철도시스템 통신 안전성 확보를 위한 방법 제시 및 도구 구현

논 문
59P-1-2

Implementation of Methodology & Tool for Communication Safety Guarantee in Railway System

조 현 정* · 황 종 규† · 김 용 규**
(Hyun-Jeong Jo · Jong-Gyu Hwang · Yong-Kyu Kim)

Abstract - Safety-critical systems related to the railway communications are currently undergoing changes. Mechanical and electro-mechanical devices are being replaced by programmable electronics that are often controlled remotely via communication networks. Therefore designers and operators now not only have to contend with component failures and user errors, but also with the possibility that malicious entities are seeking to disrupt the services provided by theirs systems. Recognizing the safety-critical nature of the types of communications required in train control operations, the communications infrastructure will be required to meet a number of safety requirements such as system faults, user errors and the robustness in the presence of malicious attackers who are willing to take determined action to interfere in the correct operation of a system. In this paper, we proposed the safety strategies employed in the railway communications and a security mechanism for Korean railway communication system. Also, we presented the developed means for validation and determination of communication safety based on the proposed security mechanism in the railway system.

Key Words : Railway Communication, Safety Assessment, Safety Verification Tool, Railway Communication

1. 서 론

최근 들어 컴퓨터 및 통신 기술의 발달에 따라 철도시스템에서 기존의 기계 및 전기식 열차제어시스템들이 전자식으로 변경되어가고 있으며, 이처럼 열차제어시스템들이 컴퓨터화 되어감에 따라 시스템의 안전성을 확보하기가 매우 어려워지게 되었다. 특히, 본래 열차제어시스템은 열차의 안전운행을 책임지는 매우 바이탈한 장치들로서 높은 안전성이 요구되어짐은 물론이고, 컴퓨터를 활용한 열차제어시스템이 급격하게 기존의 기계 및 전기적인 열차제어시스템을 대체함으로 인해 발생하는 대규모 인명피해나 경제적 손실을 방지하기 위해 열차제어시스템의 엄격한 안전성 활동 체계 및 평가기술이 요구되고 있다. 이처럼 열차제어시스템은 다른 어느 시스템보다도 높은 안전성을 요구하고 있어서, 열차신호제어 통신 링크 간의 안전성 확보 또한 마찬가지로 매우 중요해짐에 따라 열차제어시스템의 통신부분 안전성과 관련한 기존 유럽규격이던 EN 50159-1/-2 규격이 IEC 62280-1/-2로 국제 규격화되어 전송시스템에 연결되어 있는 안전관련 장치들 간의 안전 통신을 위한 요구사항을 제시하고 있다[1-2].

또한, 국내에서는 몇 년 전부터 철도신호시스템 CTC (Centralized Traffic Control) 통신서버와 다른 신호설비 또는 외부설비들 간의 인터페이스를 위한 통신 프로토콜들이 표준으로 제정되어 철도공사의 통합 CTC 시스템에 적용되고 있다. 철도신호설비들 간 통신 프로토콜의 표준으로써 현재 점대점 정보전송 방식과 네트워크 정보전송 방식에 대한 두 가지가 제정되어 있으며, 이들 표준 프로토콜들 또한 열차제어시스템과 마찬가지로 바이탈 제어정보들이 전송되는 통신링크로서 매우 높은 안전성이 요구되고 있다[3-4]. 점대점 링크기반의 표준은 CTC와 LDTS/EIS(Local Data Transmission System/Electronic Interlocking System) 사이의 통신 프로토콜로서, 두 장치 모두 바이탈한 철도신호설비들이며 접속권한이 없는 다른 접속으로부터의 위협이 거의 없는 폐쇄형 전송시스템 특성을 가지고 있다. 네트워크 기반의 표준은 CTC와 SCADA(Supervisory Control And Data Acquisition) 사이의 통신 프로토콜로서 SCADA 설비가 신호시스템은 아니지만 전송시스템에 연결된 장치들이 알려져 있으며, 시스템 운용도중에 장치들이 추가되거나 삭제될 가능성이 적고 또한 접속권한이 없는 다른 접속으로부터의 위협이 적은 폐쇄형 전송시스템의 특성을 가지고 있다. 따라서 현재 국내에 제정 및 운용 중인 표준 프로토콜은 모두 IEC 62280-1 규격의 적용이 가능하다고 볼 수 있지만, 현재 진행 중인 철도공사 분당선의 지능형 열차제어시스템 구축사업의 경우 지상과 차상간의 인터페이스가 무선랜 기반으로 하고 있어 제3자에 의한 통신링크의 간섭 및 훼손의 가능성이 있으므로 개방형 전송시스템으로 IEC 62280-2 규격이 적용되어야 한다. 이러한 지능형 열차제어시스템의 통신 프로토콜은 아직 표준화되지 않고 있어, 열차

* 정 회 원 : 한국철도기술연구원 주임연구원
** 정 회 원 : 한국철도기술연구원 연구실장 · 공박
† 교신저자, 정회원 : 한국철도기술연구원 책임연구원 · 공박
E-mail : jghwang@krri.re.kr
접수일자 : 2009년 8월 7일
최종완료 : 2009년 9월 11일

제어시스템 무선 통신 안전성 확보를 위한 절차와 방법론을 개발하여 해당 기술을 적용할 필요가 있음을 알 수 있다.

철도 통신망에서 안전성을 위협하는 요소로는 시스템 부품과 소프트웨어의 오류 또는 고장에 의한 안전성 문제와 철도 통신망이 폐쇄형 전송시스템에서 개방형 전송시스템으로 변화함에 따라 발생하는 보안문제로 나눌 수 있다. 폐쇄형 통신망 관점에서의 일대일 통신 링크에 대한 주요한 위험요소는 에러와 고장 때문이라는 가정 하에 안전 최우선 시스템을 설계하는 것이 충분하였지만, 그러나 개방형 통신망 관점에서 시스템의 안전성은 악의적이고 고의적인 공격자의 증가에도 안정적인 동작을 필요로 한다. 즉, 폐쇄형 전송시스템에서는 물리적 전용의 유선회로를 사용함으로써 오류나 고장에 대한 안전 대책만 요구되었지만, 무선통신이나 인터넷 등을 중심으로 하는 물리적으로 독립되지 않은 전송회로를 사용하는 개방형 전송시스템으로 변화함에 따라 안전뿐만 아니라 인증받지 않은 접속으로 인한 고의방해 등에 대한 엄격한 보안대책이 필요하다. 따라서 본 논문에서는 무선 철도시스템 통신부분 안전성 확보를 위해 비인가자의 침입, 오류데이터 유입 등의 위험원으로부터 통신망 데이터 링크 보호 및 안전 전송을 위한 방법론을 제시하고자 한다. 이를 위해 먼저 2장에서 철도시스템 통신부분 안전성 평가 체계 분석을 통한 통신망 보안 위험원 도출과 데이터링크 보안 방법을 제시하였다. 3장에서는 우리가 제시한 방법을 통해 구현한 개방형 기반 열차제어 통신시스템의 안전성 검증 도구의 구현 결과를 보여준 후에 4장에서 제시한 방법론의 결과 적용에 대한 논의를 바탕으로 결론을 맺고자 한다.

2. 철도시스템 통신을 위한 안전성 평가기술 체계

안전 중심의 응용을 위한 기존의 철도 통신은 설치비용이 고가이고, 유지와 보수가 어려운 폐쇄형 통신망에 기반을 두고 있다. 이러한 시스템은 많은 부분에서 명확한 대체 통신 방법의 부재로 인해 융통성 있는 열차제어시스템의 도입이 늦어지는 결과를 초래하였다. 그러나 새로운 통신 기술의 기반이 되는 무선 통신 및 TCP/IP 프로토콜의 사용은 개방형 통신기술의 설치와 관련된 기반구조 구축비용의 감소에도 불구하고, 다양한 철도 통신 서비스를 제공할 수 있다. 경제적인 관점에서 이러한 해결책이 나타나는 반면에 개방형 통신시스템의 사용은 안전과 관련된 보안에 문제점이 발생하였다[5-7]. 열차를 개방형 통신시스템 기반 원거리제어 또는 통신기반의 열차제어(CBTC: Communication Based Train Control)로 바꾸고자 하는 것은 언급되기 시작한지 어느 정도 시간이 흘렀으며, 최근에는 추진력을 얻어서 증가되고 있는 경향을 보이면서 안전과 보안 측면에서 특유의 문제점을 나타내고 있다. 따라서 열차제어시스템 통신부분의 안전전송 통신을 위한 요구사항을 국제 규격화하여 IEC 62280-2에서 권고하고 있는 것이다. 규격에서는 개방형 전송시스템에 대한 통신 안전성에 대한 위협을 도출하기 위한 위험원 분석과 응용 계층에서의 이들 위험원에 대한 방어대책 및 안전성 평가 절차 등을 제시하고 있다[8-9]. 본 논문에서는 국제규격 기준에 근거하여 무선 철도시스템 안전성 평가 항목과 기준 정의 및 평가 절차 등을 분석하였다.

개방형 전송시스템은 양단간에 사용자에게 알려져 있지 않은 외부 영향에 대한 민감한 전송 특성을 지닌 하나 이상의 종류의 전송 매체로 구성된 임의의 경로를 통해, 사용자에게 알려져 있지 않은 프로그램에 따라서 메시지의 경로 설정이 가능한 네트워크 제어 및 관리 시스템을 기본 능력으로 한다. 개방형 전송시스템은 먼저 제어 및 보호 시스템 설계자에게 알려져 있지 않으며, 미지의 포맷으로 미지의 정보량을 보내는 전송시스템의 타 사용자가 있을 수 있고, 둘째로 시스템 관리자로부터 승인 없이 데이터를 읽고 또는 모방하기 위하여 타 사용자로부터 보내지는 데이터에 대한 접속을 시도할 가능성이 있는 전송시스템의 사용자도 존재할 수 있다. 마지막으로 안전 관련 데이터의 무결성에 대한 추가적인 위협을 주는 종류에 관계없는 위협들에 의해 영향을 받는다. 또한 개방형 전송시스템 전송링크는 전송시스템에 연결되어 있는 둘 이상의 안전 관련 장비간의 모든 사항(H/W, S/W, 전송 매체 등)으로 구성되는 것으로 간주된다.

시스템 참조구조는 어떠한 내부적 전송 보호 방식이 포함되었는가 와는 상관없는 비신뢰 전송시스템에 안전과 관련된 및 안전과 무관한 시스템들이 연결되는 개방형 전송시스템을 사용하는 그림 1과 같은 구조이다. 그림 1에서 안전관련 전송시스템은 비신뢰 전송시스템(고 집적 회로로 구현된 전송 기능 포함)과 관계되고, 어떠한 안전 요구사항도 개방형 전송시스템의 비신뢰 특성에 부과되지 않아야 한다. 그리고 개방형 전송시스템 기반 안전 관련 전송 기능은 IEC 62280-2에 기준하여 제시하며, 이 구조는 안전관련 전송 기능과 안전 관련 접속 보호 기능에 바탕을 둔다. 안전 관련 전송 기능에 대한 기능적이고 기술적인 안전에 대한 입증은 IEC 62280-2 표준체계를 따라 응용 계층에서 수행되고, 비신뢰 전송시스템에 대해서는 어떠한 안전 요구 사항도 부과되지 않고, 다만 안전성과 관련한 측면들은 안전 관련 장비 내에서 동작하는 안전 절차와 안전 부호화를 적용함으로써 그림 2와 같은 전송 매체 상에서의 안전 관련 메시지 표현 모델을 얻는다. 안전절차와 안전코드는 응용 계층에서 수행된다.

개방형 전송시스템의 위험사건 식별을 위한 위협의 원인 분석은 검토된 사례가 외부 환경과 상호 작용하는 네트워크를 다루고 있다는 고려로부터 분석이 시작된다. 폐쇄형 전송망

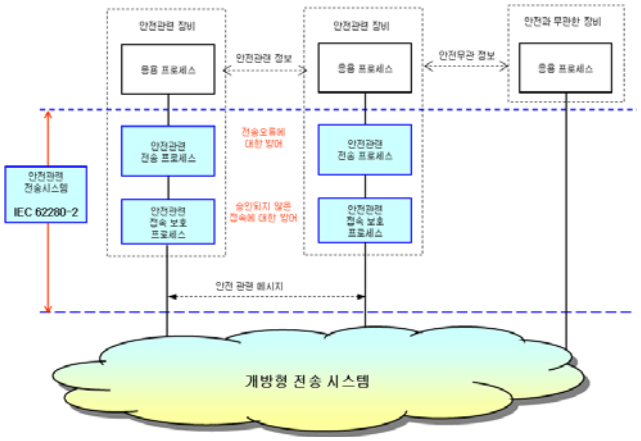

그림 1 개방형 비신뢰 전송 시스템을 사용하는 안전관련 시스템 구조

Fig. 1 Structure of safety-related system using a non-trusted open transmission system

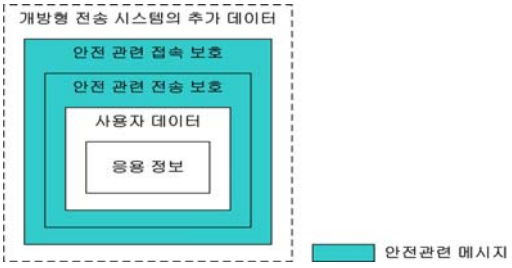

그림 2 개방형 전송매체 상에서의 안전관련 메시지 표현 모델
Fig. 2 Model of a safety-related message

기반에서의 위협의 원인에 외부 환경 개체의 인적 특성에 의해 발생하는 위험 사건 중 개방형 전송망 기반에서 고려되어야 하는 권한이 없는 사용자(파괴자, 침입자)에 의한 위험이 추가된다. 각각의 위협은 이를 발생시키는 위험 사건의 집합으로 간주될 수 있으며, 위협과 위험 사건과의 관계는 폐쇄형 전송망 기반에서의 위협과 위험 사건에서 통신 선로 도청과 하드웨어 손상 또는 파괴, 공인되지 않은 소프트웨어의 수정, 공인되지 않은 메시지의 전송, 채널의 청취 등이 위험 사건으로 추가된다. 이 중 통신 선로 도청과 공인되지 않은 소프트웨어의 수정으로 인해서 발생할 수 있는 위협으로는 반복, 삭제, 삽입, 순서 재배열, 손상, 지연, 허위 등이 있으며, 하드웨어 손상 또는 파괴에 의해서는 삭제와 손상, 지연이 발생할 수 있다. 또한 공인되지 않은 메시지 전송에 의해서는 반복과 삭제허위가 발생할 수 있다.

개방형 전송시스템에 있어서 안전관련 전송과 관련하여 가능한 일련의 위협을 도출하는 두 가지 상이한 접근법이 확인되었다. 첫 번째 방법은 주 위험원으로부터 시작하여, 위험에 이르는 모든 가능한 위험 사건을 분류하는 것으로 마무리된다. 두 번째 방법은 대상 시스템과 관련된 위험 사건의 모든 가능한 원인을 분류하기 위하여 고려되는 시스템(즉, 네트워크와 외부 환경)의 두 가지 주요 개체의 정의로

표 1 개방형 전송망 기반 위협/위험 사건에 대한 방어 대책
Table 1 Hazard cases, threates and defenses based on open transmission system

위험 사건	위협						
	반복	삭제	삽입	순서 재배열	손상	지연	허위
하드웨어의 규칙적인 고장	X	X	X	X	X	X	X[1)]
소프트웨어의 규칙적인 고장	X	X	X	X	X	X	X[1)]
혼선		X	X		X		X[1)]
통신 선로 파괴		X			X	X	
안테나의 잘못된 정렬		X			X		
배선 오류		X	X		X	X	X[1)]
하드웨어의 불규칙적인 고장	X	X	X	X	X	X	X[1)]
하드웨어의 노화	X	X	X	X	X	X	X[1)]
조정이 안 된 장비의 사용	X	X	X	X	X	X	X[1)]
적합하지 않은 장비의 사용	X	X	X	X	X	X	X[1)]
부정확한 하드웨어 교체	X	X	X	X	X	X	X[1)]
페이딩 효과		X		X	X	X	
EMI		X			X	X	
인적 실수	X	X	X	X	X	X	X[1)]
열잡음		X			X		
자기 폭풍		X			X	X	
화재		X			X	X	
지진		X			X	X	
번개		X			X	X	
전송 시스템의 과부하		X				X	
통신 선로 도청	X	X	X	X	X	X	X[1)]
하드웨어 손상 또는 파괴		X			X	X	
공인되지 않은 소프트웨어의 수정	X	X	X	X	X	X	X[2)]
공인되지 않은 메시지의 전송	X		X				X[2)]
채널의 청취[3)]							
방어 대책	- 순서번호 사용 - 시간 도장	- 순서 번호 사용	- 순서 번호 사용 - 출처와 도착지식별자 - 귀환 메시지 - 식별 절차	- 순서 번호 사용 - 시간 도장	- 안전코드 사용 - 암호화 기법 사용	- 시간 도장 - 만기 - 순서 번호 사용	- 귀환 메시지 - 출처와 도착지식별자 - 식별 절차 - 안전코드 사용

1) 이와 같은 경우, 잘못된 경로 설정 등과 같은 오류로 인해 올바른 메시지가 잘못된 수신단에 전달된다. 송신단 주소의 명기가 한 가지 가능한 대처 방안이다.
2) 이와 같은 경우, 메시지는 초기부터 그릇된 것이다. Key의 사용 등과 같은 강력한 방어가 요구된다.
3) 위험 사건인 “채널의 청취”에 대하여 위협은 없다고 보는 것이 타당하다. 사실 기밀성은 시스템의 요구사항이다. 이는 특정한 응용과 관련되어져야 한다.

부터 시작하며, 이와 같은 사건들은 사건들에 의해 발생되는 위협들과 연관 지어진다. 개방형 전송망 기반의 안전성 제공을 위해서는 보안을 고려한 안전성이 보장되어야 한다. 즉, 통신 안전성이 위협 및 위험 사건에 의해 피해를 입는 위험을 줄이기 위해 적정한 레벨의 방어 대응책이 마련되어야 한다. 철도 통신에서 주어진 잠재적인 위협에 의해 발생하는 통신 붕괴는 사후 법률적인 제재를 가하는 형태로의 처벌은 의미가 없다. 즉 공격에 대해 먼저 대비하여 방어하는 방법이 최선책이다. 일반적으로 이러한 방어 대책으로는 다음과 같은 전략들을 사용한다.

- 순서 번호 사용(Sequence number): 전달되는 메시지의 순서 재배열 및 반복 및 삭제를 막기 위해 사용
- 시간 도장(Time stamp): 전달되는 메시지의 순서 재배열 및 반복 그리고 지연을 막기 위해 사용
- 귀환 메시지 및 만기(Positive acknowledgement and time-out): 전달되는 메시지의 삭제 및 지연을 막기 위해 사용
- 메시지 인증(Message authentication): 전달되는 메시지의 허위를 막기 위해 사용
- 메시지 무결성 보호(Message integrity protection): 전달되는 메시지의 허위 및 손상을 막기 위해 사용

위의 전략들을 사용하여 위협에 대한 방어 대책들을 요약하면 다음 표 1과 같이 정리할 수 있다. 표 1에 제시된 것과 같이 위협 종류는 반복, 삭제, 삽입, 순서 재배열, 손상, 지연, 위장 등으로 구분된다. 이 중 반복 위협에 대해서는 순서 번호 사용과 시간도장을 통하여 방어할 수 있으며, 이에 대한 보안 요구 사항으로는 기밀성 및 유효성이 요구된다. 삭제에 대한 방어 대책으로는 순서 번호 사용이 있으며, 유효성이 보안 요구사항으로 존재한다. 삽입 위협에 대해서는 순서 번호나 출처와 도착지 식별자, 귀환 메시지 사용으로 방어가 가능하고, 보안 요구 사항으로는 기밀성과 인증이 요구된다. 순서 재배열은 순서 번호 사용과 시간도장으로 위협에 대해 보안을 유지할 수 있으며, 이에 대한 보안 요구사항으로는 유효성이 유지되어야 한다. 위협의 종류 중 지연에 대해서는 시간도장(Time stamp)과 만기(time-out)를 이용하여 방어가 가능하며, 유효성이 관련 보안 요구사항으로 존재한다. 마지막으로 허위에 대한 위협의 방어 대책으로는 귀환 메시지 사용, 메시지 인증, 메시지 무결성 보호의 방법들이 존재한다. 그리고 이에 대한 보안 요구사항으로는 기밀성과 인증이 있다.

분석된 위협과 위험 사건에 대한 방어 대책 또한 표 1에 위협 및 위험 사건과 함께 같이 정리하였다. 반복 위협에 대한 방어 대책으로는 순서 번호 사용과 시간 도장을 사용하는 방법이 있으며, 삭제 위협의 경우는 순서 번호 사용으로 방어가 가능하다. 삽입 위협은 순서 번호나 출처와 도착지 식별자, 귀환 메시지 식별 절차를 통해서 삽입 위협에 대해 방어할 수 있으며, 순서 재배열 위협은 순서 번호 사용과 시간 도장을 사용하는 방어 대책이 존재한다. 또한 손상 위협에 대해서는 안전 코드 사용과 암호화 기법 사용을 통해 방어가 가능하고, 지연 위협은 시간 도장과 만기를 통해 위협에 대해 방어할 수 있다. 마지막으로 허위에 의한 위협은 메시지 인증 및 해시 함수 사용을 통해 방어가 가능하다. 표 1에서 권한이 없는 사용자(침입자 또는 파괴자)에 대한 위험 사건들이 포함되었음을 확인할 수 있으며, 위에 언급한 각각의 위협에 대한 특정 방어 방법별 해당 내용 및 요구사항에 대한 전체적인 위협에 대한 안전성 보장을 위한 평가 절차는 IEC 62280-2 규격에 상세히 나와 있다.

3. 철도시스템 통신 안전 전송을 위한 도구 구현

본 논문에서 개발한 열차제어시스템 통신 안전 전송을 위한 안전성 평가 검정도구는 개방형 전송시스템 기반 상위 응용 계층 안전성 보장 프레임 생성 및 해제 모듈과 개방형 안전 전송 및 확인을 위한 도구이며, 전체 개발 도구의 기본 구조를 그림 3과 같이 요약하여 나타낼 수 있다. 이와 같은 개방형 열차제어시스템의 안전 전송을 위해 개발한 안전성 평가 검정도구의 구현 결과를 3.1절과 3.2절에 정리하였다.

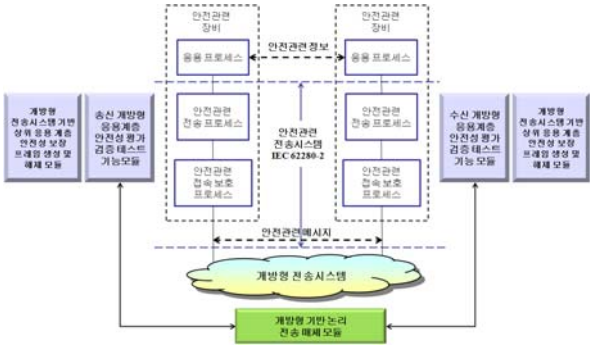

그림 3 개방형 안전성 평가 검정 테스트 도구 전체 구조

Fig. 3 Total structure of tesing tool for safety evaluation in the open transmission system

3.1 개방형 철도 전송시스템 안전성 보장 프레임 생성 및 해제 모듈 개발

그림 3에 나타낸 것과 같이 개방형 전송시스템 기반 상위 응용 계층 안전성 보장 프레임 생성 및 해제 모듈의 기능은 상위 응용 계층 안전성 보장을 위해 송신부에서 새로운 프레임을 생성하고, 수신부에서는 기능 검정 및 해제하는 것으로 상위 응용레벨 안전 코드 생성 및 확인 기능이라 할 수 있다. 상위 응용 계층으로부터 전달받은 전송 메시지는 기존의 개방형 전송시스템인 경우 그림 4와 같은 구조이다. 이와 같은 구조는 개방형 열차제어신호 관련 전달 메시지 구조로서 TCP/IP 기반의 안전 무관 하위 계층(Ethernet)을 통하여 전달되어, 여러 가지 위협(반복, 삭제, 삽입, 순서 재배열, 손상, 지연, 허위)에 대해 안전한 전송이 보장 되지 않는다.

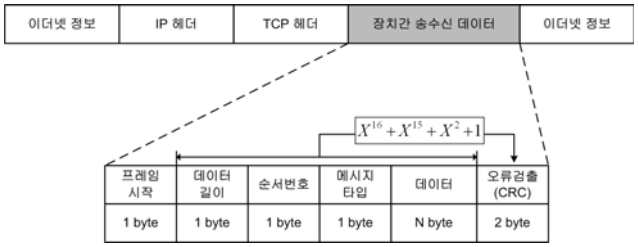

그림 4 기존 개방형 철도 신호 장비 CTC와 SCADA로 전송되는 메시지의 기본 전송 프레임 구조

Fig. 4 Basic transmission frame structure of the transmitted message beween CTC and SCADA

따라서 개방형 열차제어 전송시스템에서 안전한 전송을 위해 본 논문에서 제안한 그림 5의 데이터 순서 번호 필드는 반복, 삽입, 순서 재배열, 지연 위협에 대한 방어 대책이며, 특히 전송 중에 있는 데이터가 안전 무관 하위 계층 전송 장비들의 결함이나 오작동으로 인해 발생하는 순서 번호 혼동 위협으로부터 응용 계층에서 보호 역할을 한다. 본 논문에서는 이러한 순서 번호 혼동 위협으로부터 보호하기 위해 필요한 정보를 포함하는 데이터 순서번호 필드를 정의하고, 필드의 크기를 1byte로 추가한다. 순서 번호 필드는 송신기 응용 계층에서 생성하여 TCP/IP 계층으로 전달되며, 수신된 TCP/IP 계층을 통해 수신기 응용계층에서 확인 후 재전송 요청 등의 정보를 활용한다.

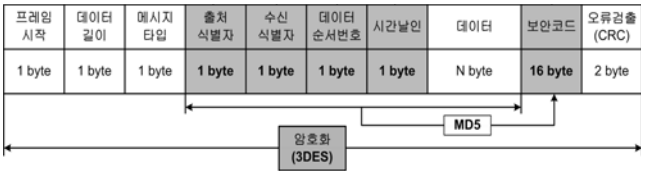

그림 5 제안한 개방형 전송 시스템에서 안전성을 향상 시킨 전송 프레임 구조

Fig. 5 Proposed transmission frame structure of improving safety performance in the open system

그림 5의 시간도장(시간날인) 필드 또한 반복, 삽입, 순서 재배열, 지연 위협에 대한 방어 대책이며, 전송 중에 있는 데이터가 안전 무관 하위 계층 전송 장비들의 결함이나 오작동으로 인해 발생하는 위협으로부터 보호 역할을 한다. 본 논문에서는 이러한 오래된 정보나 데이터의 삭제를 위해 필요한 정보를 포함하는 시간도장 필드를 정의하고, 필드의 크기를 1byte로 추가한다. 시간도장 필드는 송신기 응용 계층에서 생성하여 TCP/IP 계층으로 전달되며, 수신된 TCP/IP 계층을 통해 수신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈에서 확인 후 해당 정보를 활용한다. 또한 그림 5에서 개방형 전송시스템의 송신기 응용 계층에서 전송될 정보에 출처 식별자와 수신식별자를 포함하여 메시지 프레임을 만들어 TCP/IP로 넘겨준다. 본 논문에서는 이러한 식별자 사용으로 반복, 삽입, 허위 위협으로부터 보호하여 허가된 접속자임을 확인한다. 그림 5에서 두 식별자를 위해 식별자 데이터 필드의 크기를 각각 1byte로 추가하여 송신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈에서 생성 및 수신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈에서 확인한다.

그림 5의 보안코드 필드는 손상에 대해 보안코드를 만들어 보호하는 수단으로 본 논문에서는 송신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈에서 미국의 NIST(National Institute of Standards and Technology)에서 표준화한 MD5(Message- Digest algorithm 5)를 활용하여 출처 식별자 필드부터 장치 간 송수신 데이터 필드까지를 대상으로 16byte의 보안코드를 생성하여 첨부한 후 TCP/IP로 전달한다[10-11]. 수신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈은 TCP/IP 계층으로부터 해당 정보 프레임을 전달받아 아래항의 복호화 과정을 거친 후 손상이나 허위 여부를 판단하여 정보로 활용한다.

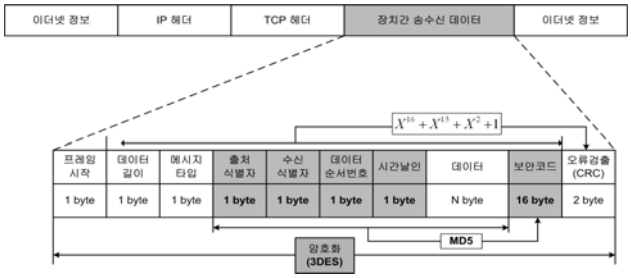

그림 6 개방형 전송 시스템 새로운 보안 프레임 구조

Fig. 6 The new proposed security frame structure in open transmission system

마지막으로 그림 5의 암호화 필드는 허위에 대해 보안코드를 만들어 보호하는 수단으로 본 논문에서는 송신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈에서 미국의 NIST에서 표준화한 3DES(Triple Data Encryption Standard)를 활용하여 프레임 시작 필드부터 장치 간 CRC(Cyclic Redundancy Check) 오류 검출 코드 필드까지를 대상으로 암호화 후 TCP/IP로 전달한다[12-13]. 수신부 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈은 TCP/IP 계층으로부터 해당 정보 프레임을 전달받아 복호화 과정을 거친 후 허위 여부를 판단하고 후속 조치를 위해 보안코드 검증 단계로 전달한다. 그림 6은 위의 5가지 보안에 대한 내용을 고려하여 구성한 새로운 보안 프레임으로 CTC와 SCADA에서 이용하기위해 본 논문에서 제안한 새로운 프레임 구조의 적용을 도식화하여 나타낸 것이다.

3.2 개방형 철도 안전 전송 및 확인을 위한 도구 구현

그림 3에 제시된 것과 같이 개방형 안전성 평가 도구 구현을 위한 기본 구조는 다음과 같이 크게 2개의 모듈로 구성되어 있다. 우선 안전 관련 전송 기능(IEC 62280-2)과 관련하여 개방형 안전성 테스트 기능 모듈과 비신뢰적 개방형 전송시스템에 기반한 전송 매체를 대신한 개방형 기반 논리 전송 매체 모듈로 구성되어 있다. 이와 같이 그림 3에서의 개방형 안전 전송 및 확인을 위한 테스트 도구는 2개의 기능 모듈로 구성되며, 각각의 모듈에 대해 기능적으로 설명하면 다음 표 2와 같다.

표 2를 보면 앞서 설명한 바와 같이 허위나 손상오류에 대한 안전성 제공을 위해 MD5와 3DES를 적용함을 확인할 수 있으며, 일반적으로 MD5는 손상에 대한 해결책으로 안전코드를 해쉬 함수를 이용하여 구한 후 전달 메시지에 생성 부착하고, 개방형 망을 통해 전달한 후 같은 해쉬 함수를 적용한 안전코드와 비교하여 전달 메시지의 손상 유무를 판단한다. 본 논문에서 MD5를 사용한 이유는 비교적 계산이 복잡하지 않아 시간이 적게 소요되고 보호 기능이 강한 점을 고려하였으며, 해쉬함수 충돌에 대한 문제는 3DES를 동시에 사용하여 암호화와 복호화 과정을 거쳐 손상 오류에 대해 보호가 가능하므로 문제 해결이 가능하다. 허위 오류에 대한 안전성 제공을 위해서는 3DES를 사용하였는데 이에 대한 이유는 ISO/IEC 10116 등에 따른 표준화된 동작 모드가 권장되므로 일반적으로 잘 알려진 DES의 권장에 따라 한 단계 복호화와 암호화 과정을 더 거치는 3DES를 사용한 것이다.

표 2 개방형 안전성평가를 위한 검증 테스트도구 기능모듈
Table 2 Function module of validation testing tool for safety evaluation in the open system

모듈 구분	기능	설계 기능 상세 설명
송신 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈	순서번호 혼동	사용자 데이터에 순서번호 생성
	기한이 지난 데이터 오류	사용자 데이터에 시간도장 생성 첨부
	허가된 사용자 식별	사용자 데이터에 송신기/수신기 식별자 생성 첨부
	손상 오류	사용자 데이터에 안전코드 생성첨부(MD5)
	허위	사용자 데이터에 송신기/수신기 식별자 생성 첨부
		사용자 데이터 해당 부분 암호화(3DES)
		사용자 데이터에 안전코드 생성첨부(MD5)
수신 개방형 응용계층 안전성 평가 검증 테스트 기능 모듈	순서번호 혼동	보안 프레임 순서번호 확인
	기한이 지난 데이터 오류	보안 프레임 시간도장 및 만기 확인
	허가된 사용자 식별	보안 프레임 송신기/수신기 식별자 확인
	손상 오류	보안 프레임 안전 코드 확인
	허위	보안 프레임 송신기/수신기 식별자 확인 또는 보안 프레임 안전 코드 확인 또는 보안 프레임 암호화 확인
개방형 기반 논리 전송 매체 모듈	양쪽 송수신부의 전송 매체를 대신한 개방형 기반 논리 전송 매체 모듈로 안전 전송에 대한 위협 행위를 시뮬레이션	송신부 개방형 응용 계층 안전성 평가 검증 테스트 기능 모듈로부터 수신한 보안 프레임에 위험 사건과 위험간의 난수 발생 형태로 각종 위협 생성 및 전송 보안 프레임에 반영 후 수신부 개방형 응용 계층 안전성 평가 검증 테스트 기능 모듈로 전달

개방형 안전성 테스트 기능 모듈은 송신부와 수신부로 구성되어 있으며, 하위의 개방형 기반 논리 전송 매체 모듈을 통해 통신이 이루어진다. 그림 7은 개방형 안전성 테스트 기능 모듈 구조를 보여주는 그림이다. 그림 7을 구성하고 있는 개방형 기반 논리 전송 매체 모듈은 양쪽 송수신부의 전송 매체를 대신하는 논리 전송 매체 모듈로 비신뢰적 개방형 전송 시스템의 행위를 시뮬레이션하는 기능을 수행한다. 이와 같이 설계된 개방형 기반 논리 전송 매체 모듈의 구조는 다음 그림 8과 같다. 개방형 기반 논리 전송 매체 송신부 모듈은 2개의 세부 모듈 “난수 생성에 의한 위협 생성 세부 모듈”과 개방형 안전성 테스트 기능 모듈로부터 “수신된 메시지 임의 변경 세부 모듈”로 구성된다. 먼저 “난수 생성에 의한 위협 생성 세부 모듈”은 개방형 안전성 테스트 기능 모듈로부터 메시지를 수신하여 비신뢰적 개방형 전송 시스템의 행위를 시뮬레이션하기위해 난수에 의한 위협을 생성하는 기능을 수행하고, 그리고 “수신된 메시지 임의 변경 세부 모듈”은 생성된 위협의 종류에 따라 수신 프레임의 내용을 임의 변경하는 기능을 행한다. 결론적으로 그림 7의 송신부 개방형 응용 계층 안전성 평가 검증 테스트 기능 모듈로부터 수신한 보안 프레임에 위험 사건과 위협 간의 난수 발생 형태로 각종 위협 생성 및 전송 보안 프레임에 반영 후, 그림 7의 수신부 개방형 응용 계층 안전성 평가 검증 테스트 기능 모듈로 전달하는 기능을 담당한다.

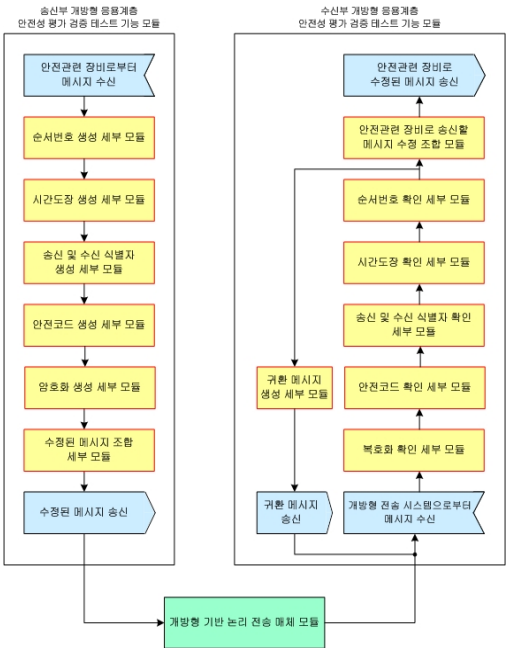

그림 7 개방형 안전성 테스트 기능 모듈
Fig. 7 Safety testing function module for the open transmission system

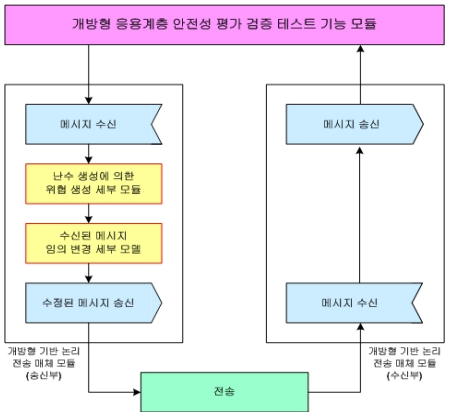

그림 8 개방형 기반 논리 전송 매체 모듈
Fig. 8 Logic transmission media module based on the open system

이와 같은 과정을 통해 구현한 개방형 열차제어 전송시스템 기반 안전 전송 및 확인을 위한 도구는 실제 열차제어 장치 양쪽 송수신부의 전송 매체를 논리 전송 매체 모듈로 대체하였으며, 안전 전송에 대한 위협 행위를 시뮬레이션 프로그램 수행을 통해 실제의 경우와 같이 시행하였다. 이처럼 개발된 시뮬레이션 도구의 전체적인 동작은 다음과 같다. 먼저 시뮬레이션 돌릴 횟수를 입력받고 입력받은 값에 대해 시뮬레이션을 원하는 만큼 수행한다. 그리고 보낼 메시지를 만든 후 위험 사건 25 가지를 랜덤으로 돌려 선택하는데 여러 개의 조합이 가능하다. 각각의 위험 사건에 대해 1에서 100까지의 수를 랜덤으로 선택하고 10 미만일 때 해당 위험 사건 발생한다. 또한 위험 사건들에 대해 가질 수 있는 위협 중 랜덤으로 선택하고 여러 위험 사건에서 어떤 위협이 동시에 나타난다면 선택될 확률이 높아진다.

각각의 위협들에 대해 1에서 100까지의 수를 랜덤으로 정하고 각각의 오류에 대해 다음과 같이 정하여 사용하였다.

- 손상: 15 미만일 때
- 지연: 위 위협이 선택 안 되고 20 미만일 때
- 반복: 위 위협들이 선택 안 되고 20 미만일 때
- 삭제: 위 위협들이 선택 안 되고 20 미만일 때
- 순서 재배열: 위 위협들이 선택 안 되고 20 미만일 때
- 삽입: 위 위협들이 선택 안 되고 50 미만일 때
- 허위: 위 위협들이 선택 안 되고 80 미만일 때
- 정상: 모든 위협들이 선택 안 되었을 때

이러한 과정을 입력받은 만큼의 수만큼 계속해서 매번 위협을 잘 체크하는지 검사하고 통계 값을 보여준다. 개발된 시뮬레이션 도구로 동작하는 전체과정은 그림 9와 같이 화면에 나타난다. 그림 9에는 위험 사건별 시뮬레이션 프로그램 수행으로 생성된 위험 사건별 횟수가 나타나 있다. 또한, 전체 위험별 횟수에 대한 개방형 열차제어시스템의 안전 전송 및 확인 건수에 대한 퍼센트도 화면에 나타낼 수 있다. 개방형 전송시스템에서 상위 응용 계층 보안 프로세스 레벨 위협 사건별로 기인해 나타나는 오류의 종류는 반복 오류, 삭제 오류, 삽입 오류, 순서 재배열 오류, 손상 오류, 지연 오류, 허위 오류 및 오류 없음으로 구분하여 동작한다. 반복 오류는 그림 10과 같이 나타나며, 송신 순서 번호 및 수신 순서 번호 값이 다르고 이에 따라 계산된 CRC 값도 다르다. 위험사건으로는 인적 실수와 화재가 도출되었다. 발생한 반복 오류 7회에 대해 모두 에러를 검출해 내었다.

이와 같은 방법으로 순서 재배열 오류는 그림 11과 같이 나타나며, 계산된 CRC 16의 송수신 값이 다르고 송신 순서 번호와 수신 순서 번호가 다르다. 위험사건으로는 하드웨어의 불규칙적인 고장, 부정확한 하드웨어 교체, 자기 폭풍, 전송 시스템의 과부하, 공인되지 않은 소프트웨어의 수정 등이 도출되었다. 순서 재배열 오류 6회에 대해 모두 에러를 검출하였다. 또한, 위험이 없는 경우는 그림 12와 같이 나타나며

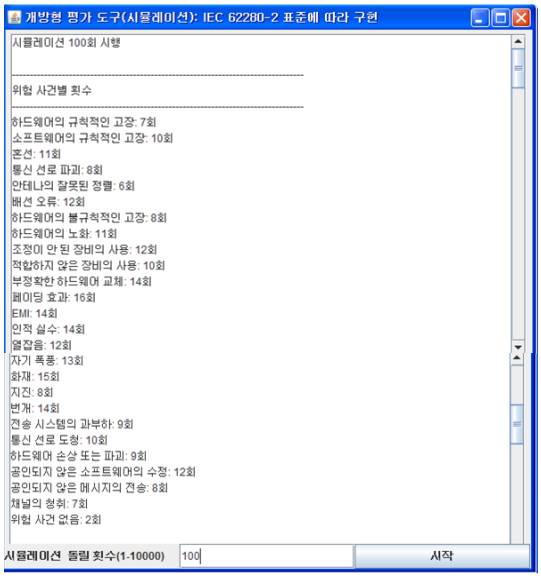

그림 9 개방형 평가 도구 전체 위험별 횟수 화면

Fig. 9 The screen of frequencies at total hazard cases in the validation tool of open transmission system

모든 값이 송수신 모두 일치한다. 위험이 없는 정상적 15회에 대해 에러가 없음을 확인하였다.

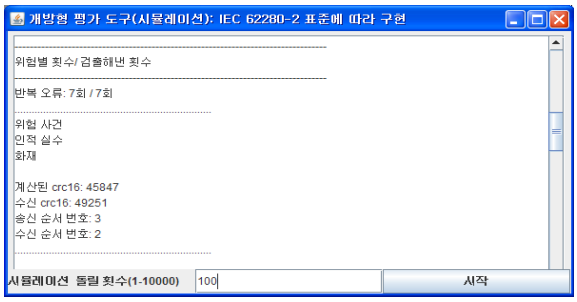

그림 10 반복 오류

Fig. 10 The case of repetition error

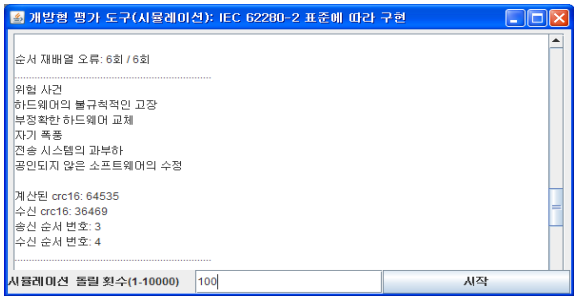

그림 11 순서 재배열 오류

Fig. 11 The case of Resequence error

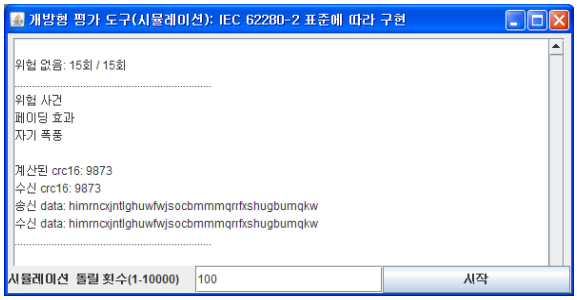

그림 12 위험이 없는 경우

Fig. 12 The case of no hazards

4. 결 론

최근 열차제어시스템 통신부분과 관련된 안전 최우선 장치들은 많은 변화를 겪고 있는데, 이는 기계적이고 전기적인 장치들이 통신망을 통한 원격제어가 이루어지는 견고한 상태와 프로그램 가능 전자장치로 대체되고 있다는 점이다. 이러한 변화로 인한 사용자 에러, 결함 구성요소 그리고 시스템에서 제공하는 서비스의 고의적 파괴 요소 등에 대비하여 안전성 및 보안성을 고려해야만 한다. 기존의 수많은 열차제어 신호방식기법은 철도통신에서 안전기능을 위해 통신 프로토콜 프레임에서 CRC 사용을 통한 데이터 무결성 메커니즘 제공으로 에러 검출과 링크 고장에 대한 안전성을 제공하기에 충분한 것으로 고려되어 왔다. 이러한 기존의 철도 통신은 설치비용이 고가이고, 유지와 보수가 어려운 폐쇄

형 통신망에 기반을 두고 있었으나, 새로운 통신 기술의 기반이 되는 무선 통신 및 TCP/IP 프로토콜의 사용은 개방형 통신기술의 설치와 관련된 기반구조 구축비용의 감소에도 불구하고 다양한 철도 통신 서비스까지 제공할 수 있기 때문에, 열차를 개방형 기반 원거리 제어로 바꾸고자 하는 것은 추진력을 얻어 더욱 증가되는 추세이다.

그러나 전송 또는 통신 기반의 열차 제어(CBTC)에 관한 이러한 경향은 안전과 보안 측면에서 특유의 문제점을 나타내고 있으며, 개방형 통신망 관점에서 시스템의 안전성은 악의적이고 고의적인 공격자의 증가에도 안정적인 동작을 필요로 하게 되었다. 결론적으로 철도 통신 안정성에 대한 위협은 더 복잡하고 더 다양한 위험원으로부터 안전성을 보장하기 위해서 개방형 통신망의 안전과 보안 측면에서 위협에 대한 강력한 대처를 강구하여야 한다. 따라서 본 논문에서는 개방형 열차제어시스템 통신 전송의 안전성 확보를 위해서 국제규격을 기반으로 하여 체계적인 안전성 평가 항목과 보안대책 제시 및 개방형 전송시스템 기반 안전성 평가 기술 체계를 분석하여 제시하였다. 또한, 분석 및 제시한 기본 설계를 바탕으로 열차제어시스템 개방형 통신 안전 전송을 위한 도구를 구현하였다. 본 도구는 개방형 전송시스템 기반 상위 응용 계층 안전성 보장 프레임 생성 및 해제 모듈과 개방형 안전 전송 및 확인을 위한 테스트 도구로 구성되며, 본론에서 도구의 구체적인 구현 과정 및 개발 결과를 제시하였다. 본 논문에서 분석 제시한 열차제어시스템 통신 안전 전송을 위한 방법 및 도구를 적용할 경우 바이탈한 국내 열차제어시스템 통신 분야의 철도제어신호 전송방식에서 보다 높은 안전성 확보가 가능할 것으로 기대되며, 개발한 본 도구는 개방형 열차제어 전송시스템의 정보 전송방식의 안전성 제공을 위한 보안 모듈로서의 활용이 충분히 가능하다고 본다.

감사의 글

감사의 글 : 본 논문은 국토해양부가 출연하고 한국건설교통평가원에서 위탁 시행한 철도종합안전기술개발사업(열차안전C03)의 연구비지원에 의해 수행되었습니다.

참 고 문 헌

[1] IEC 62280-1, "Safety-related communication in closed transmission systems," 2002.
[2] IEC 62280-2, "Safety-related communication in open transmission systems," 2002.
[3] 철도 6330-3348, "철도신호시스템 점대점 정보전송 방식," 2005.
[4] 철도 6330-3349, "철도신호시스템 네트워크 정보전송 방식," 2005.
[5] Knight J. C., "Software Challenges in Aviation Systems," Computer Safety, Reliability and Security, 21st International Conference, SAFECOMP, Lecture Notes in Computer Science, Vol. 2434, pp. 106-112, Sep. 2002.
[6] Dehbonei D., Mejia F., "Formal Methods in the Railway Signalling Industry," in Naftalin et. al., pp. 26-35, 1994.
[7] Gnesi S., Latella D., Lenzini G., Abbaneo C., Amendola A., Marmo P., "A Formal Specification and Verification of a Safety Critical Railway Control System," Proceedings of the 5th International Workshop on Formal Methods from Industrial Critical Systems, Apr. 2000.
[8] Laprie J. C., "Dependable Computing and Fault Tolerance: Concepts and Terminology," Proceeding of FTCS-25, Vol. 3, pp. 2-11, 1996.
[9] Leveson N. G., "Software: System Safety and Computers," Addison-Wesley, 1995.
[10] R. Rivest, "The MD4 Message-Digest Algorithm," published within Internet, 1992.
[11] RFC(Request For Comments) 1321, "The MD5 Message-Digest Algorithm," , 1992.
[12] Tanenbaum A. S., "Distributed Operating systems," Prentice-Hall, 1995.
[13] [DES] FIPS(Federal information processing standard) PUB 46, "Specifications for the Data Encryption Standard," 1977.

저 자 소 개

조 현 정 (趙 賢 庭)

2003년 한국항공대학교 항공전자공학과 졸업. 2005년 광주과학기술원(GIST) 정보통신공학과 졸업. 2005년~현재 한국철도기술연구원 열차제어통신연구실 주임연구원.
Tel : 031-460-5458
Fax : 031-460-5449
E-mail : hjjo@krri.re.kr

황 종 규 (黃 宗 奎)

1994년 건국대학교 전기공학과 졸업. 1996년 동 대학원 석사졸업. 2005년 한양대학교 전자통신전파공학과 박사졸업. 1995년~현재 한국철도기술연구원 열차제어통신연구실 책임연구원.
Tel : 031-460-5438
Fax : 031-460-5449
E-mail : jghwang@krri.re.kr

김 용 규 (金 容 圭)

1987년 단국대학교 전자공학과 석사졸업. 1993년 프랑스 Institute National Polytechnique de Lorraine 제어공학 DEA 및 1997년 동대학원 Ph.D 졸업. 1997년~현재 한국철도기술연구원 열차제어통신연구실장.
Tel : 031-460-5434
Fax : 031-460-5449
E-mail : ygkim1@krri.re.kr