V2V 환경에서 양자내성전자서명 알고리즘 성능 비교 분석

서유진, 임우상, 김영식*

대구경북과학기술원

{dmfive, lws0815, ysk}@dgist.ac.kr

Performance Comparison of Post-Quantum Digital Signature Algorithms in V2V Environment

Yujin Seo, Woo-Sang Im, Young-Sik Kim*

DGIST.

요 약

본 연구는 양자컴퓨팅 기술의 급속한 발전으로 기존 공개키 암호 체계의 안전성이 위협받는 상황에서, V2X(Vehicle-to-Everything) 통신 환경 중 V2V(Vehicle-to-Vehicle)에 적용할 수 있는 양자 내성 전자서명 알고리즘의 성능을 비교 분석하였다. 실험 대상으로는 미국 NIST의 표준 양자내성암호 서명인 ML-DSA와 한국양자내성암호 공모전에서 선정된 HAETAE를 선정하였다. 시뮬레이션 환경은 OMNeT++ 5.7과 Veins 5.2 기반 WAVE 프로토콜로 구축하였으며, SUMO 1.18.0을 활용하여 3차선 고속도로 시나리오에서 총 1,000회 실험을 수행하였다. 실험 결과, HAETAE-120은 ML-DSA-44 대비 E2E 지연시간에서 더 빠른 성능을 보였다. 이러한 차이는 HAETAE-120의 서명 크기(1,474B)가 DSRC 최대 페이로드(2,304B) 이내여서 단일 프레임 전송이 가능한 반면, ML-DSA-44는 서명 크기(2,420B)가 이를 초과하여 2개 패킷으로 분할 전송해야 하기 때문이다. 특히 MAC 계층 지연이 E2E 지연의 지배적 요소로 작용하였으며, ML-DSA-44는 패킷 분할로 인해 HAETAE-120 대비 2.4배 높은 MAC 지연을 나타냈다. 차량 밀도 증가에 따른 분석에서도 HAETAE-120은 PDR(Packet Delivery Ratio) 측면에서 높은 신뢰성을 유지하였다. 두 알고리즘 모두 V2X 요구사항인 100ms 이하의 E2E 지연을 충족하였다.

Ⅰ. 서론

양자컴퓨터의 급격한 발전은 현재 널리 사용되는 RSA 및 ECDSA 기반 전자서명 알고리즘의 보안성을 근본적으로 위협하고 있다. 특히 V2X 통신 환경은 차량 안전과 직결되므로 보안성 확보가 필수적이다 [1]. 이에 NIST는 양자내성암호(PQC) 표준화를 진행하여, 2024년 양자 내성 전자서명 표준 FIPS 204-ML-DSA(CRYSTALS-Dilithium)를 발표하였으며, 한국에서도 한국양자내성암호연구단 공모전에서 선정된 HAETAE 알고리즘이 주목받고 있다 [2, 3]. E2E(End-to-End) 지연은 송신 애플리케이션에서 수신 애플리케이션까지의 패킷 전달 시간을 의미한다. 안전 측면에서 V2X 애플리케이션은 저지연을 요구한다. PQC 적용으로 메시지 크기가 증가하면 프레임 전송시간과 채널 점유가 늘어나 혼잡 및 MAC 접근 지연이 악화될 수 있으므로, V2X 환경에서 그 영향을 정량적으로 분석할 필요가 있다. 본 연구에서는 SUMO 교통 시뮬레이터와 OMNeT++/Veins를 활용하여 V2V 환경에서 HAETAE-120과 ML-DSA-44의 E2E 성능을 비교 분석한다.

Ⅱ. 본론

V2V 환경에서 BSM(Basic Safety Message)은 차량 간 충돌 방지 및 교통안전을 위해 엄격한 지연시간 요구사항을 갖는다. 기존 V2X 환경에서 BSM의 서명 알고리즘으로는 ECDSA가 사용된다. 그러나 V2X 환경은 차량 안전과 직결되므로 양자 컴퓨터에 의해 보안이 위협받는 기존 ECC 기반 전자서명 알고리즘에서, 안전한 PQC로의 전환이 필요하다.

V2X 환경에서 BSM은 WAVE 프로토콜 스택을 통해 전송되며, IEEE 1609.2 보안 서비스에 따라 서명된다. 그림 1과 같이 WAVE 프로토콜 스택은 IEEE 1609.3 표준에 따른 V2X 메시지 전송 프로토콜인 WSMP, IEEE 1609.2 표준에 기반한 V2X 보안 프레임워크 및 서명·인증서 처리 기능, 그리고 RFC 8200에 기반한 IPv6 프로토콜로 구성된다 [5].

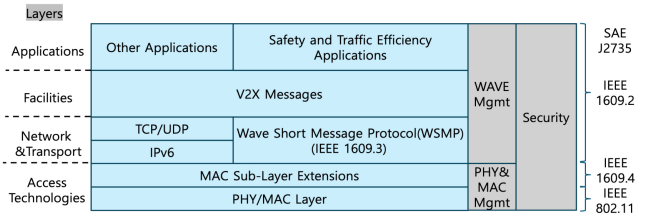

그림 1 WAVE protocol stack

PQC 서명 알고리즘을 적용한 BSM 패킷은 기존 ECDSA 대비 크기가 증가하므로, 본 연구에서는 이를 고려하여 전용 단거리 통신(DSRC)과 WAVE 프로토콜 환경을 기반으로 시뮬레이션을 구성하였다 [6]. IEEE 802.11p 표준 MAC 프레임의 최대 페이로드는 2,304 bytes이나, 본 연구에서는 WAVE/DSRC 환경에서 일반적으로 사용되는 2,000 bytes를 단편화 임계값으로 설정하였다 [6]. 이 값은 SPDU 헤더, 인증서, BSM 페이로드를 포함한 전체 프레임 크기를 고려한 것이다. V2V 환경에서 각 차량은 100ms 주기로 BSM을 브로드캐스트한다.

표 1. 각 알고리즘 별 파라미터 사이즈

파라미터	HAETAE-120	ML-DSA-44
공개키 크기	992 bytes	1,312 bytes
서명 크기	1,474 bytes	2,420 bytes

알고리즘 선정 시에는 V2V 환경의 성능 요구사항과 통신 부하를 고려

하여 NIST 보안 등급 2에 해당하는 알고리즘을 선택하였다.

표 1에서 서명 크기를 비교하면, HAETAE-120은 ML-DSA-44 대비 약 39% 작아 데이터 전송량이 많은 V2V 환경에서 대역폭 효율성이 높음을 알 수 있다.

실험 환경은 OMNeT++ 5.7과 Veins 5.2를 사용하여 WAVE 환경으로 구축하였으며, SUMO 1.18.0을 통해 실제 차량 이동성을 반영하였다. 암호 연산은 HAETAE reference 코드 및 ML-DSA reference 코드의 실제 C 라이브러리를 사용하였다. 시뮬레이션 시나리오는 2km 길이의 3차선 고속도로를 가정하였고, 총 1,000회 실험을 수행하였다. 차량 수는 실험 조건에 따라 다르게 설정하였다.

E2E 지연 시간은 서명 생성 시간, MAC 계층 지연 시간, 패킷 분할(fragmentation) 시간, 전파(propagation) 시간, 검증 시간으로 구성된다. 특히 MAC 계층 지연 시간은 패킷 분할 시 각 fragment마다 별도의 채널 접근이 필요하므로 크게 증가한다.

표 2. E2E 지연 시간 구성 요소 분석(차량 50대 기준, 단위 : ms)

E2E 구성요소\알고리즘	HAETAE-120	ML-DSA-44
Sign 시간	0.636	0.462
MAC 계층 지연 시간	5.882	14.386
전파 시간	0.001	0.001
패킷 분할 시간	0.000	0.014
검증 시간	0.177	0.271
Total E2E	**6.697**	**15.134**
분할	NO	YES(2개)

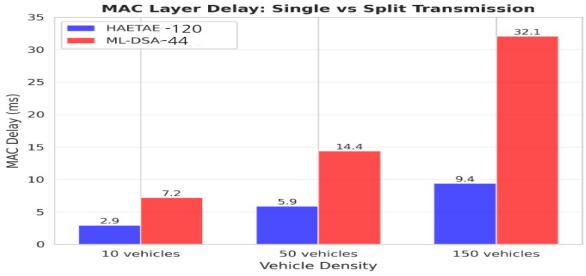

그림 2 MAC 계층 지연 비교

두 알고리즘 모두 V2X 요구사항인 100ms 이하의 E2E 지연을 충족하였다. 그러나 표 2에서 확인할 수 있듯이 MAC 계층 지연이 전체 E2E 지연에서 지배적인 비중을 차지하며, ML-DSA-44는 2개 패킷 분할로 인해 MAC 계층 지연이 HAETAE-120 대비 2.4배 증가하였다. 그림 2에서 보이는 바와 같이 ML-DSA-44의 서명 크기(2,420 bytes)는 DSRC/WAVE 환경의 최대 BSM 패킷 크기(2,000 bytes)를 초과하므로 2개 패킷으로 분할 전송이 필요하며, 이로 인해 HAETAE-120보다 지연 시간이 더 길다.

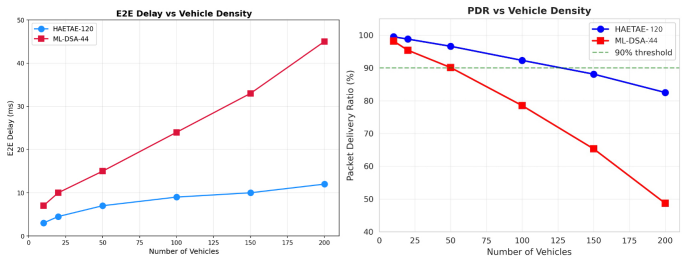

그림 3 차량 밀도 증가에 따른 성능 변화

그림 3에서 확인할 수 있듯이 차량 밀도가 증가할수록 HAETAE-120이 ML-DSA-44보다 우수한 성능을 보인다. ML-DSA-44는 패킷 분할로 인해 HAETAE-120 대비 MAC 계층 지연이 최소 2.4배 더 크다. 아울러 HAETAE-120은 PDR(Packet Delivery Ratio) 측면에서도 높은 신뢰성을 유지한다.

Ⅲ. 결론

본 연구에서는 V2V 환경에서 양자내성 전자서명 알고리즘인 HAETAE-120과 ML-DSA-44의 E2E 성능을 SUMO/OMNeT++ 기반 시뮬레이션을 통해 비교 분석하였다.

실험 결과, HAETAE-120은 ML-DSA-44 대비 약 56% 낮은 6.697ms의 E2E 지연 시간을 달성하였다. 이는 HAETAE-120의 서명 크기(1,474B)가 WAVE 최대 BSM 패킷 크기(2,000B) 이내여서 단일 프레임 전송이 가능하지만, ML-DSA-44는 서명 크기(2,420B)가 이를 초과하여 2개 패킷 분할이 필요하기 때문이다. 특히 MAC 계층 지연이 E2E 지연의 지배적 요소로 작용하였으며, ML-DSA-44는 패킷 분할로 인해 HAETAE-120 대비 2.4배 높은 MAC 지연을 보였다. 차량 밀도 증가에 따른 성능 분석에서도 HAETAE-120이 ML-DSA-44보다 우수한 확장성을 나타냈으며, PDR(Packet Delivery Ratio) 측면에서도 높은 신뢰성을 유지하였다. 두 알고리즘 모두 V2X 요구사항인 100ms 이하의 E2E 지연을 충족하였으나, 고밀도 환경에서의 안정성 측면에서는 HAETAE-120이 V2X 적용에 더 적합함을 확인하였다. 본 연구 결과는 국내 V2X 시스템의 양자내성암호 전환 시 HAETAE 도입의 기술적 타당성을 뒷받침하며, 향후 국내 자율주행 보안 표준 수립에 중요한 기반 자료로 활용될 것으로 기대된다.

ACKNOWLEDGMENT

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2024-00442085, 자율주행 차량 서비스 보호를 위한 V2X 무선통신 인프라 보안 핵심기술 개발).

참 고 문 헌

[1] Y. Seo et al. “Post-Quantum Cryptography Migration on V2X Certificate Using KpqC Algorithms,” ICUFN 2025, 2025

[2] NIST, “Module-Lattice-Based Digital Signature Standard,” FIPS204, 2024

[3] J. H. Cheon, et al., “HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures,” Cryptology ePrint Archive, Paper 2023/624, 2023.

[4] SAE International, "SAE J2945/1: On-Board System Requirements for V2V Safety Communications," 2020.

[5] IEEE, "IEEE 1609.2: Standard for Wireless Access in Vehicular Environments—Security Services," 2022.

[6] Y. Li, “An overview of the DSRC/WAVE technology,” In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, 2010.