사물인터넷을 위한 난수생성기의 속성 분석

여연수*, 김현성*,**

*경일대학교, **말라위대학교

*didistn123@naver.com, **kim@kiu.ac.kr

Feature Analysis of Random Number Generator for Internet of Things

Yeonsu Yeo*, (Corresponding author)Hyunsung Kim*,**

*Kyungil University, **University of Malawi

요 약

최근 사물인터넷을 위한 보안 기법들은 대부분 난수를 사용한다. 하지만 다양한 시스템에서 사용하고 있는 난수생성기에 대한 특성 분석이 필요하다. 본 논문에서는 기존에 Kim과 Jeong이 제안한 센서기반 난수생성기를 살펴보고, 다양한 사물인터넷환경에서의 난수 요구사항 분석을 통해 난수생성기의 특성을 분석하고자 한다. 본 논문에서 도출된 사물인터넷 환경의 난수 특성에 기반한 사물인터넷 환경을 위한 난수생성기의 개발은 보안 및 프라이버시 제공에 있어서 필수 불가결한 요소이다.

Ⅰ. 서론

사물인터넷은 4차 산업혁명 핵심 산업 중 하나로 초연결사회에서 주목받는 기술이다. 사물인터넷 관련 다양한 기술이 개발되면서 사물인터넷을 위한 다양한 보안 및 프라이버시를 위한 기법들이 제안되고 있다. 최근 제안된 사물인터넷을 위한 보안 및 프라이버시 기법들은 대부분 연산 오버헤드가 작은 요구사항을 가진다. 특히, 이들 기법들은 대부분 난수 생성에 대한 요구사항을 가진다. 지금까지 개발된 다양한 난수생성기가 있지만, 이들에 대한 특성 분석을 통한 보안 적합성 관련 연구가 제시되지 못했다[1-4].

본 논문에서는 기존의 난수생성기에 대한 분석을 위해 난수 속성을 파악하고 이를 통하여 사물인터넷 환경을 위한 난수생성기의 보안 요구사항들을 도출하고자 한다.

Ⅱ. 센서 기반 난수생성기

본 장에서는 Kim과 Jeong이 제안한 사물인터넷을 위한 센서기반 난수생성기의 개요를 살펴본다[2].

2.1 연구 환경

사물인터넷을 구성하기 위해서 기본 장치와 키 발급 서버 그리고 데이터베이스서버, 그리고 게이트웨이와 시스템을 사용하는 사용자로 구성된다. 암호화 알고리즘은 AES (Advanced Encryption Standard)와 RSA (Rivest Shamir Adleman)를 이용하였다.

2.2 통신 과정

먼저 디바이스에서 만들어진 온도와 습도 값을 물리 난수생성기를 통해 만들어진 진난수로 생성된 대칭키로 암호화한다. 대칭키는 게이트웨이로부터 저달받은 공개키로 암호화된다. 그리고 대칭키로 암호화된 온도와 습도 값과 공개키로 암호화된 대칭키는 접근 서버에 저장된다. 그리고 데이터를 전송할 때 게이트웨이와 디바이스 사이의 상호 인증 과정을 거치기 위해 5단계로 구성된 상호 인증 프로토콜을 적용한다. 상호 인증이 정상적으로 완료되면 접근 서버에 저장된 정보를 보여준다. 즉, 사용자는 웹 브라우저를 이용하여 디바이스에서 측정된 센싱 값을 확인할 수 있으며, 게이트웨이의 해시값과 이를 만들기 위해 사용되었던 해시값도 함께 확인할 수 있다.

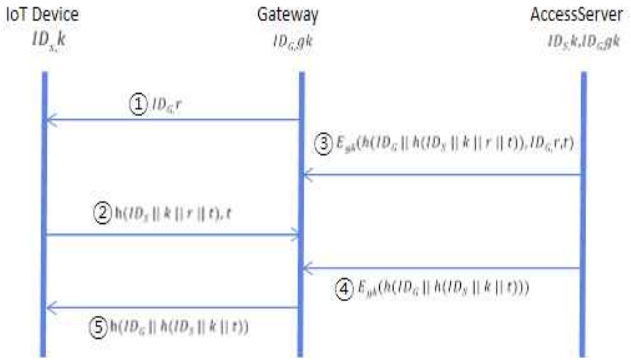

그림 1. 인증 프로토콜

2.3 인증 프로토콜

Kim과 Jeong은 그림 1에서 보여준 5단계로 구성된 상호 인증 프로토콜을 다음과 같이 제시하였다.

단계 1: 게이트웨이는 랜덤 값 *r*, 자신의 식별자 *ID*를 디바이스에 보낸다.

단계 2: 디바이스는 랜덤 값 *t*와 디바이스 식별자 *IDs*, 디바이스와 게이트웨이 간의 비밀키 *k*, 디바이스의 랜덤 값 *r*, 디바이스의 랜덤값 *t*를 이용하여 해쉬한 값을 보낸다.

단계 3: 게이트웨이는 수신한 해시 값과 자신의 식별자 *IDg*와 랜덤 값 *r*, *t*를 세션키 *gk*로 암호화하여 접근 서버에 전송한다.

단계 4: 접근서버는 수신한 데이터를 복호화하고 *IDg*, *k*, *r*, *t* 값을 이용하여 디바이스의 정당함을 인증한다.

단계 5: 게이트웨이는 접근 서버로부터 수신한 데이터를 복호화하고 디바이

스의 정당함을 인증한 후 $h(IDg||h(IDs||k||t)$를 계산하여 디바이스에게 전송한다.

2.4 이미지 센서 기반 난수 생성

센서를 기반으로 하여 난수를 생성하는 코드로 Picam이라는 카메라를 이용하여 라즈베리파이에 연결하고 촬영한 이미지를 난수로 사용한다. 사용한 소스 코드는 그림 2와 같다. 사용한 코드는 캡춰한 이미지의 픽셀 하나하나의 값을 bgr 배열로 변환을 한 후 이를 바이트(bytes)로 변환함으로서 난수를 생성한다.

```
# Random number generation
dev = PiCamera()
dev.resolution = (1024, 768)

def init_devdata():
    start = time.time()
    raw = PiRGBArray
    dev.capture(rawCapture, format="bgr")
    image = raw.array
    print("rand time: ", time.time() -start)

    global g_did, g_skey, g_dt
    g_did = b"10"

    g_skey = bytes([int(image[255,100,0])
                    int(image[255,100,1]), int(image[255,100,2])])
    ......
    b_dt = bytes([int(image[255,100,1])])

# Result : (1024 * 767 * 24 * 8 = 150994944 bit)
time: 0.6538541316986084
```

그림 2. 난수 생성 코드

Ⅲ. 특성 분석

본 장에서는 난수 생성기가 가져야 할 특성에 대해 정의하고 이를 기반으로 하여 Kim과 Jeong이 제안한 센서기반 난수생성기의 사물인터넷 환경에서 요구되는 특성을 분석한다.

3.1 난수의 개요

본 논문에서는 난수 생성기가 생성한 난수는 다음과 같은 요구 사항을 만족하는 것으로 한다.

(1) 난수 생성기에서 생성된 숫자는 거의 균일하게 분포되어야 한다.
(2) 난수 생성기에서 생성된 숫자는 상호 독립적이어야 한다.
(3) 난수 생성기에서 생성된 동일한 숫자는 충분히 긴 시간을 가져야 된다.
(4) 난수 생성기에서 생성된 숫자는 예측이 불가능해야만 한다.

3.2 사물인터넷 요구사항 분석

본 절에서는 Kim과 Jeong이 제안한 난수생성기를 난수 속성에 기반하여 분석함으로서 사물인터넷 환경에서 요구되는 난수 생성기의 속성을 도출한다.

(1) 주기성

주기성이란 반복이 다시 시작할 때까지 수열의 길이를 의미한다. 변화하지 않는 규칙이 존재하는 한 이 규칙에서 정의해놓은 길이를 넘어서는 개수의 난수를 요구할 경우 같은 난수를 생성하는 주기가 발생한다. Kim과 Jeong의 난수생성기는 센서로부터 캡춰한 이미지의 픽셀 하나하나를 이용하여 이를 바이트로 변환함으로서 난수를 생성하였다. 하지만, 사물의 픽셀 이미지의 고정된 속성으로 인해서 주기성을 보장하기 어렵다. 즉, 주기성을 위해서는 생성된 난수의 분포를 명확히 할 수 있는 방법에 대한 추가적인 속성 보증이 필요하다.

(2) 규칙 노출 가능성

난수생성기는 사전에 정의해둔 규칙과 초기(Seed)값을 통하여 일반적으로 난수를 생성한다. 이러한 이유로 규칙이 변하지 않는 한 난수생성기는 같은 동일한 난수가 생성되게 된다. 즉, 같은 초기값이 여러 차례 대입하는 것으로 해당 초기값을 통해 규칙적인 난수가 생성될 수 있다. 이로 인해 난수생성기의 규칙이 노출된 초기값으로 생성된 난수는 예측 가능하다. 특히, Kim과 Jeong의 난수는 센서로부터 캡춰한 이미지 픽셀을 이용하고, 이로인해 이미지간 차이가 발생할 수 있는 요소 적용을 센서에서 제시할 수 있어야 한다. 이러한 환경 설정에 대한 추가적이고 구체적인 방안을 제시한다고 하더라도 이미지들 간에 존재하는 규칙 노출 가능성은 여전할 것이다.

(3) 상호독립성

상호독립성은 주기성과 반대적인 속성을 의미한다. 즉, 각각의 값은 다른 값에 종속되지 않은 상태를 말한다. 즉, 모든 값은 규칙을 가지지 않는 속성을 말한다. 하지만, Kim과 Jeong의 난수생성기는 센서를 통해 획득한 이미지 픽셀을 이용하므로 상호연관성을 가지는 난수가 생성될 확률이 높다. 난수간의 상호독립성 보장이 어렵다.

Ⅳ. 결론

본 논문에서는 사물인터넷을 위한 난수 생성기가 생성하는 난수의 속성 분석을 Kim과 Jeong이 제안한 센서기반 난수생성기의 특성 분석을 통하여 제시하였다. 특히, 난수에 있어서 예측 가능성은 보안관련 주요 취약점으로 이어질 수 있다. 하지만 최근 제시되고 있는 사물인터넷을 위한 보안 기법들은 다양한 난수생성기에서 생성된 도전(Challenge)-응답(Response) 기법을 사용하므로 암호학적 난수생성기의 사용은 보안 기법의 설계에 있어서 아주 중요하다. 즉, 예측 가능성 문제가 제시된 난수생성기의 사용은 다양한 보안 및 프라이버시 침해에 문제가 될 수 있다.

본 논문에서 도출한 사물인터넷에서 요구되는 난수생성기의 속성을 제시할 수 있는 난수생성기의 개발은 아주 중요한 문제이다. 다양한 사물인터넷을 위한 경량의 암호학적 난수생성기는 주기성, 무규칙성, 상호돌립성을 가질 수 있도록 개발되어야 할 것이다.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

참 고 문 헌

[1] Y. S. KIM, "Fourth Industrial Revolution(4IR) Hyper-Connected Society and Internet of Things Age", *The Korea Contents Association Review*, vol. 17, no. 3, pp. 14-19, 2019.

[2] J. S. Kim, J. H. Jeong, "Development of the Encryption System for IoT Device Based on Random Number Generator Using Sensor", *Journal of Korean Institute of Intelligent Systems*, vol. 30, no. 6, pp. 459-464, 2020.

[3] S. K. Lee, "A Study on Pseudo-random Number Generator with Fixed Length Tap unrelated to the variable sensing nodes for IoT Environments", *Journal of the Korea Academia-Industrial*, vol. 19, no. 2, pp. 676-682, 2018.

[4] S. Y. Min, J. S. Lee, "Device Mutual Authentication and Key Management Techniques in a Smart Home Environment", *Journal of the Korea Academia-Industrial*, vol. 19, no. 10, pp. 661-667, 2018.