자원 제약적인 사물인터넷 장비를 위한 타원곡선 암호와 하드웨어 가속 기반의 보안 방안

최준혁, 손동현 권태경*
서울대학교

{jhchoi2015, dhson}@mmlab.snu.ac.kr, *tkkwon@snu.ac.kr

Elliptic curve cryptography and hardware acceleration based security for resource constrained IoT devices

Junhyeok Choi, Donghyun Son, Ted " Taekyoung" Kwon
School of Computer Science and Engineering, Seoul National University

요 약

최근 급격히 성장하고 있는 사물인터넷은 우리 주변에 만연한 사물을 인터넷으로 연결하려는 새로운 패러다임 중 하나로, 다양한 사물을 인터넷에 연결함으로써 기존에 비해 넓어질 커넥티비티(Connectivity)에 대한 기대로 인해 큰 주목을 받고 있다. 이러한 사물인터넷의 등장에 따라 사물인터넷 종단 간의 인증, 인가 및 보안 통신의 중요성 역시 부각되지만, 기존의 보안 체계는 비교적 고성능의 종단을 위하여 설계되었기 때문에 사물인터넷으로 연결되는 메모리, 연산 능력 등의 자원이 제약되는 장비에는 적합하지 않다. 따라서 본 논문에서는 타원곡선 암호화 기법과 하드웨어 가속 기법을 이용하여 기존의 보안 체계와 비슷한 보안 수준을 유지하면서 메모리 및 연산 비용을 줄일 수 있는 방안에 대해 보여주고자 한다.

1. 서론

현재 우리는 모든 사물이 네트워크를 통해 인간과 연결되는 초연결(hyper-connectivity)시대로 진입하는 길목에 있다. 2000 년대 이후 모든 사물이 네트워크에 연결된다는 유비쿼터스 네트워크에 대한 논의가 진행되어 왔다. 스마트폰 이후의 센서의 대중화, 통신모듈 가격 하락 등에 의해 기술적, 경제적 한계를 극복하면서 사물인터넷(Internet of Things)의 기술이 앞으로 더 적극적으로 활용될 전망이다[1].

사물인터넷을 통해 우리 주변의 사물들이 인터넷으로 연결되면서 통신의 주체가 되는 각 종단(End point) 간의 인증(Authentication) 및 인가(Authorization), 그리고 보안 채널을 통한 암호화된(Encrypted) 데이터 송·수신 등의 보안 관련 이슈 역시 중요한 쟁점으로 부각되고 있다. 사물인터넷의 특성상, 인터넷으로 연결되는 객체로는 센서 노드 등의 저사양 장비 역시 포함될 수 있으나 이런 자원 제약적인 사물인터넷 장비의 경우 메모리 및 연산 능력 등의 자원 부족으로 인하여 보안 통신을 위해 요구되는 암호화 키(key)나 암호화 연산이 기존의 장비에 비해 큰 부담으로 다가올 수 있다.

본 논문에서는 이러한 자원 제약적인 장비에 대한 보안 연산을 효율적으로 수행하기 위하여 두 가지 방법으로 접근한다. 먼저 i)공개 키 암호화 방식을 통한 상호 인증 과정에서 기존에 널리 사용되고 있는 RSA(Rivest, Sharmir, Adelman) 암호를 대신하여 타원곡선 암호(Elliptic curve cryptography, 이하 ECC)를 도입하여, 보다 짧은 길이의 키를 사용하여 컴퓨팅 자원에 대한 요구량을 감소하는 방안을 제시한다. 그리고 ii)암호화 연산을 소프트웨어적인 방법이 아닌 전용 하드웨어 가속 모듈의 도움을 통해 수행하여 연산 수행에 소요되는 시간을 줄일 수 있도록 한다.

2. 관련연구

2.1. 타원곡선 암호

타원곡선 암호는 유한체(finite field) 상의 타원곡선이 가지는 대수학적 구조에 기반하여 설계된 공개 키 암호화 방식이며, 1985 년에 워싱턴 대학의 수학 교수 닐 코블리츠(Neal Koblitz)와 IBM 연구소의 빅터 밀러(Victor Miller)가 각각 독립적으로 제안했다. 여기에서 말하는 타원곡선이란 일반적으로 y2 = x3 + ax + b 를 만족하는 점들의 집합이다.

RSA 암호가 큰 숫자를 소인수분해 하는 것이 어렵다는 것에 기반을 두고 있다면, 타원곡선 암호는 알려진 특정한 점에 대한 무작위 타원 곡선의 이산 로그를 찾는 것이 어렵다는 사실에 기반을 두고 있다. 여기에서 어렵다는 것은 이론상 계산이 가능하지만, 이를 실제로 계산하는 데에 오랜 시간이 걸린다는 것을 의미한다.

반면, 타원 곡선 암호의 장점은 RSA 방식에 비하여 짧은 키를 가지고도 그와 비슷한 보안 수준을 확보할 수 있다는 것이다. 아래의 표에 따르면 전문가들이 권장하는 AES-256 세션 키 관리를 위하여 RSA 를 이용한다면, 15360 비트의 키를 사용해야 하며, 이는 자원 제약적인 장비에서는 적합하지 않다. 그에 비해 ECC 암호의 경우 512 비트의 키를 사용하므로 자원 제약적인 환경에서도 이용할 수 있다[2].

Security Bits	Symmetric Encryption Algorithm	Minimum Size (bits) of Pulbic Keys	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

Table 1. RSA 와 ECC 의 키 길이 비교

2.2. 하드웨어 가속

계산량이 많아 오랜 시간이 소요되는 연산의 경우 소프트웨어적인 방법을 통해 수행하는 것보다 전용 하드웨어 모듈의 힘을 빌리는 것이 효율적일 수 있다. 전용 하드웨어로 수행하는 연산의 경우, 프로세서를 통한 연산의 순차적으로 실행되는 과정을 동시적으로 처리할 수 있기 때문에 빠른 연산속도를 기대할 수 있다.

3. 실험 설계 및 결과

3.1. 실험 환경

실험은 Texas Instrument 의 CC2538 개발 키트를 이용하여 수행하였다[3]. CC2538 모듈은 본래 ZigBee 통신을 위한 SoC(System on Chip)이며 최대 32MHz 클락 속도를 가지고, 32KB 의 메모리(RAM)를 가지고 있기 때문에, 자원 제약적인 사물인터넷 장비로 간주할 수 있다. 더불어 AES 및 RSA, ECC 연산에 대한 하드웨어 가속을 지원하기 때문에 본 실험에 적합하다.

CC2538 장비에는 내장형 운영체제인 Contiki-OS 2.7 을 올려서 구동하였으며[4], 실험을 위한 암호화 및 복호화 연산은 relic-toolkit 이라는 경량화 암호학 라이브러리를 이용하였다[5]. 하드웨어 가속 실험은 해당 라이브러리가 지원하는 ECC 연산을 CC2538 의 하드웨어 가속 모듈을 통한 연산으로 대체하여 수행하였다.

실험은 고정된 100 byte 의 문자열에 대하여 ECC 암호화 및 복호화 연산을 수행한 후, 각각의 과정에 소요된 시간을 측정하는 것이다. 타원 곡선은 160 bit 의 키 길이를 가지는 brainpoolP160r1 를 사용하였다[6]. 위 암호화 및 복호화 과정을 relic-toolkit 의 기본 ECC 연산을 사용하여 수행한 결과와 하드웨어 가속 모듈을 사용하여 수행한 결과를 각각 측정하여 비교하였다.

3.2. 실험 결과

그림 1 은 하드웨어 가속을 사용한 경우와 사용하지 않은 경우의 ECC 암호화 및 복호화에 소요된 시간을 비교한 것이다. 기존의 암호화 연산은 수행하는 데에 약 108 초가 소요되었으나, 하드웨어 가속을 통해 574ms 로 단축할 수 있었으며, 약 190 배의 차이를 보였다. 복호화 연산의 경우 기존의 93 초에서 가속을 통하여 187ms 로 단축할 수 있었으며, 약 500 배의 차이를 보였다. 전체 수행 시간을 비교해 보아도, 200 초 이상이 소요되던 작업을 1 초도 걸리지 않고 수행할 수 있기 때문에 상당히 의미 있는 정도의 성능 향상을 거두었다고 볼 수 있다. 암호화와 복호화 연산의 성능 증가폭이 다른 이유는 암호화 과정에 가속을 할 수 없는 부분이 더 많이 포함되어 있기 때문으로 보인다.

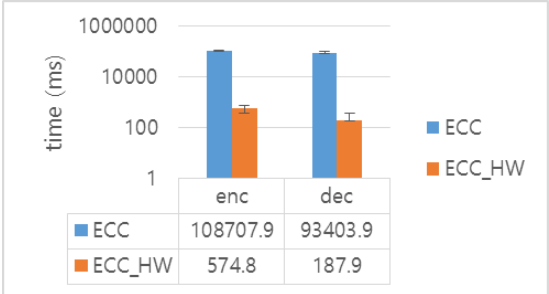

그림 1. 암호화 및 복호화 소요 시간

4. 결론 및 향후 연구

본 논문에서는 자원 제약적인 장비에 적합한 새로운 보안 방안을 제시하였다. 이는 두 가지 방법을 통해 이루어지는데, 타원곡선 암호를 통해 비교적 짧은 키를 이용하면서도 기존과 같은 수준의 보안을 유지할 수 있으며, 하드웨어 모듈을 통해 암호화 연산을 가속하여 부족한 연산 능력을 보완하였다. 우리는 실험을 통해 하드웨어 가속을 사용하는 경우, 연산 수행 시간이 눈에 띄게 줄어드는 것을 확인할 수 있었다.

본 연구의 실험에서는 하드웨어 가속을 사용했을 때의 암호화 및 복호화 과정의 성능 변화만을 측정하였다. 하지만 실제 TLS/DTLS 등의 보안 프로토콜의 동작 과정에는 통신 오버헤드 및 보안 인자 관리 등의 작업이 더해진다. 이러한 일련의 과정에서 병목 요소를 분석하고, 하드웨어 가속을 통해 실제로 어느 정도의 성능 향상이 가능할지에 대한 연구가 필요할 것이다.

ACKNOWLEDGMENT

이 논문은 2015 년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2015R1A5A7037372).

참 고 문 헌

[1] 석왕헌, 송영근, 고순주, "통신환경 변화에 따른 M2M 산업 생태계 및 파급효과 분석," IT 이슈리포트 2013-7, ETRI, 2013.06.

[2] Kerry Maletsky, "RSA vs ECC Comparison for Embedded Systems White Paper," 2015, Atmel.

[3] CC2538 Development Kit. http://www.ti.com/tool/cc2538dk

[4] Contiki-OS, http://www.contiki-os.org

[5] relic-toolkit. https://github.com/relic-toolkit

[6] M. Lochter, J. Merkle. "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation," RFC 5639, Mar. 2010.