2020 년도 한국철도학회 춘계계학술대회 초록집 KSR2020S031

철도 무선통신용 암호키관리 기술의 국내 적용에 관한 연구

지정근*†, 김창훈*, 윤용기**, 성동일***

초 록 무선통신 기반 열차제어시스템은 공공망을 사용하여 열차제어 메시지를 송·수신한다. 따라서 정보의 신뢰성, 안전성을 보장하기 위해 암호화 기법을 사용한 메시지 보안이 필수적이다. 현재 국내 무선기반 열차제어시스템(KTCS-2)은 700Mhz 공공안전망 주파수 대역을 사용한 LTE-R 방식에 기반을 두고 있으며 메시지 암복호화를 위해 Off-line 방식의 암호키관리 기술을 적용하였다. 이러한 방식에 더해 유럽의 열차제어시스템 ERTMS/ETCS 베이스라인3에서는 키관리에 대한 운영적인 측면을 고려하여 GSM-R 기반 TLS-PKI(Transport Layer Security-Public Key Infrastructure) 방식의 On-line 암호키관리 기술을 개발하여 적용하고 있다. 본 연구에서는 On-line 암호키관리 기술을 국내 LTE-R 기반 열차제어시스템에 적용하기 위한 방안을 제시하였다.

† 교신저자: 유경제어(주) 기술연구소(jkji@daum.net)
* 유경제어(주) 기술연구소
** 한국철도기술연구원
*** 한국철도시설공단 기술연구처