철도 신호 제어프로토콜의 검정 및 적합성시험 도구 개발에 관한 연구

서미선*, 황진호*, 김성운*, 황종규**, 이재호**
*부경대학교 정보통신공학과
**철도기술연구원
e-mail:jljpms@mail1.pknu.ac.kr

A Study on Development for Verification and Conformance Test Tool of Rail Signal Control Protocol

Mi-Seon Seo*, Jin-Ho Hwang*, Sung-Un Kim*, Jong-Gyu Hwang **, Jea-Ho Lee**
*Dept of Telematics Engineering, Pu-Kyong National University
**Korea Railroad Research Institute

요 약

본 논문에서는 LTS(Labeled Transition System)로 명세화된 철도 신호 제어 프로토콜의 동작의 정확성을 형식기법을 통해 검정하고 적합성 시험을 위한 시험계열을 자동으로 생성해 주는 도구로서 프로토콜 검정기와 적합성 시험 계열 생성기를 개발하였다. 본 도구는 과거에 사용되었던 비정형적 방법의 많은 오류와 모호함을 제거하고 프로토콜 개발시간 및 비용을 절약해 줌으로써 철도 신호 제어시스템의 안전성 및 신뢰성을 보장해 줄뿐만 아니라, 다른 시스템에도 응용되어 검정 및 시험을 효율적으로 수행하게 해주는 도구이다.

1. 서론

정보통신 관련 소프트웨어 시스템들이 점점 더 대형화, 복잡화, 다양화되어 감에 따라, 시스템간의 신뢰성 있는 통신을 위해서는 명세의 무결성 및 완전성을 검정하고, 원래 명세에 맞게 프로토콜이 구현되었는가를 검사함으로써 정확하고 효율적인 프로토콜을 개발하는 것이 필수적이다.

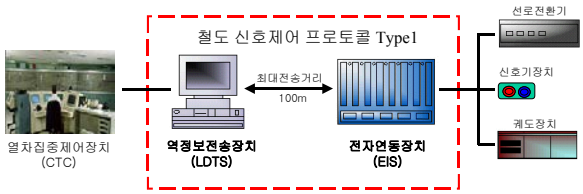
하나의 프로토콜을 개발하기 위해서는 사용자 요구사항 분석, 구조적 설계, 서비스 명세, 프로토콜 명세, 프로토콜 검정, 구현 및 적합성 시험의 단계를 거쳐야 하는데 그 중에서 특히, 프로토콜 검정과 적합성 시험은 가장 핵심적인 과정이다. 프로토콜 검정이란 사용자 요구사항과 명세와의 일치성을 구현전에 확인하는 단계로, 모든 프로토콜에 필수적인 정확성을 만족하는지를 모형검사(model checking)방법을 사용하여 자동적, 형식적으로 검정하는 기술이다[1]. 그리고 적합성 시험이란 프로토콜 표준으로부터 관련 제품 구현의 올바름을 검정하는 시험으로, 프로토콜 명세로부터 시험 계열을 생성하고 이를 구현에 적용함으로써 적합성 여부를 판단하는 일련의 과정이다[2].

이러한 검정 및 시험을 위해 과거에 사용된 비정형적 방법은 명세의 모호함과 불완전성 등의 많은 오류와 비효율성을 내포하고 있다. 따라서 개발에 소요되는 비용 및 시간을 절약함과 동시에 효율적이고 자동적인 개발을 수행하기 위하여, 본 논문에서는 LTS로 명세화된 철도 신호 제어 프로토콜의 동작의 정확성을 형식기법을 통해 검정하고, 적합성 시험을 위한 시험계열을 자동으로 생성하여 철도 신호 제어시스템의 안전성 및 신뢰성을 보장하게 해주는 프로토콜 검정기와 적합성 시험 계열 생성기를 개발하였고, 또한 검정 및 시험에 매우 강력한 성능을 보임을 실험적으로 증명하였다.

2. 검정 및 시험대상

철도 신호 제어 시스템의 구성은 (그림 1)과 같고, 본 논문에서 검정 및 시험할 대상인 철도 신호 제어프로토콜 type 1은 CTC(Centralized Traffic Control)로부터 제어명령을 전송받는 역정보전송장치(LDTS : Local Data Transmission System)와 신호전환기, 신호기 등의 현장신호설비를 제어하고 감시하는 전자연동장치(EIS : Electronic Interlocking System) 사이의 정보를 전송하는 방식이다.

LDTS는 EIS에게 폴링 메시지와 진로설정이나 선로전환기 혹은 주신호기 등을 제어하는 제어 메시지를 전송하고, EIS는 LDTS에게 현장 신호설비들의 상태정보 메시지와 제어 메시지에 대한 응답(ACK)을 전송하여 통신한다.

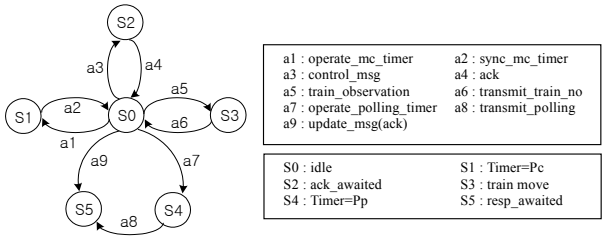


(그림 1) 철도 신호 제어 프로토콜 type 1

3. 프로토콜 검정기

(1) 모형검사를 이용한 프로토콜 검정

통신 프로토콜이 적절한 기능을 하기 위해서는 프로토콜 각 해당 상태의 deadlock과 livelock 및 비정상적인 도달(reachability)과 같은 잠재적 설계 에러가 없어야 하며, 사용자 요구사항과 일치하고 다른 프로세서와의 원활한 통신이 이루어져야 한다. 본 프로토콜 검정기는 deadlock, livelock, reachability, liveness 그리고 determinist와 같은 프로토콜의 특성을 보다 구체적으로 검정해 준다[3]. 프로토콜의 안전성과 필연성 특성을 검정하기 위해서는 프로토콜의 행위 특성을 나타내는 레이블 천이 시스템(Labeled Transition System)을 이용해 시스템을 명세하는데[4], LTS 작성시 주의할 점은 모든 천이가 반드시 초기상태 'S0'에서 시작해서 'S0'로 종결해야 한다는 것이다.

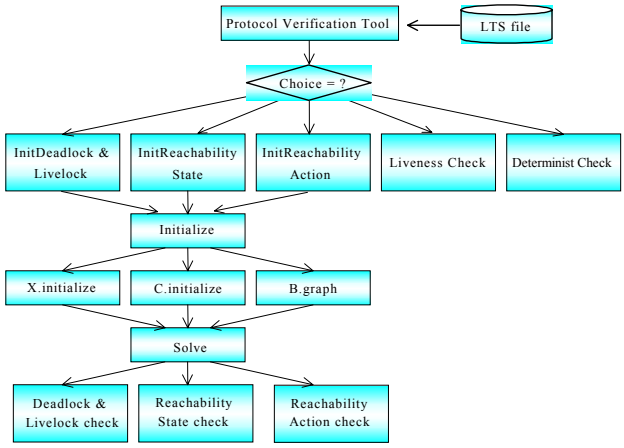


(그림 2) LDTS에 대한 LTS 모델링

(그림 2)는 역정보전송장치 LDTS의 상태와 행위의 천이관계를 LTS로 모델링한 것이다. 모형검사방법은 시스템 상태의 부분 집합이 공통적으로 만족하는 고정점을 가진 modal mu-calculus 논리식을 이용하여 시스템의 특성을 명세하며, R.cleaveland와 B.steffen에 의해 개발된 Solve 알고리즘[5]을 사용하여 위의 LTS로 명세화 된 철도 신호 제어 프로토콜을 검정한다.

(2) 프로토콜 검정기 알고리즘

위에서 기술한 모형검사 방법을 기반으로 구현된 프로토콜 검정기의 구성은 (그림 3)과 같다.



(그림 3) 프로토콜 검정기 구성도

본 프로토콜 검정기는 LTS 모델의 각 시퀀스를 현재 상태(Si), 행위(Action), 다음 상태(So)로 구성한 LTS 파일을 입력으로 하며 검사하고자 하는 대상을 선택하도록 한다. 사용자가 'Deadlock & Livelock', 'Reachability State', 'Reachability Action' 중에서 한 항목을 선택하면, 각각 정의된 modal mu-calculus 논리식에 따라서 초기화(initialize)를 하게 되는데, 초기화 모듈은 bit array를 초기화하는 X.initialize, counter array를 초기화하는 C.initialize, 그리고 edged-labeled directed graph를 생성하는 B.graph procedure를 호출하게 된다. 다음으로 X.initialize와 C.initialize, B.graph에 Solve 알고리즘을 적용시킨 후, bit array 및 counter array의 결과를 이용해서 Deadlock & Livelock, Reachability State, 그리고 Reachability Action을 검사하게 된다. 그러나 만약 사용자가 'Liveness' 또는 'Determinist'를 선택할 경우, 모형검사 알고리즘과는 상관없이 'Liveness check'는 초기상태에서 도달가능한 모든 상태와 행위를 출력하고, 'Determinist check'는 어떤

특정한 상태에서 동일한 행위에 의해 다음 상태가 두 가지 이상 존재하는지를 검사한다.

4. 적합성 시험 계열 생성기

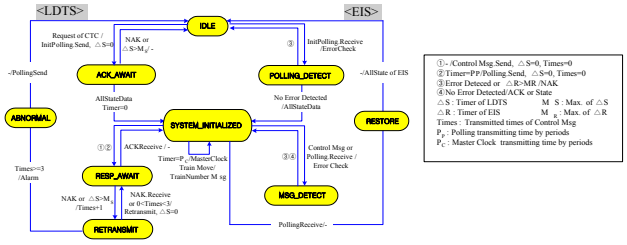
(1) UIO 시퀀스를 이용한 적합성 시험 계열 생성

적합성 시험은 주어진 명세 S(Specification)를 기초로 하여 생성된 시험 계열(test cases)을 이용하여 구현 I(Implementation)가 원래 명세(혹은 표준) S에 합당하게 구현되었는지를 시험하는 것이다[2]. 구현된 적합성 시험 계열 생성기는 각 천이에 해당하는 UIO(Unique Input/Output) 시퀀스와 시험 계열을 자동 생성해 줌으로써 철도 정보전송방식 구현 제품의 개발 생산 및 품질을 안정적으로 유지해준다.

UIO 시퀀스는 시험하는 천이 후에 도착한 상태의 유일한 입력/출력 시퀀스를 시험 계열에 포함시켜 적용한 후, 구현 I/O FSM(Input/Output Finite State Machine)의 결과 상태를 확인하는 방법으로, 적합성 시험 계열은 명세에 나타나 있는 각 천이에 도착 상태의 UIO 시퀀스를 연결하여 (식 1)과 같은 적합성 시험 계열 생성식에 적용함으로써 생성한다[6].

$$R_i \cdot \text{shortest-path}(S_0\text{-}S_i) \cdot T_{ij} @ \text{UIO}(S_j) \quad \text{(식 1)}$$

(그림 4)는 UIO 시퀀스를 이용하여 적합성 시험 계열을 생성하기 위해 통신 프로토콜의 제어(control) 부분을 모델링하는 I/O FSM으로 LDTS와 EIS간의 상호 동작을 표현한 것이다.

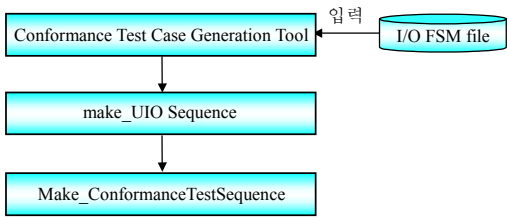


States	Descriptions of states
IDLE	A state before communicate between the LDTS and the EIS.
ACK_AWAITE	LDTS is waiting for ACK after transmitting a polling msg.
POLLING_DETECTE	EIS receives a polling msg, then checks the errors.
SYSTEM_INITIALIZED	Communication is initialized as LDTS receives ACK.
RESP_AWAITE	LDTS is waiting for ACK after transmitting a control msg.
RETRANSMIT	A state for retransmit, when receive NAK or expire the timer
MSG_DETECTE	EIS is checking a received control msg.
ABNORMAL	An abnormal state that LDTS receives a NAK or no reply after retransmission of three times.
RESTORE	A state restored from abnormal state to normal state.

(그림 4) 철도 신호 제어 프로토콜의 I/O FSM 모델링

(2) 적합성 시험 계열 생성기 알고리즘

기술된 'UIO 시퀀스를 이용한 적합성 시험 계열 생성' 방법을 기반으로 구현된 적합성 시험 계열 생성기의 전체 구성도는 (그림 5)와 같다.

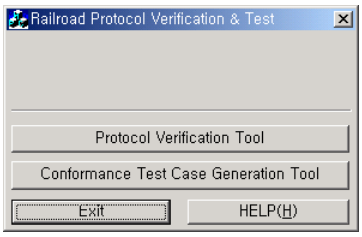


(그림 5) 적합성 시험 계열 생성기 구성도

적합성 시험 계열 생성기는 I/O FSM 모델의 각 시퀀스를 현재 상태(Si), 행위(Action), 다음 상태(So)로 구성한 FSM 파일을 입력으로 하며, 먼저 각 상태에 대해 유일하게 존재하는 UIO 시퀀스를 생성한 후, 각 행위에 대해 시험대상을 초기화 상태로 보내는 R_i, 초기상태에서 해당 시험천이까지의 shortest path, 시험천이 T_{ij}, 그리고 도착 상태의 UIO 시퀀스를 연결함으로써 시험 계열을 생성한다.

5. 개발도구의 구현

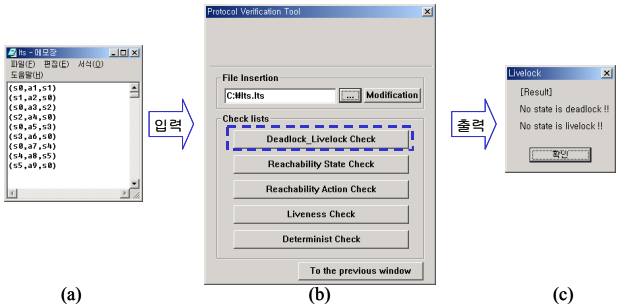
(그림 6)은 제안된 검정 및 시험 방법을 기반으로 개발된 철도 신호 제어 프로토콜을 위한 프로토콜 검정기 및 적합성 시험 계열 생성기이고, 사용자가 쉽게 다룰 수 있도록 윈도우 NT 환경 하의 GUI 기능에 의해 visual C++을 이용하여 구현되었다.



(그림 6) 프로토콜 검정기 및 적합성 시험 계열 생성기

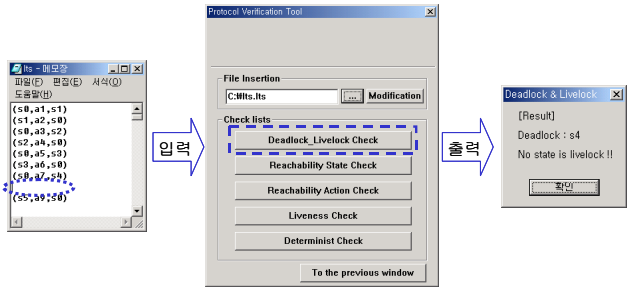
(1) 프로토콜 검정기

기술된 알고리즘을 사용하여 구현된 프로토콜 검정기의 실행화면은 (그림 7)의 (b)와 같다.



(그림 7) 완전한 모델 입력에 대한 검정기 실행화면

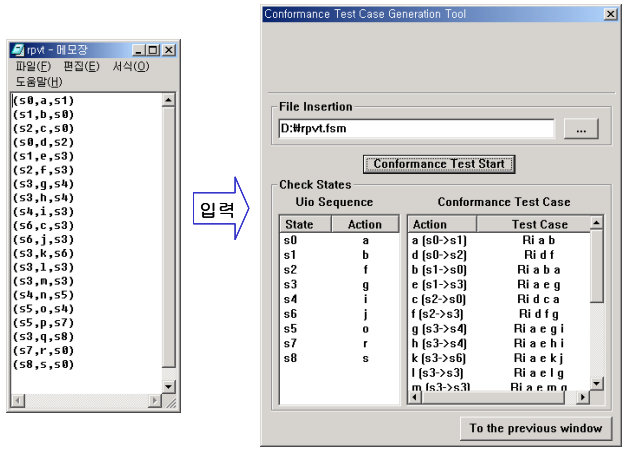
(그림 7)은 완전한 모델을 입력한 예로서, (그림 7)의 (a)와 같이 확장자가 lts인 완전한 LTS 모델을 입력으로 한 뒤, 'Deadlock_Livelock Check'를 실행하면, 내부의 모형검사 알고리즘을 수행하고, 결과로써 deadlock과 livelock이 발생하지 않았음을 출력한다. 또한 (그림 8)은 상태 'S4'에서 deadlock이 발생한 모델을 입력한 예로, 잘못된 입력으로 인한 deadlock의 발생과 발생한 장소를 출력하고 'Modification' 버튼을 사용해서 모델을 수정할 수 있도록 하였다.



(그림 8) Deadlock 발생 모델에 대한 검정기 출력

(2) 적합성 시험 계열 생성기

기술된 알고리즘을 사용하여 구현된 적합성 시험 계열 생성기의 실행화면은 (그림 9)와 같다.



(그림 9) 적합성 시험 계열 생성기 실행화면

확장자가 fsm인 파일을 검색하여 입력으로 하고 'Conformance Test Start' 버튼을 누르면, 각 상태에 대한 UIO 시퀀스와 각 천이에 대한 적합성 시험 계열이 출력된다.

5. 결론 및 향후 계획

본 논문에서는 정형기법으로 명세화된 모델에 대해 철도 신호 제어 프로토콜 동작의 정확성을 형식기법에 의해 검정하고 적합성 시험을 위한 시험계열을 자동으로 생성해주는 프로토콜 검정기 및 적합성 시험 계열 생성기를 개발하였다. 개발에 사용된 알고리즘은 검정 및 시험하고자 하는 사항별로 각각 모형 검사 방법 및 UIO 시퀀스를 이용하는 방법을 사용함으로써, 시스템 모델을 매우 정확하고 명료하게 검사하도록 하여 비형식적 방법에서 야기될 수 있는 오류와 모호함을 제거한다.

그리고 개발된 도구는 철도 신호 제어 시스템에 사용됨으로써, 프로토콜 개발시간 및 비용을 절약해 주고 철도 기술의 안전성 및 신뢰성을 보장해 줄뿐만 아니라, 더 나아가 다른 시스템에도 응용되어 사용될 수 있다.

참고문헌

[1] D.Schwabe, Formal Techniques for the Specification and Verification of Protocol, Ph.D Thesis, Univ. of California Los Angeles, Apr., 1981.

[2] R.J.Linn, Conformance Testing for OSI Protocols, Computer Network and ISDN Systems 18, 1989.

[3] A.teng and M.Liu, "A Formal Model for Automatic Implementation Logical Validation of Network Communication Protocol", NBS Computer Networking Symp., pp.114-123, 1978.

[4] P.V.Koppol and K.C.Tai, "Conformance Testing of Protocol Specification as Labeled Transition System", International Workshop on Protocol Test System, IWPTS95, pp.143-158, Evry, France, September, 1995.

[5] R. Cleaveland, B. Steffen, "A Linear-Time Model-Checking Algorithm for the Alternation-Free Modal Mu-Calculus", Formal Methods in System Design 2(2) : pp.121-147, 1993.

[6] 김상기, 김성운, 정재윤, "형식기술기법에 의한 AIN 프로토콜 적합성 시험 계열 생성", 한국정보처리학회논문지, 제4권 제2호, pp.552-562, 2월, 1997.