KIPS Tr. Comp. and Comm. Sys.
Vol.3, No.10 pp.323~328 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2014.3.10.323

A Design of Secure Electronic Health Information Management Protocol in the Internet of Things Environment

Jeong Hyo Park† · Kim Nak Hyun†† · Yong Hoon Jung††† · Moon Seog Jun††††

ABSTRACT

ZigBee based on the most vulnerable part of u-Healthcare system that uses the ZigBee communication is the wireless section. ZigBee communication sectors to identify vulnerabilities in this paper, we propose to compensate. ZigBee has been raised from the existing vulnerabilities organize and ZigBee also uses the 64bit address that uniquely identifies a vulnerability that was defined as exposure. And to prevent the exposure of a unique identifying address was used to address a temporary identification. ZigBee security services, the proposed system during the Network Key for encryption only use one mechanism of Residential Mode is used. Residential Mode on all nodes of the entire network because they use a common key, the key is stolen, your network's security system at a time are at risk of collapse. Therefore, in order to guard against these risks to the security policy Network Key updated periodically depending on the method used to. The proposed evaluation and comparative analysis of the system were exposed in the existing system can hide the address that uniquely identifies a public key Network Key also updated periodically, so that leaks can occur due to reduced risk.

Keywords : U-Healthcare, ZigBee, Wireless Communication Vulnerabilities, Unique Identification of a 64bit Address, Temporary Identification Address, Security Policy

사물 인터넷 환경에서 안전한 전자의료정보 관리 프로토콜 설계

박 정 효† · 김 낙 현†† · 정 용 훈††† · 전 문 석††††

요 약

지그비 기반의 U헬스 시스템에서 가장 취약한 부분인 지그비 통신을 사용하는 무선 구간에서의 취약점을 분석하고 해당 취약점을 보완하기 위해 본 논문을 제안한다. 지그비에서 기존에 제기되었던 취약점들 이외에 본 논문에서는 지그비 통신에서 사용하는 64bit의 고유식별주소를 노출하는 것 자체를 취약점으로 규정하고 고유식별주소의 노출을 막기 위해 임시식별주소를 사용하였다. 제안 시스템은 지그비 보안 서비스 중에서 암호화를 위해 하나의 네트워크 키만을 사용하는 레지덴셜 모드의 메커니즘을 사용한다. 레지덴셜 모드는 전체 네트워크의 모든 노드들이 하나의 공통키를 사용하기 때문에 키가 유출될 경우 지그비 네트워크의 보안체계가 한 번에 무너질 위험성이 있다. 그러므로 이러한 위험에 대비하기 위해 네트워크 키를 보안 정책에 따라서 주기적으로 갱신하는 방식을 사용했다. 본 제안 시스템의 평가와 비교 분석에서는 기존 시스템에서 노출되었던 고유식별주소를 숨길 수 있고, 공용 네트워크 키 또한 주기적으로 갱신하므로 키 유출로 인해 발생할 수 있는 위험성을 감소시켰다.

키워드 : U헬스, 지그비, 무선 통신 구간 취약점, 64bit의 고유식별주소, 임시식별주소, 보안정책

1. 서 론

u-Healthcare는 IT기술과 선진의료기술이 결합된 고부가가치 융·복합 산업으로 환자의 생체신호 및 건강정보를 측정하고 유무선 네트워크를 통하여 데이터를 의료기관에 전송한 후 분석하고 다시 피드백해줌으로써 환자의 질병에 대한 원격 관리가 가능할 뿐만 아니라, 일반인의 건강관리도 가능한 서비스로 정의하고 있다[1].

u-Healthcare 서비스는 의료비 절감과 사회경제적 비용 감소, 시장규모 증가 등의 경제·산업적 파급효과, 공공의료 서비스와 예방관리 보건 등에 관한 사회·정책적 효과를 기대할 수 있는 가장 효과적인 대안으로서 많은 국가에서 추진하고 있다[7].

특히, 우리나라에서 u-Healthcare 서비스의 도입은 신기술의 적용과 기반 연계기술 확보 및 확산 등의 기술적 파급효과를 기대할 수 있어 유망한 신성장 동력원으로서 시장규

† 정 회 원 : 숭실대학교 컴퓨터통신학과 박사수료
†† 정 회 원 : 숭실대학교 컴퓨터통신학과 박사과정
††† 준 회 원 : 숭실대학교 컴퓨터학과 박사
†††† 종신회원 : 숭실대학교 컴퓨터학과 교수
Manuscript Received : September 2, 2014
Accepted : October 8, 2014
* Corresponding Author : Jeong Hyo Park(helios914@ssu.ac.kr)

모가 급속히 상승할 것으로 예측하고 있고, 노인환자를 위한 원격모니터링으로 연간 1.4조 원의 순편익이 발생하는 것으로 보고 있다. 따라서 그동안 u-Healthcare 서비스를 활성화하기 위하여 정부 차원의 시범사업과 함께 법제도, 기술표준화, 서비스모델 개발 등 다양한 분야에서 관련 연구가 진행되어왔다[2].

또한, u-Healthcare 분야의 성장 가능성이 높아짐에 따라 주요 선진국들은 고령화 사회 대비 및 의료비 절감, 사회복지 서비스의 일환으로 국가적 차원의 전략 프로젝트로 u-Healthcare를 추진 중에 있다[5].

u-Healthcare에서 생체정보를 측정하여 전송하는 센서 네트워크 환경은 Bluetooth나 ZigBee를 고려할 수 있는데 전력소모량이 더 적은 ZigBee가 u-Healthcare 환경에 더 적합하다고 볼 수 있다. 하지만 ZigBee와 같은 센서 네트워크는 무선 통신 특성 때문에 전송데이터의 기밀성 보호에 취약점을 가지고 있다[5]. 또한 센서 네트워크 환경에서 전송되는 데이터에 각 센서노드의 고유식별값이 꼬리표처럼 붙어 다닌다고 할 수 있는데, 이러한 데이터 전송과 식별 방식은 개인 프라이버시를 침해할 위험요소로 다가올 수 있다.

2. ZigBee의 취약점

IEEE 802.15.4를 포함한 ZigBee 표준 보안 서비스에서 확실한 정의가 내려져있지 않은 부분에 대해 서술하고, 본 논문에서 해결하고자 하는 취약점에 대한 내용을 설명한다.

ZigBee 보안 표준에서는 키 설정 방법에 대한 정의가 없다. 모든 키의 설정을 통제할 수 없고 초기 설정과정에서 키 유출에 위협이 있다.

링크 키와 네트워크 키를 선택하는 과정에서 비용과 보안에 대한 딜레마가 있다. 링크 키는 네트워크의 모든 노드들 사이에서 1:1의 암호화 키를 설정하는 것이고, 이에 대한 키 교환, 저장, 관리 등의 비용적인 문제가 발생한다. 네트워크 키는 하나의 PAN(Personal Area Network)에서 공통의 네트워크 키를 사용하여 암호화 통신 채널을 설정하는 방식이다.

새로운 노드가 네트워크에 접근할 때 키 분배에 대한 취약점이 발생한다. 네트워크에 새로운 노드가 접근하여 통신하고자 할 때, 마스터 키를 분배하는 과정에서 안전하지 않은 채널을 사용하여 마스터 키를 전송하기 때문에 이러한 취약점이 발생한다[17].

2.1 ZED(ZigBee End Device) 인증 문제

ZED는 ZigBee Network에 합류하기 위하여 Fig. 1과 Fig. 2와 같은 과정을 거친다.

보안 모드에 따라 새로운 디바이스가 접근할 때 네트워크 키를 전송하는 Residential Mode와 마스터 키를 전송하는 Commercial Mode로 나눌 수 있다. ZigBee Alliance에서는 Trust Center를 사용하여 네트워크에 접근하는 새로운 노드의 가입을 수락하거나 거절하는 방식을 사용하도록 권고하고 있다[13].

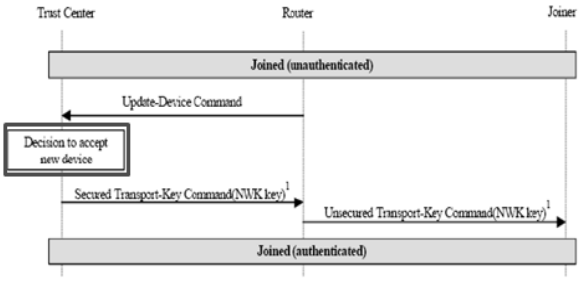

Fig. 1. An Authentication Process of Residential Mode

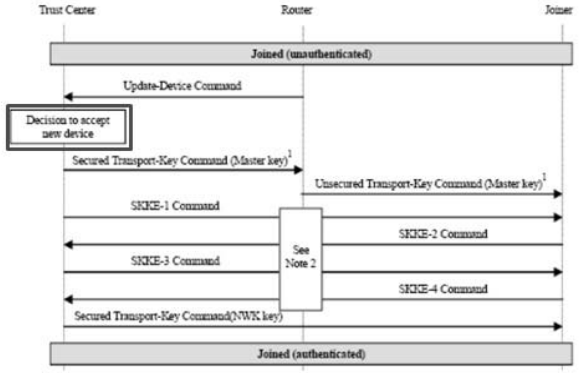

Fig. 2. An Authentication Process of Commercial Mode

2.2 키 노출 문제

ZigBee는 대칭키암호방식인 AES(Advanced Encryption Standard) 암호화알고리즘을 사용하여 안전한 통신을 수행한다. ZigBee에서 사용되는 키는 Link Key, Network Key가 있다. Link Key를 사용하여 각 노드 간에 1:1 안전한 통신을 수행하고, Network Key를 사용하여 안전한 네트워크 통신을 지원한다. Fig. 1과 Fig. 2를 보면 안전하지 않은 채널을 통하여 네트워크 키와 마스터 키를 전송하는데 이 과정에서 키 노출의 문제점이 발생한다.

특히 마스터 키의 노출로 인하여 앞으로 생성될 링크 키와 네트워크 키가 노출될 수 있으며, 이것은 네트워크 전체에 대한 기밀성을 깨트릴 수 있는 위협으로 작용할 수 있다.

2.3 고유식별값 노출 문제

ZigBee의 식별체계는 각 개인 영역 네트워크를 식별하는 64bit Extended PAN ID, 네트워크의 각 노드를 고유하게 식별할 수 있는 64bit 주소, 각 네트워크에서 사용하는 임의 발급 주소인 16bit 네트워크 주소로 나눌 수 있다. Fig. 3에서 ZigBee 식별체계를 확인할 수 있다.

ZigBee에서 각 노드의 고유식별값인 64bit 주소는, 네트워크에서 노드를 고유하게 구분하여 각 노드를 식별하는 용도로 사용된다. 우리가 컴퓨터에서 사용하는 IP주소라고 생각하면 쉽게 이해할 수 있다.

하지만 매번 통신을 수행할 때마다 고유한 식별값을 사용하는 것은 u-Healthcare 환경에서 취약점으로 작용할 수 있다. 센서노드에서 생체신호를 측정하여 데이터를 전송하는

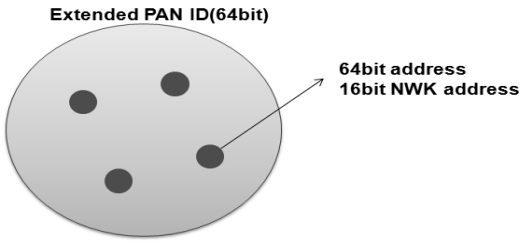

Fig. 3. An Identification of the ZigBee System

데, 어떤 센서에서 전송되는 데이터인지 꼬리표가 붙어있다고 볼 수 있다. 공격자가 데이터를 확인할 수 있고 그것이 누구의 생체신호인지 알 수 있다면 이것은 심각한 프라이버시 위협으로 볼 수 있다. 누구의 의료 데이터인지 파악하기 위해서 각 센서노드의 64bit의 주소가 악용될 우려가 있다.

3. 제안 프로토콜

3.1 시스템 개요

u-Healthcare 환경에서 가장 취약한 부분이 ZigBee 통신이 이루어지는 무선구간이며 본 논문에서는 해당 통신구간의 취약한 부분을 분석하고 개선방안을 제시한다.

본 제안 시스템에서는 u-Healthcare 환경에서 ZC(ZigBee Coordinator)를 사용자가 휴대하는 모바일 디바이스, 즉 스마트폰으로 가정하였다. ZED(ZigBee End Device)는 사용자의 생체신호를 측정하고 ZC로 전송하는 센서노드이다.

제안 시스템의 구성은 Fig. 4와 같이 ZED, ZC, 사용자, u-Healthcare Center, Medical Center, 의료진으로 구성되어 있다.

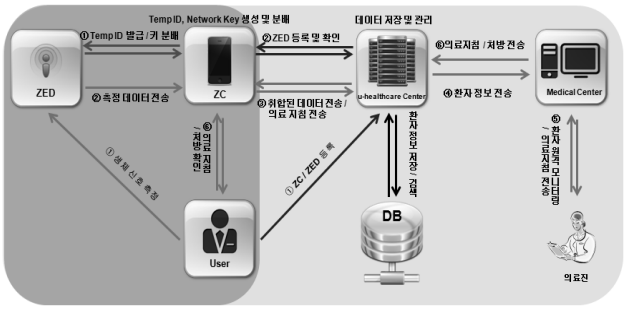

Fig. 4. A Configuration of the Proposed System

1) ZED(ZigBee End Device)

ZED는 사용자의 신체에 위치하여 사용자의 생체신호를 측정하여 ZC에 전송하는 역할을 담당한다. 기존의 ZED와의 차이점은 초기 등록과정이 있고, ZC와의 통신에서 사용하던 64bit 고유주소를 사용하지 않고 등록 시에 발급받은 임시주소를 사용하여 ZC와 통신을 한다는 점이다. 등록과정에서 ZED의 64bit 고유주소와 ZC의 정보가 u-Healthcare 센터에 등록되어, ZC의 요청에 의해 ZED 정보가 전송된다.

2) ZC(ZigBee Coordinator)

ZC는 사용자가 휴대하는 스마트폰이라고 가정한다. ZC는 ZED가 측정한 데이터를 취합하는 역할을 하며 PAN에서 각 ZED의 임시주소를 발급하고 키 분배를 담당한다.

보안 정책에 따라 설정된 임계 시간에 의해 각 임시주소와 키는 지속적으로 갱신된다. 본 제안 프로토콜에서는 비교적 자원 소모가 적은 Residential Mode의 네트워크 키를 사용하여 하나의 PAN에서 하나의 네트워크 키를 사용하는 방식으로 구성하였고 이것의 취약점을 ZC의 주기적인 키 갱신을 통해서 보완하였다.

3) u-Healthcare Center

u-Healthcare Center는 최초 등록단계에서 ZED, ZC의 정보를 사용자로부터 등록받고 ZC의 요청이 오면 해당 데이터를 ZC에게 전송하며, ZC에서 전송하는 취합된 생체신호 데이터를 저장 및 관리한다. 전송받은 데이터를 Medical Center에 전송하는 역할을 담당하고 전체 u-Healthcare 시스템에서 사용자와 의료진을 연결하는 중간 다리 역할을 한다. u-Healthcare 서비스를 제공하는 Service Provider의 역할을 수행한다.

4) Medical Center

Medical Center는 u-Healthcare Center에서 전송된 사용자의 생체신호를 수신하여 사용자의 상태를 모니터링하며, 원격 진료를 진행하는 의료진과 사용자를 연결하는 역할을 수행한다. 의료진은 모니터링 자료를 기반으로 새로운 의료지침을 작성하여 u-Healthcare Center로 다시 전송한다. Medical Center는 의료기관의 u-Healthcare 담당 기관으로 볼 수 있다.

3.2 세부 프로토콜

전제 프로토콜의 구성은 등록 단계, 갱신 및 분배 단계, 데이터 전송 단계로 구성된다.

1) 등록 프로토콜

등록 프로토콜은 Fig. 5와 같으며 USER, u-Healthcare Center, ZC, ZED로 구성되어있다.

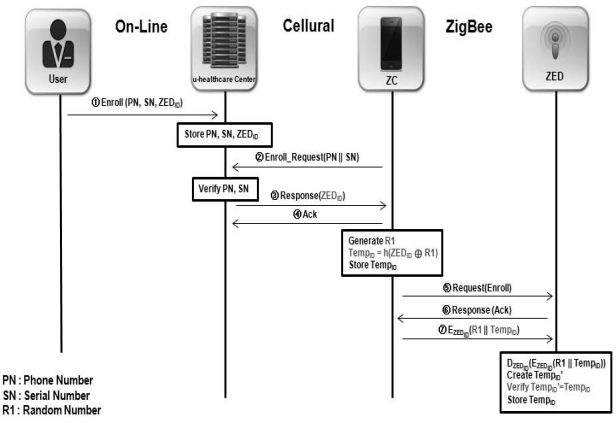

Fig. 5. A Registration Protocol

① Enroll(PN, SN, ZEDID) : 사용자는 u-Healthcare Center에 사용자의 ZC인 스마트폰의 PN, SN 정보와 새롭게 추가하는 ZED의 ID인 ZEDID를 등록한다.

사용자로부터 등록 데이터를 입력받은 u-Healthcare 센터는 해당 데이터를 저장한다.

② Enroll_Request(PN || SN) : 사용자는 자신의 ZC로 u-Healthcare Center에 접속하여, 자신의 스마트폰 데이터를 전송하여 인증하고 ZEDID를 요청한다.

ZC의 요청을 접수한 u-Healthcare Center는 ZC가 보낸 정보를 검증한다.

③ Response(ZEDID) : ZC의 인증 수행 후에 u-Healthcare Center는 ZC에게 ZEDID를 전송한다.

④ Ack : ZC는 u-Healthcare Center로부터 데이터를 정확히 수신하였다는 Ack 메시지를 전송한다.

ZC는 수신한 ZED의 ID를 저장하고 ZEDID를 기반으로 임시 ID인 TempID = h(ZEDID ⊕ R1)를 생성하고 저장한다.

⑤ Request(Enroll)~⑥ Response(Ack) : ZC는 등록 요청 메시지를 전송하고 ZED는 이에 응답한다.

⑦ EZEDID(R1 || TempID) : ZC는 ZED의 ID를 비밀 키로 암호화하여 임시ID를 분배한다.

TempID를 수신한 ZED는 해당 메시지를 복호화하고 DZEDID(EZEDID(R1 || TempID)) 수신한 R1값을 사용하여 TempID를 생성, 검증하고 저장한다.

2) 갱신 및 분배 프로토콜

갱신 및 분배 프로토콜은 Fig. 6과 같이 ZC와 ZED로 구성된다.

ZC는 새로운 랜덤 값 Ri를 생성하고 기존의 TempID를 기반으로 새로운 New_TempIDi = h(Old_TempIDi ⊕ New_Ri)를 생성한다. 기존 TempID를 Old_TempID라고 하고 새로 생성한 TempID는 New_TempID로 표현한다.

또한 분배할 네트워크 키는 ZC가 관리하는 전체 ZED의 TempID를 기반으로 생성한다.

① Request(Update) : ZC는 갱신 요청 메시지를 ZED에게 전송하여 갱신 및 분배 단계의 시작을 ZED에게 알린다.

② Response(Old_TempIDi) : 갱신 요청 메시지를 수신한 ZED는 이에 대한 응답으로 자신의 Temp ID를 전송한다.

③ Old_TempIDi || EZEDIDi(Ri || NetKey || New_TempIDi) : ZC는 각 ZED에게 Old_TempID를 기반으로 새로운 생성한 랜덤 값 Ri, 네트워크 키, 새로운 TempID를 암호화하여 전송하고 ZED는 자신의 Old_TempID를 확인하여 메시지를 수신한다.

메시지를 수신한 ZED는 해당 메시지를 복호화하고 (DZEDIDi(EZEDIDi(Ri || NetKey || New_TempIDi))), 획득한 Ri를 기반으로 TempID를 생성하여 수신한 New_TempIDi와 비교하여 검증한다. 검증된 New_TempIDi와 수신한 NetKey를 저장한다.

④ Ack : ZED는 데이터의 정확한 수신과 갱신 및 분배 과정의 완료를 Ack 메시지를 송신하여 ZC에게 알린다.

위의 단계를 통하여 갱신 및 분배 과정을 완료한다.

3) 데이터 전송 프로토콜

데이터전송 프로토콜은 Fig. 7과 같이 Medical Center, u-Healthcare Center, ZC, ZED로 구성된다. 데이터 전송 단계에서 중점 부분은 ZC와 ZED의 ZigBee 통신구간이므로 나머지 부분은 데이터 전송의 간략한 단계로 표현했다.

① Data_Trans_Request(TempID) : ZED는 사용자의 신체에서 측정한 데이터를 ZC에게 전송하기 위해서, TempID를 포함한 데이터 전송요청 메시지를 보낸다.

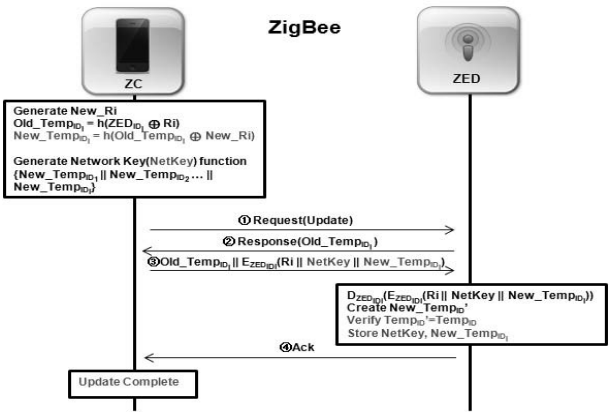

Fig. 6. An Update and Distribution Protocol

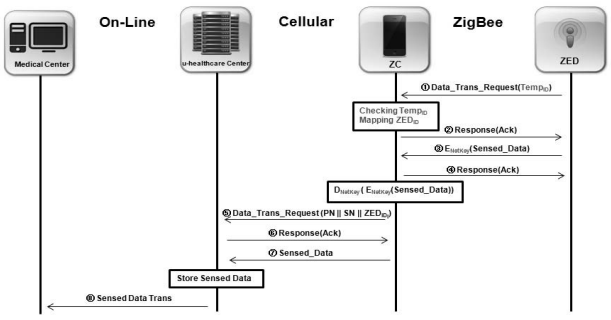

Fig. 7. A Data Transfer Protocol

ZED의 요청을 수신한 ZC는 TempID를 기반으로 저장된 실제 ID인 ZEDID와 비교하여 해당 ZED를 식별한다.

② Response(Ack) : ZC는 ZED를 식별한 후에 Ack 메시지를 응답으로 전송한다.
③ ENetKey(Sensed_Data) : ZC의 Ack 메시지를 수신한 ZED는 네트워크 키로 암호화된 메시지 ENetKey(Sensed_Data)를 ZC에게 전송한다.
④ Response(Ack) : ZC가 ZED에게 Ack 메시지를 송신하여 ZC와 ZED 간의 데이터 전송을 완료한다.

메시지를 수신한 ZC는 해당 메시지를 복호화(DNetKey(ENetKey(Sensed_Data)))하여 저장한다.

ZigBee 통신 구간 이후에는 셀룰러 네트워크 구간과 On-Line 구간은 안전한 채널로 가정하며 추가적인 암호화 및 보안 과정은 생략한다.

⑤ Data_Trans_Request(PN || SN || ZEDIDi) : ZC는 복호화된 메시지를 셀룰러 네트워크를 통하여 u-Healthcare Center로 전송한다. ZC의 식별과 ZED의 식별을 위하여 ZC의 PN, SN, ZEDID를 전송한다.
⑥ Response(Ack) : ZED의 데이터 전송 요청을 수신한 u-Healthcare Center는 수신한 인증정보를 검증하고 등록된 데이터와 비교하여 검증한다. 그리고 검증이 성공하면 ZC에게 Ack 메시지를 보낸다.
⑦~⑧ Sensed_Data : ZC는 측정된 데이터를 전송하고 u-Healthcare Center는 수신한 데이터를 저장하고 Medical Center에 전송한다.

4. 성능 분석

제안 시스템은 ZigBee Residential Mode를 사용했으며 키 유출의 위협을 방지하기 위해서 주기적인 키 갱신을 방식을 사용했다. 고유식별값 노출로 인하여 발생 가능한 프라이버시 침해 위협을 방지하기 위해서 임시식별값을 사용하고 이 또한 주기적으로 갱신하여 공격자가 노드를 식별할 수 없도록 하였다. 제안 시스템의 구현 결과와 기존 시스템을 비교한 결과는 Table 1과 같다.

비교 분석에 사용된 항목들은 기존 시스템에서 변경되어야 하는 부분을 위주로 작성했다. 기존 시스템에서는 64bit의 식별값이나 16bit의 임의식별값들이 노출되었다. 데이터 전송과 같은 일반적인 통신과정에서는 오버헤드를 줄이기 위해 PAN에서 임의 지정하는 16bit의 식별주소를 사용해도 되지만 키 요청, 키 전송 등의 주요한 통신에서는 64bit의 고유 주소가 필수적으로 사용되어야 한다. 제안하는 방식은 64bit의 고유식별주소 대신에 주기적으로 갱신되는 임시식별값을 사용하기 때문에 식별값 노출을 피할 수 있다.

Table 1. Experimental results

구 분	Residential Mode	Commercial Mode	제안 방식
64bit 고유식별값	노출	노출	노출 안 됨
임시식별값 저장	nx16bit	nx16bit	(2nx64bit)
저장해야 할 키의 수	Network Key +Master Key	(NxLink Key) +Master Key+ Network Key	Master Key+ Network Key
공격자 ZED 식별	가능	가능	불가능

두 번째로 기존 시스템에서는 PAN에서 임의로 부여하는 16bit의 식별값을 사용하고 제안 방식은 64bit의 임시식별값을 사용한다. 또한 임시식별값 분배 과정에서의 동기화 문제 발생을 대비해 Old_TempID 역시 저장하고 있으므로 추가적 공간이 요구된다. PAN을 관리하는 ZC는 각 노드별로 ZEDID, Old_TempID, New_TempID를 저장해야 하지만 상대적으로 자원의 제약이 더 많을 것으로 판단되는 ZED에서는 Old_TempID + New_TempID = 128bit의 공간만을 필요로 한다.

세 번째 항목은 ZC와 ZED가 저장하고 있어야 하는 비밀키의 개수를 나타낸 것이다. 제안 시스템은 기존 Residential Mode에 Network Key를 사용한 방식과 일치하므로 Commercial Mode의 비밀 키 저장 공간보다는 n×128bit만큼의 저장 공간을 절약할 수 있고 공용 Network Key 사용으로 상대적으로 취약한 Residential Mode의 단점을 주기적인 키 갱신을 통해서 해결했다.

공격자의 ZED 식별 항목은 기존 시스템에서 각 노드들의 고유식별값 노출로 발생할 수 있는 프라이버시 침해의 가능성을 판단하고자 선택한 평가 항목이며 제안 시스템은 이런 위협에서 안전한 것으로 평가할 수 있다.

Table 2에서 하루 24시간을 기준으로 각 갱신 주기별 연산량을 나타냈다. ZC에서 모든 ZED의 TempID와 Network 키를 관리, 저장, 분배해야 하기 때문에 ZC에 집중되는 연산량을 측정했다. n은 ZED의 수, R은 랜덤 넘버 생성, h는 해쉬함수, Kf는 키 생성 함수, E는 암호화, D는 복호화, 1T는 갱신 및 분배의 트랜잭션을 나타낸다. 마지막 분배 항목은 1T의 갱신 및 분배 과정에서의 ZC와 ZED가 주고받는 메시지의 개수를 나타낸 것이다.

Table 2. Amount of computation per update cycle

구 분		1시간	6시간	24시간
Key	ZC	n(24(R+h+Kf+E+1T))	n(4(R+h+Kf+E+1T))	n(R+h+Kf+E+1T)
	ZED	24(D+h+1T)	4(D+h+1T)	D+h+1T
Temp ID	ZC	n(24(R+h+E+1T))	n(4(R+h+E+1T))	n(R+h+E+1T)
	ZED	24(D+h+1T)	4(D+h+1T)	D+h+1T
분배		24(4m)	4(4m)	4m

5. 결 론

본 논문의 제안 시스템은 u-Healthcare 환경에서 전송하는 생체신호 데이터의 민감성을 고려하여 보안 강도를 높이기 위하여 제안한 논문이다. u-Healthcare 시스템에서 ZigBee 통신을 사용하는 ZC와 ZED 사이의 무선 통신 구간을 해당 시스템의 가장 취약한 구간으로 판단하고 해당 구간의 취약점을 파악했다.

기존에 파악된 취약점 이외에 ZigBee 통신에서 각 노드 간의 64bit의 고유식별주소를 사용하는 것이 개인의 민감한 데이터를 주고받는 u-Healthcare 시스템에서는 취약점이 될 수 있다고 판단했다.

각 취약점들을 보완하기 위해 ZigBee Residential Mode의 Network 키를 사용하는 방식을 사용했다. Residential Mode는 Commercial Mode에 비해서 사용하는 비밀 키가 Network 키 하나로 제한되어있기 때문에 ZC가 관리해야 할 키의 개수가 줄어드는 장점이 있다. 하지만 Network 키가 유출되었을 때 전체 PAN의 보안이 무너지는 상황을 방지하기 위한 대책으로 정책에 따라서 Network 키를 주기적으로 갱신하는 방식을 사용했다.

고유식별주소 노출을 피하기 위해서 임시식별주소를 사용하였고 이를 통해서 공격자가 각 센서노드를 식별하는 것을 막을 수 있었다. 센서노드를 공격자가 고유하게 식별하기 때문에 발생할 수 있는 프라이버시 침해의 위협을 방지 할 수 있었다.

ZC에 집중되는 오버헤드를 측정하기 위해서 기존 시스템에 비하여 추가되는 연산을 파악하였고 해당 연산량을 표로 나타냈다. ZC와 ZED의 자원을 고려해서 키와 임시식별값을 갱신하는 주기를 결정하는 것이 중요할 것으로 보인다.

향후에는 ZigBee 통신에서 사용하는 16bit의 임의식별주소 역시 여러 센서노드들이 모였을 때 PAN을 고유하게 식별 가능할 것으로 예상되며, 각 PAN을 식별하는 Extended PAN ID 역시 동일하다. 이에 대한 취약 사항을 분석하고 보완해야 할 것이다.

References

[1] Ik-Seob Lee, Ki-Hyang Hong, Gang-Shin Lee, and Jae-Il Lee, “Preliminary Diagnosis Model for a New IT Service: Improving the Information Security of u-Services with Zigbee”, PROCEEDINGS OF WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY, Egypt; World Academy of Science, Engineering and Technology, pp.155-158, 2007.

[2] Moazzam Khan, Fereshteh Amini, and Vojislav B. Misic, “The Cost of Security: Performance of ZigBee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster”, Mobile Adhoc and Sensor Systems(MASS), 2006 IEEE International Conference on, IEEE, pp.876-881, 2006.

[3] Pavel Ocenasek, “Towards Security Issues in ZigBee Architecture”, Human Interface, Part I, HCII 2009, LNCS 5617, pp.587-593, 2009.

[4] ZigBee Alliance, “ZigBee-PRO Stack Profile: Platform restrictions for compliant platform testing and interoperability”, 2008.

[5] Byung-Mun Lee, Heon-Cheol Lim, and Un-Ku Kang, “Mutual Authentication Protocol based on the Effective Divided Session for the Secure Transmission of Medical Information in u-Health”, *Journal of Digital Contents Society, The Korea Contents Society*, pp.142-151, 2011.

[6] Tae-Min Song, Sang-Hyun Jang, “u-Healthcare: Issue and Research Trends”, Health-welfare Policy Forum, The Korea Institute for Health and Social Affairs, pp.70-86, 2011.

[7] Dae-youl Seo, Jin-chul Kim, Kyoung-Mok Kim, and Young-Hwan Oh, “Effective Parent-Child Key Establishment Algorithm used ZigBee Sensor Network”, Journal of Telecommunication, THE INSTITUTE OF ELECTRONICS AND INFORMATION ENGINEERS, pp.35-45, 2006.

박 정 효

e-mail : helios914@ssu.ac.kr
2001년 숭실대학교 컴퓨터학과(학사)
2009년 숭실대학교 정보보안학과(석사)
2011년~현 재 숭실대학교 컴퓨터통신학과 박사수료
관심분야 : anonymous authentication, multi-factor authentication, diversity authentication techniques

김 낙 현

e-mail : knh@kisa.or.kr
2012년 숭실대학교 컴퓨터학과(석사)
2013년~현 재 숭실대학교 컴퓨터통신학과 박사과정
관심분야 : Biometrics Authentication, Encryption Protocol, Information Security

정 용 훈

e-mail : s0178@ssu.ac.kr
2004년 숭실대학교 전자계산원(학사)
2006년 숭실대학교 컴퓨터학과(석사)
2010년 숭실대학교 컴퓨터학과(박사)
관심분야 : anonymous authentication, multi-factor authentication, multimedia security

전 문 석

e-mail : mjun@ssu.ac.kr
1981년 숭실대학교 컴퓨터학과(학사)
1985년 Univ. of Maryland at Baltimor(석사)
1989년 Univ. of Maryland at Baltimore(박사)
현 재 숭실대학교 컴퓨터학과 교수
관심분야 : Cryptology, network security, information security, e-passport