무선통신기반 열차제어시스템의 EM 공격 분석

EM attack analysis of wireless communication based train control system

강기현†, 이종우*, 여현령*

Ki hyun Kang†*, Jong woo Lee* , Hyeon ryeong Yeo*

초 록 철도 수송의 고품질 서비스가 증가함에 따라, 동일한 요소로도 철도 열차제어시스템을 취약하게 만들 수 있다. 현재 철도열차제어시스템 제어용 망의 보안은 철도열차제어시스템에 대한 새로운 위험으로 떠오르고 있다. 망과 연결된 IED(Intelligent Electronic Devices), 제어기 및 SCADA 시스템에 대한 많은 위험요소들이 있으며 전자적 공격은 지역 전체의 열차제어시스템의 붕괴 또는 국가전체로 철도 운행불능으로 이어질 수 있다. 열차제어시스템을 감시하고 제어하는 모든 전자장치들은 전자침입에 대해 취약부분이 될 수 있다. 본 논문은 무선통신기반 열차제어시스템이 정보송신 중 받을 수 있는 EM 공격을 분석하고 그에 대한 대책 방안을 살펴보았다.

주요어 : 무선통신기반, CBTC , 열차제어시스템, EM 공격 분석 및 방지대책

1. 서 론

CBTC 시스템은 선로 변 및 신호기기실에 설치되어있다. 신호기기실 및 제어센터는 독립망으로 이루어져 어느 정도 외부침입을 차단할 수 있다. 그러나 분리된 신호 기기실은 안전성을 확보할 수 있지만, 현장에 설치된 장치들은 연결구조가 취약하다. 이것은 단순히 제어기와 SCADA 시스템 간의 위험 뿐만 아니라, 열차제어시스템을 감시하고 제어하는 모든 전자장치 IED, PLC 및 RTU 등과 RTU와 새로운 자동화된 장치 모두 전자침입과 전자공격에 취약하다. 대한 취약성을 규명하여 대비를 해야한다.

Table 1 열차제어시스템의 위협에 따른 공격분류

구분		공격대상	
		물리적	전자적
공격목표	물리적	물리적절도	정보, 데이터 및 지적재산에 대한 사보타지
		제어 시스템파괴	절도
	전자적	시스템 기능이상	정보, 데이터 혹은 지적재산의 손실을 발생하는 절도 및 사보타지
		시스템 기능저하 및 손실 발생하는 사보타지	

† 교신저자: 서울과학기술대학교 철도전문대학원 철도전기신호공학과
(bam-bi@seoultech.ac.kr)
* 서울과학기술대학교 철도전문대학원 철도전기신호공학과

2. 본 론

2.1 CBTC-Wifi 시스템 구성과 서브시스템

wifi 를 이용한 CBTC 시스템은 중앙관리장치, 선로 변 관리장치 및 AP 안테나 등으로 구성되어 있다.

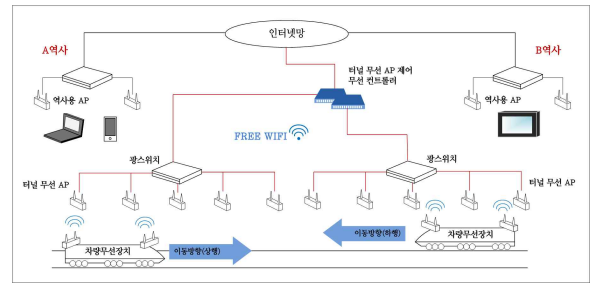

Fig. 1 CBTC-Wifi system architecture

Table 2 CBTC-Wifi subsystem

서브시스템	기능	특성	설치 위치	EM 공격
차량	▪ 허용속도산정 ▪ 열차속도감시 ▪ ATO 운전	이동체	외부	○
Wayside Signal Equipment	선행열차위치	PES	선로 변	
AP	정보전달	PES	선로 변	

2.1.1 LTE-R 시스템 구성과 서브시스템

LTE-R 시스템은 무선을 이용하여 열차제어에 필요한 패킷을 통하여 지상과 차상 간을 통신 한다.

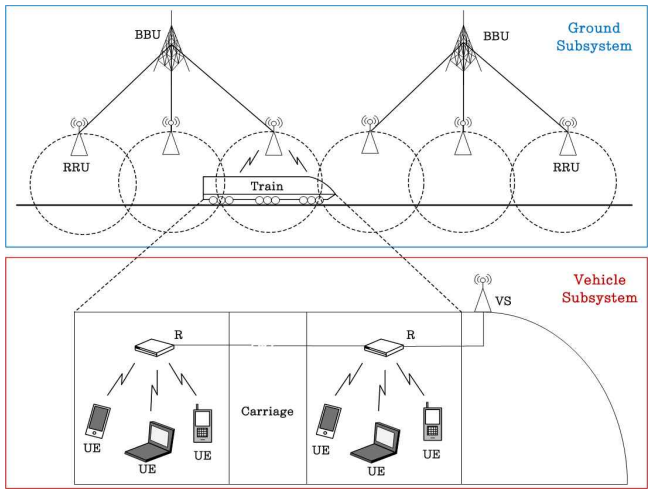

Fig. 2 LTE-R system architecture

Table 2 LTE-R subsystem

서브시스템	기능	특성	설치 위치	EM 공격
차량	▪ 허용속도산정 ▪ 열차속도감시 ▪ ATO 운전	PES	외부	○
BTS(RRU)	Telegram 전달	PES	선로 변	
Antenna	Telegram 전달	PES	선로 변	

2.2 위험원과 위협행위

구분	위협행위	
Wifi LTE-R	무선으로 전송되는 정보의 간섭	차상으로의 정보전달이 무선으로 이루어지기 때문에 강력한 무선 송출기에 의한 텔레그램을 교란시킬 수 있다.
	가짜 텔레그램	공격자는 열차제어정보의 명세, 텔레그램 등에 의해서 정확한 양식으로 정보는 전송할 수 있으며, 그로인해 차상장치는 잘못된 정보를 인식하지 못한다.
	가짜 차량	가짜 발리스는 진짜 발리스 열할을 할 수 있다.
	텔레그램에 대한 응답	가짜 지상 텔레그램에 의해 작동된 차상 텔레그램을 전송함에 따라서, 공격자는 가짜 텔레그램을 이용하여 텔레그램 정보를 인지할 수 있다.
	열차제어의 구조 및 변수의 노출	
	검지할 수 없는 방법으로 AP 파괴	
	무선 시스템의 비밀 정보 및 상태 정보 추출	
LTE-R	virus, worm 및 spyware 를 침투시킬 수 있다.	

2.3 예상 EM 공격 방법 및 대책

CBTC-Wifi		
구분	지상 AP	차상장치
입력정보	Telegram	Telegram
출력정보	Telegram	열차속도
위험원	- 허용속도보다 높은 속도정보 - 속도정보 삭제	- 허용속도보다 높은 속도정보 - 속도정보 삭제
위협행위	- 유도에 의한 가짜정보에 의한 허용속도보다 높은 속도정보 - 유도에 의한 속도정보 삭제	유도에 의한 정보변질
EM 공격	Narrow band	Narrow band
관련 Subsystems	AP	차상안테나
대응방안	IP 다중화	IP 다중화

LTE-R		
구분	Basic Transceiver Station	차상장치
입력정보	Telegram	Telegram
출력정보	Telegram	열차속도
위험원	- 허용속도보다 높은 속도정보 - 속도정보 삭제	- 허용속도보다 높은 속도정보 - 속도정보 삭제
위협행위	- 유도에 의한 가짜정보에 의한 허용속도보다 높은 속도정보 - 유도에 의한 속도정보 삭제	유도에 의한 정보변질
EM 공격	Narrow band	Narrow band
관련 Subsystems	AP	차상안테나
대응방안	- IP 다중화 - 무선 channel 다중화	- IP 다중화 - 무선 channel 다중화

3. 결 론

CBTC 시스템은 telegram 형태의 열차정보를 안테나를 통하여 송·수신을 하게 되어 있어 EM 공격에 상당히 취약하다.

Wifi 시스템은 AP까지는 광통신을 이용하기 때문에 EM 공격에 강하지만, Antenna는 EM파를 수신하기에 최적의 상태이기 때문에 EM 공격에 매우 취약하다. 따라서 EM 공격을 즉시 검지해야 하며, 대책으로는 다중 화된 telegram 전달 시스템이 필요하다.

LTE-R 시스템은 RRU까지는 광통신을 이용하기 때문에 EM 공격에 강하지만,

Antenna는 EM파를 수신하기에 최적의 상태이기 때문에 EM 공격에 매우 취약하다. 따라서 EM 공격을 즉시 검지해야 하며, 대책으로는 다중 화된 telegram 전달 시스템이 필요하다.

그러므로, EM 공격 취약성 때문에 다중 IP 및 다중 채널등과 같은 다중 화된 통신채널을 사용해야 할 것이며, 실제 상황에 적용하기 위해서는 심도 있는 검토가 필요하다.

참고문헌

[1] 한국정보통신기술협회 (2016) LTE 기반 철도 통신 시스템 구조.

[2] 신분당선 주식회사(2017) 신분당선 열차제어 시스템 소개.

[3] 김재현 (2014) 무선통신 기술의 이해 LTE(-A).

[4] 조한벽 (2007) LTE기반 철도통신 시스템 기술 개발 동향.

[5] Alcatel-Lucent (2017) The LTE Network Architecture.

[6] LINHAI ZHAO (2005) MODELING AND SIMULATION OF BALISE UP-LINK DATA TRANSMISSION BASED ON FINITE ELEMENT METHOD.

[7] Linfu Zhu (2016) Interaction Analysis and Optimization of Multi-antenna in Dual-channel Balise.

[8] Perambur S. Neelakantaswamy (2017) ON THE THREAT RO DIELECTRIC-BASED ELECTRONIC DEVICES AND COMPONENTS FROM REPETITIVE NONSINUSOIDAL ELECTRICAL OVERSTRESSES.

(한국철도학회 정기학술대회 Full Paper -Template 작성일: 2018.2.7)