철도 신호시스템을 위한 새로운 통신 프로토콜의 성능해석 및 검증

論 文
53B-6-4

Formal Verification and Performance Analysis of New Communication Protocol for Railway Signaling Systems

李 在 浩* · 黃 宗 奎* · 朴 容 震** · 朴 貴 泰***
(Jae-Ho Lee · Jong-Gyu Hwang · Young-Jin Park · Gwi-Tae Park)

Abstract - In accordance with the computerization of railway signaling systems, the interface link between the signaling systems has been replaced by a digital communication channel. At the same time, the importance of the communication link has become increasingly significant. However, there are some questionable matters in the current state of railway signaling systems in KNR. First, different communication protocols have been applied to create an interface between railway signaling systems although the protocols have the same functions. Next, the communication protocols currently used in the railway fields have some illogical parts such as structure, byte formation, error correction scheme, and so on. To solve these matters, the standard communication protocol for railway signaling systems is designed. The newly designed protocol is overviews in this paper. And the simulation is performed to analysis the performance of data link control for designed protocol. According to this simulation, it is identified that the link throughput of new protocol is improved about 10% and the frame error rate is improved than existing protocol. And it is verified the safety and liveness properties of designed protocol by using a formal method for specifying the designed protocol. It is expected that there will be an increase in safety, reliability and efficiency in terms of the maintenance of the signaling systems by using the designed communication protocol for railway signaling.

Key Words : FDT(Formal Description Technique), Railway Signaling Protocol, Formal Verification, Modal-μ Calculus, LTS(Label Transition System)

1. 서 론

철도 신호제어장치들은 각자 고유기능을 수행함으로써 철도시스템의 안전운행을 도모하고 있다. 따라서 대부분의 신호장치는 철도특유의 안전측 동작(Fail-safe)을 보장하기 위하여 기존에는 기계적 또는 전기적인 계전기 로직에 의해 각 장치 고유의 기능을 수행하였다. 그러나 최근에 들어 전자, 컴퓨터, 통신 기술의 발달에 따라 철도 신호제어장치들도 전자화된 장치로 바뀌고 있는 추세이다. 이처럼 신호제어장치들이 전자화되어감에 따라 각 장치간 인터페이스를 위한 링크도 디지털 통신채널로 대체되어가고 있다. 따라서 이러한 각 장치간 인터페이스를 위한 통신링크에 대한 중요성이 증대되고 있다.

대부분의 철도 신호제어장치들은 온도, 진동, EMI(ElectroMagnetic Interference) 등의 운용환경이 가혹한 선로변에서도 안전하게 동작하여야 하므로 안전동작을 위한 높은 신뢰성이 신호장치 뿐만 아니라 신호장치간의 통신링크에도 필수적으로 요구되는 사항이다. 국내에서는 사용되는 신호장치간의 프로토콜은 각 제작사별, 각 노선별 서로 상이함으로 인해 통신시스템을 포함한 신호제어시스템의 안전성 저하는 물론이고 유지보수에도 어려움이 있어 철도신호제어시스템을 위한 새로운 표준화된 프로토콜에 대한 요구가 증대되고 있다. 따라서 본 논문에서는 이러한 문제점들을 해결하기 위해 국내의 철도 신호시스템을 위한 높은 신뢰성을 갖는 새로운 표준 프로토콜을 개발하였다.

현재 철도청의 철도 신호시스템에 사용되고 있는 통신 프로토콜에는 몇 가지 문제를 가지고 있다. 첫째로 철도 신호시스템을 위한 기존 프로토콜들은 여러 제조사로부터 공급됨에 따라 동일한 기능을 가지고 있음에도 불구하고 실제로는 서로 다른 프로토콜들이 적용되고 있어, 통신 시스템뿐만 아니라 전체 신호제어시스템의 신뢰성 저하 및 유지보수에 많은 어려움이 있다. 두 번째로는 기존에 적용되고 있는 프로토콜들이 구조, 바이트 형식, 에러수정방식 등에서 다소 불합리한 하게 되어있다는 것이다. 이외에도 여러 가지 개선되어야 할 점들이 기존 프로토콜들을 분석하면서 도출되었다. 이러한 문제들로 인하여, 통신링크에 대한 신뢰성의 감소와 유지보수와 관련하여 많은 어려움이 존재해 왔으므로 높은 신뢰성을 갖는 표준 프로토콜을 필수적으로 요구되어졌다. 기존 프로토콜의 문제에 관련된 더 상세한 내용은 2절에 기술하였다.

* 正 會 員 : 韓國鐵道技術研究員 先任研究員
** 非 會 員 : 漢陽大學校 電氣通信電波工學部 敎授, 工學博士
*** 正 會 員 : 高麗大學校 電氣電子電波工學部 敎授, 工學博士
接受日字 : 2004年 2月 25日
最終完了 : 2004年 3月 27日

이러한 문제를 해결하면서 고 신뢰성을 갖는 새로운 프로토콜의 개발을 위해서는 철도 신호시스템의 통신링크에 적용에 대한 성능해석이 수행되어야 한다. 본 논문에서는 이러한 철도신호용 데이터링크 프로토콜들의 성능분석을 위해 Matlab/Simulink 기반의 시뮬레이션 툴을 개발하여, 이 툴을 이용하여 철도신호용에 적합한 최적의 프로토콜 변수들을 설정하는 등 새로운 프로토콜을 설계하였다[4-6].

하지만 이렇게 비정형적 방법(Informal method)에 의해 개발된 프로토콜은 오류와 비효율성을 내포할 가능성이 내재하고 있어, 이러한 프로토콜이 바이탈 철도 신호시스템에 적용되게 되면 치명적인 결함이나 사고를 발생시킬 수 있다. 따라서, 새롭게 설계된 프로토콜을 정형적인 방법에 의해 검정하기 위하여 유한상태 레이블 천이시스템 (LTS : Labeled Transition System)으로 모델링하였으며, 대수적 명세기법 중 프로토콜의 행위특성을 가장 강력하게 표현하는 Modal μ-calculus를 사용하여 명세화하고 모형검사(Model checking) 알고리즘인 Solve 알고리즘을 적용하여 프로토콜의 명세특성인 안전성과 필연성 특성을 검정하였다[7,8].

본 논문은 철도신호를 위한 표준화된 통신 프로토콜의 설계를 위하여 다음과 같이 구성되어있다. 2절에서는 기존 통신 프로토콜의 검토를 통하여 문제점을 분석하고, 3, 4절에서는 프로토콜 성능해석을 수행하여 프로토콜을 설계하여, 5절에서 설계된 프로토콜의 우수성을 확인하기 위하여 기존 및 설계된 프로토콜에 대한 시뮬레이션을 통한 성능해석 결과를 나타내었으며, 6절에서는 설계된 통신 프로토콜에 대한 안전성 검증을 위하여 형식적 방법을 도입한 결과 설계된 통신 프로토콜이 안전성과 필연성을 확보하고 있음을 보였으며, 마지막으로 결론을 기술하였다.

2. 철도신호를 위한 기존 통신프로토콜의 검토

그림 1은 한국철도의 철도신호시스템 전체 구성을 나타낸 것으로, 그림에서와 같이 많은 신호시스템들이 서로 인터페이스되면서 하나의 신호제어시스템으로 운용되고 있다. 본 절에서는 여러 신호제어장치들 중 가장 대표적인 전자연동장치(EIS : Electronic Interlocking System)와 역정보전송장치(LDTS : Local Data Transmission System)간의 인터페이스를 위한 현재의 주요한 프로토콜을 요약하였다.

전자연동장치는 선로변의 신호기나 선로전환기의 제어를 통하여 열차진로의 안전을 확보하는 장치이며, 역정보전송장

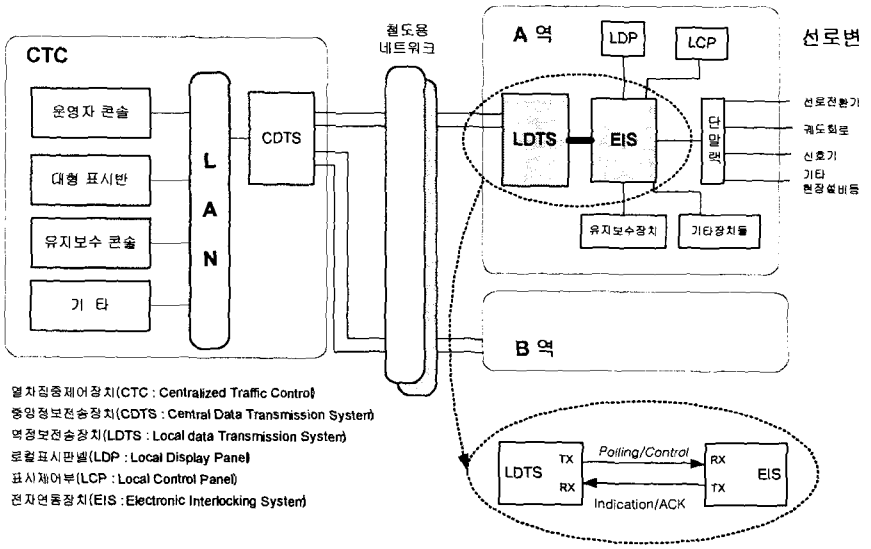


그림 1 철도청의 신호시스템의 구성

Fig. 1 Configuration of signaling systems for KNR

치는 전자연동장치와 제어센터의 열차집중제어장치(CTC : Centralized Traffic Control)와 정보교환을 위한 통신장치이다. 즉, LDTS는 CTC로부터 제어명령을 받아 EIS로 전송하고, 반대로 현장신호장치들의 상태정보를 EIS로부터 받아 CTC로 전달하는 통신허브 역할을 담당하고 있어, 철도신호시스템의 동작에 매우 중요한 링크이므로 만약 이 링크에 어떠한 결함이나 오류가 포함되어 있으면 심각한 사고를 초래할 수 있다.

LDTS와 EIS 사이의 통신 링크에는 현재 여러 가지의 통신 프로토콜이 적용되고 있으나 I/O 프로토콜이라 불리워지는 프로토콜이 가장 많이 적용되고 있다. 따라서 이하 본 논문에서는 이 I/O 프로토콜을 기존 프로토콜이라 한다. 이 프로토콜은 디지털 통신을 위해 설계된 프로토콜이 아닌 기존의 전기연동장치를 전자연동장치로 교체하면서 만들어지게 된 기형적인 구조를 가지고 있다. 즉, 기존시스템에서 LDTS는 기존의 전기 연동장치의 계전기 접점 제어를 위해 여러 장의 I/O 보드를 통해 인터페이스를 하였다. 하지만 LDTS는 그대로 두고 전기연동장치를 전자연동장치로 교체되면서 기존의 인터페이스 방식을 그대로 사용하면서 그림 2와 같은 구조의 통신프로토콜이 사용되게 되었다. 즉 디지털 통신으로 바뀌었음에도 기존의 전기식처럼 I/O 보드별 통신 방식을 사용하고 있어, 이 기형적인 프로토콜이 I/O 프로토콜이라 불리고 있다.

Flag Bit 7	6	5	4	3	2	1	0
1	Destination Type Number			Destination ID Number			
0	Source Type Number			Source ID Number			
0	Long/Short Bit	Long : Message Type, bit 0-6					
		Short : Message Type, bit 0-6					
0	Long : Length of Message(includig bytes 1-4)						
	Short : Termination Checksum						
0	Long : Data Bytes 1...n						

그림 2 I/O 프로토콜의 메시지 프레임 형식(EIS ⇒LDTS)

Fig. 2 Transmitted message frame format of I/O protocol (EIS ⇒LDTS)

이 프로토콜은 여러 가지 문제점들을 가지고 있다. 첫째로 아직도 LDTS에서는 EIS와의 디지털 통신을 하면서도 EIS를 I/O 보드로 인식하는 방식을 사용하여 각각 할당된 주소로 통신을 하고 있다. 즉, 그림 2에서와 같이 메시지 헤더에 'Destination Type Number'와 'Destination ID Number' 필드의 존재가 그 예이다. 일반적인 점대점 통신 프로토콜에서 실질적인 메시지 전송에 전혀 필요가 없는 이러한 데이터필드가 사용될 이유가 없다. 두 번째로는 송수신 전송메시지의 바이트 형식이 일반적인 형식과 다르다는 것이다. 일반적으로 1바이트는 8비트로 구성되지만 기존 프로토콜에서는 1바이트는 그림 2에서 보인 것처럼 9비트로 구성되어 있으며, 이 9th 비트를 이용하여 메시지의 시작을 확인하도록 하고 있다. 즉, 메시지의 처음 바이트를 제외하는 모든 바이트의 9th 비트는 0이 되게 된다. 이러한 방식을 사용하는 것은 이들 신호설비들에 적용한 프로세서가 이러한 바이트 구성을 지원하기 때문에 가능한 방식이며, 다른 CPU를 사용할 경우에는 적용이 불가능한 방식이다. 컴퓨터의 라이프싸이클이 너무 빨라 9비트 바이트 형식을 지원하는 컴퓨터 시스템이 현재는 거의 사용되지 않고 있으며, 일반적으로 8비트 바이트 형식이 표준으로 받아들여지고 있다. 이에 따라 요즘의 프로토콜들은 메시지의 시작을 나타낼 때는 프레임의 맨 처음에 프레임의 시작을 의미하는 필드를 삽입함으로써 메시지의 시작이 확인되는 구조를 사용하고 있다. 이상과 같이 위 두 가지의 문제 외에도 부가적인 사소한 문제가 있지만 이 두 가지의 문제점이 가장 핵심적인 요점이 되고 있다.

3. 성능해석 모델

성능해석을 위한 데이터 링크 제어시뮬레이션의 주된 목적은 신호형태나 E_b/N_0, 물리적인 링크조건, 에러제어 등과 같은 다양한 링크 조건 하에서 처리율, FER(Frame Error Rate) 등을 해석하는 것이다. 이 중 BER(Bit Error Rate or Bit Error Probability)의 계산이 데이터 링크 프로토콜 시뮬레이션을 위한 첫 번째 단계이다. 전송된 비트 에러율은 다음의 식(1)로 표현된다[14-15]. 이 식(1)로부터 프레임 에러율은 식(2)와 (3)과 같이 얻어질 수 있다. 식(2)에서 P_n은 에러검지코드를 CRC 코드를 사용한 경우로, 적용된 코드에 따라 조금씩 변경되게 된다.

$$P_b = Q\left(\sqrt{\frac{E_b(1-\cos\theta)}{N_o}}\right) \tag{1}$$

여기서, P_b : 전송된 비트 에러확률

E_b : 1비트의 신호에너지

N_0 : 잡음전력 스펙트럼 밀도

θ : 2개의 2진 신호벡터간의 각

Q : 상보 오류함수

$$P_n \le 2^{(k-n)}\left[\,1+(1-2P_b)^n-2(1-P_b)^n\,\right] \tag{2}$$

$$P_{fe} = \frac{P_n}{(1-P_d)} \tag{3}$$

여기서, P_n : 에러를 검지 못할 확률

P_{fe} : 프레임 에러확률

k : 정보비트 수, n : 코드비트 수

데이터 링크의 에러제어는 일반적으로 자동재전송요구(Automatic repeat request : ARQ)를 사용하고 있으며 구성은 정지-대기(Stop-and-Wait : SW), Go-Back-N(GBN) 및 Selective-Reject(SR) ARQ이며, 이들 각각에 대한 처리율(Throughput)은 다음과 같다. 데이터 링크 프로토콜 성능해석을 위한 프레임에러확률(P_{fe})과 처리율(η_{-ARQ}) 수식의 자세한 유도과정은 [3]에 설명되어져 있다.

$$\eta_{SW-ARQ} = \frac{k}{(T_D N_R)R_S} = \frac{\frac{k}{n}(1-P_d)}{1+\frac{n'}{n}} \tag{4}$$

$$\eta_{GBN-ARQ} = \frac{(k/n)(1-P_d)}{1+(n'/n)P_d} \tag{5}$$

$$\eta_{SR-ARQ} = \frac{k}{n}(1-P_d) \tag{6}$$

위에서 설명한 것과 같은 수학적인 모델링을 기반으로 철도신호를 위한 새로운 프로토콜 설계를 위한 데이터링크 프로토콜 성능해석 툴을 개발하였으며, 이 프로그램을 통해 P_b를 계산하고 이를 바탕으로 BER, FER를 계산하고 마지막으로 FER과 처리율을 계산할 수 있다. 또한 개발된 툴에서는 GUI(Graphic User Interface)를 통해 데이터링크 프로토콜의 다양한 파라메터들을 조정할 수 있도록 하여 보다 효과적인 성능해석이 가능하도록 하였다. 데이터링크 프로토콜에서 가장 중요한 측정기준은 프레임 에러율, 처리율 및 전송시간이다. 그러나 Fail-safe 특성을 갖는 철도 신호제어 시스템의 통신링크에서는 전송되는 데이터 량이 제한되어 있으며, 이 제한되어 있는 데이터들이 높은 신뢰성을 가지면서 보다 정확하게 전송되는 것이 무엇보다도 중요하다. LDTS와 EIS 사이 통신링크에서도 전송되는 데이터 량이 제한되어 통신링크에서의 지연시간은 주요한 요점이 되지 않으며, FER이나 처리율이 주요한 성능평가 메트릭이 된다.

4. 새로운 철도신호용 프로토콜

앞 절에서 언급한 것처럼, 기존의 프로토콜에는 몇 가지

문제점들을 가지고 있다. 즉, 프로토콜 구조에서 불합리한 특성을 가지고 있고 같은 기능에도 불구하고 인터페이스 링크에 여러 가지의 다양한 프로토콜들이 적용되어지고 있다. 이러한 문제점들의 해결을 위해 본 논문에서는 철도신호용 새로운 프로토콜을 제안한다. 이 제안된 프로토콜의 상세한 설명은 [2],[3]에 설명되어져 있다.

설계된 프로토콜은 기존 프로토콜의 단점을 제거한 향상된 구조와 메커니즘을 가지고 있다. 더욱이 이 프로토콜에서는 표 1에서처럼 STX와 ETX 필드를 추가함으로써 송수신 전송프레임의 시작과 끝을 정확히 하였다. 이 필드들은 기존 프로토콜에서의 9th 구성과 같은 기능을 제공한다. 또한, 기존파일에 있는 불필요한 필드들인 Destination과 Source Type/ID은 제거하였다. 메시지 프레임의 전송동안 에러검지성능을 향상시키기 위하여, 기존 프로토콜에서의 BCC 코드를 CRC-16 에러검지 코드를 사용하여 에러검지확률을 향상시켰다[1][3]. 표 1은 설계한 통신 프로토콜의 전송 메시지 구조를 보이고 있다.

표 1 설계한 프로토콜의 전송 메시지 형식

Table 1 Message format of designed communication protocol

STX	Data Length	Sequence Number	Message Type	Data	CRC	ETX
1 byte	1 byte	1 byte	1 byte	N byte	2 byte	1 byte

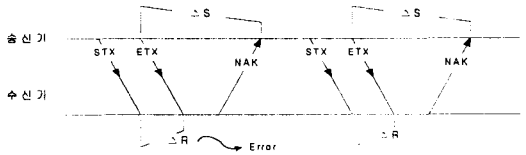
여기서, - STX : 메시지 프레임의 시작
- Data Length : Message Type부터 CRC 앞까지 메시지 길이(최대 255 바이트)
- Sequence Number : 메시지 전송순서, 0x00~0xFF
- Message Type : 전송되어지는 메시지 형식
- Data : 실제 전송되는 데이터로 Data 필드의 길이는 정보 전송에 따라 가변
- CRC : CRC 16($X^{16}+X^{15}+X^2+1$)
- ETX : 메시지 프레임의 마지막

메시지의 흐름제어는 SW ARQ 방식을 적용하였고, 메시지 전송 시 에러검출을 위하여 CRC 16 에러검지코드가 사용되어 ACK/NAK 제어메시지가 에러검출과 흐름제어를 위하여 사용되어지고, 메시지는 에러 검지의 경우에 재 전송되도록 하였다. 다음은 재전송 메커니즘을 표시한 것이다.

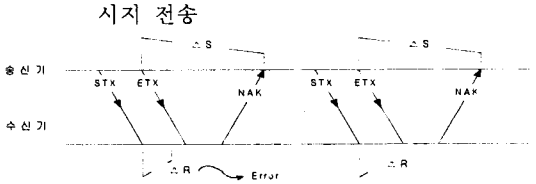
(a) 송신측에서 다음의 경우 발생 시 동일한 메시지를 수신측으로 재 전송하게 되며, 최대 3회까지 재 전송한다.

① 수신측으로부터 NAK을 응답받는 경우

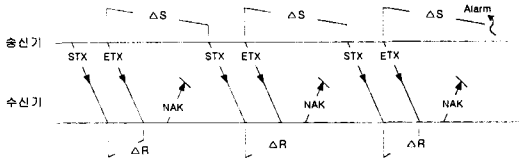
Case I : 수신측에서 에러검지코드에 의한 전송프레임의 에러검지할 경우와 수신측에서 시퀀스번호에 오류가 발생한 경우 송신측으로 NAK 메시지 전송



Case II : 수신타이머 설정시간 $\triangle R$이 끝났음에도 송신측으로부터 ETX 메시지를 받지 못하는 경우 오류로 판정하여 송신측으로 NAK 메시지 전송



② 송신측에서 메시지를 전송함과 동시에 송신타이머 $\triangle S$를 동작시켜 이 타이머 설정시간이 경과하여도 수신측으로부터 ACK나 NAK과 같은 어떠한 응답 메시지도 받지 못하는 경우



(b) 동일 메시지를 3번 재 전송하였음에도 수신측으로부터 어떠한 응답도 받지 못하는 경우 송신측은 통신링크 에러로 판단한다. 그리고 송신측은 전송메시지를 버리고 링크에러 처리하게된다. 이때 송신측은 링크의 복구를 확인하기 위하여 0x00시퀀스 번호를 갖는 폴링메시지를 수신측에 주기적으로 전송한다.

5. 성능해석 결과

데이터 링크 제어와 관련하여 설계된 프로토콜 성능을 검정하기 위하여, 2절과 4절에서 기술한 기존 프로토콜과 새롭게 설계한 프로토콜을 표2와 같은 조건 하에서 3절에서 제시된 성능해석모델을 기반으로 프레임 에러 확률과 링크 처리율이 성능 측정기준으로 시뮬레이션이 수행되었다. 시뮬레이션에서 통신 링크 주위의 환경인 Eb/No 의 범위는 -10~20 [dB]로 하였으며, 전송매체는 일반 동 케이블 조건으로 하였다. 다음의 본 논문에서 ARQ 방법을 하나로 고정시킨 시뮬레이션 결과만을 제시하였으며, 또한 이를 다른 방법으로 적용할 경우의 성능 해석한 결과들도 본 논문에서 제시한 결과와 유사함을 확인할 수 있었다[1].

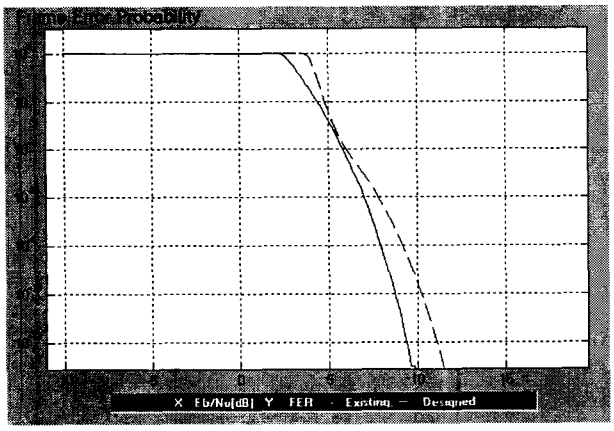
표 2 시뮬레이션 조건

Table 2 Simulation conditions

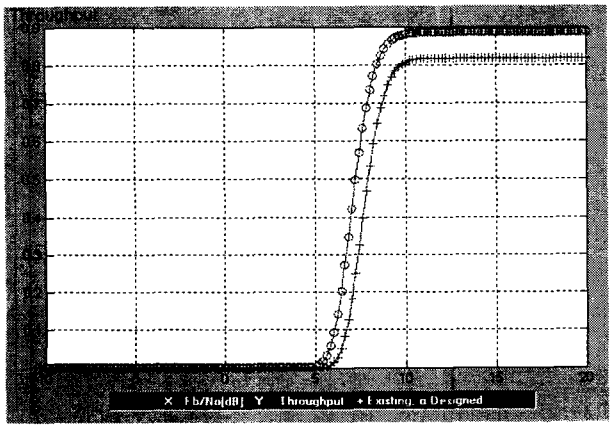
Eb/No	-10 ~20 [dB]
Signal Type	Bipolar
데이터 필드 길이	100[Byte]
물리적 링크거리	100[m]
전송매체 전달속도	2×10^8[m/s]
ARQ 방법	SW ARQ

표 2의 시뮬레이션 조건 하에서 기존 프로토콜과 설계된 프로토콜의 성능해석이 수행되었으며, 그림 3(a)는 새로운

프로토콜과 기존 프로토콜의 프레임 에러확률 시뮬레이션 결과를 비교한 것으로 5 [Eb/No]에서 기존 프로토콜은 약 10^{-4}~10^{-3} 이지만 새로운 프로토콜에서는 10^{-5}~10^{-3}으로 향상되었음을 확인할 수 있으며, 시뮬레이션에서 적용한 대부분의 E_b/No 범위에서 새로운 프로토콜이 기존의 것보다 우수하다는 것을 보여준다. 그림 3(b)은 두 프로토콜의 처리율 특성을 나타낸 것으로 처리율이 설계된 프로토콜이 10[dB]에서 약 10%정도 향상되었음을 확인할 수 있다. 이러한 시뮬레이션 결과들을 통해 설계된 프로토콜이 기존의 프로토콜에 비해 우수한 성능을 가지고 있음이 확인되었다.



(a) 프레임 에러 확률



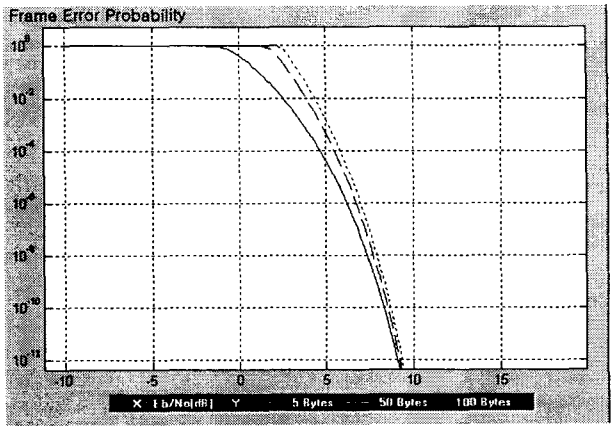
(b) 처리율

그림 3 성능해석결과 비교

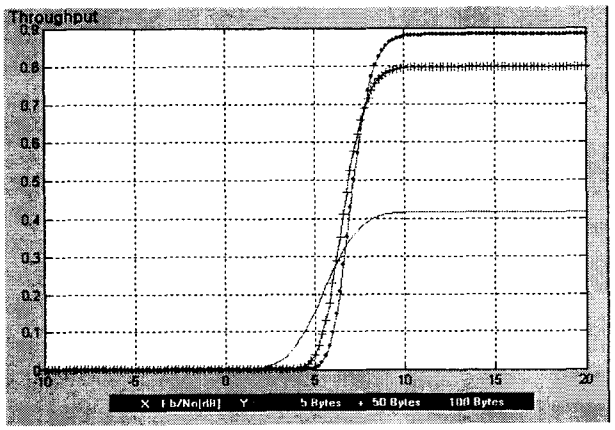
Fig. 3 Comparison of performance analysis results

그림 4는 설계된 프로토콜의 데이터 필드 길에 따른 성능 특성을 보여주고 있다. 그림 4(a)는 프레임 에러확률 특성을 나타내며, 메시지 프레임의 데이터 필드 길이와 관련하여 조금씩 다른 값을 나타내고 있다. 전송된 데이터의 에러확률은 일반적으로 메시지 프레임 길이, 에러제어 방법, 흐름제어 방법 등과 같은 여러 가지 파라메터들에 의해 영향을 받는다. 그러나 그림 4(a)의 결과는 프레임 에러확률이 전송되는 메시지 프레임 길이에 의존적이고 설계된 프로토콜에서는 영향이 낮은 것으로 분석되었다.

그림 4(b)는 데이터 필드길이가 각각 5, 50 및 100바이트일 때 링크처리율을 나타내고 있다. 이것은 링크 처리율이 전송되는 프레임 길이에 매우 많은 영향을 받음을 알 수 있다. 전송되는 메시지의 에러율은 철도신호의 높은 신뢰성 요구 때문에 처리율보다 더 중요한 필수적인 성능지수이다. 따라서 새로운 프로토콜에 대한 데이터 필드길이가 가변되도록 하는 것이 철도신호시스템의 프로토콜 구성에 더 적합하다.



(a) 설계된 프로토콜의 프레임 에러확율



(b) 설계된 프로토콜의 처리율

그림 4 데이터 필드의 변화에 따른 성능비교

Fig. 4 Performance comparison with varying data field

6. 설계된 프로토콜의 검증

통신 소프트웨어 대한 사용자 요구사항의 복잡화 및 다양화에 따라서 비정형적인 방법에 의한 개발은 오류와 비효율성을 내포할 수 있다. 철도신호시스템과 같이 바이탈한 제어시스템에 적용되는 프로토콜에도 이러한 모호성이 존재하게되면 신호시스템의 제어에 치명적인 결함이나 사고를 불러일으킬 수 있다. 그러므로 철도신호시스템과 같은 바이탈 시스템을 위한 통신프로토콜은 형식적인 방법에 의해 정확하게 구현 및 검정되어야 한다. 따라서 프로토콜 설계에 있어서 심각한 오류를 형식적인 방법에 의해 검증하는 정형검증(Formal Verification)이 필요하다.

본 연구에서는 이를 위해 철도신호를 위한 설계된 프로토콜을 검정하기 위하여 중간모델인 유한상태 레이블 천이시스템 (LTS : Labeled Transition System)으로 모델링하였으며, 대수적 명세기법 중 프로토콜의 행위특성을 가장 강력하게 표현하는 Modal μ-calculus를 사용하여 명세화하고 모형검사(Model Checking) 알고리즘인 Solve 알고리즘을 적용하여 프로토콜의 명세특성인 안전성과 필연성 특성을 검정하였다.

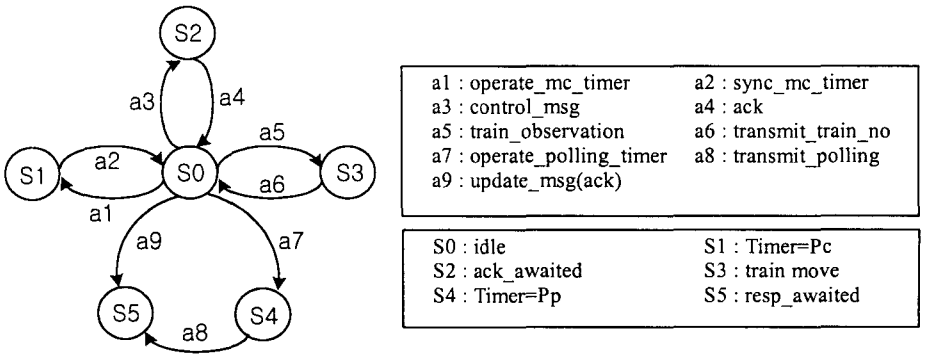


그림 5 설계된 프로토콜의 LTS 모델링
Fig. 5 The LTS modeling for designed protocol

6.1 LTS 모델링

LTS는 프로토콜을 검정하는 정형명세 기법 중 프로토콜 정형명세를 위한 의미모델로서 많이 사용되며 다음과 같이 정의한다[16].

$$LTS = \langle S, L, T, s_o \rangle \tag{7}$$

여기서, S : 상태들의 집합(a set of states)
L : 관찰 가능한 행위집합(a set of observable actions)
$T \subseteq Sx(L+\tau)xS$: 천이 관계 (transition relation)
$s_o \in S$: 초기상태(initial state)

이 정의에서 심볼 "τ"는 비결정형 모델(Non-determinant Model)을 위해 이용되는 시스템 내부 혹은 관찰이 가능하지 않은 행위(Internal 혹은 Inobservable Action)를 나타낸다. 그림 5는 제시된 프로토콜을 프로토콜 정형 명세를 위한 의미모델인 LTS로 모델링한 것이다.

6.2 검정항목

프로토콜의 개발에 있어서 중요한 부분인 프로토콜 명세화를 위한 검정은 그들의 명세화에 의해 규정되어진 것처럼 시스템 기능에서 확실성의 수준을 증가시키기 위하여 사용되어지는 상호보완적인 기법이다. 즉, 설계된 프로토콜에서 Deadlock과 Livelock 상태, 비정상적인 Reachability 및 잠재적인 설계오류가 존재하지 않음을 검증하여야만 한다.

프로토콜 검정은 프로토콜 명세의 정확성(Correctness), 안전성(Safety)과 필연성(Liveness) 및 일관성(Consistency) 등을 알아보는 것으로 모형검사에서 보다 구체적으로 검정해야 하며, 모형검사기로 불리어지는 알고리즘인 LTS로 표현된 모델이 정확성을 만족하는지를 검정하기 위하여 사용되어진다. 여기에는 다음과 같은 2종류의 특성이 있다:

- 안전성(Safety)은 부당한 상태나 행위가 결코 일어나지 않은 상태이다. 즉, 시스템은 결코 받아들일 수 없는 상태로 들어가지 않는다. 통신 프로토콜에서 안전성 잘 알려진 예로는 Deadlock 이나 Livelock이 없는 것이다

- 필연성(Liveness)은 정당한 상태와 행위가 결국 일어나는 상태이다. 즉, 미리 정해진 상태와 행위가 필수적으로 발생한다. 이것은 도달성으로 정의된다.

6.3 Modal μ-calculus

Kozen[10]의 Modal μ-calculus는 통신 프로토콜의 안전성과 필연성 특성을 표현하는 최소 및 최대 고정점 연산자를 사용함으로써 Temporal 특성을 표현하는 강력한 로직이다. Modal μ-calculus에서, 구문은 원자명제(Atomic Propositions), $\wedge$(논리곱 : Conjunction), $\vee$(논리합 : Disjunction), [ ](필연성 : Necessity), < >(가능성 : Possibility), ν(최대고정점 : Greatest Fixed Point) 및 μ(최소고정점 : Least Fixed Point)로 구성되며, 일반화된 Modal μ-calculus의 논리식은 다음과 같다.

$$\Phi ::= tt \mid ff \mid Z \mid \Phi_1 \wedge \Phi_2 \mid \Phi_1 \vee \Phi_2 \mid [k]\Phi \mid \langle k \rangle \Phi \mid \Phi \mid \mu Z.\Phi \mid \tag{8}$$

여기서, ν & μ : 각각 최대, 최소 고정점을 표현하는 연산자
tt & ff : 각각 모든 상태에 대하여 참인 것과 거짓인 것을 나타냄
Z : 명세적 변수
k : 행위집합의 원소
Φ : 프로세스 특성을 나타내는 논리식

안전성은 프로토콜의 부당한 상태 즉, Deadlock이나 Livelock과 같은 상태를 배제하는 특성이고, 필연성은 통신 프로토콜에서 Reachability와 Liveness를 만족시키는 특성이다. 만약 다음의 Modal μ-calculus 논리식이 각각 참이라면, 이것은 설계된 통신 프로토콜의 안전성과 필연성이 정확히 검정되었다는 것을 의미한다.

- 상태에 대한 안전성 : $\nu Z.\Phi \wedge [-]Z$
- 행위에 대한 안전성 : $\nu Z.\Phi[k]ff \wedge [-]Z$

- 상태에 대한 필연성 : $\mu Z.\Phi \vee (\langle - \rangle tt \wedge [-]Z)$
- 행위에 대한 필연성 : $\mu Z.\Phi \langle - \rangle tt \wedge [k]Z$

6.4 프로토콜의 정형검정

이 절에서 식(8)에 표현된 Modal μ-calculus 논리식을 사용하여 설계된 프로토콜을 검정하는 것으로 이것은 프로토콜의 정확성을 조사한다는 것을 의미한다. 예를 들면, 만약 설계된 프로토콜의 LTS에 Deadlock과 Livelock이 존재하지 않게 구성되어 있다면 식(8)은 참이 된다.

$$\nu Z.(\mu Y.A \vee (\langle - \rangle tt \wedge [-]Y)) \wedge [-]Z \quad 단,\ A=\{S0\} \quad (9)$$

위 식(9)에 모형검사 알고리즘인 Solve 알고리즘[11]을 적용하여 검정결과를 산출한다. 그림 6은 최소, 최대 고정점을 사용하여 식(9)로부터 생성된 최소블럭(Min Block)과 최대 블럭(Max Block)을 나타내고, 그림 7은 Edge-labeled Directed Graph G로 표현된 변수들의 천이관계를 보여준다.

$B_1 \equiv \min\{X_1 = X_2 \vee X_3$	$B_2 \equiv \max\{X_7 = X_1 \wedge X_8$
$X_2 = A$	$X_8 = [-]X_7\}$
$X_3 = X_4 \wedge X_5$	
$X_4 = [-]X_1$	
$X_5 = \langle - \rangle X_6$	
$X_6 = tt\}$	

그림 6 최대 및 최소 블록
Fig. 6 Max block and min block

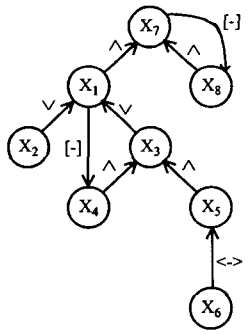


그림 7 Edge-labeled directed 그래픽 G
Fig. 7 Edge-labeled directed graph G

그림 8은 Solve 알고리즘의 초기화 규칙에 의해 초기화된 비트-벡터, 계수기 및 배열 M을 나타낸다. 그리고 그림 9는 배열 M[i]가 공집합(Empty)이 될 때까지 갱신알고리즘을 적용하여 비트-벡터와 카운터를 갱신한 결과로 검정대상인 Deadlock 및 Livelock을 판단할 수 있다.

Deadlock은 비트-벡터의 요소에 의해 판단되는데, 그림 9의 결과에서, 원소명제(Atomic Proposition) A와 관련된 X2 요소를 제외하고 모든 비트-벡터는 1로 갱신되어 설계된 프로토콜의 LTS모델에서 Deadlock이 없음을 발견할 수 있다. 또한, Livelock은 계수기(C)의 요소를 통하여 검지될 수 있다. 그림 9의 결과 계수기의 모든 요소가 0으로 갱신되어 LTS모델에서 Livelock이 없음을 발견할 수 있다. 이들 결과로부터, 설계된 프로토콜에 대한 위 표현된 LTS모델은 논리식 $\nu Z.(\mu Y.A \vee (\langle - \rangle tt \wedge [-]Y)) \wedge [-]Z$, $A=\{S0\}$을 만족하므로, 이 프로토콜은 완전성을 만족하는 적정한 모델로 검정되었다.

X	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
S0	0	1	0	0	0	1	1	1
S1	0	0	0	0	0	1	1	1
S2	0	0	0	0	0	1	1	1
S3	0	0	0	0	0	1	1	1
S4	0	0	0	0	0	1	1	1
S5	0	0	0	0	0	1	1	1

C	X_3	X_4
S0	2	4
S1	2	1
S2	2	1
S3	2	1
S4	2	1
S5	2	1

M[1]=<<S0, X2>, <S0, X6>, <S1, X6>, <S2, X6>, <S3, X6>, <S4, X6>
<S5, X6>>
M[2]=< >

그림 8 비트-벡터, 계수기 및 배열M[i]
Fig. 8 Bit-vector, counter and array M[i]

X	X_1	X_2	X_3	X_4	X_5	X_6	X_7
S0	1	1	1	1	1	1	1
S1	1	0	1	1	1	1	1
S2	1	0	1	1	1	1	1
S3	1	0	1	1	1	1	1
S4	1	0	1	1	1	1	1
S5	1	0	1	1	1	1	1

C	X_1	X_2
S0	0	0
S1	0	0
S2	0	0
S3	0	0
S4	0	0
S5	0	0

M[1]=< >
M[2]=< >

그림 9 결과 비트-벡터, 계수기 및 배열M[i]
Fig. 9 Resulted bit-vector, counter and array M[i]

7. 결 론

본 논문은 철도신호시스템을 위해 새롭게 설계된 통신 프로토콜 구조와 그 성능 결과를 나타내었다. 신호시스템을 위한 기존 프로토콜은 몇 가지 문제점들을 가지고 있었다. 이러한 문제를 해결하기 위하여 신호제어시스템을 위해 높은 신뢰성을 갖는 새로운 프로토콜을 설계하였다. 데이터 링크 제어에 대한 설계된 프로토콜의 성능해석을 기존의 프로토콜과 새롭게 설계한 프로토콜을 동일 조건 하에서 시뮬레이션을 수행하여 처리율이 약 10%, 프레임 에러확률은 5 [Eb/No]에서 약 10-4~10-3에서 10-5~10-3으로 향상되는 등 성능이 개선되었음을 확인할 수 있었다. 또한 일반적으로 비정형적인 방법을 사용함으로써 설계된 프로토콜 내에 포함 가능성이 있는 모호성을 제거하기 위하여, 프로토콜은 LTS로 명세화하고 모형검사 알고리즘을 통하여 안전성과 필연성을 검정하는 정형검증기법을 적용하여 안전성 및 필

연성을 검정하였다. 따라서 철도신호시스템을 위해 새롭게 설계된 통신 프로토콜을 사용함으로써 신호시스템의 안전성, 신뢰성 및 유지보수의 효율성의 증가가 기대되어진다.

참 고 문 헌

[1] J. G. Hwang and J. H. Lee, "Performance analysis of data link protocol for railway signaling", Proceeding of World Congress on Railway Research (WCRR2003), Oct. 2003.

[2] 철도용품 규격, 철도 6330-3328 : 열차집중제어장치와 전자연동장치간 정보전송방식(Protocol), 철도청, 2002.

[3] 황종규, 이재호, "전자연동장치와 역정보전송장치간 인터페이스를 위한 데이터링크 프로토콜 성능해석", 한국철도학회 논문지, 제6권 제2호, pp.135-141, 6. 2003.

[4] T. Kasami, T. Klove, and S. Lin, "Error detection with linear block codes", IEEE Trans. Inform. Theory, Vol. IT-29, pp. 131-136, 1983.

[5] S. Lin, D. J. Costello and M. J. Miller, "Automatic repeat request error control schemes", IEEE Trans. Commun., Vol. 22, pp. 5-17, 1984.

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

[9] D. Kozan, "Results on the prepositional mu-calculus", Theoretical Computer Science, 27: 333-354, December 1983.

[10] R. Cleaveland, "Tableau-based Model-Checking in the Propositional Mu-Calculus", Acta Informatica 27 : 725-727, 1990.

[13] O. Burkart and B. Steffen, "Model Checking the Full Modal Mu-Calculus for Infinite Sequential Processes", LFCS Report ECS-LFCS-97-355, 1997.

[16] 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, 1995.[16]

저 자 소 개

이 재 호 (李 在 浩)

1964년 9월 29일생. 1987년 광운대학교 전자공학과 졸업. 1989년 동 대학원 전자공학과 졸업(공석), 2000년 고려대학교 메카트로닉스학과 박사과정수료, 1995년~현재 한국철도기술연구원 전기신호연구본부 선임연구원

Tel : 031-460-8536, Fax : 031-460-5449

E-mail : jhlee1@krri.re.kr

황 종 규 (黃 宗 奎)

1969년 8월 6일생. 1994년 건국대학교 전기공학과 졸업, 1996년 건국대학교 전기공학과 석사, 2000년~현재 한양대학교 전자통신전파공학부 박사과정, 1995년~현재 한국철도기술연구원 전기신호연구본부 선임연구원

Tel : 031-460-5438, Fax : 031-460-5449

E-mail : jghwang@krri.re.kr

박 용 진 (朴 容 震)

1969년 일본 와세대 대학교 전자공학과 졸업, 1971년 일본 와세대 대학교 전자공학과 석사, 1978년 일본 와세대 대학교 공학박사, 1978년~현재 한양대학교 전자통신전파공학부 교수

Tel : 02-2290-0355, Fax : 02-2281-6579

E-mail : park@hyuee.hanyang.ac.kr

박 귀 태 (朴 貴 泰)

1975년 고려대학교 전기공학과 졸업. 1987년 동 대학원 전기공학과 졸업(공석), 1981년 동 대학원 전기공학과 졸업(공박), 1981년~현재 고려대학교 전기전자전파공학과 교수

Tel : 02-3290-3218, Fax : 02-921-1325

E-mail : gtpark@elec.korea.ac.kr