Journal of KIIT. Vol. 21, No. 10, pp. 185-192, Oct. 31, 2023. pISSN 1598-8619. eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2023.21.10.185

철도 보안인증시스템에서 보안인증서의 실시간 유효성 검증 방법

최 현 영*

Real-time Validation Method of Security Certificate in Railway Security System

Hyeon Yeong Choi*

본 연구는 한국철도기술연구원 주요사업의 연구비 지원으로 수행되었습니다.

요 약

열차의 안전한 운영을 위한 열차제어시스템은 차상-지상 제어장치 간 무선통신을 통해 열차제어 메시지를 전송한다. 열차제어 메시지의 무결하고 안전한 전송과 장치의 인증은 열차제어시스템에서 필수적으로 요구되어 제어장치 간 전송되는 데이터에 전자서명 기술을 적용한 철도 보안인증시스템이 제안되었다. 보안인증서의 유효성 검증을 위해 기존에는 CRL 또는 OCSP를 사용하였으나 철도 운영 환경에서 실시간성을 보장하기 어려운 문제점이 있다. 본 논문에서는 철도 보안인증시스템에서 사용되는 보안인증서의 유효성을 실시간으로 검증하고 관리할 수 있는 방법을 제안하고 이를 구현한 결과를 제시한다. 구현 결과는 인증서 폐지 목록의 갱신을 실시간으로 확인하고 이에 대한 정보를 보안단말기에 전송함으로써 전자서명 시 사용되는 보안인증서의 유효성을 실시간으로 검증 가능함을 보여준다.

Abstract

The train control system transmits train control messages through wireless communication between onboard and wayside control devices for safe train operation. Since the train control system requires counterfeiting, falsification, and authenticity verification of the train control messages, the railway security system based on digital signature technology was proposed. Previously, the validity of the security certificate was verified through CRL or OCSP, but it is difficult to guarantee real-time validation in a railway operation condition. In this paper, we propose a method to verify and manage the validity of security certificates in real time and present its implementation results. The implementation results show that the validity of the security certificate can be verified in real time by checking the CRL update in real time and transmitting the update information to the railway security device.

Keywords

railway communication, railway security system, security certificate, certificate revocation list

* 한국철도기술연구원 책임연구원
- ORCID: https://orcid.org/0000-0001-8028-2957

· Received: Sep. 13, 2023, Revised: Oct. 06, 2023, Accepted: Oct. 09, 2023
· Corresponding Author: Hyeon Yeong Choi
Korea Railroad Research Institute 176 Cheoldobangmulgwan-ro, Uiwang, Korea
Tel.: +82-31-460-5573, Email: hchoi@krri.re.kr

Ⅰ. 서 론

열차의 안전 운행을 위한 열차제어 메시지의 무결하고 안전한 전송은 열차제어시스템에서 필수적으로 요구된다. 이를 위해 열차제어 장치 간 전송되는 데이터에 전자서명 기술을 적용하여 장치의 인증과 통신 메시지의 신뢰성을 보장하는 철도 보안인증시스템과 관련한 연구가 이루어지고 있다[1]-[4]. 열차는 운영 중 노선의 분기 또는 합류를 통해 운행 노선이 변경되거나, 상행선 운행 종료 이후 하행선 운행 시 열차번호를 신규로 부여받기 때문에 열차의 정보가 운행 중에 빈번하게 변경될 수 있다. 따라서 철도 보안인증시스템은 이러한 철도 운영 및 환경 조건에 부합하여야 한다. 특히 열차제어시스템의 가용성을 저해하지 않도록 경량화된 보안인증 기술과 이를 위한 보안인증서 관리 기술이 필수적이다. 전자인증을 위한 보안인증서는 발급기관(인증기관), 발급자의 전자서명, 소유자, 일련번호, 공개키 정보, 유효기간 등 전자인증에 필요한 주요한 정보를 포함한다. 또한, 보안인증서의 생성, 폐지, 갱신 등을 통해 인증서의 관리가 이루어지며, 유효기간 내의 인증서라 하더라도 보안 공격이나 비정상적인 사용이 감지되면 인증서를 폐지하여 인증서의 무결성을 유지한다.

보안인증서의 유효성 관리 기술로 인증서폐지목록(CRL, Certificate Revocation List) 기반의 방법과 온라인 인증서 상태 프로토콜(OCSP, Online Certificate Status Protocol)을 이용하는 방법이 사용되고 있다[5]-[10]. CRL은 유효기간 내의 인증서 중 비정상적인 사용이나 보안 공격 등으로 더 이상 인증서가 유효하지 않을 때 인증기관에서 폐지한 인증서의 목록이며, 인증기관에서 CRL을 관리한다. 인증기관에서는 주기적으로 CRL을 생성하고 공지하며, 보안인증서를 사용하는 클라이언트에서는 인증기관이 제공한 URL(Uniform Resource Locator)을 통해 CRL을 다운로드하여 인증서의 일련번호를 통해 해당 인증서의 유효성을 확인한다[5][6]. 그러나 인증기관이 CRL을 갱신하는 주기는 인증기관의 정책을 따르며(일반적으로는 24시간 주기로 갱신됨), 누적된 CRL의 다운로드 시 부하 발생 및 속도 저하로 인해 실시간으로 보안인증서의 유효성을 검증하는 것은 불가능하다[9][10]. 이러한 CRL을 주기적으로 갱신하고 다운로드하는 단점을 보완하기 위해 OCSP를 사용한다[7]-[10]. OCSP는 온라인 인증서 상태 프로토콜이며 인증기관이 OCSP 서버를 운용한다. 클라이언트는 인증서의 유효성 검증을 위해 원하는 인증서 상태 조회 요청을 OCSP 서버로 송신하고, OCSP 서버는 인증서버로부터 CRL을 다운로드 받아 해당 인증서의 상태를 조회하고, 요청에 회신을 준다. 따라서, OCSP는 CRL에 비해 빠르게 응답을 처리할 수 있으나, 다수의 클라이언트가 인증서 상태 요청을 하는 경우 OCSP 서버에서 요청이 들어올 때마다 CRL을 새롭게 다운받아야하는 부담이 발생하므로 응답지연이 발생할 수 있다[9][10].

실시간으로 변경되는 열차의 운영 조건에 대응하기 위해 철도의 보안인증시스템은 보안인증서의 유효성/무결성 관리를 실시간으로 수행하여야 하며, 보안인증서를 사용하는 클라이언트 또한 보안인증서의 유효성을 실시간으로 검증할 수 있어야 한다. 본 논문에서는 철도 보안인증시스템에서 장치의 인증과 전자서명 시 사용되는 보안인증서의 유효성을 실시간으로 검증하고 관리하는 방법을 제안한다. 보안인증서의 실시간 유효성 검증 및 관리를 위해 CRL을 사용하되, 보안인증서 폐지 이벤트 발생 시, CRL 배포 관리자(CDM, CRL Distribution Manager)를 통해 실시간으로 CRL 업데이트를 보안단말기에 통지하여 최신의 CRL을 유지하고 인증서 유효성 검증의 실시간성을 확보할 수 있도록 한다. 본 논문의 구성은 다음과 같다. 2장에서는 보안인증서의 유효성 검증을 위한 CDM의 구성과 CRL 갱신을 확인하여 통지하는 방법을 설명하고, 3장에서는 철도 보안인증시스템에 CDM을 구현하여 적용한 검증 결과를 제시한다.

Ⅱ. 보안인증서 유효성 검증을 위한 CRL 배포 관리자

그림 1은 철도 보안인증시스템의 구성도이며, 철도 차상-지상 간 열차제어 메시지 전송 시 통신보안을 위해 열차제어장치와 통신장치 사이에 보안단말기가 위치한다.

보안단말기에서 열차제어 메시지의 무결성 검증, 암복호화 등을 수행하며, 이를 위해 보안 인프라 관리서버와 별도의 통신을 통해 보안인증서, 암호화 키 등을 전송받는다. 보안 인프라 관리서버는 보안인증서버와 키관리서버로 구성되며, 통신 보안을 위한 인증서 및 암호화 키의 생성, 배포, 삭제, 폐지 등을 관리한다. 이러한 철도 보안인증시스템 구조에서, 보안인증서의 실시간 유효성 검증 기능은 보안인증서버의 하부 기능으로써 CDM에 의해 수행된다.

그림 2는 CDM의 구성과 보안인증서버와 보안단말기 간 인터페이스를 나타낸다. 보안인증서 폐지 이벤트가 발생하면, 보안인증서버는 해당 인증서를 폐지하고 CRL을 발행한다.

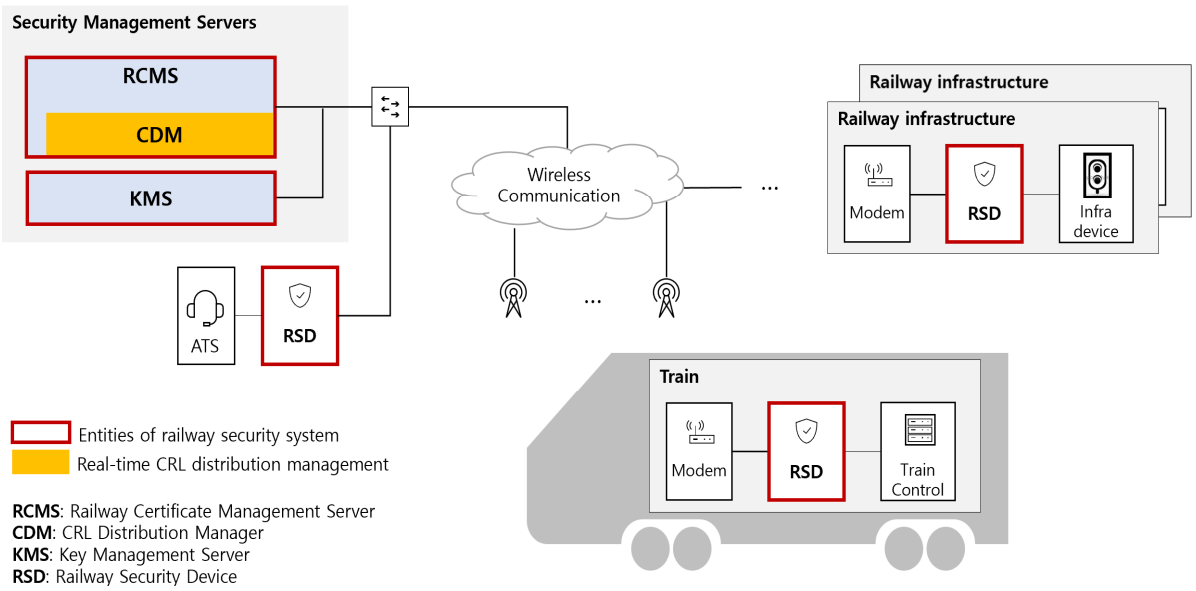

그림 1. 철도 보안인증시스템의 구성도
Fig. 1. Configuration of railway security system

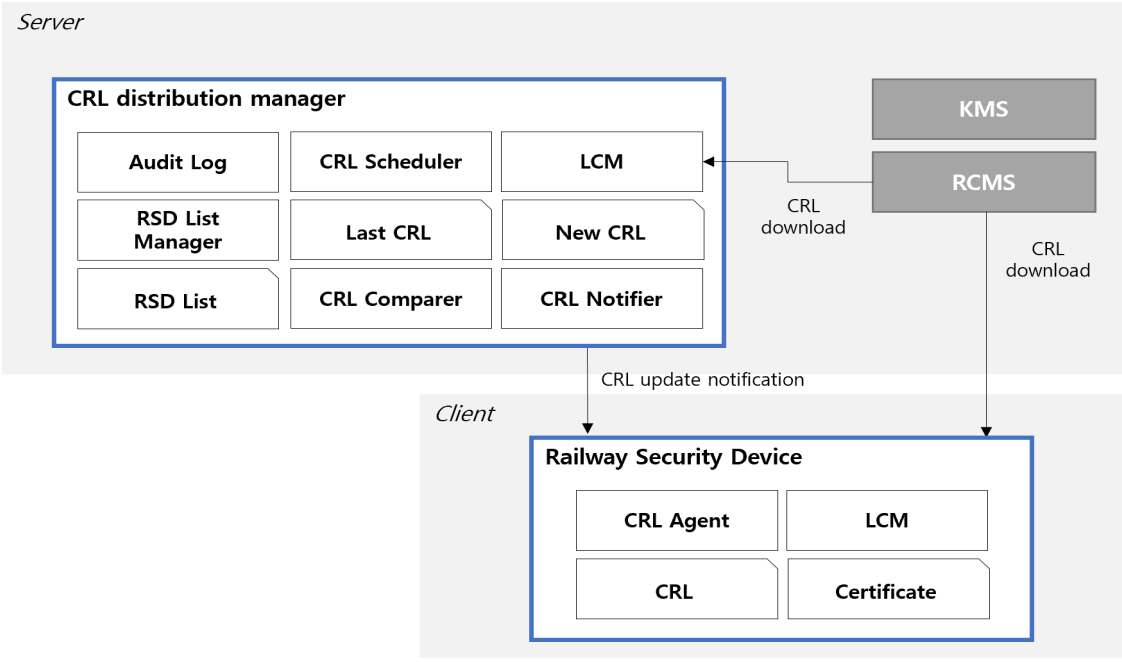

그림 2. CRL 배포 관리자 구성도
Fig. 2. Configuration of CRL distribution manager

CDM은 주기적으로 보안인증서버의 CRL 갱신 상황을 확인하고 보안단말기에게 CRL 업데이트를 통지하는 기능을 수행한다. 이로써 보안단말기가 항상 최신의 CRL을 확보하여 보안인증서의 유효성을 검증할 수 있도록 한다.

그림 2의 CDM 구성 요소 중 CRL 스케줄러는 CRL 갱신을 확인하는 스케줄을 정의하며, LCM (Local Configuration Manager)를 통해 보안인증서버와 통신하여 최신의 CRL을 안전하게 수신받는다. LCM을 통해 받은 CRL을 신규 CRL 모듈에 저장하며, 최근 CRL 모듈에 저장된 기존의 CRL과 비교하여 CRL이 갱신되었는지 CRL 비교 모듈에서 확인한다. CRL이 갱신되었을 경우, CRL 통지 모듈을 통해 CRL 갱신 여부를 보안단말기에게 통지한다. 보안단말기에 CRL 갱신 정보를 실시간 통지하기 위해, CDM 내부에 보안단말기 정보를 수신받아 보안단말기 목록을 저장하는 기능을 포함된다. 감사로그는 시스템 변경 및 CRL 변경 등 주요 정보를 저장한다. 보안단말기의 CRL 에이전트는 CDM으로부터 CRL 업데이트 정보를 수신받고, LCM을 통해 보안인증서버에 접속하여 새로운 CRL을 다운로드 받아 자신이 보유한 보안인증서의 유효성을 실시간으로 확인한다.

그림 3은 실시간 CRL 업데이트 절차에 대한 시퀀스 다이어그램을 보여준다. 인증서 폐지 이벤트가 발생하면 보안인증서버에서 CRL을 업데이트한다. CDM은 보안인증서버에 주기적으로 CRL을 확인하여 전송받고, 기존 저장된 CRL과 비교하여 CRL의 업데이트 여부를 확인한다. CRL이 업데이트 되면 보안단말기에 CRL 업데이트 사실을 통지한다. CRL 업데이트 통지를 받은 보안단말기는 보안인증서버에서 CRL을 다운로드하고, 이를 통해 보안인증서의 유효성을 확인한다.

III. CRL 배포 관리자의 구현 및 검증

본 장에서는 상기 기술된 보안인증서의 실시간 유효성 검증을 위한 CDM을 구현하여 기능 및 성능 검증의 수행 결과를 논의한다. 먼저 CDM은 HTTP(Hyper Test Transfer Protocol)를 이용하여 CRL 요청, CRL 다운로드 기능을 구현하였으며 기존 철도 보안인증시스템의 보안인증서버 및 보안단말기와 연계되도록 하였다.

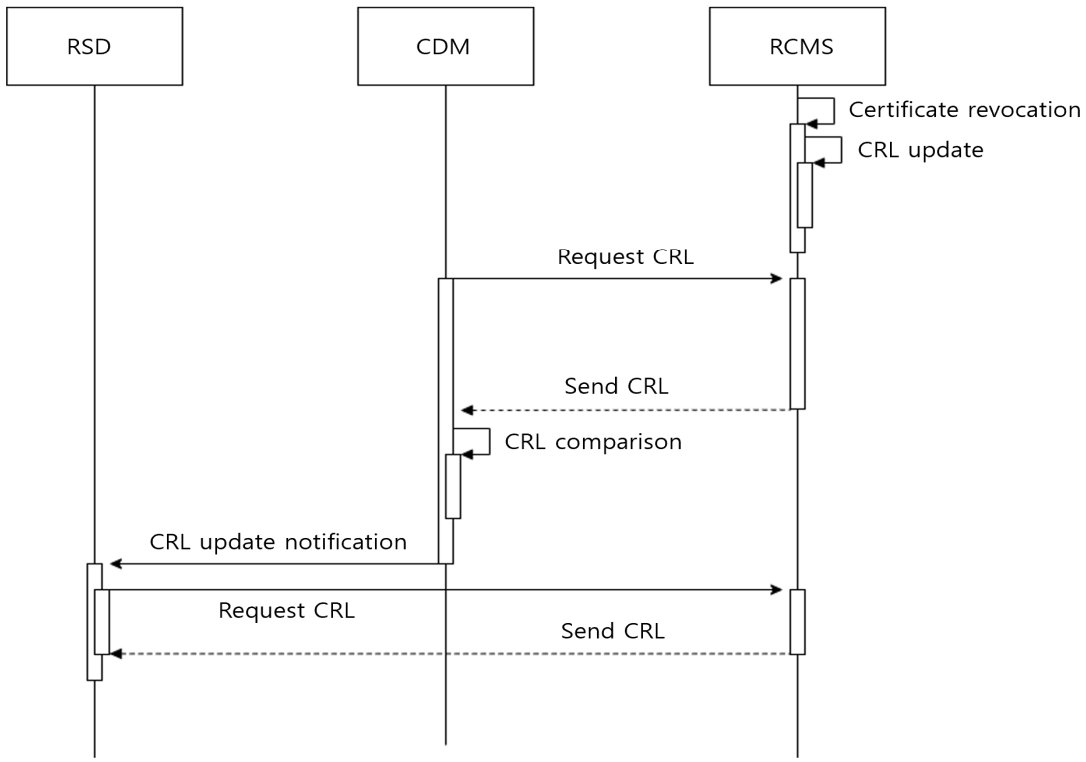

그림 3. 실시간 CRL 갱신 시퀀스 다이어그램
Fig. 3. Sequence diagram of real-time CRL update procedure

그림 4는 CDM을 통한 보안단말기의 CRL 갱신 기능 검증을 위한 시나리오를 보여준다. 보안인증서버에서 보안인증서 폐지 이벤트 발생 시 CRL을 갱신하고, CDM은 이를 확인하여 CRL 갱신 정보를 2대의 보안단말기에 통지한다. 각각의 보안단말기는 보안인증서버로부터 신규 CRL을 다운로드하여 최신의 CRL을 저장한다. CDM은 보안인증서버의 CRL 갱신 확인을 위해 500 ms 주기로 폴링하도록 설정하였으며, CRL 갱신을 확인한 시점부터 2대의 보안단말기에서 갱신된 CRL 다운로드를 완료할 때까지의 기능과 시간을 확인하였다.

먼저 철도 보안인증시스템의 보안인증서버에서 임의로 보안인증서를 폐지하여 그림 5와 같이 CRL을 신규로 배포한다. 보안인증서버에서 신규로 CRL을 배포한 시간은 2020-11-11 18:05:46이다.

그림 6은 CDM에서 보안인증서버가 배포한 CRL의 갱신 확인을 위한 로그를 나타낸다. 그림 6의 시간 2020-11-11 09:05:46,777은 CDM에서 CRL을 다운로드한 시간으로 UTC(universal time coordinated) 기준이므로, CRL 다운로드 완료 시간은 9시간을 더한 2020-11-11 18:05:46,777이다. CRL 갱신을 확인한 시간은 2020-11-11 18:05:46,781이다.

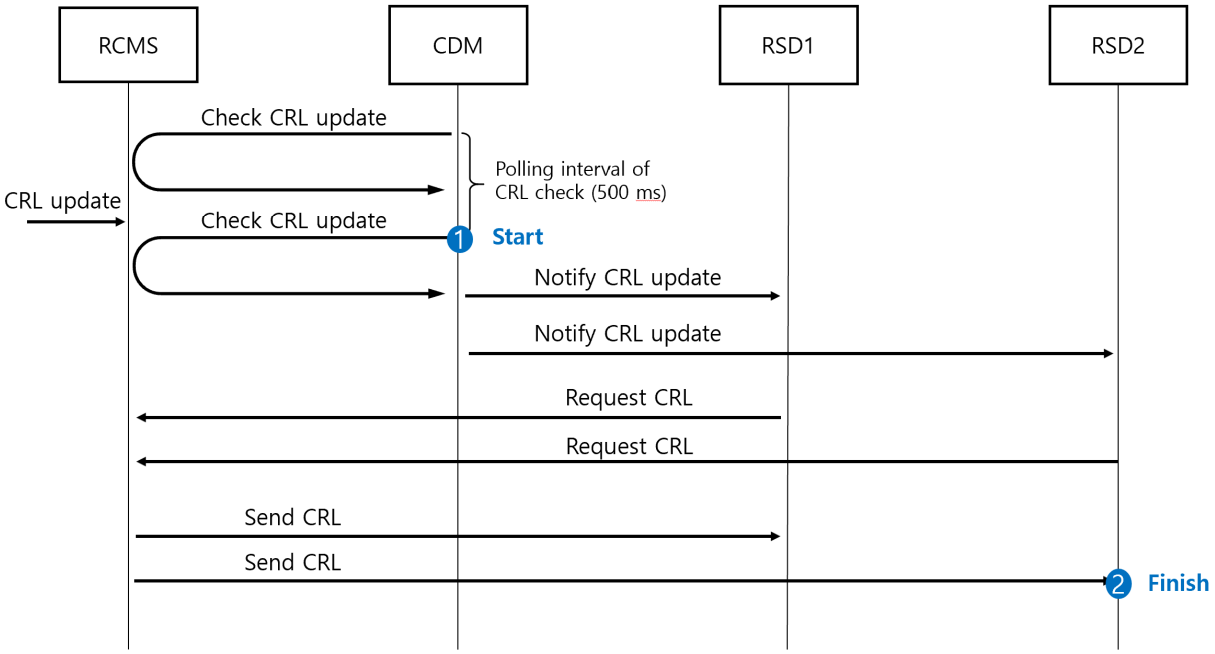

그림 4. CRL 배포 관리자 검증 시나리오
Fig. 4. Verification scenario of CRL distribution manager

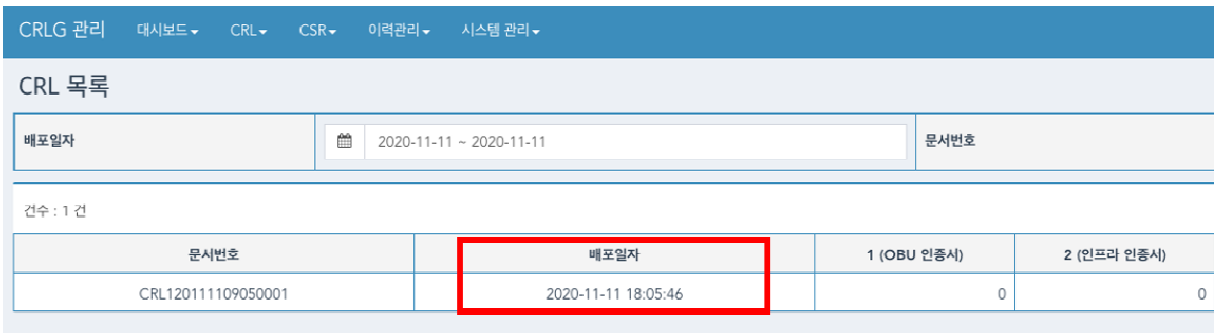

그림 5. 보안인증서버의 CRL 갱신
Fig. 5. CRL update of railway certificate management server

그림 7은 보안단말기에서 CRL 갱신 정보를 수신받아 보안인증서버에 신규 CRL을 요청하여 다운로드받는 로그를 보여준다. 보안단말기에서 보안인증서버에 CRL을 요청하는 시간은 2020-11-11 09:05:46,786(UTC)이며, CRL 다운로드 후 갱신을 완료한 시간은 2020-11-11 18:05:46,840으로 측정되었다. 이를 통해 보안인증서버에서 CRL을 폐지한 이후 CDM을 통해 보안단말기에서 CRL을 갱신하기까지 걸린 시간은 63 ms로 측정되었으며, CDM이 주기적으로 보안인증서버에 CRL 갱신을 체크하는 폴링 주기(500 ms)를 고려하면 보안인증서의 유효성 검증 시간은 563 ms임을 확인하였다.

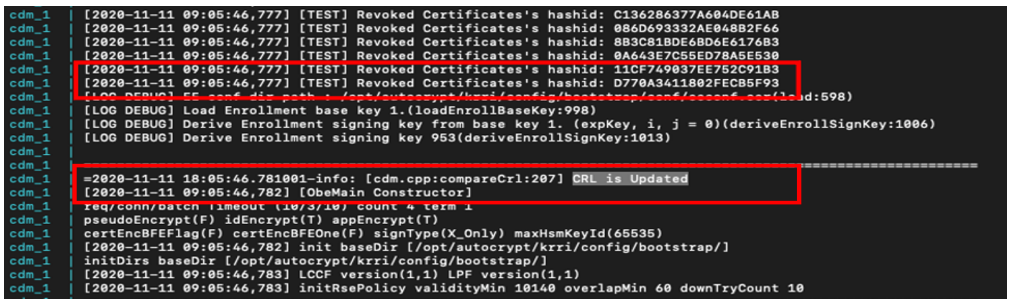

그림 6. CRL 배포 관리자의 CRL 갱신 확인
Fig. 6. CRL update check of CRL distribution manager

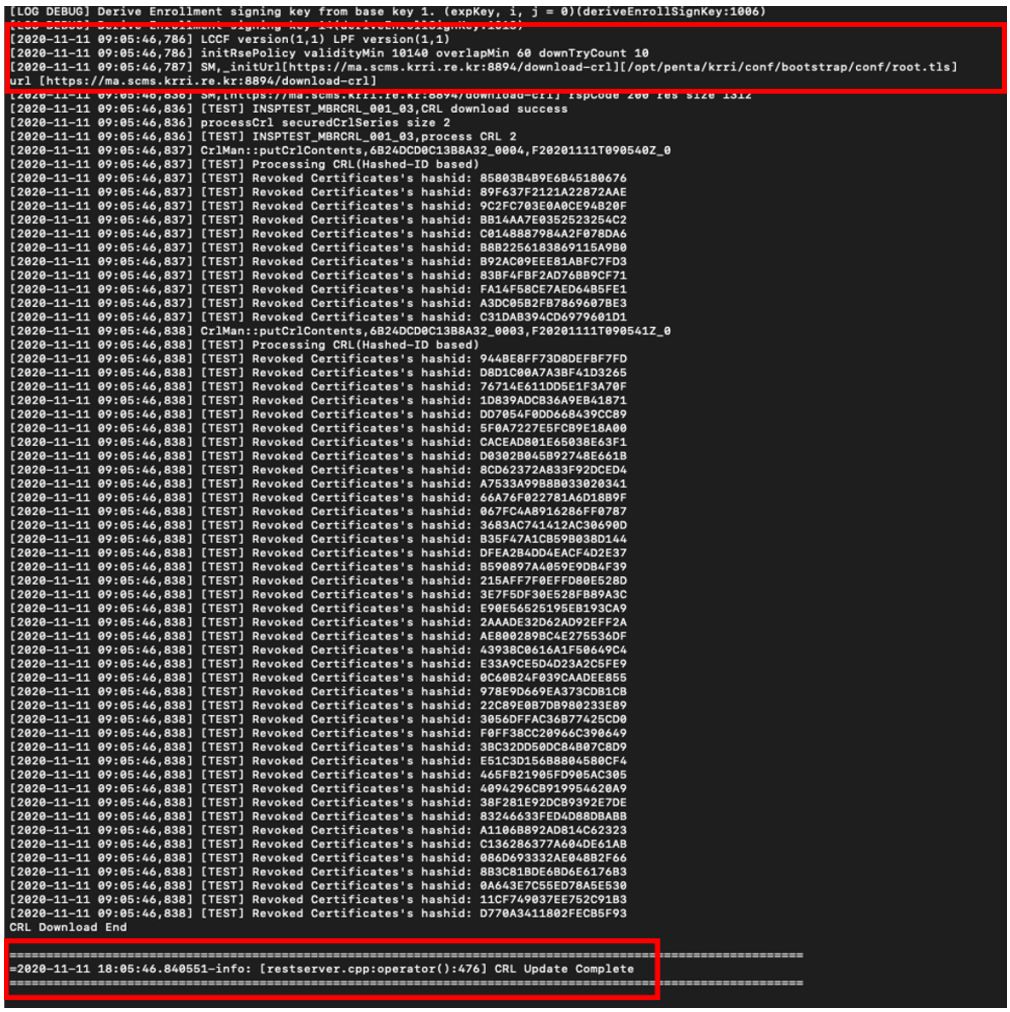

그림 7. 보안단말기의 CRL 갱신
Fig. 7. CRL update of railway security device

CDM을 통한 철도 보안인증시스템에서의 보안인증서 실시간 유효성 검증 성능을 확인하기 위해 앞서 기술한 검증 시나리오를 바탕으로 100회 반복 테스트를 수행하였다. 그림 8은 CDM에서 CRL 갱신을 확인 후 보안단말기에서 신규 CRL을 다운로드하기까지 측정한 시간을 보여준다. 100회 반복 테스트 결과 CRL 갱신 시간은 최소 32 ms, 최대 463 ms, 평균 74 ms로 측정되었다. CDM의 폴링 주기를 고려하였을때 최대 1초 이내로 보안단말기에서 보안인증서버의 CRL 갱신을 확인할 수 있었다. 시험 결과는 CDM을 통해 실시간으로 CRL의 갱신 확인 및 다운로드가 가능함을 보여주며, 이를 바탕으로 철도 보안인증시스템의 보안단말기에서는 보안인증서의 실시간 유효성 검증이 가능하다.

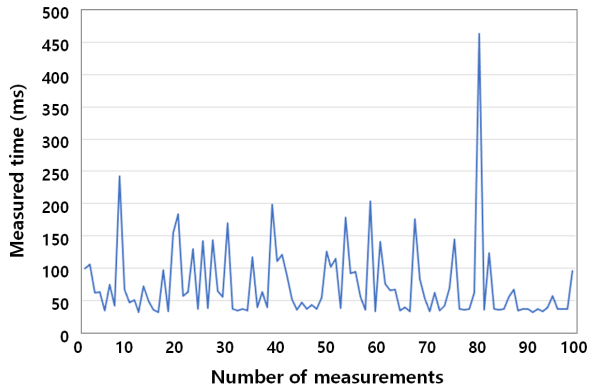

그림 8. CRL 배포 관리자의 성능 평가
Fig. 8. Performance evaluation of CRL distribution manager

표 1은 기존의 보안인증서 유효성 검증 방법들과 본 논문에서 제안하는 방법을 비교한 표이다. 기존 방법인 CRL을 직접 다운로드하여 확인하는 방법은 갱신 주기 내 발생된 폐지 이벤트를 바로 확인하지 못하는 오프라인 방식이며, OCSP와 CDM 방식은 온라인으로 인증서 폐지 사실을 실시간으로 확인할 수 있다. 하지만 다수의 클라이언트가 보안인증서의 유효성 검증을 요청하게 되면 OCSP 서버는 매번 CRL을 새롭게 다운받아 처리해야 하는 부담이 발생하는데 반해, CDM은 CRL 갱신 정보를 실시간으로 확인하여 클라이언트에게 통지하여 서버의 부담은 감소하고 클라이언트는 실시간으로 보안인증서의 유효성을 검증할 수 있다.

표 1. 기존 방법과의 비교
Table 1. Comparison of CRL validation methods

Function	CRL	OSCP	CDM
on-line	X	O	O
real-time	X	O	O
server burden	-	O	X
update notification	X	X	O

Ⅳ. 결 론

열차의 안전 운행을 위한 열차제어시스템은 무선통신을 통해 전송되는 열차제어 메시지의 무결하고 안전한 전송이 필수적이다. 이를 위한 철도 보안인증시스템은 실시간으로 변경되는 열차의 운영 조건에 대응하기 위해 보안인증서의 실시간 유효성 관리가 요구된다. 본 논문에서는 철도 보안인증시스템의 장치 인증 및 전자서명을 위한 보안인증서의 실시간 유효성 검증 및 관리를 위한 CDM을 제안하였다. 보안인증서 폐지 이벤트 발생 시, 보안인증서버에서 발급하는 CRL을 CDM을 통해 CRL 갱신 여부를 확인하고, 이를 보안단말기에 통지하여 보안단말기가 최신의 CRL을 유지할 수 있는 구조를 제안하고 이에 대한 성능평가 결과를 제시하였다. CDM은 주기적으로 보안인증서버의 CRL 갱신 여부를 확인하고, 갱신 시 보안단말기에 이를 통지하여 보안단말기가 신규 CRL을 다운로드 받는 시간은 최대 463 ms로 측정되었다. CDM의 폴링 주기를 감안하더라도 최대 1초 이내로 보안단말기에서 신규 CRL을 다운로드하여 보안인증서의 유효성 확인이 가능함을 확인하였다. CDM의 성능 검증을 위해 본 시험에서는 2대의 보안단말기를 사용하였으나, 신규 CRL 다운로드는 동시에 병렬로 처리가 가능하므로 보안단말기의 대수가 증가하더라도 성능에 영향을 미치지 않을 것으로 판단된다. 향후에는 보안단말기의 수를 확장하여 CDM을 통한 보안인증서의 유효성 검증 방법의 확장성을 확인하고자 한다.

References

[1] R. D. Pascoe and T. N. Eichorn, "What is communication-based train control?", IEEE Vehicular Technology Magazine, Vol. 4, No. 4, pp. 16-21, Dec. 2009. https://doi.org/10.1109/MVT.2009.934665.

[2] H. Y. Choi and S.-Y. Chae, "Analysis of cyber-security threats and countermeasures for radio-based train control systems", Journal of the Korean Society for Railway, Vol. 23, No. 1, pp. 70-79, Jan. 2020. https://doi.org/10.7782/JKSR.2020.23.1.70.

[3] H. Y. Choi and R.-G. Jeong, "Security of train control messages and certificate authority structure", Journal of the Korean Society for Railway, Vol. 24, No. 12, pp. 1090-1100, Dec. 2021. https://doi.org/10.7782/JKSR.2021.24.12.1090.

[4] H. Y. Choi, "A Study of Group Security Policy Management for Multicast Communications of Railway Security System", Journal of Korean Institute of Information Technology, Vol. 20, No. 10, pp. 61-69, Oct. 2022. https://doi.org/10.14801/jkiit.2022.20.10.61.

[5] M. Naor and K. Nissim, "Certificate revocation and certificate update", IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, pp. 561-570, Apr. 2000. https://doi.org/10.1109/49.839932.

[6] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008. https://doi.org/10.17487/RFC5280.

[7] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, Jun. 2013. https://doi.org/10.17487/RFC6960.

[8] Korea Internet & Security Agency, "Online Certificate Status Protocol Specification", Sep. 2009. https://rootca.kisa.or.kr/kcac/down/TechSpec/5.2-Online%20Certification%20Service%20Protocol.pdf [accessed: Sep. 11, 2023]

[9] Y. Liu, W. Tome, L. Zhang, D. Choffnes, D. Levin, B. Maggs, A. Mislove, A. Schulman, and C. Wilson, "An End-to-End Measurement of Certificate Revocation in the Web's PKI", In Proc. of the 2015 Internet Measurement Conference (IMC '15). Association for Computing Machinery, New York, NY, USA, pp. 183-196, Oct. 2015. https://doi.org/10.1145/2815675.2815685.

[10] Y. J. Kim and T. M. Chang, "A Study on Efficient CRI managing for Certificate Status Validate in Distributed OCSP", Journal of The Korea Society of Computer and Information, Vol. 13, No. 3, pp. 91-98, May 2008.

저자소개

최 현 영 (Hyeon Yeong Choi)

2003년 2월 :
서울시립대학교(공학사)
2005년 8월 : KAIST(공학석사)
2010년 2월 : KAIST(공학박사)
2013년 5월 ~ 현재 :
한국철도기술연구원 책임연구원
관심분야 : 철도 신호, 통신, 보안