

2018

춘계학술발표대회

논문집

일시 2018년 4월 27일(금) ~ 28일(토)

장소 제주대학교 아라캠퍼스 아라컨벤션홀

주최 사단법인 한국인터넷정보학회

주관 제주대학교

후원 네이버(주), (주)아이티센, (주)LGCNS,
(주)큐브시스템, LG히다씨(주), (주)워드바이스에세이리뷰



D-1-3 전해수생성기의 스케일제거 알림	133
권윤중(세명대)	
D-1-4 Wi-Fi 및 RFID 후방 산란을 이용한 모바일 RFID 판독기 및 CRFID 센서 태그 프로토콜	135
백승구, 이태진(성균관대)	
D-1-5 Fog Cloud Network 기반 데이터 처리 시스템 설계	137
손수락, 이병관(가톨릭관동대), 정은희(강원대)	
D-1-6 자율차량을 위한 OBDL(Optimized Back-propagation based Deep Learning) 알고리즘 설계 ...	139
정이나, 이병관, 손수락, 김경덕(가톨릭관동대)	
D-1-7 시각 장애인을 위한 경량화 된 스마트 지팡이	141
정재엽, 정진웅, 염상길, 추현승(성균관대)	
 D-2. IoT 2 / 인터넷교육및응용 (좌장: 서영균 교수(경북대))	
D-2-1 스마트폰 통제 IoT 플랫폼	145
원경필, 정진웅, 염상길, 추현승(성균관대)	
D-2-2 스마트시티 인프라 구축현황 분석 및 사이버보안 고려사항 연구	147
송진우, 김효빈, 홍기섭, 서정택(순천향대)	
D-2-3 ZigBee 프로토콜 취약점 및 보안 요구사항 분석	149
조정석, 곽진(아주대)	
D-2-4 정신 질환 환자를 위한 쉬운 런치 패드	151
장종권, 안효훈, 염상길, 추현승(성균관대)	
D-2-5 SIMD 기반의 IoT 디바이스 인증 프로토콜 설계에 관한 연구	153
최슬기, 곽진(아주대)	
D-2-6 개방형 교육 플랫폼 기반 학습 프로세스 마이닝 및 애널리틱스 기술 연구	155
김현아, 김광훈(경기대)	

SIMD 기반의 IoT 디바이스 인증 프로토콜 설계에 관한 연구

최슬기*, 궤 진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *skchoi.isaa@gmail.com, **security@ajou.ac.kr

A Study on SIMD-based Authentication Protocol Design for IoT Device Authentication

Seul-Ki Choi*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

IoT 디바이스에 대한 인증은 안전한 IoT 서비스를 제공하는데 있어서 매우 중요한 과정이라고 할 수 있다. 이에 대하여 저전력·저성능의 IoT 디바이스에 적합한 인증 프로토콜에 대한 연구가 활발히 진행되고 있다. 따라서 본 논문에서는 경량화 및 고속화를 위하여 SIMD 기반의 IoT 디바이스 인증 프로토콜과 제안 프로토콜의 고속 병렬화 효과를 증대시킬 수 있는 알고리즘으로 LEA-128-CTR과 Chaskey 알고리즘을 선정하여 그 효과를 실험하였다.

1. 서 론

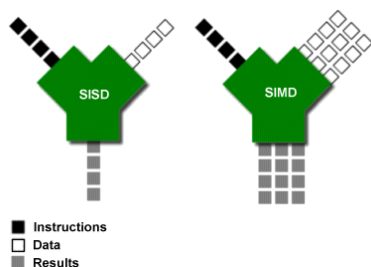
IoT 디바이스들을 활용한 IoT 서비스들을 통해 우리 사회는 더욱 편리해지고 있다. 하지만 이러한 IoT 디바이스들에 대하여 적절한 인증 절차가 이루어지지 않는다면 사회적인 큰 혼란을 야기할 수 있기 때문에 IoT 디바이스 인증에 대한 다양한 연구들이 진행되고 있다. 하지만 저전력과 저성능의 특징을 가진 IoT 디바이스들이 많기 때문에 이에 대하여 인증 절차에 대한 경량화와 고속화에 대한 연구가 필요하다.

따라서 본 논문에서는 경량화와 고속화를 위한 IoT 디바이스 인증 프로토콜을 제안한다.

2. 관련 연구

2.1 SIMD

SIMD는 Single Instruction Multiple Data의 약자로 하나의 명령어(Instruction)로 여러 개의 데이터를 동시에 처리하는 기법을 말한다.



(그림 1) SISD와 SIMD의 처리 구조

그래픽 관련 처리와 같이 멀티미디어 분야에 자주 사용된다. SIMD를 제공하는 CPU의 경우에는 Intel의 MMX, SSE 시리즈들과 ARM에서 개발한 NEON 등이 있다. SIMD는 일반적인 프로그램에서 주로 이용되는 SISD(Single Instruction Single Data) 방식보다 많은 양의 데이터를 처리할 때 처리 속도의 효율성을 향상시킬 수 있는 장점을 가지고 있다. 아래 그림 1은 SISD와 SIMD 처리 구조를 나타내고 있다.

2.2 Chaskey

Chaskey MAC(Message Authentication Code) 알고리즘은 32비트 마이크로 컨트롤러에서 사용 가능한 MAC 알고리즘으로 키 스케줄링을 제거함으로써 암호화 수행 시 걸리는 Cycle의 횟수를 줄여 경량화하였다. 또한 ARX(Addition, Rotation, XOR) 연산만으로 구성되어 수행 속도가 매우 빠른 장점을 가지고 있다[1].

따라서 32비트 마이크로 컨트롤러를 대상으로 구현한 32비트 프로세서 IoT 디바이스에 적용 가능한 알고리즘이다.

3. 제안 사항

3.1 적용 가능 대상 프로세서

본 논문에서 제안하는 SIMD 기반의 인증 프로토콜은 다양한 IoT 디바이스에 널리 보급 및 분포되어있는 ARM 프로세서를 적용 대상으로 삼고 있다.

그 중에서도 단순히 정보의 수집 기능만을 수행하는 IoT 센서들이 아닌 이러한 IoT 센서들로부터 정보를 수집하고 1차 가공하거나 스스로 처리할 수 있는 기능을 갖춘 IoT 디바이스들을 본 논문의 제안사항의 대상이다.

이러한 IoT 디바이스들은 ARM 프로세서들 중 Cortex A 이상의 프로세서들을 탑재하고 있는데 Cortex A 프로세서가 탑재되어 적용되고 있는 IoT 산업 분야별 디바이스의 예시는 아래 표 1과 같다[2].

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2015-0-00403)

(표 1) Cortex A 프로세서 활용 분야

산업 분야	디바이스 종류
스마트홈	홈게이트 웨이, 자동온도조절장치
의료	스마트워치
교통	자동차 센서, ECU(Electronic Control Unit)
에너지	RTU(Remote Terminal Unit)

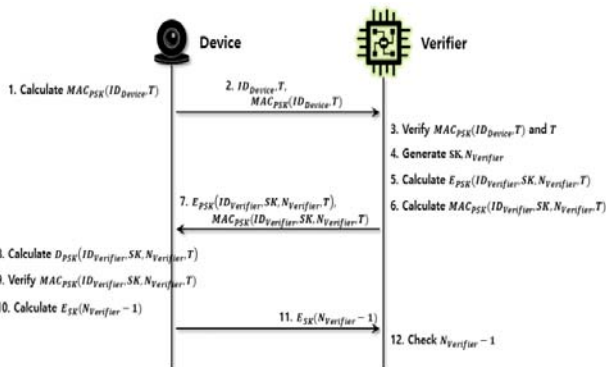
3.2 SIMD 기반의 인증 프로토콜

제안하는 프로토콜은 저전력 및 저성능의 IoT 디바이스를 고려하여 사전 비밀 키 분배 방식을 활용하였다. 프로토콜에서 사용하는 표기법에 대한 설명은 아래 표 2와 같다.

(표 2) Cortex A 프로세서 활용 분야

표기법	설 명
ID_x	x의 식별자 (ID)
T	타임스탬프
N_x	x가 생성한 난스 값
PSK	사전에 공유된 비밀키 (Pre-shared Key)
SK	세션 키 (Session Key)
$E_k(\dots)$	k로 암호화 (Encryption)
$D_k(\dots)$	k로 복호화 (Decryption)
$MAC_k(\dots)$	k로 메시지 인증 코드 생성
$Device$	IoT 디바이스
$Verifier$	검증자 (게이트웨이 혹은 사용자 디바이스)

아래 그림 2는 SIMD 기반의 인증 프로토콜의 전체적인 과정을 나타내고 있다.



(그림 2) SIMD 기반의 인증 프로토콜

본 논문에서 제안하는 프로토콜을 보다 고속화하기 위하여 ARM Cortex A에서 제공하는 SIMD 기술인 Neon을 적극적으로 활용할 수 있는 병렬 처리에 적합한 암호 알고리즘 및 MAC 알고리즘을 선정하였다.

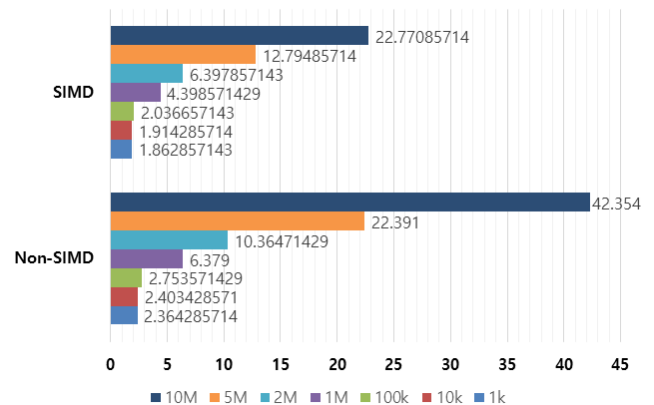
(표 3) 제안 프로토콜에 적합한 알고리즘 선정

기능	알고리즘
암/복호화	LEA-128-CTR
메시지 인증 코드	Chaskey

LEA-128-CTR은 ARX 연산만으로 이루어져 있으며, CTR 모드의 경우에는 암/복호화 모두 병렬처리가 가능하기 때문에 SIMD를 활용하여 고속화가 가능하며, 암호화 코드만 필요하기 때문에 코드 크기 또한 최소화 할 수 있다.

또한 Chaskey 알고리즘의 경우에도 ARX 연산만으로 구성 되어있고, 32비트 마이크로 컨트롤러에 적용 가능하도록 만들어진 고속 MAC 알고리즘이다. 또한 키 스케줄링의 과정이 없기 때문에 마찬가지로 코드 크기를 최소화할 수 있다는 장점을 가지고 있다.

아래 그림 3은 제안 프로토콜에서의 검증자(Verifier) 측면에서 다양한 여러 IoT 디바이스에 대한 인증을 처리할 때 SIMD를 사용한 경우와 사용하지 않은 경우의 인증 데이터 처리 속도를 나타낸 그래프이다.



(그림 3) SIMD 활용 여부에 따른 인증 데이터 처리 속도 비교

인증 데이터가 많을수록 SIMD를 활용한 고속 병렬의 효과가 높아지는 것을 확인할 수 있다.

4. 결 론

본 논문에서는 IoT 디바이스에 대한 인증 절차를 수행하기 위한 프로토콜을 제안하였다. 제안 프로토콜은 다양한 산업 분야에서 보급 및 적용되어 활용되고 있는 ARM Cortex A 프로세서의 IoT 디바이스들의 인증 과정을 보다 경량화하고 고속화하기 위한 방법으로 SIMD 기술을 적극적으로 활용할 수 있는 프로토콜을 제안하였다.

향후에는 ARM 외에도 다양한 프로세서에서 활용 가능한 IoT 인증 프로토콜의 경량화에 대해 연구할 예정이다.

참 고 문 헌

- [1] Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel and Ingrid Verbauwhede, "Chaskey: An efficient MAC Algorithm for 32-bit Microcontrollers", SAC 2014, vol.8781, pp.306-323, 2014.
- [2] 미래창조과학부, "사물인터넷(IoT) 환경에서의 암호인증기술 이용 안내서", 2016.
- [3] Liu Cheng, Lin shenwen, Li Yingbo, Li Na and Wang Xuren, "A Secure and Lightweight Authentication Protocol for RFID", Electronics Information and Emergency Commucation, pp.317-320, May 2015.