# 고속 병렬형 PS-LFSR을 적용한 u-헬스케어 보안 시스템 구현

김낙현* · 이영동** · 김태용** · 장원태** · 이훈재***

## Implementation of u-Healthcare Security System by applying High Speed PS-LFSR

NackHyun Kim* · YoungDong Lee** · TaeYong Kim** · WonTae Jang** · HoonJae Lee***

본 연구는 2010년도 한국연구재단 지원과제에 의한 연구 결과임

요 약

유비쿼터스 컴퓨팅 기술과 헬스케어 기술이 접목되어 시간과 장소에 구애받지 않고, 지속적인 건강관리가 가능한 u-헬스케어 기술이 급부상하고 있으며, 한국의 최첨단 정보 환경을 기반으로 하여 향후 급증할 의료수요에 대처하기 위한 u-헬스케어 기반기술이 절실한 실정이다. 특히, u-헬스케어 분야에서 다루는 정보는 주로 건강이나 생명과 밀접한 관계가 있는 관련 정보로서 극히 개인적인 사항을 주로 포함한다. u-헬스케어 서비스가 보안 및 프라이버시 측면에서 많은 취약점과 위협이 존재한다는 점을 볼 때, 데이터 보호를 위한 기술적 대안이 기본적으로 요구된다. 이에 본 논문에서는 안전한 u-헬스케어 시스템을 위해 u-헬스케어 센서모듈을 설계 및 제작하고, USN의 안전성 및 데이터 보호를 위해 NLM-128 알고리즘을 TinyOS상에서 소프트웨어적으로 구현하여 USN 센서노드에 탑재하였다. 그리고 NLM-128 알고리즘에 고속 병렬형 PS-LFSR을 적용하여 암호화 시간을 단축 시켰다. u-헬스케어 응용을 위한 USN 보안센서노드는 환자의 몸에 부착되어 각종 생체 신호를 계측할 수 있으며, 계측된 생체신호들은 무선메쉬네트워크(Wireless Mesh Network)를 통해 통합서버로 전송되며, 그 결과는 실시간으로 모니터링이 가능하였다.

ABSTRACT

The emerging of ubiquitous computing and healthcare technologies provides us a strong platform to build sustainable healthcare applications especially those that require real-time information related to personal healthcare regardless of place. We realize that system stability, reliability and data protection are also important requirements for u-healthcare services. Therefore, in this paper, we designed a u-healthcare system which can be attached to the patient's body to measure vital signals, enhanced with USN secure sensor module. Our proposed u-healthcare system is using wireless sensor modules embedded with NLM-128 algorithm. In addition, PS – LFSR technique is applied to the NLM-128 algorithm to enable faster and more efficient computation. We included some performance statistical results in term of CPU cycles spent on NLM-128 algorithm with and without the PS-LFSR optimization for performance evaluation.

키워드

유비쿼터스 센서 네트워크, 정보보호, 스트림 암호, PS-LFSR

Key word

Ubiquitous Sensor Networks, Information security, Stream cipher, PS-LFSR

* 준회원 : 동서대학교 유비쿼터스 IT학과
** 정회원 : 동서대학교 컴퓨터정보공학부
*** 정회원 : 동서대학교 컴퓨터정보공학부 (교신저자, hjlee@dongseo.ac.kr)

접수일자 : 2010. 07. 27
심사완료일자 : 2010. 08. 31

## Ⅰ. 서 론

USN(ubiquiotous sensor network)은 다수의 센서 노드로 구성된 무선 네트워크로써 다양한 위치에 설치된 센서 노드들로부터 사람과 사물, 그리고 환경 정보를 인식하고, 인식한 정보를 통합·가공해 언제, 어디서나, 안전하고 자유롭게 이용할 수 있게 하는 정보서비스 인프라를 뜻한다[1]. 유비쿼터스 센서네트워크 기술은 언제, 어디서나 시공간의 제약 없이 컴퓨터 환경에 접속할 수 있는 유비쿼터스 패러다임이 확대되면서 전 세계적으로 활발하게 연구되고 있는 기술 분야중의 하나이다. 그리고 기술적으로 RFID(radio frequency identification), WSN(wireless sensor network) 등의 내용을 포함하고 있으며, 관련 소프트웨어 플랫폼으로는 TinyOS, Nano Qplus, Contiki, LiteOS등이 있으며, 다양한 표준과 프로토콜을 지원한다. 관련 표준으로는 IETF의 6LoWPAN, ROLL, CoRE와 함께 ZigBee, Wireless HART, ISA 100 등이 있다.

센서네트워크의 기술은 본질적으로 무선통신 인프라를 기본으로 하고 있으며, 수많은 센서노드들이 외부 환경 정보를 센싱하고, 센서 노드간에는 IEEE 802.15.4 [2] 무선 통신을 이루어 정보를 전송한다. 센서노드 간 통신 정보에 대한 기밀성이 제공되지 않는다면 전송되는 데이터들은 공격자에 의해 쉽게 노출된다. 따라서, 센서 노드간의 통신되는 데이터에 대한 암호화를 통해 기밀성의 보장은 필수 요소이다.

특히, u-헬스케어 서비스는 타 유비쿼터스 컴퓨팅 기술 분야에 비해 다루어지는 정보의 대부분은 개인 의료 데이터로, 개인의 생명과 직접적인 연관성을 띄고 있는 극히 개인적인 사항을 주로 포함한다[3]. 따라서 이와 같은 정보가 노출되어 조작 및 악용될 경우 개인의 생명의 위협은 물론, 사회적으로도 큰 경제적 손실을 초래 할 수 있다.

이와 같이 u-헬스케어 서비스가 보안 및 프라이버시 측면에서 많은 취약점과 위협이 존재한다는 점을 볼 때, 생체정보의 수집, 전송 및 저장에서의 높은 신뢰성을 확보하기 위하여 암호화에 관한 연구가 절실히 필요하다.

이에 본 논문에서는 안전한 u-헬스케어 시스템을 위해 u-헬스케어 센서 모듈을 설계 및 제작 하였고, USN의 자원적인 제약 사항을 고려해 저전력·경량 암호 알고리즘인 NLM-128 암호 알고리즘을 TinyOS상에서 소프트웨어적으로 구현하여 USN 센서노드에 탑재하였다. 그리고 고속 병렬형 PS-LFSR을 적용하여 데이터의 암호화 시간을 단축하여, u-헬스케어 시스템의 성능 향상을 확인 하였다.

## Ⅱ. u-헬스케어 보안 시스템

본 논문에서 제안하는 안전한 u-헬스케어를 위한 보안 시스템의 전체적인 구조는 그림 1과 같다. USN 센서노드, 센서 모듈, 운영/관리서버, 보안/인증 서버, 통합 서버로 구성된다.

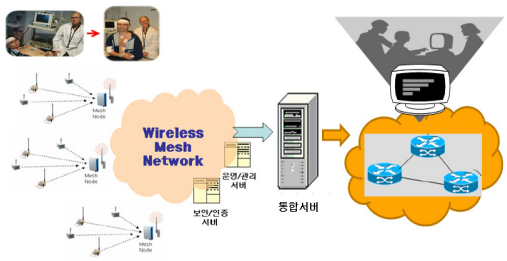


그림 1. u-헬스케어 시스템 구조
Fig. 1 System architecture of u-Healthcare

### 2.1 USN 센서 노드

제작한 생체센서모듈로부터 계측된 생체신호를 무선으로 전송하기 위하여 USN 센서노드를 이용하였다. USN 센서노드의 내부 하드웨어 블록 다이어그램은 그림 2에 나타내었다.

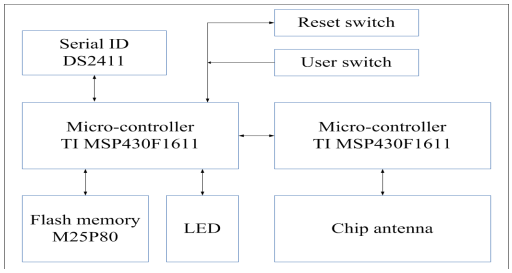


그림 2. 센서노드 내부 하드웨어 블록 다이어그램
Fig. 2 Block diagram of wireless sensor node

USN 센서노드는 MSP430F1611(TI, USA) 마이크로 컨트롤러와 IEEE 802.15.4를 적용한 RF트랜시버 (CC2420, Chipcon AS, Norway)[4], 외부 플래시메모리 (M25P80, STMicroelectronics, USA)로 구성하였다. MSP430F1611은 16bit RISC로 내부에 48KB의 프로그램 메모리와 10KB의 램을 가지고 있으며, 12비트 ADC 8채널을 가지고 있다. RF트랜시버 모듈로 사용된 CC2420은 IEEE 802.15.4/ZigBee를 지원하는 RF 칩으로 2400-2483.5 MHz 대역을 지원하며, 직접시퀀스 대역확산(Direct Sequence Spread Spectrum)방식으로 동작하며, O-QPSK 변조 방식과 250 Kbps 전송률을 지원이 가능하다.

무선통신부는 송수신 형태 및 주파수, 기능에 따라 다양한 형태로 이루어지고 있으며, IEEE 802.15.4-2006 표준과 ZigBee를 기반으로 하여 제안된 주파수 대역은 868-868.8 MHz 대역의 유럽 주파수 대역과 902-928 MHz 대역의 북미 주파수 대역, 그리고 ISM 밴드로서 세계 공용으로 사용 가능한 2.45GHz 대역으로 구분하고 있다. 무선통신부의 RF는 direct conversion 또는 Low-IF 구조로 송수신 방식을 제안하여 저전력을 위한 회로 설계로 시스템 구동이 이루어지며, modem에서는 BPSK, O-QPSK, ASK 등 다양한 변/복조 방식의 지원 및 동기 알고리듬을 구현하고 있다. MAC의 경우, OS 독립적인 스케줄러 관리 및 RF와 모뎀의 레지스터 세팅 기능을 제공한다. 현재, 무선통신부에서의 low duty cycle 적용 및 wake-up circuit 기술 등의 USN 센서노드의 전류 소모를 감소하기 위한 저전력 기술 개발이 진행되고 있다.

### 2.2 u-헬스케어 센서모듈

본 논문에서는 u-헬스케어 시스템 구현을 위해 심전도와 가속도 센서를 함께 갖춘 통합 모듈 형태의 생체신호 측정용 센서모듈을 구현하였다. 심전도 센서부는 USN 센서노드 하단의 51핀 확장커넥터를 통해 상호 연결되며, 인체의 심장 상태를 측정할 수 있도록 설계 및 제작하였다.

1개의 계측 증폭기와 다수의 OP-AMP를 이용하여 심전도 측정회로를 적용한 센서보드로서 저전력이며, 작은 사이즈로 사용자가 편리하게 개인의 건강상태를 측정할 수 있도록 하였다.

표 1. USN 센서 노드 세부 사양
Table. 1 Specification of the USN sensor node

| MCU | MSP430F1611 |
|---|---|
| RF transceiver | CC2420 |
| Band width | 2.4GHz |
| RF range | ≈ 100m |
| Interface | RS-232 Interface(RTS/CTS-type) |
| POWER | 2.5V - 3.9V<br>(From battery or Cellular phone) |

미세한 인체 신호를 증폭하기 위한 증폭부 설계와 잡음 신호를 제거하기 위한 필터링부를 설계하고, 심전도 센서 증폭부와 필터부 기능 구현을 위해 전극에서 유도된 전압은 차동증폭기로 구성하였다. 심전도 측정뿐만 아니라 가속도 센서를 사용하여 인체의 움직임 신호의 측정이 가능하다. 이러한 생체센서의 전원공급과 측정된 생체신호의 무선전송을 위하여 USN 센서노드를 사용하였으며, 센서노드의 아날로그 신호 입력부에 생체센서를 연결하여 시스템을 구성하였다.

### 2.3 NLM-128 암호 알고리즘

NLM-128[5]은 새로운 스트림 암호인 NLM 시리즈 중 하나로, 127 bit의 LFSR 한 개와 129 bit의 NFSR 하나로 구성된다. 또한 이들을 합쳐 256 bit의 내부 메모리를 가지며, 128 bit 키와 128 bit의 초기화 값으로 내부 메모리를 채우게 된다. 그리고 NLM 생성기는 LFSR, NFSR 수열과 carry와 메모리 수열의 결합에 의해 키 수열이 출력되며, 원시 다항식 Pa(x)와 de Bruijn [6]의 기약 다항식인 Pb(x), 두 개의 다항식을 가지게 된다. NLM-128은 2256 비도 수준(security level)을 갖는 스트림 암호로서, 안전성 및 구현 용이성 등의 특징을 갖기 때문에 RFID/USN 등의 저전력형 적용이 용이한 암호이다.

두 개의 키 값 $k$와 초기화 벡터 $iv$는 각각 128 비트의 크기를 가지고 함께 256 비트의 내부 메모리를 가지게 되며 또한, 초기화 프로세스는 키 재생성에 사용된다. 키 수열 생성기의 초기 상태를 생성하기 위하여 자체적으로 생성기를 두 번 사용하며, $La$의 연산을 시작하게 되면 $La = (k \oplus iv) \bmod 2^{127}$ 식에 따라 128 비트의 키(key) 값 $k$와 128 비트의 초기화 값 $iv$를 XOR하여 $La$의 값을 얻게 된다.

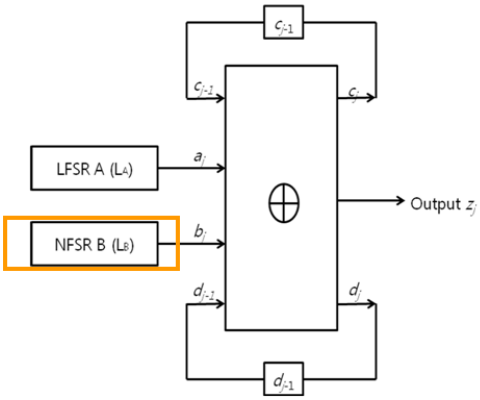


그림 3. NLM 암호 알고리즘
Fig. 3 NLM encryption algorithm

129 비트 *Lb* 초기 상태는 128 비트 키(key) *k*를 1 비트 좌측 이동하고 우측에 "0"을 두며, 또한 128 비트 초기값(*iv*)의 왼쪽에 "0"을 추가하여 129 비트 값을 만든 후에, 각각의 129 비트 두 레지스터를 비트 별 XOR 연산하여 초기화 시키게 된다. 즉, $Lb=(k<<1)\oplus(0|iv)$ 이렇게 초기화시킨 NLM-128 암호 알고리즘을 통하여 256 비트의 출력 문자열을 생성한다. 암호의 재사용을 위하여, 이 출력 문자열의 처음 128 비트를 *La*의 초기 상태를 채우는데 사용하고 나머지 129 비트는 *Lb*의 초기 상태를 채우는데 사용한다. 두 번째로 실행되는 암호 알고리즘은 257 비트 길이의 문자열을 출력하며, 이를 이용하여 다음 번 암호화 실행 시 새로운 키 수열 생성을 위하여 키 수열의 초기 상태로 사용한다. 이때 사용된 NFSR B 레지스터는 키 수열 발생기의 비선형성을 높이기 위하여 de Bruijn[6] 수열을 사용하였으며, Park & Chang[7]이 제시한 효과적인 de Bruijn 수열 발생기를 사용하였다.

- 키 수열의 특성

PN 이진 수열들을 위한 세 가지 기본 요구사항은 긴 주기, 높은 선형복잡도, 좋은 통계 특성이며, 긴 주기는 암호화된 긴 메시지를 사용할 때 동일한 키 수열의 재사용을 방지하고, 높은 선형복잡도는 Berlekamp-Massey 알고리즘[8]을 이용한 공격에 견딜 수 있도록 한다. 마지막으로 좋은 통계적인 특성은 키 수열이 "0"과 "1" 중 어느 한 방향으로 치우친 취약점을 이용한 공격에 견딜 수 있게 한다.

NLM-128 키 수열 특성을 관측하기 위한 실험은 표 2와 같다. 짧은 길이에 대한 예제는 서로 다른 길이의 두 LFSR을 가지며, 각각의 쌍에 대해서 서로 다른 귀환 다항식을 선택되었다. 실험에서 귀환 다항식 탭 위치 선택은 키 수열 특성에 큰 영향이 없으며, LFSR 길이는 각각의 쌍(예, 5, 7)에 대하여 짧은 길이에 대해서 모든 초기 상태로 시뮬레이션 하였다. 예를 들면, 레지스터 길이 5, 7을 선택할 경우 결과에 따른 선형복잡도는 3,814이다. 주기와 선형복잡도에 대한 시뮬레이션 결과는 표2와 같다. 표에서 얻어진 값들로부터 선형복잡도와 주기의 방정식은 다음과 같다.

표 2. NLM-128 키수열에 대한 선형 복잡도, 주기 검증(짧은 단수)
Table. 2 linear complexity, period of NLM-128 key stream

| Register Lengths | Linear Complexity | Period |
|---|---|---|
| 5, 7 | 3,814 | 3,968 |
| 7, 7 | 15,622 | 16,256 |
| 5, 9 | 15,872 | 15,872 |
| 7, 8 | 32,512 | 32,512 |
| 5, 11 | 53,487 | 63,488 |
| 7, 9 | 65,205 | 65,204 |
| 7, 10 | 130,046 | 130,048 |
| 9, 9 | 261,633 | 261,632 |

따라서 LNM-128에 대한 주기(P)와 선형복잡도(*LC*)는 아래 식(1), (2)와 같다.

$$P=(2^{L_1}-1)(2^{L_2}) \quad (1)$$

$$LC\approx(2^{L_1}-1)(2^{L_2}) \quad (2)$$

[특성] NLM-128(n = 256)에 대한 선형 복잡도의 최소값 및 주기값은 식 (3), (4)와 같다.

$$LC\approx(2^{127}-1)\times(2^{129})\approx 2^{256} \quad (3)$$

$$P=(2^{127}-1)\times(2^{129})\approx 2^{256} \quad (4)$$

NLM-128의 설계 기준강도는 $2^{256}$이며, TMTO(time memory tradeoff) 공격에 대한 안전성을 고려하면 $2^{128}$이 된다. 여러 가지 공격에 대하여 기본적인 키 수열특성은

큰 선형복잡도 및 긴 주기 때문에 안전하다.

### 2.4 PS-LFSR

고속 통신의 발달로 데이터 암호화의 고속화 역시 필수 요소로 자리 잡고 있다. 이에 본 논문에서는 LFSR을 고속화하기 위하여 한 클럭에 m번의 이동이 이루어지는 고속 병렬형 PS-LFSR (parallel-shifting LFSR)[9]을 본 실험에 적용하였다.

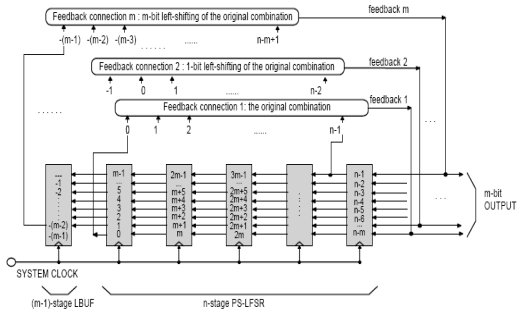


그림 4. (n,m) PS-LFSR
Fig. 4 (n,m) PS-LFSR

일반적으로 LFSR은 최대 주기성을 갖으며 소프트웨어나 하드웨어로 구현이 용이하기 때문에 스트림 암호의 키 수열 발생기(Key stream generator)나 확산 스펙트럼 통신의 의사 잡음 발생기(pseudo noise generator)등에 많이 사용된다. 고속 스트림 암호 구현을 위한 기본 요소로서, 고속 병렬형 PS-LFSR은 그림 4와 같이 표시 할 수 있다. n-단 LFSR을 기존의 LFSR과 동일한 원리이며, (m-1)-단 LBUF(left buffer)는 다음 클럭에서 입출력 값을 저장할 버퍼의 역할을, feedback array는 m-병렬 귀환 함수들의 배열을 의미한다. 모든 비트가 m-비트 단위로 병렬 이동(parallel shifting) 하기 위하여 병렬 경로가 구성되어야 하며, 귀환 탭에서도 m-묶음의 XOR 조합 연산을 거쳐 feedback array에 모인 후 LFSR의 m-비트 블록 부분으로 좌측 이동되고, 계속해서 왼쪽으로 블록 크기 (m) 단위 만큼 병렬 이동된다. 결국 한 클럭에 m-비트 이동 후 m-비트(또는 그 이하) 출력을 동시 생성하는 발생기로서 긴 주기에서의 출력 수열은 단 한번만 사용되므로 랜덤특성, 주기 등 비도 특성이 일반 LFSR과 동일함을 알 수 있다. 또한 비트 단위의 출력을 발생하는 일반 LFSR과 비교할 때 PS-LFSR은 암호화 처리 속도가 m배 빨라질 수 있다.

## Ⅲ. 실험 및 결과

본 논문에서는 u-헬스케어 보안 시스템 구현을 위해 심전도와 가속도 신호 측정용 통합센서모듈을 구현하고 암호알고리즘을 적용하여 안전한 생체신호 전송이 가능하도록 하였다. 구현된 통합센서모듈의 레이아웃은 그림 5에 나타내었다.

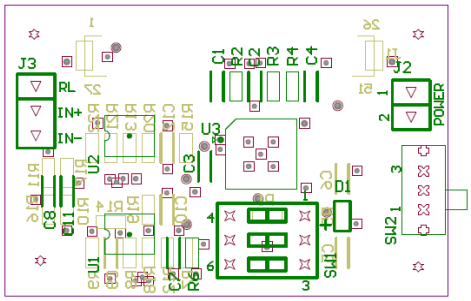


그림 5. 통합센서모듈 레이아웃
Fig. 5 Layout of integrated sensor module

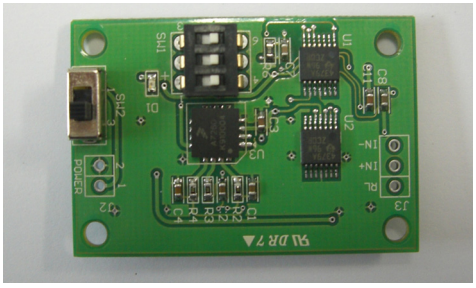

그림 6. 심전도, 가속도 통합 센서모듈
Fig. 6 Integrated sensor module with ECG and accelerometer

설계한 통합센서모듈을 그림 6과 같이 제작하였으며, 심전도 센서부와 가속도 센서부를 통합 구성하였다. 그림 7은 본 논문에서 사용한 USN 센서노드와 제작한 통합센서모듈을 장착한 모습을 나타내며, 측정된 심전도 및 가속도 센서 데이터는 USN 센서노드의 확장 커넥터를 통해 원격지 통합서버로 전송될 수 있었다. 이러한 u-헬스케어와 관련된 생체정보들을 안전하게 전송하기

위하여 NLM-128 알고리즘을 USN 센서노드에 탑재하여 기존 USN 센서노드와 차별화된 보안 USN 센서노드로서 적용이 가능하도록 하였다.

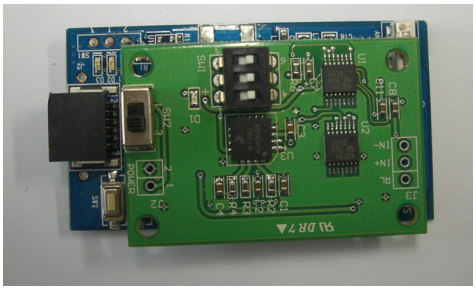

그림 7. 센서노드와 통합 센서 모듈 장착 모습
Fig. 7 Sensor node and integrated sensor module

그림 8은 NLM-128 암호 알고리즘의 구동 확인을 위한 테스트 환경을 도식화한 그림이다. 보안/인증서버인 PC와 베이스 스테이션인 *BS*와는 USB포트를 이용한 유선으로, 베이스 스테이션과 센서노드인 *SN*간은 ZigBee 무선통신방식을 적용 하였다. 사용자가 PC에서 입력한 임의의 메시지 *M*은 베이스 스테이션으로 전송되고, 베이스 스테이션에서는 수신받은 메시지 *M*을 암호화한 후 암호화된 메시지 *C*를 *SN*에게 전송한다. 그리고 센서노드는 메시지 *C*를 복호화한 *M'*를 생성하고 *C*와 *M'*을 베이스 스테이션을 통해 PC로 전송한다. PC에서 *M*과 *M'*를 비교하여 NLM-128암호 알고리즘이 정상적으로 설계된 것을 확인 할 수 있다. 그 결과는 그림 9에서 나타내었다.

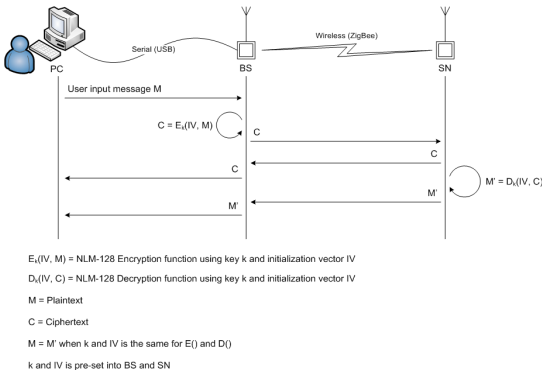


그림 8. 시뮬레이션 흐름도
Fig. 8 Simulation flowchart

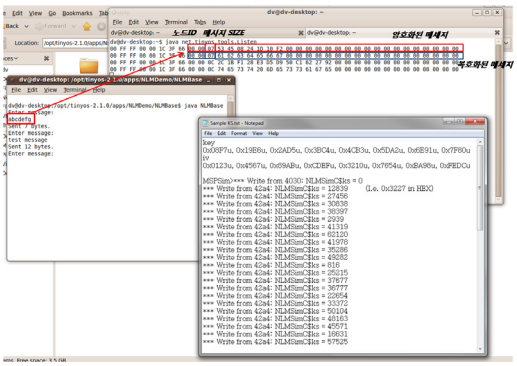

그림 9. 시뮬레이션 결과
Fig. 9 Simulation results

표 3은 본 논문에서 제안한 고속 병렬형 PS-LFSR을 적용한 센서노드에서의 메모리 사용 정보에 대한 결과이다. 센서노드가 부팅시 기본적으로 사용하고 있는 ROM과 RAM은 각각 1398 바이트와 4 바이트 이다. 실험결과 NLM-128 알고리즘을 적용한 후 사용 ROM과 RAM은 각각 3174 바이트 와 128 바이트로 나타났다. 그리고 PS-LFSR을 적용 시킨 후 ROM과 RAM의 사용 정보는 5664 바이트와 139 바이트로 증가한 것을 확인 할 수 있다.

표 3. 메모리 사용 정보 (Byte)
Table. 3 Status memory

| Memory Utilization | Base Node | NLM -128 | NLM-128 using PS-LFSR |
|---|---|---|---|
| ROM (Debug) | 2142 | 4206 | 6644 |
| ROM (Optimized) | 1398 | 3174 | 5664 |
| RAM | 4 | 128 | 139 |

본 실험에서는 28 바이트 크기의 난수를 평문으로 설정하고, 각각 1000번의 반복 실행을 통하여 평균치를 표 4에 표기 하였다. 그리고 반복 실행시마다 초기화 벡터 *iv*를 초기화 하여 재설정함으로써, 재 동기화 시간을 확인 할 수 있다. 초기 설정 및 키 스케줄링과 암호화 부분에서는 표 4와 같은 결과로 PS-LFSR을 적용 한 뒤의 CPU cycle이 현저하게 줄어드는 것을 본 실험을 통해 확인 할 수 있었다.

표 4. 프로파일 데이터 개요
Table. 4 Summary of profile data

| Operation (CPU Cycle) | NLM-128 | NLM-128 using PS-LFSR |
|---|---|---|
| Initialization/Key scheduling (per key/IV) | 227059 | 75401 |
| Encryption (per byte) | 3539 | 804 |

## Ⅳ. 결 론

본 논문에서는 u-헬스케어 보안 시스템 구현을 위해 심전도와 가속도 신호 측정용 통합센서모듈을 구현하고, u-헬스케어와 관련된 생체정보들을 안전하게 전송하기 위하여 NLM-128 알고리즘을 USN 센서노드에 탑재하여 기존 USN 센서노드와 차별화된 보안 USN 센서노드로서 적용이 가능하도록 하였다. USN 환경에서 안전한 생체신호 전송을 위한 실험은 전송할 모든 생체데이터들을 암호화 한 뒤 그 암호화 데이터를 베이스 스테이션으로 전송하였으며, 베이스스테이션에서는 수신받은 암호문을 복호화 하여 원래 전송하고자 하는 데이터를 안전하게 수신할 수 있었다. 또한 본 논문에서 제안한 고속 병렬형 PS-LFSR을 적용함으로서 전송 받은 데이터에 대한 암호화 속도를 향상시킬 수 있음을 실험 결과로 확인하였다.


### 감사의 글

본 연구는 2010년도 한국연구재단 지원과제에 의한 연구 결과임


### 참고문헌


[1] 이신경, 이해동, 정교일, 최두호 “안전한 USN을 위한 정보보호기술 동향,” 전자통신동향분석 제 23권, 제 4호, pp. 72-79, 2008.

[2] http://www.ieee802.org/15/pub/TG4.html

[3] 송지은, 김신효, 정명애, 정교일, “u-헬스케어 보안 이슈 및 기술 동향,” 전자통신동향분석 제 22권, 제 1호, pp. 119-129, 2007.

[4] Chipcon, Inc., “CC2420 Data Sheet,” http://www.chipcon.com/files/CC2420_Data_Sheet_1_3.pdf

[5] HoonJae Lee, SangMin Sung, and HyeongRag Kim, “NLM-128, An Improved LM-type Summation Generator with 2-bit memories,” *Proceedings of 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT),* pp. 577-582, 2009.

[6] A.biryuikov and A.Shamir, ″Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers,″ *Advances in Cryptology, Proceedings of ASIACRYPT00, LNCS 1976,* pp.1-13, 2000.

[7] T. Chang, B. Park, Y.H.kim, ″An Efficient Inplementation of the D-Homomorphism for Generation of de Bruijin Sequences,″ *IEEE Transactions on Infromation Theory,* vol. 45, no. 4, pp. 1280-1283, 1999.

[8] J. L. Massey, ″Shift-Register Synthesis and BCH Decoding,″ *IEEE Trans. Theo,* vol 1. IT-15, no.1, pp. 122-127, 1969.

[9] Hoonjae Lee, and Sangjae Moon “Parallel stream cipher for secure high-speed communications,” *Signal Processing,* pp. 259-265, 2002.


### 저자소개


**김낙현(Nack Hyun Kim)**

2009년 동서대학교 정보네트워크 공학과(공학사)
2009년～현재 : 동서대학교 유비쿼터스 IT학과 (석사과정)

※관심분야 : 정보보안, 암호이론

**이영동(YoungDong Lee)**

2004년 동서대학교 정보통신공학과(공학사)
2006년 동서대학교 컴퓨터 네트워크학과(공학석사)
2009년 동서대학교 유비쿼터스IT학과(공학박사)
2009년~현재 : 동서대학교 BK21 u-헬스케어사업팀 연구교수
※관심분야 : 유비쿼터스 헬스케어, 무선센서네트워크

**김태용(TaeYong Kim)**

1993년 부경대학교 전자공학과 (공학사)
1997년 오카야마대학 전기전자 공학과(공학석사)
2001년 오카야마대학 자연과학연구과(공학박사)
2002년~현재 동서대학교 컴퓨터정보공학부 교수
※관심분야 : 무선통신, 수치해석, 미들웨어 응용

**장원태(WonTae Jang)**

한국해양정보통신학회논문지 제14권 제4호 참조

**이훈재(HoonJae Lee)**

1985년 경북대학교 전자공학과 졸업 (학사)
1987년 경북대학교 전자공학과 졸업 (석사)
1998년 경북대학교 전자공학과 졸업(박사)
1997년~1998년 국방과학연구소 선임연구원
1998년~2002년 경운대학교 조교수
2002년~현재 동서대학교 컴퓨터정보공학부 부교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격