Regular paper | Journal of the KIECS. pp. 695-702, vol. 17, no. 4, Aug. 31. 2022, t. 114, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2022.17.4.695

스마트 철도 통신기반 위험요인에 따른 정보보호 방안

박은경*

Information Security Strategy by Risk Factors based on Smart Railway Communications

Eun-Kyung Park*

요 약

최근 들어 활발하게 연구되고 있는 스마트 철도 시스템은 통신기술과 정보기술 등 ICT(: Information & Communication Technology) 기반으로 자동화 단계를 넘어 지능화 단계로 진입하고 있다. 스마트 철도에 사용되고 있는 ICT 기술은 일반적으로 정보침해에 취약한 특성을 보여 다양한 정보보호 기술의 지원을 받고 있다. 고속/대량 운송 수단으로서 철도 시스템의 스마트화에는 그 기반을 이루는 ICT 기술을 위한 정보보호 방안의 강구가 필수적이다. 따라서 본 논문에서는 스마트 철도 통신기반의 잠재적 위험 요인을 살펴보고 이에 대응할 수 있는 정보보호 요소를 고찰하여 스마트 철도 통신을 위한 단계별 정보보호 방안의 필요성을 제시한다.

ABSTRACT

Smart railway system, which has been actively studied in recent years, is entering the intelligent stage beyond the automation stage based on ICT (Information & Communication Technology) such as communication technology and information technology. ICT technology used in smart railways is generally supported by various information protection technologies as it is vulnerable to information infringement. As a means of high-speed/mass transportation, it is essential to devise an information protection plan for ICT technology that forms the basis for smartening the railway system. Therefore, this paper presents the necessity of step-by-step information protection that measures for smart railway communication by examining potential risk factors of smart railway communication base and considering information protection factors that can respond to them.

키워드

CBTC, ICT, Smart Railway Communication, Information Security, Risk Factors
통신 기반 열차 제어 장치, 정보 통신 기술, 스마트 철도 통신, 정보 보호, 위험 요인

Ⅰ. 서 론

대규모 승객 및 화물 운송을 위한 철도는 안전한 운영을 위해 철도 인프라, 차량, 전철전력, 신호통신, 관제 등 다양한 시스템이 존재하며, 각 시스템은 유기적으로 연결되어 운영된다. 또한 각 시스템의 운영 및 감시, 관리, 유지보수 등의 목적으로 다양한 정보가 철도 통신 네트워크를 통해 전송되고 공유되므로 이러한 철도 통신 네트워크를 통해 전송되는 데이터는 열차의 안전한 운영과 직결된다.

* 교신저자 : 동양대학교 철도전기융합학과
• 접 수 일 : 2022. 06. 30
• 수정완료일 : 2022. 07. 21
• 게재확정일 : 2022. 08. 17
• Received : Jun. 30, 2022, Revised : Jul. 21, 2022, Accepted : Aug. 17, 2022
• Corresponding Author : Eun-Kyung Park
Dept. of Electric Railway Convergence Science, DongYang University,
Email : rupek2014@dyu.ac.kr

철도 시스템의 스마트화는 철도에 요구되는 기기 또는 장치들을 인터넷 등의 통신망으로 연결하여 각종 데이터를 적시에 수집/분석/분배하여 대응하게 하는 등 운영의 지능화를 추구하는 과정으로서 통신기술과 정보기술을 기반으로 구축된다.

정보 시스템이 이용되는 체계에서 정보보호 대책은 시스템의 올바른 운영을 위하여 반드시 필요하다. 특히 대량 운송 수단으로 운영되는 고속철도에서 정보보호 방안은 시스템의 안전과 효율적 운영을 위한 필수 조건이라 할 수 있다.

스마트 철도 통신 시스템에 사용되는 LTE-R(: Long Term Evolution - Railway), 5G/B5G(: 5th Generation / Beyond 5th Generation) 등의 이동통신 기술, IoT(Internet of Things), 인터넷 등의 네트워크 기술, 위성통신 및 GPS(Global Position System) 등의 부가통신 기술 뿐 아니라 정보 기술로서 딥러닝, 빅데이터, AI(Artificial Intelligence), 블록체인 및 클라우드 등의 기술은 편리함과 효율성을 제공해 주지만 보안이 취약하게 되면 외부 사이버 공격 및 정보 침해의 대상이 될 수 있다[1].

따라서, 스마트 철도 시스템의 안정적 구축 및 운영을 위해 통신 기술 및 정보 기술 침해에 대한 사례를 통하여 대응 방안을 구축하는 것은 매우 중요하다.

본 연구에서는 스마트 철도 시스템의 잠재적 위험요인과 정보침해 대응 방안으로서 정보보호 요소를 살펴보고 이를 토대로 정보활용 단계별 침해 요소를 분석하여 정보활용 단계별 정보보호 방안의 필요성을 제시한다.

II. 스마트 철도 통신

CBTC(: Communication Based Train Control)는 통신기반 열차제어장치로서 정보전송을 위한 통신링크를 제공할 뿐 아니라 움직이는 열차의 위치를 측정할 수 있는 시스템이다. 기존의 위치결정 시스템보다 더욱 정확하게 이동열차의 실시간 위치를 찾아내어 더욱 많은 정보량을 신뢰성 있게 전송할 수 있다는 것이 장점이다[2].

이러한 CBTC 등을 활용하여 제어/관제 시스템의 자동화를 추구해 온 철도 시스템은 최근 들어 ICT(: Information & Communication Technology) 기술을 토대로 한 지능형 시스템으로서 스마트 철도로 진화되고 있다. 특히 철도 인프라의 운영 최적화, 자동화의 요구에 따라 ICT기반으로 하는 다양한 신규시장이 형성되어 타 운송수단 대비 접근성, 편리성, 신속성, 안전성 등의 요인으로 철도운송에 대한 수요가 증가하고 있다.

스마트 철도는 철도 서비스 플랫폼, 모바일 기술 및 모바일 서비스를 통합한 시스템[4]으로 그림 1과 같이 철도 구축/운영/관리의 전반에 걸쳐 통신 기술과 정보 기술을 활용하여 자동화를 넘어 지능화를 추구하는 새로운 철도 시스템이다[3].

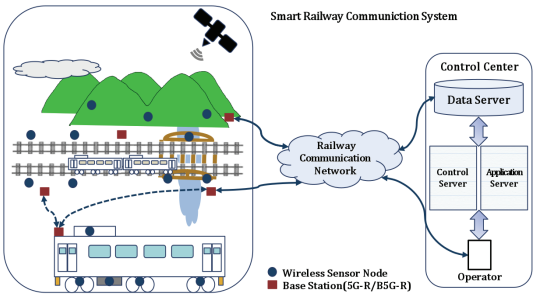

그림 1. 스마트 철도 통신 시스템[3]

Fig. 1 Smart railway communication system

그림 1의 스마트 철도 통신 시스템의 통신은 그림 2와 같이 열차통신, 관리통신 및 승객통신을 기본 요소로 하며, 이 기본 요소 간에 교차 통신 및 상위의 융합/응용 통신으로 구성될 수 있다[3-5].

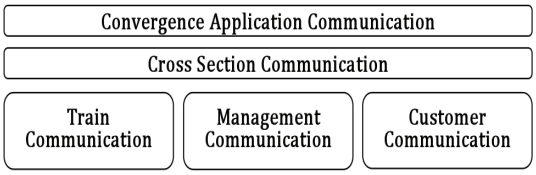

그림 2. 스마트 철도 통신 요소[3][5]

Fig. 2 Smart railway communication element

스마트 철도 통신 서비스는 그림 3과 같이 빅데이터, 딥러닝, AI 및 블록체인을 기반으로 하는 서버기반 정보 서비스, 열차/관리/승객 통신을 지원하는 각종 응용 서비스 및 각 서비스의 사용 정보를 보호하기 위한 정보보호 서비스로 구성된다.

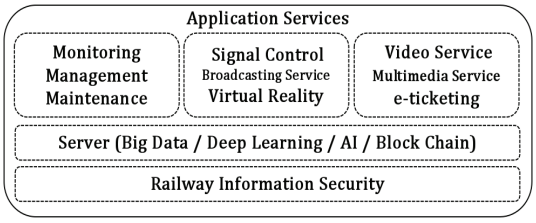

그림 3. 스마트 철도 통신 서비스[3]

Fig. 3 Smart railway communication service

또한 이에 대한 수요로 철도 인프라의 사용을 자동화하고 최적화하는 솔루션과 승객예약 및 정보시스템, 화물 운영정보시스템, 철도 교통관리, 운영 및 자산관리, IP기반 보안모니터링, 통신, 발권 및 철도 분석과 같은 여러 구성 요소가 해당한다[6].

이외 스마트 철도 통신 서비스로 클라우드 기술 및 GPS 등의 ICT 기술이 사용될 수 있으며, 이를 보호하기 위한 정보보호 기술 역시 필요하다.

특히 ICT 기반의 철도무선망으로 진화된 LTE-R 시스템은 음성, 영상, 열차제어 등 모든 종류의 진보된 철도서비스에 대해 통합된 형태로 안정적이고 신뢰성 있는 서비스 제공을 목적으로 한다.

III. 스마트 철도 통신기반의 위험요인

3.1 스마트 철도 통신 기술의 위험요소

철도안전과 연관된 열차제어를 위한 데이터는 지연되거나 손실되는 경우 열차사고로 이어질 수 있기 때문에 열차운행 중에는 반드시 가용성과 안정성이 확보되어야 한다.

현재 철도시스템은 무선통신을 기반으로 한 원격무인화가 적용되고 있어 철도통신 네트워크를 통해 전송되는 데이터는 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 데이터의 무결성을 확보하는 것이 절대적이다[10].

철도는 폐쇄적이고 독립적인 통신망을 사용하는 기반시설의 특성으로 인해 사이버 보안 위협에 비교적 안전하다는 인식이 보편적이었으나 시스템 업그레이드나 원격제어를 위해 인터넷 환경에서 파일 전송 시 사용되는 TCP/IP 프로토콜을 사용하는 경우가 적지 않다. 또한 시스템에서 생성되는 데이터를 실시간으로 확인하여 운영의 편리성과 민첩성을 높이기 위해 인터넷에 연결하는 상황도 늘어나고 있어 철도 통신망의 보안 취약점이 발생하고 있음을 알 수 있다[1][8].

철도 운송시스템은 매일 많은 양의 승객을 이동시키는 개방형 시스템으로 고정 경로를 따라 예정된 역에 정차함으로 많은 수의 접근 지점이 발생한다. 이러한 개방성, 접근성, 확장성 및 경제성이라는 특성을 유지하면서 보안수준이 향상된 철도에 최적화된 보안관리체계가 필요하다. 그림 4는 사람으로 인해 위험요인이 발생하면 센서가 위협을 감지하여 경보를 울리고 관제센터 보안 담당자의 확인과 동시에 신호 및 트래픽 제어시스템을 보호하는 철도통신 인프라 보안 기술이다[9].

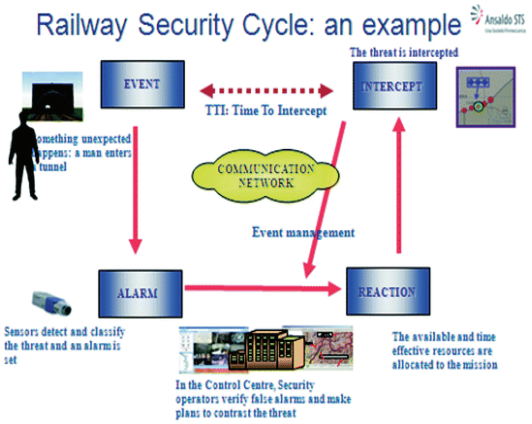

그림 4. 철도통신 인프라 보안 시스템[9]

Fig. 4 Rail communication infrastructure security system

그러나 현재 열차제어장치로 활용되고 있는 CBTC의 경우 통신정보에 의존하고 있어 통신망에 문제가

발생하면 열차의 운행 위치를 검지하지 못해 고밀도 배차가 불가능하여 치명적인 문제를 일으킬 수 있다.

CBTC는 열차제어의 모든 기능이 무선 통신정보에 집중되어 있어 열차가 운행되는 동안 계속해서 안정적인 로밍을 제공하지 못하거나 외부에서 해킹했을 경우 열차 제어권 전체를 공격받을 수 있게 된다[2][10].

또한 사이버 공격받을 경우 열차 혹은 철도 제어 기능이 마비되어 열차 추돌과 탈선 사고로 이어져 열차 안전운행에 큰 위협이 된다.

3.2 스마트 철도 통신 기술의 위험사례

철도통신시스템의 사이버 공격 사례를 보면 2011년 7월 중국 저장성 원저우 솽위마을의 20m 높이의 고가다리 위에서 고속열차 추돌사고가 발생했는데 사고 원인이 사이버 공격으로 인한 전력계통 소프트웨어 오류로 분석되었다. 요인은 전력제어시스템에 침입한 웜 바이러스를 정밀 점검한 결과 바이러스 공격대상의 최대 파괴 효과를 높이기 위해 시스템에 침투하여 정상적인 전력 및 전압 데이터를 기록, 전송하여 경보시스템 및 관리자가 발견하지 못하도록 한 것이다. 공격에 성공하면 시스템의 통제력이 상실되고 전력제어 시스템 역시 통제력이 소멸하여 열차를 마비시킨 사례로 조사되었다[1-7].

두 번째는 국내에서 발생한 것으로 2013년 1월 서울메트로의 종합관제소 신호관제 기계실 내 열차운행 제어컴퓨터(TCC : Traffic Control Computer)가 다수의 바이러스에 감염된 사례이다. TCC는 열차 운행을 자동제어하고 운행상태 표시, 화면표시, 열차번호 이동 등을 제어하는 주 컴퓨터 장치로, 이러한 TCC내 PC를 관리하면서 컴퓨터 바이러스 차단을 위한 '실시간 모니터링 감시' 및 '네트워크 침입차단 백신기능'을 활성화하지 않았기 때문에 신호제어 폐쇄망 내에 다양한 바이러스가 침투한 것으로 분석되었다. 이에 따라 트래픽 증가로 정보자원이 소모되는 현상 즉 CPU 점유, 통신소켓 버퍼 고갈이 계속 소모되고 있었으나 근원적 치료 없이 방치된 피해사례로 조사되었다[1], [11].

다음 해인 2014년 7월 또 한 차례 서울메트로의 핵심 컴퓨터 서버가 5개월 이상 북한소행으로 추정되는 사이버 공격을 받은 것인데 이에 따라 PC 관리 프로그램 운영 서버 2대가 해킹당하여 PC 213대에서 인가받지 않은 사용자 접속이 발견되었으며 PC 58대는 악성코드에 감염된 것으로 조사되었다. 이러한 사이버 공격은 대부분 통신환경에서 이루어지며 Rogue AP (access point)와 IP 스푸핑(spoofing) 그리고 데이터 변조 등 다양한 기술이 사용된 것으로 분석되었다[1][8][11].

Ⅳ. 스마트 철도 통신 정보보호 방안

일반적 관점에서 정보보호는 무결성, 기밀성, 가용성, 인증 및 부인봉쇄의 5대 요소를 기본으로 한다.

무결성은 정보의 무단 변경 방지, 기밀성은 정보 내용의 유출 방지, 가용성은 정보 유효성의 존속, 인증은 이용자의 타당성, 부인봉쇄는 행위 부인 방지를 목적으로 하고 있다.

각각 요소들은 일반적 차원 또는 일반 정보 시스템에서 정보보호 요구를 충족하기 위한 기본적인 대응 방안이 될 수는 있으나 특수한 분야 또는 산업 분야의 정보침해에 대한 효과적인 대응 방안으로 고려하기에는 부족함이 있을 수 있다.

초고속 철도 시스템과 같이 대량 수송을 목적으로 정밀하고 안정된 제어/관제가 요구되는 철도 시스템의 운영을 위한 정보보호에는 정보보호 요소별 대응 방안을 넘어 정보 활용 단계별 정보보호 방안이 필요하다.

특히 적절한 정보의 수집, 이동, 분석/대응을 전제로 하는 지능화된 시스템으로서 스마트 철도의 정보보호 방안은 시스템 전반의 운영 상태를 결정짓는 매우 중요한 요소가 될 수 있다.

본 연구에서는 이와 같은 스마트 철도 정보보호 필요성을 고려하여 정보의 수집, 이동 및 분석/대응의 3단계를 스마트 철도 정보 보호를 위한 단계별 대응 방안으로 제시한다.

정보 수집 단계의 보호는 철도 운영 및 관리에 필

요한 정보의 수집에 사용되는 각종 장치 및 센서의 보호 방안으로 정보 침해 공격으로 인한 오작동, 과작동, 측정 정보의 무단 변경에 대한 대응이 될 수 있다.

이동 단계의 보호는 측정된 정보가 측정 위치에서 서버로의 이동 또는 서버에서 서버간의 이동에서 발생할 수 있는 각종 유형의 정보침해에 대한 대응 방안이다. 일반적인 통신망에서 발생될 수 있는 유형의 정보침해 이외에 고속 이동 간에 가해 질 수 있는 정보침해가 추가로 고려되어야 한다.

많은 수의 노드로 구성될 가능성이 큰 철도 통신에서는 악성 노드가 통신에 개입하게 될 가능성이 매우 높고 이는 철도 통신 시스템의 성능에 치명적인 결과를 초래할 수 있게 된다. 실제로 철도 통신에서 약 50개의 악성 노드가 공격을 시도할 경우 패킷 전달률이 20%까지 낮아지고, 이에 대해 시큐어 링크로 대응할 경우 80%까지 회복할 수 있는 것으로 연구된 바 있다[12].

이동 단계 공격은 모바일 노드가 공격 대상이 될 수 있어 모바일 통신에서 발생할 수 있는 블랙홀, 그레이홀 등의 홀 공격이 치명적인 요소가 될 수 있다. 특히 그레이홀 공격의 경우 짧은 시간에 정보의 일부분만을 전송에서 이탈시켜 서버가 수신되지 못한 정보를 고려하지 않고 수집 데이터를 분석하게 함으로써 열차 운영정보 생성에 치명적 결함을 초래할 수도 있다.

분석/대응 단계의 공격으로는 서버 침해, 서버에서 분석된 대응 방안의 침해 등이 있을 수 있다. 서버 침해는 서버의 작동 불능, 오작동 및 짧은 시간에 이루어지는 간헐적 기능 상실 공격 등이 있을 수 있다. 대응 침해는 수집된 자료를 토대로 서버가 분석하여 도출한 대응의 오류 방안 생성 공격, 대응방안 전달 타깃의 오지정 및 대응 방안 이동간의 무단 변조 공격, 서버에서 생성이 없는 위조된 대응 방안의 생성/전달 공격 등이 있을 수 있다.

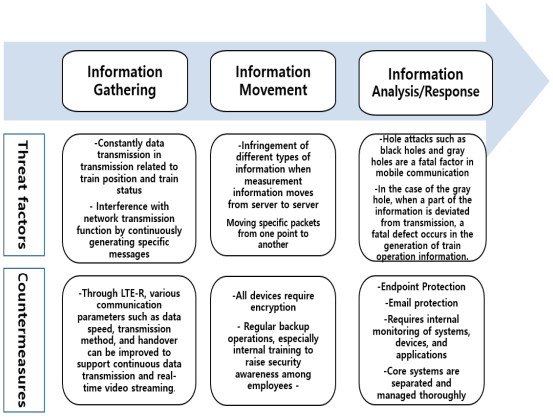

그림 5. 단계별 위협요인 및 대응방안

Fig. 5 Step-by-step threat factors and countermeasures

그림 5는 위에서 제시한 단계별 위협요인에 따른 대응방안을 도식화 하였다. 먼저 정보 수집 단계에서 특정 메시지를 지속적으로 발생시켜 네트워크 전송기능을 방해할 위험에 대비하여 끊임없는 데이터 전송과 영상 스트리밍이 실시간으로 지원 가능한 LTE-R로 우선 대응이 가능하다. 이동 단계에서는 특정 패킷들을 한 지점에서 다른 지점으로 이동시키려 할 때를 대비하여 모든 디바이스에 암호화와 정기적인 백업 작업이 필수적이다. 특히 철도운영기관 직원들의 보안 인식 개선을 위해 정기적인 내부교육도 반드시 필요하다. 분석과 대응 단계는 서버침해를 방지하기 위해 엔드 포인트 보호, 이메일 보호, 시스템과 디바이스 및 어플리케이션 등의 내부 모니터링을 강화해야 하며 핵심 시스템은 분리, 구분해서 관리하는 것이 바람직하다.

스마트 철도의 근간을 이루는 스마트 철도 통신에서는 효과적이고 효율적으로 운영되어야 할 지능형 시스템으로서 일반화된 정보보호 요소별 대응 방안을 능가해야 한다. 위와 같이 수집된 각종 운영 정보의 분석을 바탕으로 정보 수집, 이동 및 분석/대응 등의 정보 활용의 단계별 상황을 고려하였으나 추후에는 여러 유형의 정보 침해에 대한 구체적인 대응 방안의 강구가 필요하다.

Ⅴ. 결론

본 논문에서는 스마트 철도에서 기반 구조로 사용되는 통신 시스템의 필수적 요소인 정보보호 방안에 대하여 고찰하였다.

일반적인 ICT 시스템에서 사용되는 정보보호의 기본 요소로서 무결성, 기밀성, 가용성, 인증 및 부인봉쇄를 넘어서는 정보 수집, 이동, 분석/대응의 정보 활용 단계별 정보보호 방안이 스마트 철도 통신 시스템에서 필요한 것으로 분석되었다.

요소별 정보보호를 넘어 이용 단계별 정보보호 대응 방안은 고도화되고 지능화되는 스마트 철도 시스템의 기반을 이루는 통신 및 정보 기술이 융합된 통합 체계로서의 ICT 기술을 고려할 때 타당한 정보보호 방안으로 생각된다.

열차운행은 점차 무인화, 자동화로 전환되는 추세로 변화되는 무인시스템 운영으로 이전에 경험하지 못한 위험요인이 발생할 수 있음을 대비해야 한다. 특히 GTX(수도권광역급행철도) 등 대심도, 초고속화 철도추진에 따라 사고 발생 시 피해규모가 기하급수적으로 커질 수 있어 이에 대한 대응방안도 시급하다.

본 연구의 결과는 스마트 철도를 위한 통신 시스템의 정보 수집, 이동 및 분석/대응 단계별 정보 보호 필요성을 제시한 것으로서 이를 완성하기 위한 단계별 구체적인 침해요소와 그에 대한 대응방안의 강구는 지속적인 연구가 필요하다.

References

[1] H. Choi and S. Chae, “Analysis of Cyber-security Threats and Countermeasures for Radio-based Train Control Systems,” *J. of the Korean Society for Railway,* vol. 23, no. 1, 2020, pp. 70-79.

[2] J. Kim, “Smart Railway Communication Standardization Trend and Direction,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 17, no. 2, 2022, pp. 207-212.

[3] Y. Kim, S. Lee, J. Kim, and E. Park, "5G based Smart Railway Communication Technology Trends," *The Korea Institute of Information and Communication Engineering,* Busan, Korea, May 2022.

[4] S. Lin, Y. Jia, and S. Xia, "Research and Analysis on the Top Design of Smart Railway," *Journal of Physics Conference Series,* Beijing, China, Apr. 2019. pp. 1-7.

[5] Y. Kim, "Communication Structure for Smart Railway Network," *The Korea Institute of Information and Communication Engineering,* Kunsan, Korea, May 2021.

[6] KAIA(Korea Agency for Infrastructure Technology Advancement), “Smart railway safety system technology development project planning of R&D Report,” *Report,* 2019.

[7] S. Chae, B. Lee, H. Choi, and J. Bang, "Design and Implementation of Safety Functions of Communication-Based Autonomous Train Control System," *J. of Korean Institute of Communications and Information Sciences,* vol. 45, no. 1, 2020, pp. 146-154.

[8] Y. Song, J. Kim, S. Choi, and Y. Kim, “Evolution of ICT based railway radio networks,” *Information and Communication Mag.*, vol. 32, no. 12, Nov. 2015, pp. 3-9.

[9] P. D’Amore and A. Tedesco, *Railway Infrastructure Security.* Stuttgart: Springer Link, 2015, pp123-141.

[10] H. Kim, H. Oh, and J. Choi, “Trends of LTE based Railway Communication Systems,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 4, 2016, pp. 373-378.

[11] Y. Kim, “Traffic Transmission Performance of Railway Communication Network based on 5G,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 16, no. 6, 2021, pp. 1069-1074.

[12] G. Hatzivasilis, K. Fysarakis, S. Ioannidis, I. Hatzakis, G. Vardakis, N. Papadakis, and G.

Spanoudakis, "SPD-Safe : Secure Admini -stration of Railway Intelligent Transportation Systems," *J. of the Electronics,* vol. 10, no. 92, 2021, pp. 92-117.

저자 소개

박은경(Eun-Kyung Park)

1999년 국립 한국철도대학 운전과 졸업(전문학사)
2000년 인하대학교 국제통상물류대학원 공공물류전공(경영학석사)
2006년 러시아 모스크바 국립 철도대학교 대학원 철도물류학과 졸업(교통공학박사)
1994년~2014. 2월 한국철도공사 물류본부 근무
2014년~현재 동양대학교 철도전기융합학과 교수
2021.4~현재 국토교통부 항공철도사고조사위원회 비상임위원
※ 관심분야 : 스마트철도 통신시스템, 통신기반 열차제어시스템, LTE-R, ICT 융합 철도통신 등