Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 2 pp. 676-682, 2018

https://doi.org/10.5762/KAIS.2018.19.2.676
ISSN 1975-4701 / eISSN 2288-4688

IoT 환경에서 가변 센싱 노드들에 무관한 고정 길이 탭을 가지는 의사 난수 발생기에 관한 연구

이선근
전북대학교 기계시스템공학부

A Study on Pseudo-random Number Generator with Fixed Length Tap unrelated to the variable sensing nodes for IoT Environments

Seon-Keun Lee
School of Mechanical System Engineering, Chonbuk National University

요 약 WSN을 포함하는 IoT 세상이 발전할수록, IoT를 적용하는 주위환경에 따라 정보를 센싱하는 센서 시스템의 수가 매우 가변적이다. 이러한 복잡한 환경에서 각각의 센서 시스템들에 대한 보안을 수행하기 위하여 보안모듈들도 가변적으로 증감을 수행해야 한다. 이러한 문제점은 시스템 효율성과 해킹/크래킹을 고려하였을 경우, 하드웨어/소프트웨어적인 구현을 어렵게 한다.
그러므로 본 논문은 이러한 문제점을 해결하기 위하여 센싱 노드들의 수와 상관없이 일정한 주기를 가지는 의사난수를 발생시키며 이상현상을 탐지할 수 있는 기능을 가진 고정 길이 탭을 가진 의사 난수 발생기(FLT: Pseudo-random Number Generator with Fixed Length Tap unrelated to the variable sensing nodes) 구조를 제안하였다. 제안된 FLT-LFSR 구조는 IoT 환경에서 하드웨어/소프트웨어 구현에 대하여 보안레벨 및 전체 데이터 포맷팅을 일정하게 유지시킬 수 있도록 하였다. 그러므로 제안된 FLT-LFSR 구조는 센서 시스템 구현의 용이성 및 센싱 노드들의 수와 상관없이 네트워크의 확장성을 강조할 수 있도록 하였다.

Abstract As the IoT world including WSNs develops, the number of sensor systems that sense information according to the environment based on the principle of IoT is increasing. In order to perform security for each sensor system in such a complicated environment, the security modules must be varied. These problems make hardware/software implementation difficult when considering the system efficiency and hacking/cracking. Therefore, to solve this problem, this paper proposes a pseudorandom number generator (FLT: Pseudo-random Number Generator with Fixed Length Tap unrelated to the variable sensing nodes) with a fixed-length tap that generates a pseudorandom number with a constant period, irrespective of the number of sensing nodes, and has the purpose of detecting anomalies. The proposed FLT-LFSR architecture allows the security level and overall data formatting to be kept constant for hardware/software implementations in an IoT environment. Therefore, the proposed FLT-LFSR architecture emphasizes the scalability of the network, regardless of the ease of implementation of the sensor system and the number of sensing nodes.

Keywords : Fixed Length Tap, Intrusion detection, IoT, LFSR, Stream Cryptographic Algorithm

1. 서론

현재 Arduino[1], Edison[2] 등과 같은 오픈 H/W 및 오픈 S/W[3]를 기반으로 구현되는 간단한 플랫폼과 USN, 센서 시스템 기술, 근거리 통신망 등의 발달로 인해 사물인터넷(IoT: Internet of Things)[4]이 매우 빠르

*Corresponding Author : Seon-Keun Lee(Chonbuk National Univ.)
Tel: +82-63-270-4778 email: caiserrisk@gmail.com
Received October 24, 2017 Revised (1st November 20, 2017, 2nd December 13, 2017)
Accepted February 2, 2018 Published February 28, 2018

게 발전되고 있다.

그림 1은 IoT에 대한 개념도이다. IoT는 근거리 무선망, 프로세싱 및 제어흐름이 단순해야 원활한 데이터의 흐름이 생성된다. 그러나 센서 시스템 등과 같은 터미널이 주위환경에 대한 정보를 서버 또는 사용자에 전송되며 이와 반대로 엑츄에이터를 제어하기 위하여 터미널로 정보들이 전송되는 구조는 매우 복잡하고 보안에 취약한 상태로 발전할 수밖에 없다. 특히, 센서 및 엑츄에이터 가변성은 더욱 이러한 현상을 악화시킨다.

그림 1과 같은 시스템의 경우, OS 탑재 가능한 플랫폼으로 구현되어 보안에 대한 기능 강화 및 보안패치의 계속적인 업데이트를 고려하기 때문에 크게 문제되지 않는다. 그러나 그림 1 Ⓐ 부분은 일반 OS 탑재 플랫폼의 환경과 다르다. 즉, 이 영역은 OS를 탑재할 수 있는 플랫폼이 없거나 미약하며, 데이터 전송에 사용되는 토포로지가 매우 다양하다. 이러한 토포로지의 특징 중의 하나는 무한개의 센서 시스템/엑츄에이터의 연결이 가능하다는 것이다. 이때 센서 시스템/엑츄에이터의 수가 변경되면 변경되는 수 만큼의 보안 대책을 강구하여야 한다. 그러므로 센서 시스템/엑츄에이터의 수와 상관없이 일정 수준의 보안레벨을 유지시킬 필요성이 대두된다.

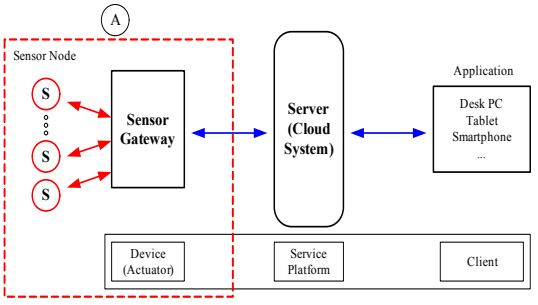


Fig. 1. IoT concept

일반적으로 Ⓐ 부분(센서게이트웨이와 센서 노드들 사이)에 적용되는 보안기법은 스트림 암호기법이다. 스트림 암호기법은 다른 암호화 기법에 비하여 악의적 공격자에 의해 쉽게 내용첨가 및 변경이 가능하다는 단점이 있지만, 리소스가 적으며, 데이터를 스트림 형태로 암호화하고, 암호화 속도가 빠르며 에러 파급 효과가 적다는 특징을 가진다[5].

스트림 암호는 LFSR (linear feedback shift register)를 이용한 난수 발생기를 이용하여 암호화하는 방식으로, 블록 암호보다 빠르게 고속으로 암호화를 처리할 수 있다. 또한 하드웨어 구조가 간단하고 저전력 소비를 요구하는 휴대 정보기기와 USN 어플리케이션에 적합하다. 그러나 LFSR을 이용한 URNG(uniform random number generator)는 균일한 출력 분포를 갖는 의사난수열을 생성한다. 따라서 난수발생기 회로 구조와 LFSR에 입력되는 초기 셋팅값(seed)을 알면 난수열을 예측할 수 있다. 그러므로 LFSR의 스테이지 수를 증가시켜 생성된 난수열이 반복되는 전체 주기를 증가시키고, 출력되는 난수들 간의 상관관계를 줄여 정보를 효율적으로 보호할 수 있다[6]. 그러나 무한대로 주기를 증가시키기 위하여 LFSR의 크기를 증대시킬 수 없고 또한 센서 노드의 급증에 대한 올바른 해가 될 수 없다. 그러므로 본 논문에서 이러한 문제점들을 해결하기 위하여 스트림 암호시스템을 적용할 수 있고, 센싱 노드들의 증감에 상관없이 고정 길이 탭을 가지는 의사 난수 발생기(FLT : Pseudo-random Number Generator with Fixed Length Tap unrelated to the variable sensing nodes) 구조를 제안하였다.

제안된 FLT 구조는 주위환경에 따른 센싱 노드 및 엑츄에이터의 수 증가 및 감소 그리고 난수주기에 대한 내용을 고려하지 않아도 되는 장점을 가지기 때문에 센서 시스템에 대한 보안 부하를 줄일 수 있다.

2. FLT-LFSR 알고리즘

IoT 및 USN의 터미널(센서 시스템 영역)에서 근거리 통신망 및 인터넷 서비스 등의 특징 때문에 블록 암호알고리즘보다 고속 동작이 가능한 스트림 암호기법이 많이 이용되고 있다. 스트림 암호기법은 LFSR 자체만으로 안전성을 제공하지 못하므로, 높은 주기성과 높은 통계적 성질을 LFSR에 결합하여 우수한 암호 알고리즘이 설계된다. 그러나 LFSR에 의해 발생된 수열은 큰 주기 및 높은 통계성을 갖지만, 출력 수열로부터 쉽게 예측이 가능하다. 일반적인 LFSR은 단지 한 사이클에 하나의 난수만을 생성하지만, 대부분의 어플리케이션이 다양화 되면서 다중 비트의 난수열이 요구되다. 이를 위해 다중 LFSR 구조[5]가 주로 사용되었으나, 구현상의 문제점과 해석의 용이성이라는 단점을 갖는다. 이와 같은 단점을 보완하기 위해 Leap-ahead 구조를 갖는 LFSR이 제안되

었다[7]. Leap-ahead 구조는 하나의 LFSR을 이용하여 다중 비트 출력을 얻을 수 있는 구조이기 때문에 구현상의 문제점은 감소되지만, LFSR의 크기와 출력 단계 수의 상관관계에 따라 생성되는 난수들의 주기가 크게 변화된다. Leap-ahead 구조는 2^n-1이 m으로 나누어지지 않을 때, 생성되는 난수 주기가 2^n-1로 되지만, 그 외의 경우에는 최대 주기가 크게 감소되어 쉽게 난수열을 예측할 수 있다는 취약점을 갖는다.

본 논문은 센서 시스템의 수에 적응되어 다중 난수열을 발생시키면서 이러한 문제점들을 해결하기 위하여 LFSR의 난수 주기를 2^n-1로 유지하면서 구현상의 문제점도 감소시킬 수 있고 센싱 노드들의 증감에 상관없이 고정 길이 탭을 가지는 의사 난수 발생기 구조를 제안하였다.

제안된 FLT 구조는 다양한 IoT/USN 구현을 위한 가변 센싱 노드들의 수에 비례적으로 LFSR 내부의 세그멘테이션(segmentation: 각각의 센서 시스템에 매핑되는 하부 블록)이 가변 되도록 한 것이다. FLT 구조는 하나의 LFSR이 다양화되는 어플리케이션에 대하여 다중 난수열이 발생될 수 있도록 할 뿐 아니라, 하나의 LFSR 안에 여러 개의 LFSR-segmentation을 두어, 각각 사용 빈도(센서 시스템의 개수)에 맞게 동작하기 때문에 구현상의 어려움을 해결할 수 있고, 분산되어 있는 각각의 센싱 노드의 사용 여부에 상관없이 주 LFSR(main LFSR)이 동작하여 센서 시스템들 모두를 포함하는 전체 시스템에 대한 보안 효율 및 난수 주기의 변화가 없도록 하였다. 그림 2는 센싱 시스템에 스트림 암호방식을 적용한 그림이다. 센싱 소자(sensing element)의 ID를 이용하여 LFSR의 seed로 사용하고, 이를 스트림 암호에 적용하게 된다. 센싱 소자들의 수가 n개 일 경우, 시스템 전체의 ID는 식 (1)과 같이 분산된 센서들에 대하여, 센싱 소자들로 구성된 센서 네트워크에 대한 각각의 ID 값에 대한 단순합이다. 각각의 $SE_i\ (i=0,1,2,\ldots,n-1)$ 값들을 1:1로 LFSR 원시다항식으로 매핑을 수행하기 위하여 식 (2)와 같이 LFSR에 대한 하부 블록(segmentation)을 수행한다.

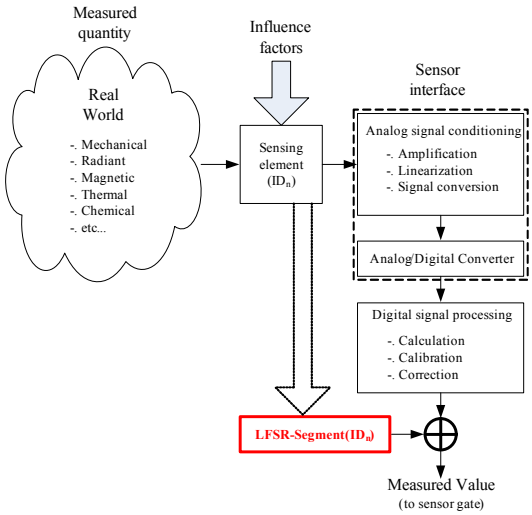


Fig. 2. Sensing system architecture

$$\begin{aligned} SE(ID) &= (SE_0, SE_1, \ldots, SE_{n-1}) \\ &= (SE_0\ \&\ SE_1\ \&\ \ldots\ \&\ SE_{n-1}) \\ &= \text{SensorGateway} \end{aligned} \tag{1}$$

하나의 센서 게이트웨이에 대하여 n개의 센서 노드들이 있다고 가정할 경우, 각각의 센싱 노드들을 n개의 하부 블록으로 할당하고 식 (1)과 같이 대등하게 분할하여 이를 식 (2)와 같이 구성한다.

$$LFSR_{gateway} = (LS_0, LS_1, \ldots, LS_{n-1}) \tag{2}$$

이때, 식 (1)과 식 (2)를 그림 3과 같이 표현할 수 있다. $GF(q^m)$를 기초체(base field) $GF(q)$상의 확대체(extension field)라 하면, $GF(q^m)$는 $GF(q)$상의 m차 기약 다항식의 residue set이다. 또한, $GF(q^m)$의 모든 원소에 대한 최소다항식은 항상 존재하고 유일하다[8]. 확대체 $GF(q^m)$의 원시 원소를 근으로 하는 최소다항식은 m차 원시다항식으로 귀결된다. α를 확대체 $GF(q^m)$의 원시원소라 하자. $\gcd(k, q^m-1)=1$ ($\gcd$: greatest common divisor)인 모든 정수 k에 대해 α^k는 $GF(q^m)$의 원시원소이고, 이 원소의 최소다항식 $g_k(x)=x^m+\sum_{i=0}^{m-1} c_i x^i$ 은 m차 원시다항식이다. 여기서, c_i는 $GF(q)$의 원소이다[8].

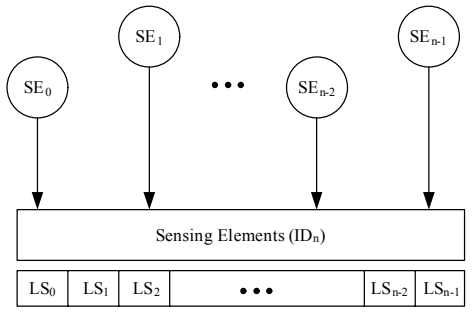


Fig. 3. Sensor network with proposed FLT

그러므로 위 정의[8]에 의하여 원시다항식 $g_k(x)$는 식 (3)을 만족한다.

$$g_k(\alpha^k) = \alpha^{km} + c_{m-1}\alpha^{k(m-1)} + c_{m-2}\alpha^{k(m-2)} + \ldots + c_0 = 0 \tag{3}$$

이때 α^h를 식 (4)와 같이 표시할 수 있다.

$$\alpha^h = a_{m-1}^{[h]} x^{m-1} + a_{m-2}^{[h]} x^{m-2} + \ldots + a_0^{[h]} \tag{4}$$

여기서 $0 \leqq h \leqq q^m - 1$ 이다. $a_i^{[h]} \in GF(q)$는 α^h $(i = 0, 1, 2, \ldots, m-1)$의 i번째 성분이다.

식 (4)를 식 (3)에 대입하고 α^{km}의 각 성분에 대하여 정리하면 m개의 미지수를 갖는 식 (5)와 같은 m개 선형방정식이 만들어진다.

$$\begin{aligned} a_0^{[km]} &= -c_{m-1}a_0^{[k(m-1)]} - c_{m-2}a_0^{[k(m-2)]} - \ldots - c_0 a_0^{[0]} \\ a_1^{[km]} &= -c_{m-1}a_1^{[k(m-1)]} - c_{m-2}a_1^{[k(m-2)]} - \ldots - c_0 a_1^{[0]} \\ &\cdots\cdots\cdots\cdots \\ a_{m-1}^{[km]} &= -c_{m-1}a_{m-1}^{[k(m-1)]} - c_{m-2}a_{m-1}^{[k(m-2)]} - \ldots - c_0 a_{m-1}^{[0]} \end{aligned} \tag{5}$$

α를 근으로 하는 원시다항식으로부터 $\alpha^k, \alpha^{2k}, \ldots, \alpha^{mk}$를 각각 계산하여 계수 $a_i^{[h]}$ $(i = 0, 1, 2, \ldots, m-1)$, $(h = 0, k, 2k, \ldots, mk)$을 얻는다. 계수 $a_i^{[h]}$를 식 (5)에 대입하여 $g_k(x)$의 계수 $c_0, c_1, \ldots, c_{m-1}$를 구할 수 있다. 이때 계수값을 구하는 방법은 matrix inversion과 A. D. Porto가 제안[9]한 방법이 있다. 여기에서 센서 네트워크의 레벨을 2-레벨로 가정할 경우, α를 상위계층(센서 게이트웨이)으로, a를 하위계층(LFSR-segmentation)으로 하여 그림 4와 같이 구성할 수 있다. 식 (4)는 m개로 구성된 a에 대한 선형방정식이다. 그러므로 n개의 SE(sensing element)로 구성된 센서 네트워크가 존재할 경우, 식 (4)를 이용하여 그림 4와 같이 구성하게 되면, 식 (4)는 다음 식 (6)과 같이 표현할 수 있다.

$$\begin{aligned} \alpha^h &= LFSR_{gateway} \\ &= a_{n-1}^{[h]} x^{n-1} + a_{n-2}^{[h]} x^{n-2} + \ldots + a_0^{[h]} \\ &= (LS_0, LS_1, \ldots, LS_{n-1}) \end{aligned} \tag{6}$$

여기서 $0 \leqq h \leqq q^n - 1$ 이다. $a_i^{[h]} \in GF(q)$는 α^h $(i = 0, 1, 2, \ldots, n-1)$의 i번째 성분이다.

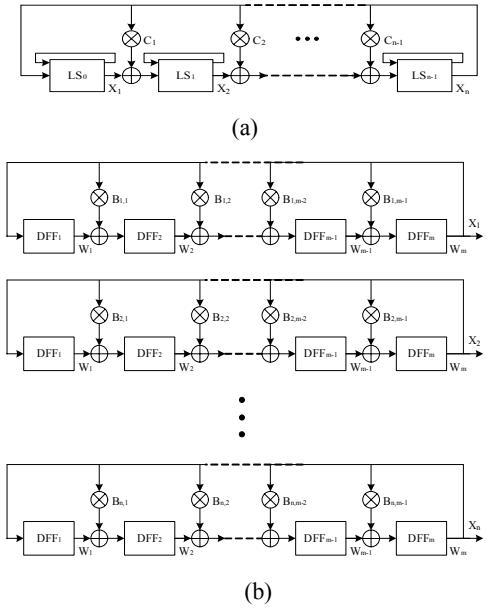


Fig. 4. Proposed FLT structure
(a) FLT sensor gate LFSR (b) FLT sensor segment LFSR

하위계층(LFSR-segmentation)의 선형방정식을 구하기 위하여 식 (6)을 식 (3)에 대입하고 α^{kn}의 각 성분에 대하여 정리한다. 그리고 a_i에 대하여 2-레벨 확장체(n-레벨 확장체에서)로 변환하고, segmentation 계수 b_i를

사용하여 정리하면 식 (7)과 같다. 이때 n개의 미지수를 갖는 식 (7)과 같은 n개 선형방정식을 가진다.

$$\begin{aligned} a_0^{[kn]} &= -b_n a_0^{[k(n-1)]} - b_{n-1} a_0^{[k(n-2)]} - \ldots - b_1 a_0^{[0]} \\ a_1^{[kn]} &= -b_n a_1^{[k(n-1)]} - b_{n-1} a_1^{[k(n-2)]} - \ldots - b_1 a_1^{[0]} \\ &\cdots\cdots\cdots\cdots \\ a_{n-1}^{[kn]} &= -b_n a_{n-1}^{[k(n-1)]} - b_{n-1} a_{n-1}^{[k(n-2)]} - \ldots - b_1 a_{n-1}^{[0]} \end{aligned} \tag{7}$$

식 (7)을 행렬식으로 다시 정리하면 식 (8)과 같다. 여기에서 식 (8)은 2^{m-1}의 주기를 갖는 하위계층인 $LS_i\,(i \leq m)$ 개가 n개로 전체를 구성하여 하나의 LFSR 구조를 갖게 된다는 것을 의미한다. 또한 식 (8)에서 하나 이상의 LS_i가 동작하지 않을 경우, 전체가 동작하지 않거나 동작하지 않는 곳의 LS_i만을 제외한 나머지는 정상적으로 동작하고, 정상적으로 동작하지 않는 영역의 LS_i는 2^{m-1} 만큼의 크기를 무의미하게 가지고 주기를 유지하기 때문에 전체 주기 2^{n-1}의 시간에는 변화가 없음을 보여준다.

$$\begin{aligned} f(x) &= c_0 + c_1 x + c_2 x^2 + \ldots + x^{n-1} \\ &= \begin{bmatrix} 0 \\ \oplus \\ b_1 a_{m-1} \end{bmatrix} + \begin{bmatrix} a_0 \\ \oplus \\ b_2 a_{m-1} \end{bmatrix} x + \begin{bmatrix} a_1 \\ \oplus \\ b_3 a_{m-1} \end{bmatrix} x^2 \\ &\quad + \ldots + \begin{bmatrix} a_{m-2} \\ \oplus \\ b_m a_{m-1} \end{bmatrix} x^{m-1} \\ &= X_1 \,\&\, X_2 \,\&\, \ldots \,\&\, X_n \end{aligned} \tag{8}$$

즉, 식 (8)과 그림 4에서 X_i는 각각의 센서 모듈들에 대한 i번째 LFSR-segmentation을 의미한다. 그러므로 센서 네트워크 내부의 하부 센서 모듈들에 대한 개수가 변화되거나 센서 모듈에 이상이 발생하여도 전체 센서 네트워크에서 스트림 처리에 대한 길이에는 변화가 없다.

3. FLT-LFSR 의사 난수 발생기 설계

FLT-LFSR 의사 난수 발생기를 설계하기 위하여 사용된 구조는 피보나치(Fibonacci) 타입이며, 데이터 크기는 8비트, 12비트, 16비트 등으로 구성하였다. FLT- LFSR 의사 난수 발생기를 설계하기 위하여 식 (7), 식(8)을 이용하였다. 이때, 식 (7) 및 식 (8)에서 주기설정은 상위계층(센서 게이트웨이)과 하위계층(LFSR- segmentation)에 대한 주기가 다양화 될 수 있기 때문에 상위계층의 일정한 주기를 유지시키기 위하여 하위계층을 중심으로 상호 한 비트씩 이동시켜 특정 주기로 일정하게 유지한다.

FLT-LFSR 설계를 위한 기본구성은 표 1과 같다. 여기에서 센서 모듈의 ID는 각 센서들에 할당된 고유 ID로써 LFSR의 초기벡터(IV)의 값을 지정해주기 위한 것이다. 기저 LFSR을 4비트, 8비트로 설정하였고, LFSR의 최종출력을 8비트, 12비트, 16비트 세 종류 4가지로 설정하였다.

Table 1. FLT-LFSR spec.

Output		LFSR primitive polynomial	Sensor Module	
upper stage	lower stage		ID	IV
8bits	4bits	$2^8 = 2^4 \cdot 2^4 = 256 \rightarrow 105$	A	1011
			B	1001
12bits	4bits	$2^{12} = 2^4 \cdot 2^4 \cdot 2^4 = 4096 \rightarrow 210$	A	1011
			B	1001
			C	1101
16bits	4bits	$2^{16} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^4 = 65536 \rightarrow 210$ $= 2^8 \cdot 2^8 = 65536 \rightarrow 595$	a	1011
			b	1001
			c	1101
			d	0110
	8bits		A	1011 0101
			B	1001 1100

제안된 FLT 구조는 하위계층을 중심으로 상호 한 비트씩 이동하고 특정 크기로 고정시켜 일정하고 특정한 주기로 유지시킨다. 그러므로 표 1에서, 상위계층 8비트에 대하여, 하위계층 4비트 LFSR 2개를 구현하여 동작시키면 주기는 105로써 항상 유지시킴을 확인하였다. 그리고 상위계층 12비트와 16비트들에 대하여 하위계층 4비트 LFSR을 사용하는 경우에도 기저가 동일하기 때문에 특정 주기는 210으로써 항상 유지시킴을 확인하였고, 상위계층 16비트에 대하여 하위계층 8비트 LFSR을 사용하는 경우에는 기저 이전과 다른 조건이기 때문에 특정 주기는 595를 유지시킴을 확인하였다.

4. FLT-LFSR 의사 난수 발생기 성능분석

그림 5는 제안된 FLT-LFSR 의사 난수 발생기 구조를 검증하기 위하여 식 (8), 표 1을 이용하기 위한 모델링 환경이다. FLT-LFSR로 유입되어지는 센싱 값들 중에 임의의 하나 또는 그 이상에서 동작하지 않거나 비인증 데이터가 유입되는 경우를 가상하여 시스템을 모델링하였다.

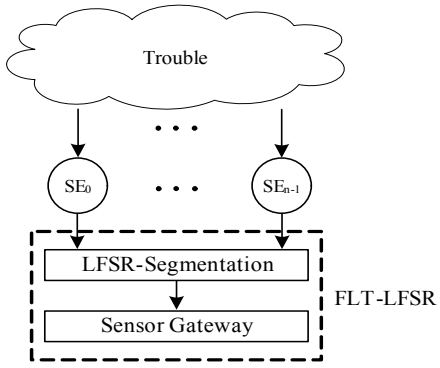


Fig. 5. Environments for FLT-LFSR pseudo-random number

그림 6은 피보나치 타입 8 비트 난수 발생기를 4비트 2개의 LFSR로 구성하여 수행한 모의실험 결과이다. 특정주기는 105를 가지며 출력을 산출하는 경우가 정상적인데, 4비트 하나의 LFSR에 이상이 발생하여 반주기 동안 출력이 산출되지 않고 있다. 이러한 상황에서 데이터의 오류가 발생한 지점에 대해서는 아무런 데이터를 발생하지 않고 있으며 또한 주기는 일정하게 유지되는 것을 확인하였다.

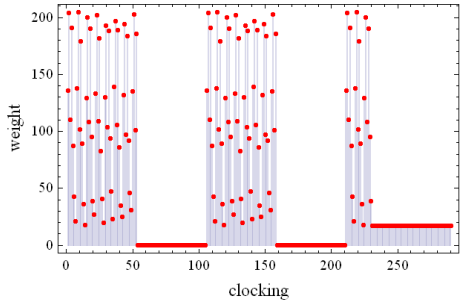


Fig. 6. 8 bits FLT-LFSR simulation result

그림 7은 4비트 3개의 LFSR을 이용하여 피보나치 타입 12 비트 난수 발생기를 구성하였으며 이에 대한 모의실험 결과이다. 특정주기는 210을 가지며 출력을 전체 주기 내에서 산출하는 경우가 정상적인데(a), 4비트 LFSR 중에서 2번째 LFSR에 이상이 발생한 경우(b), 한 주기 내에서 일정시간동안 출력이 산출되지 않고 있다.

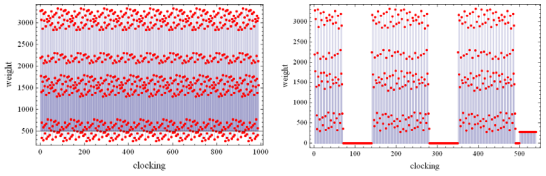


Fig. 7. 12 bits FLT-LFSR simulation result
(a) during normal operation
(b) in case of abnormal operation

이러한 상황(b)에서는 데이터 오류가 발생한 경우이므로 아무런 데이터를 발생하지 않고 그동안 “0”의 값을 산출하여 특정주기를 일정하게 유지시켜주는 것을 확인하였다.

그림 8은 피보나치 타입 16 비트 난수 발생기를 4비트 4개의 LFSR로 구성한 시스템에 대한 모의실험 결과이다. 특정주기는 210을 유지하며 출력을 산출하는 경우가 정상적인데, 4비트 LFSR 중 3번째 LFSR에 이상이 발생하여 특정주기 내의 1/4에 대한 시간동안 출력이 산출되지 않고 있으며, 특정주기가 일정하게 유지되는 것을 확인하였다.

그림 9는 피보나치 타입 16 비트 난수 발생기를 8비트 2개의 LFSR로 구성하여 수행한 모의실험 결과이다. 특정주기는 595를 가지며 출력을 산출하는 경우가 정상적인데(a), 8비트 LFSR의 두 번째 LFSR(b)에 이상이 발생하여 반주기 동안 출력이 산출되지 않고 있다. 이러한 상황에서 데이터의 오류가 발생한 지점에 대해서는 아무런 데이터를 발생하지 않는 동시에 특정주기는 일정하게 유지되는 것을 확인하였다.

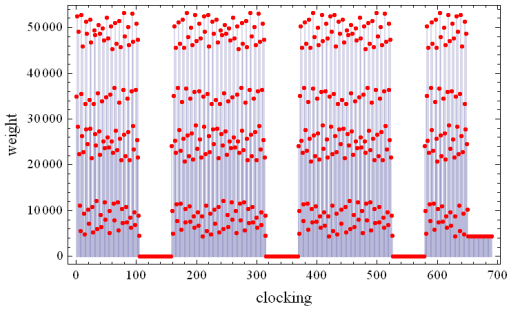
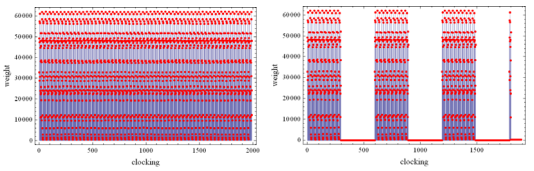


Fig. 8. 16 bits FLT-LFSR simulation result



(a) (b)

Fig. 9. 16 bits FLT-LFSR simulation result (a) during normal operation (b) in case of abnormal operation

본 논문에서는 기저가 4비트, 8비트인 LFSR을 이용하여 FLT-LFSR구조를 구성하여 시스템을 설계하였다. 시스템을 설계하여 그 결과를 확인한 결과, 각각의 기저 LFSR의 크기는 전체 FLT-LFSR의 주기를 결정짓는 주요한 요소이다. 이는 전체 시스템을 구성할 때, FLT-LFSR 알고리즘에서 기저의 영향을 다른 곳으로 전파시키지 않기 위하여, 원래 LFSR의 내용을 기본으로 세부 분할을 수행하였고, 이를 적절한 크기로 분배시켰으며, 다른 기저 LFSR에 영향을 주지 않도록 하였기 때문이다. 이러한 결과는 인접한 LFSR의 오동작이 전체 LFSR에 영향을 주지 않는다는 것을 의미하며 그 결과를 모의실험을 통하여 확인하였다.

5. 결론

IoT 환경에서 주요한 요소는 센서 시스템이다. IoT가 발전할수록 센서 시스템의 수는 매우 가변적이며 매우 복잡한 토포라지를 가지게 된다. 이러한 환경은 해킹 및 크래킹의 위험성을 더욱 증대시킬 수 있기 때문에 이에 대한 대비책이 중요하다. 이러한 중요한 시점에서 센서 시스템들의 수의 변화에 대하여 전체 시스템의 보안을 일정하게 유지시키는 것이 중요하다. 이러한 문제점을 해결하기 위하여 FLT-LFSR 구조를 제안하였다. IoT 센서 시스템의 가변 환경이거나 센서 시스템의 오동작 발생시, 특정 센서 시스템의 데이터 내용이 해킹 및 크래킹에 노출되거나 쉽게 파악될 수 있다. 그러므로 이러한 문제점이 발생하면 외부적으로 전체 주기의 변화를 가지게 된다. 제안된 FLT-LFSR 구조는 이러한 문제점을 해결하기 위하여 센서 시스템에 문제가 발생하여도 전체 시스템의 주기에 변화가 없고 문제가 발생된 부분에 대하여 아무런 동작을 수행하지 않도록 하여 IoT 시스템의 보안성을 유지시킬 수 있는 해법을 제시하였다. 이러한 방식은 다양한 암호방식을 갖추지 않고서도 정보보호에 대한 방어력을 키울 수 있는 장점이 있다.

향후, LFT-LFSR 구조는 센서 시스템에 OS가 탑재되어도 융통성 있게 시스템에 대한 보안을 유지할 수 있기 때문에 향후에 더욱 더 진가를 발휘할 것으로 생각한다.

References

[1] arduino concepts, https://www.arduino.cc/, 2017.

[2] intel edison IoT board spec., http://www. intel.com/content/www/us/en/do-it-yourself/edison.html, 2016.

[3] linux(debian, raspbean, ubuntu), http://www.linuxfoundation.org/, 2017. 10.

[4] Internet of things, http://www.kisa.or.kr/uploadfile/201306/201306101740531675.pdf, 2013.

[5] Rainer A. Rueppel, "Analysis and design of stream ci-phers", Springer-Verlag, NewYork, 1986.

[6] S. Mourad, Y. Zorain, "Principles of Testing Electronic Systems", John Wiley & Sons, 2000.

[7] X. Gu, M. Zhang, "Uniform random number generator using Leap-Ahead LFSR architecture", *2009 Int'l Conf. on Computers and Communication Security*, pp. 150-154, 2009.

[8] R. Lidl, H. Niederreiter, "Introduction to Finite Fields and Their Application", Cambridge University Pre-ss, Cambridge, 1986.

[9] A. D. Porto, F. Guida, E. Montolivo, "Fast Algorithm for Finding Primitive Polynomials over GF(q)", *Elect. Lett., B28.(2)*, pp. 118-120, 1992.
DOI: https://doi.org/10.1049/el:19920073

이 선 근(Seon-Keun Lee) **[종신회원]**

- 1997년 8월 : 원광대학교 전자공학과(공학석사)
- 2003년 2월 : 원광대학교 전자공학과(공학박사)
- 2006년 4월 ~ 2008년 2월 : 원광대학교 전자공학과 교수
- 2017년 3월 ~ 현재 : 전북대학교 기계시스템공학부 강의전담교수

<관심분야>
IoT, 임베디드시스템, H/W 암호시스템, 프로세서설계