IoT 및 모바일 기기에서의 센서를 활용한 난수발생기 현황

조성민, 서승현
한양대학교 전자공학과
e-mail: smcho3315@hanyang.ac.kr

Research of Random Number Generator Using Sensors for IoT and Mobile Devices

Seong-Min Cho, Seung-Hyun Seo
Dept of Electronic Engineering, HanYang University

요 약

IoT 기술이 발달하면서 기기들 간의 안전한 통신을 위한 보안 시스템 탑재의 필요성이 대두되었다. 보안 시스템은 암호 키의 안전성과 밀접한 관련이 있기 때문에, 안전한 난수발생기를 통해 생성한 난수를 키로 사용하는 것이 중요하다. 그러나 제한된 리소스를 갖는 IoT 기기들의 특성으로 인해, 기존 난수발생기를 IoT 기기에 구현하기 어려운 문제가 있다. 이에 IoT 기기에서 사용 가능한 난수발생기에 대한 연구들이 진행되어 왔으며, 특히 IoT 기기들이 탑재하고 있는 각종 센서를 활용한 난수발생기의 설계 방안들이 활발히 연구되고 있다. 본 논문에서는 IoT 기기에 주로 탑재되는 센서를 5가지로 분류하고, 각각의 센서별로 난수성을 측정하는 연구들을 분석한다. 우리가 조사한 바에 따르면 이러한 센서들의 출력이 충분한 난수성을 제공하고 있으며, 본 논문에서 각 센서들을 활용하여 난수발생기를 설계한 연구들을 분류하고 특징을 살펴본다.

1. 서론

난수란 무작위로 추출되며, 예측과 재현이 불가능한 성질을 지니고 있는 수를 일컫는다. 이러한 성질 때문에 난수는 암호 시스템의 여러 분야에서 사용되고 있다. 그 예로 대칭키와 공개키 암호 시스템의 비밀키 생성 시 난수가 사용되며, 식별이나 인증 프로토콜의 논스(nonce), 솔트(salt) 등에서 중요한 보안 매개변수로 난수가 사용된다.

한편, 사람과 사물간의 자유로운 통신과 정보의 교환이 가능해지는 사물인터넷(IoT, Internet of Things) 시대가 도래하면서, 동시에 IoT 기기 및 통신상에도 다양한 보안 위협들이 생겨났다[1]. 따라서 IoT 기기들에 보안 시스템을 탑재하여 안전하게 통신하는 것이 중요하며, 이러한 보안 시스템에 사용되는 키를 생성하기 위해 안전한 난수발생기(RNG, Random Number Generator)를 사용하여 난수를 생성할 필요가 있다.

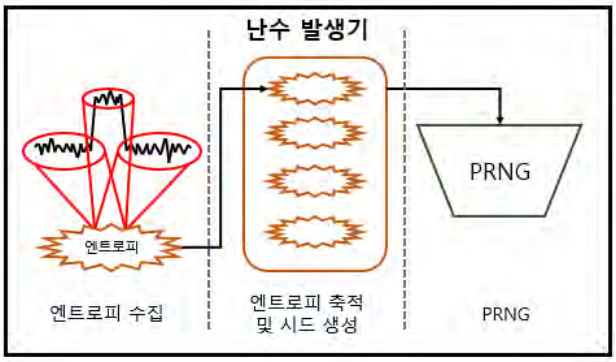
이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2018R1A2B6006903).
본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-0-01417).

기존 PC용 보안 소프트웨어에서는 Linux PRNG나 오픈 소스 암호 라이브러리의 의사난수발생기를 사용하였다. 이러한 난수발생기는 데스크톱 PC의 마우스나 키보드와 같은 사용자/외부 주변장치, 인터럽트 요청 시간, 디스크를 읽고 쓰는 시간 등 PC에서 얻을 수 있는 자원을 seed로 활용하여 난수를 생성한다[2]. 그러나 데스크톱PC에 기반하여 설계된 기존 난수발생기가 제한된 리소스를 갖는 IoT 기기에서 제대로 동작하는 것이 어려운 문제가 있다[3]. 이에 IoT 기기에서 사용 가능한 난수발생기에 대한 연구들이 진행되어 왔다. 특히, IoT 기기들이 탑재하고 있는 각종 센서를 활용하여 난수를 생성하는 방안들이 활발히 연구되고 있다. 본 논문에서는 IoT 기기에 주로 탑재되는 센서를 5가지로 분류하여, 각각의 센서별로 난수성을 측정하는 연구들을 분석한다. 또한 IoT 및 모바일 기기에서 이러한 센서들을 활용하여 난수발생기를 설계한 연구들을 분석한다.

2. 난수발생기

난수발생기는 크게 진난수발생기(TRNG, True Random Number Generator)와 의사난수발생기(PRNG, Pseudo Random Number Generator)로 분류될 수 있다. 진난수발생기는 예측 불가능성을 지니는 자연 현상과 비결정론적인 물리 현상을 기반으로 하여 난수를 생성하고, 의사난수발생기는 seed라는 초기 값을 입력 받아 결정론

적 알고리즘을 통해 난수를 생성하게 된다. 진난수발생기는 하드웨어 기반으로 설계되며 반도체나 레지스터에서 발생하는 전자적 노이즈, 방사성 물질의 붕괴 시간 등의 잡음원 신호를 이용한다. 의사난수발생기는 소프트웨어 기반으로 설계되며 해쉬 함수, 블록 암호, 공개키 암호 등을 기반으로 하여 설계된다. (그림 1)은 의사난수발생기의 구조를 나타낸다.



(그림 1) 난수발생기의 구조

엔트로피 수집 단계는 잡음으로부터 엔트로피를 수집하는 단계이며, 다음 단계에서 엔트로피를 축적하여 그것으로 시드를 생성하게 되고, 의사 난수 생성기(PRNG)를 사용하여 난수를 생성하게 된다[3].

3. 난수발생기를 위한 IoT 기기의 센서별 분석

본 장에서는 IoT 및 모바일 기기에 탑재된 센서들이 출력하는 값들의 난수성을 측정한 연구들을 분석한다. 또한 난수성을 제공하는 센서들을 활용하여 난수발생기를 설계한 연구들을 분석한다.

3.1 가속도계

가속도계는 관성에 의한 반작용을 측정하여 가속도를 측정하는 센서이다. 가속도계는 매우 다양한 기기에서 사용되며, 특히 모바일 기기 및 무선 통신을 하는 기기에서 흔히 사용된다. 2011년 Jonathan Voris 등은 진난수발생기를 위한 가속도계의 난수성을 조사하였다[4]. 이 논문에서는 가속도계가 정지해 있을 때에도 충분한 엔트로피를 도출할 수 있으며, 다양한 환경적 변화에 대해 내성이 있음을 밝혔다. 또한 제한된 자원을 가지는 RFID 태그에서 가속도계 기반의 난수발생기의 타당성을 입증하였다. 2년 후인 2013년 Christine Hennebert 등은 높은 관성으로 현상을 측정하는 온도나 기압과 같은 센서들과는 달리 가속도계가 충분한 엔트로피를 제공함을 밝혔다[5]. 또한 가속도계에서 수집된 min-entropy 양이 [4]에서 과대평가되고 있다는 것을 보였다. Joseph Loutfi 등이 스마트폰에 탑재된 가속도계의 출력 비트가 진난수발생기의 출력으로 사용될 수 있을 만큼 적합하다는 것을 보였다[6]. 그러나 이 논문에서는 가속도계 센서가 변화를 감지했을 때만 새로운 센서값이 기록되게 하였고, 가속도계의 연속적인 출력 비트에 대해서는 다루지 않았다.

이처럼 가속도계는 센서값 자체로도 충분한 엔트로피를 가지고 있으며, 이를 이용한 난수발생기도 연구되어 왔다. 2011년 Alin Suciu 등은 모바일 폰의 가속도계, 지자기, 방향 센서 등의 하드웨어 센서들로부터 얻은 센서 값을 서로 결합한 후 XOR 연산을 통해 난수를 생성하는 진난수발생기를 제안하였다[7]. 2014년에는 Andrei Marghescu와 George Teseleanu가 가속도계를 활용한 안드로이드 기반 스마트폰의 난수발생기에 대한 논문을 발표하였다[8]. 이 논문에서는 센서가 출력한 값의 Least Significant Bit (LSB)만 저장하여 난수 시퀀스를 만든 뒤 Von-Neumann 계열의 의사난수발생기를 적용하여 의사난수를 생성하였다. 2016년에는 Kyle Wallace 등이 센서가 장착된 모바일 및 IoT 기기에서 난수를 생성하는 방법을 제안하였다[9]. 이 논문에서는 37개의 안드로이드 기기에서 데이터를 수집하여 충분한 난수성을 가지는 센서를 분석하였으며, 가속도계의 출력이 충분한 난수성을 보임을 밝혔다. 또한 경량 믹싱 알고리즘을 통해 수집한 센서 값들을 결합하여 난수를 생성하는 진난수발생기를 설계하였다. 2017년 Lavinia Mihaela Dinca와 Gerhard Hencke는 가속도계, 자이로스코프, 선형 가속계, 지자기, 중력, 회전, 소리 센서 등 6가지 스마트폰 센서에서 수집한 생체 데이터의 난수성을 분석하였다[10]. 이를 통해 인간의 걸음걸이는 예측이 가능하며 따라서 랜덤 소스로 사용되어서는 안 된다는 것을 보였다. 그러나 2018년 Yingnan Sun과 Benny Lo가 발표한 논문에서는 가속도계와 자이로스코프를 함께 사용하여 걸음걸이로도 난수를 생성할 수 있음을 보였다. 단일 걸음걸이 주기와 다중 걸음걸이 주기의 평균 신호의 에너지 차를 비교하여 재배열한 후 XOR 연산을 취함으로써 걸음걸이의 예측가능성에도 불구하고 난수를 생성할 수 있었다. 이를 이용하여 보행 시 출력하는 신호의 시간적 변동에 기반한 온바디 IoT 기기에서의 난수발생기를 제안하였다[11].

3.2 자이로스코프

자이로스코프는 각운동량 원리를 이용하여 방향을 측정하거나 유지할 때 사용되는 센서이다. 자이로스코프는 가속도계와 마찬가지로 다양한 기기에서 사용되며, 특히 드론이나 가상현실(VR, Virtual Reality) 등 자세를 측정하고 보정하는 기기들에서 많이 사용된다. [6]에서는 가속도계와 더불어 스마트폰에 탑재된 자이로스코프가 3축 출력 모두 난수로 사용될 수 있을 만큼 충분한 난수성을 보임을 밝혔다.

자이로스코프는 가속도계와 마찬가지로 충분한 엔트로피를 가지고 있으며, [8]에서 가속도계와 함께 자이로스코프를 활용한 의사난수발생기를 제안하였다. [9]에서는 안드로이드 기기의 자이로스코프 출력이 난수성을 보임을 밝혔다. 또한 집합(aggregation)과 접기(folding) 기법, 축

<표 1> 센서를 활용한 난수발생기 연구별 비교

논문	활용한 센서	난수발생기 종류	활용
[7]	가속도계, 지자기 센서	TRNG	스마트폰
[9]	가속도계, 자이로스코프, 마이크	TRNG	스마트폰, IoT 기기
[11]	가속도계, 자이로스코프	TRNG	on-body IoT 기기
[12]	카메라	TRNG	스마트폰 카메라
[13]	마이크	TRNG	데스크톱PC의 마이크 입력
[8]	가속도계, 자이로스코프, 지자기 센서	PRNG	스마트폰
[14]	마이크	PRNG	스마트폰

소(reduction) 함수를 이용하여 자이로스코프의 출력을 시드로 활용한 진난수발생기를 설계하였다.

3.3 지자기 센서

지자기 센서는 지구의 자력을 검출하여 방위 정보를 얻을 수 있는 센서이며, 주로 디지털 나침반 기능을 탑재한 IoT 기기들에 사용된다. [5]에서 지자기 센서가 엔트로피를 생산하는 가장 좋은 후보 중 하나임을 밝혔으며, [6]에서는 지자기 센서 또한 3축 모두 충분한 난수성을 보임을 밝혔다.

[7]에서는 이러한 난수성을 지니는 지자기 센서를 활용하여 가속도계, 방향 센서 등과 함께 결합한 데이터 소스들을 XOR 연산을 취함으로써 난수를 생성하는 진난수발생기를 제안하였다. [8]에서는 가속도계, 자이로스코프와 함께 지자기 센서를 활용한 의사난수발생기를 제안하였다.

3.4 카메라

카메라는 cctv 등 촬영의 목적뿐만 아니라 이미지 기반의 영상처리를 하는 등 다양한 IoT 기기에서 사용된다. Xuping Zhang 등은 스마트폰의 카메라를 기반으로 한 휴대용 진난수발생기를 제안하였다[12]. 이 논문에서는 엄지손가락으로 플래시와 이미지 센서를 동시에 가린 뒤 피부와 근육 조직에 의해 약화된 빛을 이용하였다. 회색도 차이를 통해 랜덤한 비트를 생성하고 벡터-행렬 곱셈을 통해 엔트로피를 강화하였다.

3.5 마이크

음성인식 인공지능(AI) 기술이 발달하면서 마이크를 탑재한 IoT 기기들이 많아졌다. 2011년 Roger Morrison은 개인용 컴퓨터의 마이크와 오디오 입력이 난수성을 제공한다는 것을 증명하고, 아날로그 오디오 입력과 샘플링 클럭을 통해 난수를 생성하는 진난수발생기를 설계하였다[13]. 2017년에는 Faizal Wahyu Romadhon과 Prasetyo Adi Wibowo P가 스마트폰의 오디오 입력을 시드로 사용하여 메르센 트위스터 의사난수 생성 알고리즘을 통해 난수를 생성하는 의사난수발생기에 대한 논문을 발표하였다[14].

4. 결론

데스크톱PC에 기반하여 설계된 기존 난수발생기는 제한된 리소스를 가진 IoT 기기에 적용하기 어렵다. 이에 IoT 기기에 탑재된 센서를 활용하여 난수를 생성하는 방안들이 활발히 연구되어 왔다. IoT 기기에는 대표적으로 가속도계, 자이로스코프, 지자기 센서, 카메라, 마이크 등이 탑재되어 있으며, 본 논문에서는 이 5가지 센서들의 난수성을 측정하는 연구들을 분석하였다. 우리가 조사한 연구들은 IoT 및 모바일 기기에 탑재되어 있는 이러한 센서들이 충분한 난수성을 제공하고 있음을 보였다. 또한 5가지 센서들을 활용하여 IoT 기기에서 사용 가능한 난수발생기를 설계한 연구들을 분류하고 정리하였다.

참고문헌

[1] 김동희, 윤석웅, 이용필, “IoT 서비스를 위한 보안”, 한국통신학회지 (정보와통신) 제30권 제8호, pp.53-59, 2013.7

[2] 한국정보통신기술협회, “결정론적 난수발생기 - 제2부 : 해시함수 기반 난수발생기”, 정보통신단체표준(국문표준)

[3] 강하나, 유태일, 염용진, 강주성, “센서를 이용한 경량 난수발생기 설계 및 구현”, 한국통신학회논문지 제42권 제2호, pp.307-315, 2017.2

[4] J. Voris, N. Saxena, T. Halevi, “Accelerometers and Randomness: Perfect Together”, WiSec ‘11 Proceedings of the fourth ACM conference on Wireless network security, pp.115-126, 2011.6

[5] C. Hennebert, H. Hossayni, C. Lauradoux, “Entropy Harvesting from Physical Sensors”, WiSec ‘13 Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, pp.149-154, 2013.4

[6] J. Loutfi, A. Chehab, I. H. Elhajj, A. Kayssi, “Smartphone Sensors as Random Bit Generators”, 2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA), 2014.11

[7] A. Suciu, D. Lebu, K. Marton, “Unpredictable Random Number Generator Based on Mobile Sensors”, 2011 IEEE 7th International Conference on Intelligent

Computer Communication and Processing, 2011.8
[8] A. Marghescu, G. Teseleanu, “Cryptographic Key Generator Candidates based on Smartphone built-in Sensors”, 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), 2014.10
[9] K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun, “Toward Sensor-Based Random Number Generation for Mobile and IoT Devices”, IEEE Internet of Things Journal Vol.3 Issue.6, pp.1189-1201, 2016.12
[10] L. M. Dinca, G. Hancke, “Behavioural sensor data as randomness source for IoT devices”, 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), 2017.6
[11] Y. Sun, B. Lo, “Random Number Generation Using Inertial Measurement Unit Signals for On-Body IoT Devices”, Living in the Internet of Things: Cybersecurity of the IoT 2018, 2018.1
[12] X. Zhang, L. Qi, Z. Tang, Y. Zhang, “Portable true random number generator for personal encryption application based on smartphone camera”, Electronics Letters Vol.50 Issue.24, pp.1841-1843, 2014.11
[13] R. Morrison, “Design of a True Random Number Generator Using Audio Input”, Journal of Cryptology, Vol.1, No.1, 2001
[14] F. W. Romadhon, P. A. Wibowo P, “Generation of Pseudorandom Numbers from Audio Input in Smart Phone Android”, 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 2017.10