V2X 통신을 위한 ECDSA 서명 검증 병렬처리 연구

이석준, 최중용, 정병호, 권혁찬
한국전자통신연구원 정보보호연구본부
e-mail : {junny, choijy725, cbh, hckwon}@etri.re.kr

Study on Parallel Processing of ECDSA Verification for V2X Communication

Sokjoon Lee, Joongyong Choi, Byungho Chung, Hyeokchan Kwon
Information Security Research Division, Electronics and Telecommunications Research Institute

요 약

IEEE 1609.2 표준은 WAVE (Wireless Access in Vehicular Environment) 표준에서 차량간(V2V, Vehicle-to-Vehicle) 혹은 차량과 인프라간(V2I, Vehicle-to-Infrastructure) 통신 상의 응용 메시지 보호를 위해 제정되었다. 이 표준은 메시지 인증 및 무결성 검증을 위하여 NIST p256 타원 곡선 커브 기반의 ECDSA 전자 서명 기법을 사용한다. 매우 복잡한 도심 상의 출퇴근 환경에서는 수백대의 자동차가 전송하는 메시지를 정상적으로 처리하기 위하여, 차량의 OBU(On-Board Unit) 혹은 노상의 RSU(Road-Side Unit)에서 서명된 메시지의 검증 성능이 매우 중요한 이슈가 될 수 있다. 본 논문에서는 V2X 통신에서 효율적인 ECDSA 서명 검증을 위하여, OBU 혹은 RSU 환경에서 CPU 상의 병렬처리 성능을 테스트한 후 시사점을 살펴본다.

1. 서론

IEEE 1609.2 표준[1]은 차량간 통신 혹은 차량과 인프라간 통신에서 응용 메시지 신뢰성을 보호하기 위하여 제정되었다. 이 표준은 메시지 인증 및 무결성 검증을 위하여 NIST p256 타원 곡선 커브 기반의 ECDSA 전자 서명 기법을 이용한다.

매우 복잡한 도심 상의 출퇴근 환경에서 OBU 혹은 노상의 RSU 는 초당 1000 개 이상의 메시지를 처리해야 한다. 속도 개선을 위하여, ECDSA 서명에 대한 소프트웨어 구현 최적화 혹은 하드웨어 전용 칩을 사용하는 것이 가능하다. 그러나 하드웨어 전용 칩을 사용할 경우, 기존에 널리 사용되던 보드를 활용할 수 없고 새로운 보드를 설계해야 하는 문제점이 있으며, 또한 기존 커브 자체 혹은 구현된 하드웨어에 취약점이 발견될 경우 업데이트가 어려운 단점이 있다.

본 논문에서는 V2X 통신상의 서명 검증 요구사항 및 CPU 기반 병렬처리 기술에 대해서 살펴보고, 실제 환경에서 이를 시험한 후 시사점을 살펴본다.

2. 배경

2.1 V2X 통신상의 서명 검증 성능 요구 사항

기본 안전 메시지(BSM, Basic Safety Message)는 SAE J2735[2]에서 정의되어 있는 메시지로 전송 비율이 정해져 있지는 않으나 일반적으로 초당 10 개의 메시지를 보내는 것으로 가정한다. 만약 주변에 100 대의 차량이 있다면, Knezevic 등[3]이 제안한 바와 같이 초당 1000 개의 서명을 검증할 수 있어야 한다. 이들은 무선 채널 용량을 6Mbps 로 가정하였으나, 실제로는 27Mbps 까지 가능하므로 보다 더 높은 요구사항을 필요 할 수 있다. 참고로, Autotalks 의 V2X 통신용 칩셋인 CRATON[4]은 하드웨어 엔진을 활용하여 초당 2000 개 이상 서명을 검증할 수 있다고 알려져 있다.

복잡한 도심 환경(예, 통행이 많은 왕복 8 차선의 4 방향 교차로) 및 WAVE 전파 도달 거리(최대 300m 수준), 차량의 평균 간격 (본 논문에서는 30m 로 가정)을 고려하면, 차량들이 평균 30m 간격으로 줄지어 진행하는 왕복 8 차선 교차로의 중심에서는 300m 반경 이내에 320 대의 차량이 있으므로 3200 개의 BSM 을 처리해야 하며, 만약 각 차량이 10 개의 BSM 당 1 번꼴로 차량인증서를 같이 전달한다면 3500 개 수준의 ECDSA 서명을 검증할 수 있어야 한다는 성능 요구사항을 도출 할 수 있다.

2.2 CPU 기반 병렬처리 기술

최신 ARM/Intel CPU 기반 CPU 는 일반적으로 다중 코어를 장착하고 있으며, 각 코어는 독립적으로 작동하고 병렬로 데이터를 처리한다. CPU 의 성능을 최대한 활용하는데 활용할 수 있는 병렬 처리 라이브러리로는 OpenMP 와 pthread 가 존재한다. 이들을 활용할 경우, 예를 들어 물리적 코어가 4 개 있다면 싱글 코어 대비 최대 4 배까지 성능 향상이 가능하다.

3. ECDSA 서명 검증 병렬처리 시험

3.1 시험 환경

V2X 통신 환경에서 널리 사용되는 NXP i.MX6 계열의 쿼드코어 버전은 4 개의 ARM Cortex-A9 코어가 장착된 프로세서이다. 이 칩셋이 포함된 UDOO 보드[5]를 첫번째 시험 플랫폼으로 선정하였고, 비교를 위해, 이보다 성능이 좋은 삼성 Exynos5422 칩셋이 장착된 ODROID-XU4 보드[6]에서 같이 시험을 하였다. Exynos5422 칩셋은 8 코어 칩셋으로 4 개의 2.1GHz Core 와 4 개의 1.4GHz Core 를 포함하고 있다. 각 보드의 제원은 <표 1>과 같다.

<표 1> 시험 보드 제원

	Udoo Quad board	ODROID-XU4 board
CPU	NXP i.MX6Q (ARM Cortex-A9 Quad-core 1GHz)	Samsung Exynos5422 (Cortex-A15/A7 8 Core 2.1GHz/1.4GHz)
Memory	1G LPDDR3 RAM	2G LPDDR3 RAM
OS	Ubuntu 14.04 LTS	Ubuntu 14.04 LTS

3.2 시험 결과

ECDSA 서명 검증을 위하여 OpenSSL 1.1.0 1.1.0h 라이브러리에 포함된 NIST p256 커브 기반 ECDSA 서명 API 를 사용하였다. 각 보드에서의 시험은 총 10 만개의 서명을 검증하여 평균을 계산하였다. <표 2>와 <표 3>의 마지막 행은 각각 최대의 코어를 활용하도록 OpenMP 를 사용한 결과이며, 다른 행은 pthread 라이브러리를 사용하여 성능 시험을 한 결과이다.

<표 2> Udoo Quad 보드 시험 결과

Thread 수	개당검증시간 (us)	초당서명검증수	단일쓰레드 대비 성능비율
1	1613.67	619.70	100.00%
2	810.68	1233.53	199.05%
4	417.24	2395.69	386.75%
8	413.68	2417.32	390.08%
16	409.89	2439.69	393.69%
OpenMP	419.62	2383.09	384.55%

<표 3> ODROID-XU4 보드 시험 결과

Thread 수	개당검증시간 (us)	초당서명검증수	단일쓰레드 대비 성능비율
1	490.71	2037.88	100.00%
2	253.69	3941.79	193.43%
4	158.76	6298.71	309.08%
8	108.90	9183.12	450.62%
16	108.58	9209.63	451.92%
OpenMP	169.37	5904.24	289.72%

3.3 시사점

Udoo Quad 보드 시험에 따르면, 별도 하드웨어의 도움이 없더라도, i.MX6 Quad 버전에서 최대 초당 2400 개 안팎의 서명 검증이 가능(쓰레드 4 개 이상 혹은 OpenMP 사용시)하므로, Autotalks 의 CRATON 에서 주장하는 초당 2000 개의 성능을 기본적으로 만족할 수 있음을 확인할 수 있었다. 2 개의 쓰레드에서 초당 1233.53 개의 검증이 가능했으므로, Dual core 를 장착한 버전에서도 최대 초당 1000 개 안팎의 성능이 나올 것으로 예상할 수 있다.

ODROID-XU4 보드 시험에서는 코어 수인 8 개까지 쓰레드를 돌릴 때 최대 성능치에 근접하는 성능(초당 9183.12 개)을 확인할 수 있다. 그러나, OpenMP 를 사용한 성능은 초당 5904.24 개로, 4 개 쓰레드를 병렬로 돌리는 경우보다도 부족한 성능을 보이고 있다. 이는 고성능의 코어에서 서명 검증을 완료한 후, 저성능의 코어에서 서명 검증을 완료할 때까지 대기하여 생기는 현상으로 추측할 수 있다. 따라서, 성능이 다른 코어를 가진 멀티코어 CPU 환경에서 OpenMP 를 통한 병렬처리 구현시 신중하게 접근해야 함을 알 수 있다.

4. 결론

i.MX6 Quad CPU 는 CPU 의 성능을 최대한 활용하여도 초당 2400 개 정도의 서명 검증이 가능하며, 이는 2.1 절에서 요구하는 성능 요구사항을 만족하지 못한다. 다만, 소프트웨어 구현만으로 Autotalks 의 CRATON 과는 유사한 성능을 보인다는 점을 확인할 수 있었으며, 2.1 의 성능요구사항보다 더 낮은 성능을 요구하는 환경에 고려할 수 있을 것이다.

Exynos5422 CPU 수준이면 전체 CPU 성능을 최대로 활용시, V2X 환경에서 요구하는 성능을 충족할 수 있음을 확인할 수 있었다. 다만, V2X OBU/RSU 에서는 서명 검증 외에도 통신, 메시지 처리 및 다른 응용 서비스에서 리소스를 활용하게 되므로, 서명 검증을 위하여 CPU 의 성능을 몇 %까지 활용할 수 있는지에 대한 연구가 필요하다. 이 경우, 3.2 절의 성능 수치보다 낮은 성능을 보일 수 밖에 없으므로, 보다 고성능의 CPU 를 활용해야 하거나 혹은 보조적인 하드웨어(GPU 등)의 도움이 필요할 수 있으며, 이에 대한 추가적인 연구가 진행되어야 할 것이다.

Acknowledgement

이 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.B0717-16-0097, 자율주행차량을 위한 V2X 서비스 통합 보안 기술 개발)

참고문헌

[1] IEEE Std 1609.2™-2016: IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. IEEE Vehicular Technology Society, 2016

[2] DSRC Committee, “Dedicated Short Range Communications (DSRC) message set dictionary”, SAE Standard, vol. J2735, 2016

[3] M. Knezevic, V. Nikov, and P. Rombouts, “Low-latency ECDSA signature verification road toward safer traffic”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 11, pp. 3257-3267, 2016

[4] Autotalks, “V2X Security Portfolio”, https://www.autotalks.com/wp-content/uploads/2014/09/Autotalks_White_Paper_V2X_Security_Portfolio_V1.3_COMPANY.pdf

[5] Udoo Quad/Dual, https://www.udoo.org/udoo-dual-and-quad/

[6] Hardkernel ODROID-XU4, http://www.hardkernel.com/main/products/prdt_info.php?g_code=G143452239825