MTU 제약 환경에서 Post-Quantum EDHOC 성능 분석

남재호°, 박홍근, 권태경

서울대학교 컴퓨터공학부

njh215@snu.ac.kr, tonypark7277@snu.ac.kr, tkkwon@snu.ac.kr

Performance Analysis of Post-Quantum EDHOC under MTU-Constrained Environment

Jaeho Nam°, Honggeun Park, Taekyoung "Ted" Kwon

Dept. of Computer Science and Engineering, Seoul National University

요 약

본 논문은 EDHOC 프로토콜을 post-quantum 환경에서도 안전하게 사용하기 위해 최근 연구에서 제안된 variants 의 메시지 크기를 분석하고, 네트워크 환경에 따른 지연 시간을 실험적으로 비교하였다. 분석 결과, 메시지 개수뿐 아니라 메시지 크기로 인한 단편화와 링크/전송 계층의 특성이 지연 시간에 중대한 영향을 미침을 확인하였다. 특히 낮은 MTU 환경에서는 지연이 급격히 증가하여 실질적 적용에 한계가 나타났으며, 추가적인 개선이 필요함을 보였다.

1. 서 론

Ephemeral Diffie-Hellman Over COSE(EDHOC) [1]는 경량화된 인증을 기반으로 하는 DH 키 교환 프로토콜로, IoT 와 같은 자원 제약 환경에서의 안전한 통신 수립을 목표로 한다. EDHOC 는 forward secrecy 등의 보안 속성을 제공하며, 암호 연산에 COSE, 데이터 직렬화에 CBOR 을 사용함으로써 코드 크기와 연산 오버헤드를 최소화한다. EDHOC 는 CoAP 에서 OSCORE 컨텍스트를 구축하는 데 주로 활용된다.

기존 EDHOC 에서 정의된 cipher suites 는 타원곡선 기반 공개키 암호 기법에 의존하고 있다. 이러한 구조는 계산 효율성과 경량성 측면에서 IoT 환경에 적합하지만, 충분히 강력한 양자 컴퓨터가 실현될 경우 Shor 알고리즘에 의해 보안성이 근본적으로 약화될 가능성이 존재한다. 이에 대응하기 위해, EDHOC 프로토콜에 양자 내성 암호(post-quantum cryptography, PQC) 기반 KEM 및 전자서명 알고리즘을 통합하려는 확장 연구들이 진행 중이다.

최근 Fraile 등은 EDHOC 의 양자 내성 전환을 다룬 연구에서 기존 타원곡선 기반 구조를 대체하기 위한 프로토콜 설계를 제시하였다. 첫 번째 연구에서는 EDHOC 에 PQC KEM 및 전자서명 알고리즘을 통합한 구조를 설계하고, Cortex-M4 와 같은 자원 제약 환경에서의 실행 시간, 메모리 사용량, 메시지 크기 증가 등을 정량적으로 평가하였다. [2] 후속 연구에서는 한 단계 더 나아가 static DH 및 서명 기반 인증 방식을 KEM 기반 인증으로 대체하는 새로운 EDHOC 확장 방안을 제안하였다. [3] KEMTLS 등의 기존 KEM 기반 AKE 연구를 참고하여 KEM 기반 5-message EDHOC 및 3-message EDHOC-IKR 변형을 설계하였다. 해당 연구는 KEM 을 활용한 signature-free 구조가 메모리 사용량과 연산 비용 측면에서 IoT 환경에 더욱 적합함을 실험적으로 입증하였다.

그러나 앞선 연구에서는 네트워크 환경의 변화가 EDHOC 성능에 미치는 영향에 대한 분석은 수행되지 않았다. IoT 환경에서는 사용되는 링크 계층 프로토콜에 따라 MTU 가 크게 달라질 수 있으며 저전력 무선 환경에서는 수십~수백 바이트 수준으로 제한되는 경우도 빈번하다. 그러나 PQC KEM 및 전자서명 알고리즘은 기존 타원곡선 기반 기법에 비해 public key, ciphertext, signature 의 크기가 크며 최소 보안 수준의 파라미터를 사용하더라도 수백~수천 바이트에 이르는 경우가 많다. 따라서 제약이 심한 네트워크에서 EDHOC 의 적용 가능성을 평가하기 위해서는 다양한 MTU 조건 하에서의 성능 분석이 추가적으로 요구되는 상황이다.

2. (PQ-)EDHOC 프로토콜 메시지 크기 분석

EDHOC 에서는 다양한 cipher suite 와 method 를 선택할 수 있으며, 이에 따라 각 메시지 크기가 달라진다. 특히 post-quantum EDHOC 는 표준화가 아직 진행 중이다. 본 논문에서는 네트워크 환경에 따른 성능 변화를 분석하는 것이 목적이므로, 보안 수준이 낮더라도 메시지 크기를 최소화하는 옵션들을 선택한 경우를 비교 기준으로 삼았다. 또한, post-quantum EDHOC 의 경우 다양한 설계가 존재하지만 KEM-

based 방식이 개별 메시지 크기를 상대적으로 작게 유지할 수 있어 분석 대상으로 선정하였다.
타원곡선 기반 공개키 암호 기법을 사용하는 EDHOC 의 경우, RFC 표준 문서에 대표적인 메시지 크기 예시 목록이 제시되어 있다. 그 중 Initiator 와 Responder 가 모두 static DH 를 사용하는 설정이 메시지 크기가 가장 작으며, message 1~3 은 37, 45, 19 bytes 를 가진다. 이러한 크기 특성으로 인해 수십~수백 MTU 환경에서도 각 EDHOC 메시지가 단일 프레임으로 전송 가능하다는 이점이 있다.
반면, KEM-based EDHOC 의 경우에는 메시지 크기가 상대적으로 크게 증가한다. 계산 결과 Table 1 에서 확인할 수 있듯이 message 1~5 의 크기가 각각 806, 773, 790, 806, 35 bytes 로 크게 증가하는 것을 확인하였다. 이러한 차이는 MTU 와 네트워크 환경에 따라 키 교환 완료까지 걸리는 시간과 전송 효율에 상당한 영향을 미칠 수 있다. 또한, Initiator 가 Responder 의 credential 을 미리 알고 있는 IKR 상황의 경우에도 round trip 횟수는 기존 EDHOC 와 동일하게 맞출 수 있지만 message 1~2 의 사이즈가 1,500 bytes 이상으로 크게 증가한다는 문제를 확인하였다.

Message	Payload Size (bytes)		
	EDHOC (RFC 9528)	KEM-based EDHOC	KEM-based EDHOC-IKR
1 (I→R)	37	806	1595
2 (R→I)	45	773	1579
3 (I→R)	19	790	35
4 (R→I)	N/A	806	N/A
5 (I→R)	N/A	35	N/A

Table 1. EDHOC variants 에 따른 메시지 크기 예시 비교. EAD 는 사용하지 않는 것으로 가정하였으며 C_I, C_R, ID_CRED_I, IC_CRED_R 은 모두 1 byte 로 지정하였다. KEM-based EDHOC 에서는 ML-KEM 512 를 사용하였고 (public key - 800 bytes, ciphertext - 768 bytes), ML-KEM 512 가 속한 cipher suite 정의에 따라 16 bytes MAC 을 사용하였다.

3. (PQ-)EDHOC 지연 시간 비교 실험

본 실험에서는 Initiator, Responder 가 네트워크를 통해 통신하는 경우를 대표하는 EDHOC over CoAP 상황을 가정한 뒤 MTU 변화에 따라 키 교환 완료 시간에 소요되는 시간을 측정하였다. 실험 환경은 Docker container 기반으로 구성하였으며, netem 을 통해 임의의 delay 를 주입하였다. 네트워크 환경 변화가 round trip 횟수 및 지연 시간에 미치는 영향을 독립적으로 관찰하기 위해 EDHOC 관련 로직 실행 시간은 실험 결과에서 제외하였다.
CoAP over UDP 의 경우 신뢰성 및 순서 보장을 위해 CON/ACK 방식을 사용하였다. 실험 결과 MTU 가 감소할수록 메시지 단편화로 인해 필요한 round trip 횟수가 증가하였으며, 이에 따라 키 교환 완료 시간이 급격히 증가하였다. 특히 KEM-based EDHOC-IKR 은 필요 메시지 수가 3 개로 기존 EDHOC 와 동일한 구조이지만, 낮은 MTU 환경에서는 단편화로 인해 이러한 이점이 상쇄된다는 점을 확인하였다.

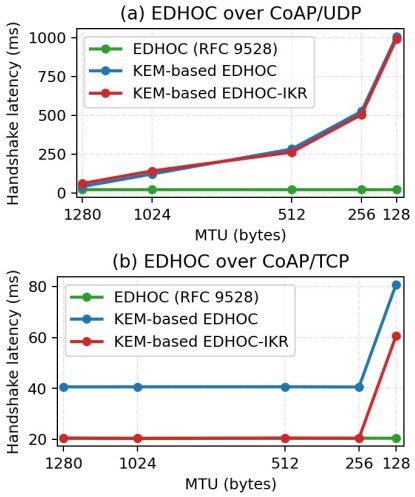

Figure 1. EDHOC variants 에 따른 키 교환 완료 시간 비교. Initiator 와 Responder 사이의 RTT 는 20ms 로 설정하였고, (a)는 CoAP over UDP, (b)는 CoAP over TCP 를 사용하였다.

CoAP over UDP 는 CoAP 의 기본 동작 방식이지만, 본 사례와 같이 단편화가 다수 발생하는 환경에서 packet loss 가 발생하는 경우 사용이 어렵다. 이에 따라 CoAP over TCP 환경을 추가적인 실험 대상으로 선정하였다. CoAP over TCP 환경에서는 필요 메시지 수가 많은 KEM-based EDHOC 가 상대적으로 불리한 특성을 보였다. 그러나 MTU 가 작아질 경우, KEM-based 방식 모두에서 message 1, 2 전체가 초기 TCP window 내에 포함되지 못하는 상황이 발생하였으며, 그 결과 키 교환 완료 시간이 2 RTT 증가하였다.

4. 결 론

본 논문에서는 EDHOC variants 의 MTU 변화에 따른 지연 시간을 분석하였고, 메시지 개수뿐 아니라 링크/전송 계층의 특성 및 메시지 크기에 따른 단편화가 지연 시간에 중대한 영향을 미침을 확인하였다.

5. Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음 (IITP-2026-2021-0-02048).

6. 참고 문헌

[1] G. Selander, J. P. Mattsson, and F. Palombini, “Ephemeral Diffie-Hellman Over COSE (EDHOC),” IETF, RFC 9528, Mar. 2024.
[2] L. P. Fraile et al., “Enabling Quantum-Resistant EDHOC: Design and Performance Evaluation,” IEEE Access, vol. 13, pp. 75861–75884, 2025.
[3] L. P. Fraile, C. Koulamas, and A. P. Fournaris, “Reinventing EDHOC for the Post-Quantum Era,” IEEE Access, vol. 13, pp. 196622–196640, 2025.