>의 도달성 그래프를 4.2절에 제시한 알고리즘을 이용해서 단축할 때, 단축 대상이 되는 노드와 에지에 시간을 <정의 7>에 따라 <그림 8>의 노드 "N_5>N_6:**1**>N_7>**1**:N_8"과 같이 표현하였다. 즉, 노드에서 소모되는 시간은 해당 노드명의 뒤에, 전이에 소모되는

시간은 전이해 가는 노드의 앞에 표시한다. 또한 "N_5>N_6:1>N_7>1:N_8, T:2"와 같이 단축된 노드에 총 소모될 수 있는 시간을 표시할 수도 있다.

<그림 8>초기 노드에서 최종 노드 중 S에 도달할 확률과 시간을 통해서 다음 <표 1>과 같은 분석 결과를 얻을 수 있다.

표 1 <그림 7>의 분석 결과
($N_5' = N_5 > N_6 : 1 > N_7 > 1 : N_8$)

시간(t)	…	5	[7,9]	[9,11]	[11,13]	……
$P_{N1\sim S}$	0	0.045	0.805	0.957	0.9874	…
경로 (누적)	N_1>N_2>N_9>S					
	N_1>N_5'>N_9>S					
	N_1>N_5>N_5'>N_9>S					
	N_1>N_5'>N_5'>N_5'>N_9>S					
	⋮					

5.3 시스템의 실행 중 분석

이장에서는 PATM으로 명세된 시스템의 실제 실행 중 지속적인 분석을 통해 동적으로 확률을 변화시켜 가는 방법을 대략적으로 기술한다. 전제가 되어야 할 것은 시스템의 실행 환경에 보조적으로 분석 환경이 포함되어 분석의 결과가 즉각적으로 반영 되어야 한다는 것이다.

시스템의 안전성, 신뢰도, 응답시간 등은 시스템의 성능을 평가하는 기준이 되는 성질들이다. 이러한 특성들을 대상으로 정형 기법을 통해 명세 및 분석을 한다고 가정하자. 만약 사용자가 "신뢰도가 99% 이상 유지되는 시스템"을 요구한다면 시스템을 명세, 분석하는 단계에서는 그 요구사항을 만족시킬 수 있는 근거가 되는 구체적인 확률적 분석 결과를 제시해야 한다. PATM에서는 5장에서 서술한 방법을 통해 이런 분석 결과를 제시하게 된다. 그러나 시스템이 실제 실행되는 환경의 변화는 예측하기 매우 어렵기 때문에 시스템의 실행 중 환경의 변화가 발생할 때마다 새로운 분석을 통해 시스템의 요구사항을 검증할 필요가 있다.

시스템의 실행 전에 수행되어지는 분석은 도달성 그래프 전체를 대상으로 한다. 그러나 시스템이 동작하고 있을 때 분석을 수행 한다면 그 분석 대상은 현재 수행되고 있는 특정 경로상의 특정 노드가 된다. 즉, 이전까지의 진행해온 상태는 이미 성공적으로 이루어진 상태이므로 분석 대상은 현재 노드에서부터 목적 노드가 포함 되어 있는 부분 그래프가 된다.

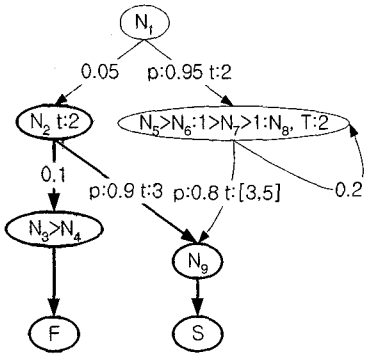

그림 10 <그림 8>의 실행 중 분석 대상

예를 들어 <그림 8>의 도달성 그래프를 분석한 <표 1>은 시스템의 시작부터 성공을 나타내는 S 노드로 전이 가능성을 나타낸다. 그러나 시스템이 실행 시 N_2에 위치하고 있다면 분석해야 할 도달성 그래프는 <그림 10>에서 굵은 선으로 표시된 부분인 <그림 8>의 부분 그래프가 된다. 또한 요구사항이 시스템이 성공적으로 종료하는 상태 S로의 전이만을 고려한다면 N_2>N_9>S의 경로만 분석하여 요구사항을 만족하는지 따지게 되고, 그 분석 결과는 3 단위시간에 전이할 확률이 0.9가 된다.

<정의 1>에서 제시한 바와 같이 확률에 영향을 주는 환경 요인은 가변 환경 요인과 고정 환경 요인으로 나뉜다. 시스템이 실제 환경에서 동작 할 때 가변 환경 요인들이 변경 되어 현재 노드에서 분석한 확률의 예상 값이 요구사항을 만족하지 못하게 될 때 분석 환경은 가변 환경 요인들의 변경을 요구하게 된다.

예를 들어 <그림 10>에서 시스템의 현재 상태는 N_2이고, 시스템이 성공적으로 종료할 확률이 0.9이상을 요

표 2 <그림 10>에 관련된 확률 요인 표

확률 요인		확률요인 값	확률요인 개별확률	성공확률
가변	자원 A의 점유 우선순위	3	0.90	0.881118
	자원 B의 점유 우선순위	1	0.98	
고정	CPU 성공율	0.999	0.999	

구하고 있다고 가정 하자. N_2에서 N_9로 전이에 관여하는 확률 변수들이 <표 2>와 같고, 전이가 성공할 확률이 0.9가 되지 않을 경우, 분석 환경은 상대적으로 가장 적은 개별 확률을 나타내는 자원 A의 점유 우선순위를 높이도록 실행 환경에 요구한다. 자원 A의 점유 우선순위를 높여서 그 확률 요인의 개별 확률이 0.92 이상이 되면 성공확률은 0.9가 넘게 된다.

여기서 제시한 시스템 실행 중 분석 환경을 통해서 소프트 데드라인으로 주어진 요구 사항에 대해 다음과 같이 고장 방지·회피(fault prevention & avoidance)를 할 수 있다. <그림 11>은 요구사항이 "에러율을 0.1 미만으로 유지하되 0.1을 초과할 경우 Δt시간 안에 에러율을 변경하라."일 경우에 대한 확률분석 도표의 예다. 주어진 요구사항은 소프트데드라인을 만족하는 요구사항이다. 먼저 명세단계에서 PATM을 통해 생성한 확률 도달성 그래프를 기반으로 실행 중 PRG의 상태가 변경 될 때마다 지속적인 확률 분석을 수행한다. 위에서 제시한 요구사항을 만족하기 위해서 현재 시스템이 위치한 상태부터 시스템의 올바른 종료를 나타내는 상태까지 전이할 확률을 구하게 된다. 만약 A라는 시점에서 전이가 성공할 확률이 0.9 미만(즉, 에러율이 0.1 이상)이 되는 분석 결과가 나왔다면, 이 시스템의 요구사항을 만족하기 위해서 앞에서 제시한 일련의 작업들을 수행하게 된다. 즉 현재 상태에서 시스템의 올바른 종료를 나타내는 상태까지 전이할 수 있는 모든 경로에 영향을 주는 환경 요인들을 분석하여 Δt시간 안에 가변 확률 요인들의 상태를 변경함으로써 에러율을 0.1 미만으로 낮추어 요구사항을 만족시켜준다. 이상의 소프트 데드라인을 만족하는 고장 방지·회피에 관한 연구는 추후에 지속되어야 할 부분이다.

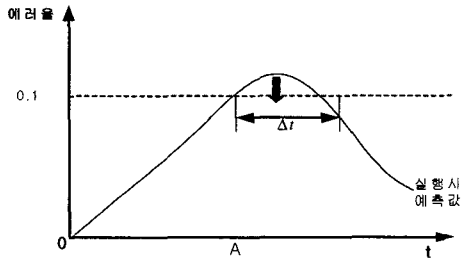

그림 11 신뢰도 분석을 통한 요구사항 만족도

6. 예제 - Sender, Medium, Receiver모델

SMR(Sender, Medium, Receiver) 모델에서 Sender는 Medium을 통해 메시지를 Receiver로 전송하며, Receiver는 Medium에서 메시지를 받았을 때 Ack 신호를 다시 Medium에게 보내고, Medium은 이 Ack 신호를 다시 Sender에게 전송하는 통신 프로토콜을 명세한 것이다. SMR 모델에서는 시간을 고려하지 않고 분석을 하였다. 이 예제에서는 다음과 같은 요구사항과 가정을 가지고 있다.

<요구사항> "SMR 모델에서 한번의 동작이 완료할 확률은 0.95 이상이어야 한다."

< 가 정 >

(1) 각 머신들은 분산 환경에서 동작하고 있다.
(2) 머신들의 통신에는 통신 회선의 대역폭(X1)과 프로세스의 통신자원 점유 우선순위(X2) 두 가지의 확률 환경 요인이 주어져 있다.
(3) X1, X2 두 환경 요인은 가변 환경 요인이다.
(4) 각 환경 요인과 확률의 관계를 <표 3>과 같이 가정한다.
(5) 분석 환경에서는 운영체제의 스케줄러(Scheduler)에 의해서 자원의 점유에 관한 우선순위가 수시로 변경 된다.

표 3 확률 요인과 확률 관계

확률 요인	값	확률	확률 요인	값	확률
X1 (대역폭)	100	1.0	X2 (우선순위)	1	0.99
	90	0.99		2	0.98
	80	0.97		3	0.95
	...	...		...	...

<표 4>에서는 실제 계산 결과를 나타내게 된다.

표 4 SMR 모델의 확률 요인과 확률 결과

확률 요인		확률요인의 값	확률요인 개별확률	성공 확률
Sender	X1 (대역폭)	100	1.0	St1: 0.98
	X2 (우선순위)	2(평균)	0.98	
Medium	X1 (대역폭)	100	1.0	Mt3: 0.98
	X2 (우선순위)	2(평균)	0.98	

SMR 모델의 구조를 나타내는 PATM 명세는 다음과 같다.

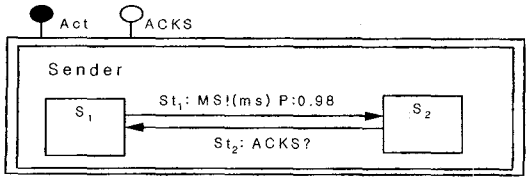

그림 12 Sender PATM

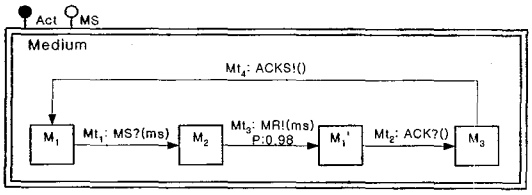

그림 13 Medium PATM

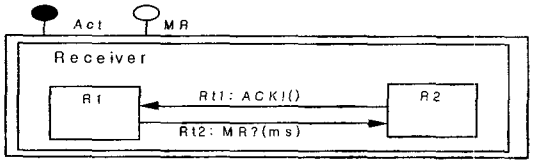

그림 14 Receiver PATM

SMR을 명세한 위의 PATM을 통해 구할 수 있는 확률 도달성 그래프는 <그림 15>와 같다. 여기에서 실행 노드의 모드는 각각 Sender, Medium, Receiver PATM의 모드를 의미하며, 각 머신은 초기상태에서 각각의 모드인 S_1, M_1, R_1에 동시에 전이한다고 가정한다. 시스템이 본질적으로 무한 반복의 수행을 가정하고 있기 때문에 시스템의 비활성화를 의미하는 종료점은 고려하지 않았다. 또한 확률에 초점을 두어 각 노드나 에지의 기타 정보는 생략한 형태로 표현하였다.

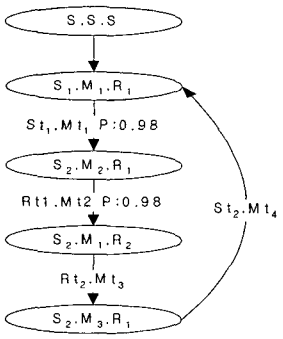

그림 15 SMR 모델의 도달성 그래프

생성된 도달성 그래프의 구조가 단순하기 때문에 단순화는 생략하도록 한다. 이 예제는 어느 정점에서 실행을 마치는 모델이 아니고 끊임없이 작업을 반복하는 모델이다. 상태<S_1,M_1,R_1>을 작업 주기의 시작점으로 보고 다시 그 상태로 돌아온 시점을 한 작업을 완료한 시점으로 보면 작업을 한번 수행을 할 확률은 0.9604가 된다. 또한 n번의 작업을 완료할 수 있는 확률은 $(0.98\times0.98)^n$이 된다. 실패할 확률은 $1-(0.98\times0.98)^n$이다.

실행 시간 중 Sender에서 통신 회선을 점유할 수 있는 우선순위 X_2가 2에서 3으로 변경 되었다면 SMR 모델이 1회 동작 할 확률은 $0.98\times0.95 = 0.931$이 되어서 요구사항을 만족 할 수가 없다. 실행 중 이러한 분석이 이루어진다면 Sender와 Medium의 통신이 발생하기 전에 분석 환경은 Sender가 동작하고 있는 시스템의 운영체제에 우선순위 변경을 요구하여 요구사항을 만족할 수 있도록 한다.

7. 결론 및 향후 연구

본 논문에서는 실시간 시스템을 위한 정형 명세 언어인 ATM을 구현한 시스템이 물리적 환경에서 실행될 때 가질 수 있는 상태에 대한 확률적 분석을 수행하기 위해 확률 개념을 통하여 확장한 확률 추상 시간 기계(PATM)를 정의하였다. PATM은 확률을 통하여 환경요인의 변화에 따른 시스템의 예측을 제공할 수 있도록 하였다. 또한 시스템의 동적 실행에서 발생할 수 있는 확률적인 상황을 예측하고 대비할 수 있도록 확률에 대한 정의와 분석 방법에 대해 기술하였다.

PATM을 이용해 아키텍처 기반으로 시스템을 명세하고, 명세된 시스템의 실행 모델인 PATM의 도달성 그래프를 이용해 시스템의 확률 및 시간 속성을 분석한다. 도달성 그래프를 분석하는 단계에서 발생하는 시간, 공간적 복잡도를 해결하기 위해 단순한 도달성 그래프를 생성하는 방법과 알고리즘 등을 제시하였다.

이러한 일련의 작업들을 통해서 시스템의 실행 과정에서 다양한 환경 요인에 의해 발생할 수 있는 불확실성을 개발 초기 단계에서 명세하고, 분석할 수 있으며, 이를 바탕으로 현실적인 시스템의 검증을 지원할 수 있게 된다.

PATM의 확률은 시스템의 실행에 영향을 주는 다양한 환경 요인들과의 관계를 고려한 값으로 표현된다. 환경요인을 시스템의 실행 중 변경 가능성에 따라 가변 확률요인과 고정 확률요인으로 나누어서 함수적 정의를 통해 시스템에 대한 영향 정도를 표현하고, 변경하여 실행을 분석한다. PATM의 확률은 다른 관련연구에서 제

시하고 있는 확률 정의와 분석, 명세 방법보다 구체적이고 실제적이다. 따라서 PATM으로 명세된 시스템을 분석 검증하는 것은 실행에 대한 사실성을 제공할 수 있다. PATM의 확률 정의를 통해 시스템의 명세 단계에서 확률 분석과, 모의실험 단계에서의 분석, 그리고 실행 단계에서의 분석이 가능해 진다.

PATM은 시스템의 구조를 명세하고, 그 실행을 예측하는 단계적인 분석 기법이며, 단계마다 GUI 형태의 정보를 사용자에게 제공한다. 이를 통해 사용자의 이해도를 높일 수 있다.

향후 연구로는 PATM을 통해 확률적인 속성을 분석하는 완성도를 높이기 위해서 시스템의 확률적 동작 패턴을 분류하고, 그에 대한 확률적 분석 기법이 연구 되어야 하며, 명세된 시스템을 검증하기 위해 실시간 시스템의 시간 속성을 검증하기 위한 시제 논리(Temporal Logic)[12]와 확률적인 속성을 통합해서 PATM을 검증하는 방법론이 연구 되어야 한다. 또한 분산성과 같은 ATM의 명세 영역 확장에 따라 확률적인 속성도 병행하여 지속적인 연구가 필요하다.

본 논문에서는 확률을 보다 구체적이고, 체계적으로 표현하고 있으나 실제 실행 환경에서 주어지는 요인들이 어떤 방식을 통해서 확률 함수를 이루는지에 대한 기술이 부족하다. 즉, 확률 요인들이 시스템에 끼치는 영향을 확률적인 수치로 추출하는 문제가 남아있다. 또한 시스템과 환경 요인간의 확률적 영향 관계에 대한 연구가 진행 된 이후 소프트 데드라인에 대한 고장 허용에 대한 연구도 지속 되어야 한다.

참 고 문 헌

[1] 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.

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

[3] Hans A. Hansson. Time and Probability in Formal Design of Distributed Systems. ELSEVIER. 1994.

[4] Marta Kwiatkowska, G. Norman, R. Segala and J. Sproston. Verifying Soft Deadlines with Probabilistic Timed Automata. *The Proceeding of WAVe'2000.* June 2000.

[5] 노경주, 박지연, 이문근. 추상 시간 기계를 이용한 순환 공학 정형 기법. 한국정보과학회 소프트웨어공학회지. 제13권 제1호. 2000. pp. 32-49.

[6] R. Alur, D. Dill. A Theory of Timed Automata. *Theoretical Computer Science 126,* 1994. pp.183~235.

[7] I. Lee, P. Bremond-Gregoire, R. Gerber. A Process Algebraic Approach to the Specification and Analysis of Resource-bounded real-time systems. *Procedings of the IEEE,* January 1994. pp.158~171

[8] Robin Miller. Communication and Concurrency. Prentice Hall. 1989.

[9] 연세 한국어 전자사전.

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

[11] 박지연, 이철, 조기환, 이문근. 실시간 시스템의 순환공학을 위한 CASE도구: SAVE. 한국정보과학회 소프트웨어공학회지. 제14권 제3호. 2001. pp. 84-97.

[12] Zohar Manna, Amir Pnueli. The Temporal Logic of Reactive and Concurrent Systems. Springer-Verlag. 1992.

이 철

2000년 전북대학교 컴퓨터과학 학사. 2002년 전북대학교 전산통계학 석사. 2002년 ~ 현재 전북대학교 대학원 컴퓨터통계정보 박사과정. 관심분야는 소프트웨어 재 역공학, 실시간 시스템, 운영체제, 컴파일러 등

이 문 근

정보과학회논문지 : 소프트웨어 및 응용 제 29 권 제 3 호 참조