Secure Oriented Architecture(SOA)에 기반한 u-Healthcare 네트워크 보안기술 프레임워크 모델

김점구* · 노시춘**

요 약

센서네트워크 구성은 특정 상황이나 환경에 대한 센싱이 가능한 센서, 수집된 정보를 처리하는 프로세서, 그리고 데이터를 송수신하는 장치 등 이다. 센서네트워크는 많은 유익함을 제공하지만 무선 네트워크 보안 취약성을 해결하지 않은상태로 정보노출 위험이 다양하게 존재한다. u-Healthcare 센서 네트워크는 센서 노드의 크기가 작아 전력소모 및 컴퓨팅 능력, 메모리 등에 제한이 가해지며, 무선을 통해 센싱된 값을 전달하는 특징을 가지므로 도청, 서비스거부, 라우팅 경로 공격이 가능하다. 본 논문에서는 센싱기능을 중심으로 한 u-Healthcare 시스템 환경의 무선보안 취약성 요소를 진단하고 u-Healthcare 보안 프레임워크 설계방법을 제시한다. 센서네트워크 기술들이 보안취약성에 대한 대책 강구 없이 기술만 발전한다면 기술이 정상적으로 활용되지 못하고 위협의 요소가 될 것이다. 이 연구를 통해 제안되는 u-Healthcare 시스템의 보안 위험 대처방법은 다양한 현장에서 의료정보와 이용자보호의 중요한 가이드로 활용될것이다.

A Study for u-Healthcare Networking Technology Framework Approach Based on Secure Oriented Architecture(SOA)

Jeom goo Kim* · SiChoon Noh**

ABSTRACT

Sensor network configurations are for a specific situation or environment sensors capable of sensing, processing the collected information processors, and as a device is transmitting or receiving data. It is presently serious that sensor networks provide many benefits, but can not solve the wireless network security vulnerabilities, the risk of exposure to a variety of state information. u-Healthcare sensor networks, the smaller the sensor node power consumption, and computing power, memory, etc. restrictions imposing, wireless sensing through the kind of features that deliver value, so it ispossible that eavesdropping, denial of service, attack, routing path. In this paper, with a focus on sensing of the environment u-Healthcare system wireless security vulnerabilities factors u-Healthcare security framework to diagnose and design methods are presented. Sensor network technologies take measures for security vulnerabilities, but without the development of technology, if technology is not being utilized properly it will be an element of threat. Studies suggest that the u-Healthcare System in a variety of security risks measures user protection in the field of health information will be used as an important guide.

Key words : u-Healthcare, Sensor Network, Framework,Secure Oriented Archtitecture

접수일(2013년 8월 31일), 수정일(1차: 2013년 9월 12일, 2차: 2013년 9월 25일), 게재확정일(2013년 9월 30일)

* 남서울대학교 컴퓨터학과
** 남서울대학교 컴퓨터학과

1. 서 론

센서 네트워크는 특정 상황이나 환경에 대한 센싱이 가능한 센서와 수집된 정보를 처리하는 프로세서, 데이터 송수신장치로 구성된다. 이 시스템을 사용하여 의료 활동에 편리함을 제공 하지만 근본적인 보안은 취약한 상태이다. u-Healthcare 센서 네트워크는 센서 노드의 크기가 작아 전력 소모 및 컴퓨팅 능력, 메모리 제한이 있으며, 무선을 통해 센싱된 값을 전달하는 특징을 가지므로 도청, 서비스거부 공격, 라우팅 경로 공격 등 다양한 공격에 노출될 수 있다. 본 논문에서는 센싱 기능을 중심으로 한 u-Healthcare 시스템 환경의 무선보안 취약성 요소를 진단하고 u-Healthcare 통합화 보안 프레임워크 설계방법을 연구한다. SOA에 기반한 u-Healthcare 네트워크보안 프레임워크를 설계하기 위한 접근방식은 보안 기능을 별도의 분리된 알고리즘이 아니라 시스템 기능 주요 단계에서 취약점을 예방하는 기능 측면으로 접근하는 방식이다. 이 연구를 통해 제안되는 보안위험 대처 방법론은 다양한 의료 현장에서 의료정보와 이용자 보호의 가이드로 활용 목적으로 secure oriented architecture 기반 u-Healthcare 센싱기술 프레임워크를 사용한다. 논문 기술순서는 서론, 관련 연구로서 요소기술, 센싱 시스템 구조도, u-Healthcare시스템 보안 취약성, 무선보안 기술 프레임워크 모델, 결론 순서이다.

2. U-Healthcare의 요소 기술

u-Healthcare는 BT(Bio Technology) 및 IT 기술을 기반으로 ubiquitous network 환경을 이용하여 사용자의 wellness와 healthcare의 needs를 충족시켜주는 정보를 제공한다. 사용자의 삶의 질(Quality of Life)을 향상시키고 의료비용을 절감하기 위한 제품, 서비스 및 시스템이다. u-Healthcare는 정보통신과 보건의료의 연결이며 언제 어디서나 예방, 진단, 치료, 사후 관리의 보건의료 서비스를 제공한다. 보건의료 서비스는 치료중심에서 예방중심, 질병관리에서 건강관리 중심으로 패러다임이 이동하고 있다. 이 같은 동향의 u-healthcare 서비스 종류는 mobile health care서비스, home health care서비스, medical fitness서비스, home nursing서비스, telemedicine 서비스 등 이다. 또한 맞춤형 의료서비스의 발전이며 분자 영상진단 분야의 발전으로 질병의 조기 진단과 맞춤치료 현실화가 가능한 계기를 만들었다. 이 분야 요소기술은 다음 <표 1>와 같이 센서기술, 인터페이스 통신, 프로토콜과 알고리즘, 데이터 기술로 구분 된다[3].

<표 1> U-Healthcare의 요소 기술, 윤형진

기 술	역 할	종 류	형 태	분 야
센서	생체신호감지검출	바이오센서,바이오칩,인식칩	착용형,내장형,비침습형	BT,NT
인터페이스/통신	생체신호전송	RF,Zigbee,인터넷,무선LAN,블루투스	휴대단말,PDA 등	IT
프로세싱/알고리즘	생체신호처리분석	분석SW,초소형칩	분석시스템SW	IT,NT
DB/기록	생체신호정보제공	데이터마이닝,바이오인포메틱스	전자기록,라이브러리	IT,BT

3. u-Healthcare 시스템 자원별 보안취약성 진단

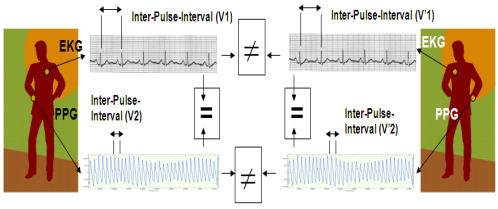
3.1 무선 애플리케이션 자원

u-Healthcare는 무선 애플리케이션으로 electrocardiographs(ECGs), Pulse oximeters, blood pressure monitors, fetal heart rate & maternal uterine monitors 등이 대표적 이다. 무선 애플리케이션은 일반적으로 bluetooth나 802.11을 기반으로 하는 아날로그 wireless medical telemetry service(WMTS) bands를 사용한다. 이 구성은 개방된 네트워크 접속환경이며 대량의 무선 트래픽의 신속한 처리가 가능하나 컴퓨터 바이러스나 해커로부터 완전한 보호가 어렵고 트래픽 중에서 개인정보가 불법적 수집, 축적되거나 처리, 이용, 유통, 유출시의 리스크가 상존한다. 무선 접속구간을 통한 정보센터로 불법 접근. 비 적격자에 의한 접근, 애플리케이션 프로그램 수정, 환자 자료가 다른 환자의 자료로 교체되는 전송 가능성이 존재한다. 시스템

상에서 질병 및 진료 내역과 가족, 유전, 병력, 약물중독 내용, 성병 등 정보노출 가능성이 상존한다[4].

3.2 신체 착용 디바이스 자원

센싱 시스템은 여러개의 센서를 의료서비스 수요자의 신체에 부착하고 센서를 통해 감지한 데이터를 가슴에 착용한 전송장치로 전송한다. CPOD (Crew Physiological Observation Device), ECG Respiration sensor 로부터의 데이터, Pulse Oximeter로부터 데이터, AccutrackerII Blood Pressure Monitor로 부터의 데이터를 모아 base station으로 전송하는 장치이다. 자체 센서로 외부와 착용자의 온도를 측정하여 환자의 정보를 전송하는 기능이 수행된다. 현재 bluetooth 프로토콜에서 지원하는 보안에 의지하고 있는데 bluetooth 프로토콜 자체에서 보안 취약점이 발생한다. u-Healthcare에서 사용하는 센싱 시스템은 Tablet PC로 데이터 전송 시 무선 데이터 통신인 bluetooth통신을 사용한다. 공격자가 엑세스 가능 시 정보를 얻을 수 있고 공격자의 Tablet PC에 인스톨하여 모든 데이터를 받을 수 있다. 취약점을 알고 있는 공격자가 작은 장비 설치로 데이터의 흐름을 잡아내고, 취약한 알고리즘을 풀어내면 환자의 중요정보에 대한 보호가 어려워 질 수 있다[5][9].



(그림 1) 장착된 센서간 정보 교신

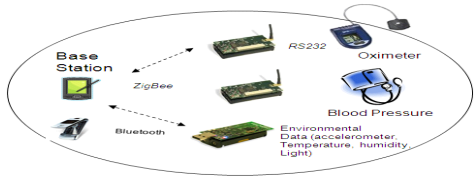
3.3 Display형 모니터링 시스템 자원

이 장치는 알림 역할뿐 아니라 환자 약 복용 정보도 읽을 수 있는데 집안 곳곳에 있는 사물에 부착된 RFID tag를 통해 가능하다. RFID 태그 전송데이터의 크기와 판독 시간도 한정되어 있으며 리더 장비나 백앤드 시스템은 성능과 자원 측면에서 한계를 가진다. RFID 기술은 물리적 공격, 위조, 스푸핑, 도청, 트래픽 분석, 서비스거부공격 등의 취약점 들을 가지고 있다. 장착된 센서들 사이의 무선 또는 유선 네트워크를 통해 연결 된다. 시스템은 TV나 벽걸이 display , 냉장고 등 다양한 화면을 통해 환자에게 필요한 정보들을 제공한다. 이 시스템은 약물 복용 환자 에게 집안 각종 display를 이용해 복용시간을 알려준다. 스니핑, 도청, 트래픽 분석 취약점을 가지고 있다 [6][7].

4. u-Healthcare 트래픽처리 단계별 보안기술 프레임워크 모델

4.1 센싱 시스템 구조 진단

u-Healthcare 센싱은 각종 센서에서 감지한 정보를 무선으로 수집할 수 있도록 구성한 네트워크 이다. 센서는 감지대상에 대한 정보를 인지, 측정, 전송하기 위해 신호로 변환하는 소자로 크게 ID 센서와 환경감지 센서로 나뉜다. 대표적 ID센서는 RFID 태그이다. 스마트 센서는 컴퓨터 기술과의 결합에 의해서 센서 기능을 대폭적으로 향상시킨 지능화된 센서이다. USN은 무선을 이용하여 스마트 센서들을 네트워크로 연결한다. OS는 tiny OS를 이용하고 무선 의료 센서와 PDA등의 디바이스를 사용한다[4].



(그림 2) 센싱시스템 네트워크 구조

4.1.1 센싱시스템 부분

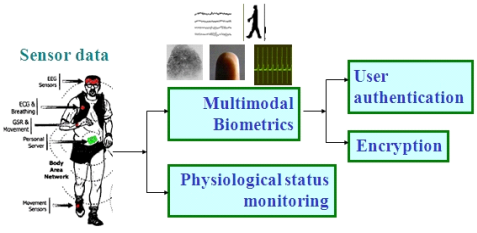
센싱시스템 부분은 외부정보나 환경을 인지하기 위한 기능을 수행하므로 대상물의 상태를 파악하고 전기 신호로 전달한다. RFID는 무선 주파수를 이용한 인식 기술. 전파를 이용해 사물에 부착 된 태그를 식별하여 정보/ID 및 주변 환경정보를 수집해 저장-가공-추적- 측위- 원격 처리- 관리-정보교환을 가능

하게 한다. Tag를 통해 읽혀진 정보는 중앙 관리센터로 전송되고 중앙 관리센터는 실시간 환자를 모니터링 한다. 센싱 시스템은 특정 상황이나 환경 센싱이 가능한 센서(sensor node)와 수집된 정보를 처리하는 프로세서, 데이터 송수신장치(sink node)로 구성 된다[2][3][4].

○ 정보제공 서버: 다양한 서비스 및 정보 제공
○ 보안게이트웨이: 외부 네트워크와 통신하기 위한 중계노드 역할을 수행하면서 보안 필터링
○ 싱크노드: 센서노드로부터 센싱 정보를 수집
○ 센서노드: 센서, 컴퓨팅, 통신 모듈을 통해 환경정보를 인지하여 전송[1][6].

4.1.2 무선랜(Wiless LAN) 부분

환자로부터 주어진 데이터를 다수 의사나 간호사에게 전달할 네트워크 레이어 흐름상 멀티캐스트가 필수이다. 각 디바이스는 이동성으로 링크채널 이 변경된다. 멀티홉 라우팅 프로토콜을 사용하는 경우 의사가 이동할 때 빠른 새로운 라우팅 경로를 찾아야 한다. WLAN은 액세스 포인트(AP)를 통해 다른 네트워크로 연결되거나 점대점 혹은 에드혹(ad hoc) 네트워킹을 만들 수 있다. IEEE 802.11b는 2.4G Hz에서 2.4835 GHz의 ISM 주파수 대역을 이용하여 도달거리 200m와 전송률 11Mbps까지 가능하다. 802.11g는 802.11b와 같은 주파수 대역을 사용하며 호환된다는 이점을 추가 하면서도 54 Mbps 전송률을 보인다. 802.11n은 여러개 안테나를 사용하는 다중입력 다중 출력 (MIMO) 기술과 직교 주파수분할 다중접속 (OFDMA)방식을 사용하여 600 Mbps 전송률을 제공한다[3][5].



(그림 3) 센싱 네트워크 보안 구조도

4.2 보안기술 요구사항

u-Healthcare용 ad hoc기반 센서 네트워크는 일반적 센서 네트워크와 요구사항이 다르다. 의료 어플리케이션은 작고, 가볍고 착용이 가능해야 한다. 의료 데이터의 유효성은 중요하기 때문에 통신 간섭에 의해 패킷이 손실되는 것을 최대한 방지하여 신뢰성 통신을 유지해야 한다. 센서 네트워크의 제약조건 및 보안 요구사항을 만족시키기 위한 기술구조는 센서 환경에 적합한 경량 암호 및 인증 기술, 경량 키관리 기술, 프라이버시 보호 기술, 부 채널 공격방지 기술 등이다. 네트워크 환경에서 암호화는 두 개 호스트 간, 혹은 두개의 응용시스템 간 적용될 수 있다. 암호화는 프라이버시, 인증, 무결성 및 데이터에 대한 제한적 접근을 제공하는 강력한 수단이다. 전자서명은 데이터에 대한 서명과 서명된 데이터에 대한 검증절차가 적용된다, 서명은 서명자의 비밀 정보인 공개키 암호 알고리즘의 비밀키를 사용함으로써 데이터의 암호화 및 검사값을 생성하는 과정이다. 검증은 서명자의 공개정보를 사용하여 정보를 보낸 사람이 누구인지를 알아내는 과정이다. 접근통제는 사용자의 접근권한을 결정하거나 사용자에게 접근 권한을 부여하기 위하여 사용자의 고유성, 사용자에 관한 정보 또는 사용자의 자격 등을 이용한다. 만약 사용자가 비 인가 된 자원에 대하여 접근을 시도하거나 인가된 자원 일지라도 불법적 방법으로 접근하고자 한다면 접근통제 기능은 접근시도를 통제한다. 데이터 무결성은 네트워크 상에서 데이터의 정확성을 점검하는 메커니즘으로 송신자와 수신자가 각각 무결성을 결정한다. 인증교환은 인증교환 메커니즘에는 패스워드와 같이 단순한 신분확인 정보를 이용하는 것부터 암호기술을 이용하는 것 까지 다양한 방법을 적용한다.

4.3 네트워크 Layer 보안 Service 구성

u-Healthcare 보안기술 프레임워크는 원칙적으로 기능흐름에 따라 요소기술이 사용되고 이 메커니즘에 보안 기능이 적용된다. 보안기술은 센서기술, 인터페이스 통신, 프로토콜과 알고리즘, 데이터 기술로 구분된다. 보안기술 요구사항을 수용하기 위한 u-Healthcare 네트워크 보안기술은 OSI 7계층을 기준으로 보안 Service 메커니즘을 설계하여 적용한다. 보안Service 설계는 트래픽 발신노드 인증, 네트워크 접근제어, 네

트워크 접속 비밀성, 선택영역 비밀보장, 트래픽흐름 비밀성, 복구기능의 접속 무결성, 선택영역 접속 무결성, 선택영역 비접속 무결성, 접속과 전송과정 부인방지로 나눌 수 있다. 이 서비스들이 어느 계층에서 제공되는지를 구분하고 이를 구현하기 위한 보안기술을 적용하면 보안메커니즘이 구성된다. 이 같은 보안 메커니즘을 네트워크 Layer 별로 체계화하면 다음 <표 2>와 같다.

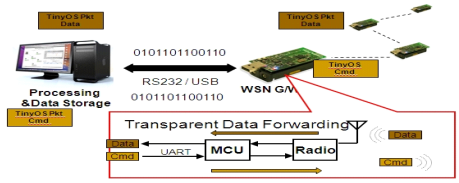
<표 2> 네트워크 Layer별 보안 메커니즘

Layer 와 Service	1	2	3	4	5	6	7
트래픽 발신노드 인증			O	O			O
네트워크 접근제어			O	O			O
네트워크 접속 비밀성	O	O	O	O			O
선택영역 비밀보장							O
트래픽흐름 비밀성	O		O				O
복구기능의접속무결성				O			O
선택영역 접속무결성							O
선택영역 비접속 무결성							O
접속과 전송과정 부인방지							O

4.4 트래픽 처리과정 별 보안 알고리즘

본 연구에서 제안하는 SOA 알고리즘을 적용하기 위해서 두가지 접근방법에 기초하는데 하나는 표준화되고 정형화된 모델 기반으로 보안 패턴 유형을 개발하여 적용하는 방법으로서 계층화된 보안 패턴 맵을 설계하여 적용하는 것 이다. 다른 하나는 보안기능을 별도의 분리된 패턴 맵 알고리즘으로 접근하는 방법이 아니라 트래픽처리 기능 핵심 단계에서 취약점을 예방하는 기능측면의 알고리즘을 적용하는 것 이다. 이 방법은 기본적 보안 메커니즘을 개발하여 정보처리 기능 구조와 동작과정에 반영하는 것 이다. 이 방식을 통해 기능 요구사항 처리 시 비 기능적 보안품질 요구사항을 해결한다. 본 연구 제안방법은 두번째 방법인 정보처리 기능 구조와 동작에서 보안을 반영하는 방법이며 다음과 같은 기능 영역에서 단말 노드상 입력 단계에서 최종 애플리케이션 기술 보안 단계까지 SOA기반 알고리즘을 적용하는 것 이다.

#1. Query(CBQ) layer : 신체 착용 디바이스 자원 또는 Display형 모니터링 시스템 자원을 통해 채집되는 센싱 트래픽은 u-Healthcare 의료 정보 단말 노드상의 입출력 단계이다. 특정 센서, 데이터 속도, 데이터전송에 필요한 필터상태 등을 나타내는 query(CBQ) layer를 이용하여 통신경로를 설정한다. Dircted Difusion과 tiny DB와 유사한 CBQ를 이용하여 최종 사용자 디바이스 (스마 트폰, PDA,Laptop)에서 데이터를 전송 요구할 수 있고, 노드에게 쿼리에서 요구하는 데이터를 publish 시키도록 요구할 수 있다. 이 과정에서 단말 노드상의 Physical Layer에서의 접속서비스 보안이 이루어지며 접속 비밀보장 과 트래픽흐름 비밀보장이 이루어져야 한다. ISO9160 기반의 DEE(Data Encipherment Equipment)간 동일한 암호화 알고리즘 키를 사용하도록 규정한다. 트래픽이 동기방식일 경우 전송되는 모든 비트를 암호화 하며 비동기방식일 경우는 시작비트와 정지 비틀 제외한 모든 비트를 암호화한다.



(그림 4) 센싱 트래픽 게이트웨이 구조

#2. Subscribe, Leave 기능 : u-Healthcare 시스템 경로상에서 subscribe는 시스템의 특정 채널과 연결이 가능한지 노드의 상태를 알려주고 leave는 publish와 subscribe의 요구를 소멸 시킨다. Send, send-done, receive 인터페이스는 tiny OS에서의 active message와 비슷한 역할을 한다. 멀티라우트 경로는 특정 채널에 forwarder에게 할당 노드에 의해 이루어진다. Forwarder는 단순히 주어진 채널로부터 받은 어떠한 메시지를 다시 브로드케스팅 한다. 노드

들은 환자의 디바이스가 데이터를 알리는 것을 요청할 때 초기화되어 라우팅 경로를 찾는 프로세스에 의해 forwarder로서의 역할을 하게 된다. 경로를 찾는 방법으로 각 노드는 publisher node ID로 구분된 노드 테이블을 가지고 있고 이 노드 테이블에는 publisher로부터 현재 노드까지 path cost와 publish로부터 다음 홉까지 최선의 경로를 가지고 있다. 이 과정에서 저장 및 전달 데이터 보호, Identity 변경 보호, 비인가 구성에 대한 OS와 application의 신뢰 측정이 이루어진다

#3. 트래픽 흐름 제어 : Request To Send control(RTS), Clear To Send(CTS) control은 X-온/X-오프 흐름제어와 비슷한 속도 정합기법 이다. 시스템과 모뎀, 또는 통신장치간 전기신호와 논리회로를 사용하여 데이터 흐름을 제어한다. 각 클러스터의 헤더들만 무선 송수신 모듈을 활성화시켜 RTS/CTS/DATA/ACK 메시지 송수신에 참여하고 클러스터 당 다수 노드들이 메시지 교환에 참여한다. 각 클러스터의 헤더들만 RTS /CTS 메시지 교환을 위해 무선 송수신 모듈을 활성화 하는데 자신 클러스터 ID가 목적지 클러스터로 지정된 RTS 메시지를 수신한 클러스터 헤더는 다수노드 들의 무선 송수신 모듈을 활성화시켜 DATA 메시지 수신과 ACK 메시지 송신에 참여한다. 이 단계에서 각 노드 접근제어는 각 구성요소들이 자원에 접근을 할 때 이루어져야 하며, 인증 작업을 통해 완성될 수 있다. 의료정보시스템 간 정보 활용이 연계, 통합화 되는 환경에서 전송계층 보안 프로토콜인 인증 및 암호화 통신 SSL/TLS를 사용한다.

#4. WAN Gateway 보안 필터링 : 현장 사용자 디바이스에서 출발하는 트래픽은 3G 무선통신망 또는 웹을 사용하여 장거리 통신망을 통해 정보 시스템 인프라에 접속된다. 공개키 알고리즘을 사용하여 웹브라우저를 이용하여 시스템에 접근 가능하도록 하고 사용자인증은 전자 서명에 기반 한 사용자 인증 기능을 적용한다. 센서 네트워크에서의 정보 전달 서비스는 메시지 교환과 전달로 인해 보안 문제가 필수적인 문제점으로 부각되고 있다. 이를 해결하기 위한 각 시스템 개체 사이의 보안은 세션 단위 보안 메커니즘을 가능하게 하고 있으며, 동기화로 인한 오버헤드를 줄일 수 있도록 해준다. 트래픽 전송과정의 보안이 이루어지기 위해서는 많은 필터들이 중간에 존재해야 한다. 필터링 작업은 정보 전달자에게 라우팅 된 메시지의 내용들을 해석 할 수 있도록 해야 한다. 보안검증 작업은 필터링이 이루어지는데 초점을 맞추며 point -to-point 커뮤니케이션이 이루어질 수 있도록 중재 하도록 한다.

#5. 동적 네트워킹 단계 : u-Healthcare 네트워크는 동적인 환경으로 다양하고 새로운 네트워크 위협 공격이 지속적으로 등장한다. 위협에 대처하기 위한 센싱 애플리케이션 보안 알고리즘은 CA(Client Application)기능적 요구 사항, publish/subscribe routing layer, 데이터 publish, query interface, RF-based location tracking 등이 구성되어야 한다. 멀티 센서 디바이스들은 모든 수신자에게 데이터를 중계하기 위해 mesh 네트워킹을 이용한 publish/ subscribe routing frame work를 기반으로 구성한다. 각 센서 노드들은 vital signs, location, identity 정보를 알리고, 각 디바이스는 발신자로부터 수신자에게 데이터를 라우팅 한다. 네트워크 안에서는 대역폭의 한계와 정보의 오버 헤드를 막기 위해 데이터 필터링과 통합 과정을 거친다. 이 과정에서 전송 계층 보안과 네트워크 계층 보안 프로토콜이 사용 되어야 한다. Network Layer 보호서비스는 대등 실체 인증, 데이터 발신처 인증, 접근제어, 접속 비밀 보장, 트래픽 흐름비밀보장, 접속 무결성이 이루어져야한다.

#6. 의료진 Location Tracking : 트래픽처리 단계중 환자와 의사, 간호사 등 단말 노드를 사용하는 관련자의 현재 위치정보를 추적 시 분산되어 있는 RF 기반 위치추적 시스템을 사용한다. 이 과정에 identity 보호 및 비 인가 구성에 대한 신뢰 측정이 이루어지도록 한다. 현재의 무선 통신 기술기반에서는 복수 환자와 의사간 통신 사용 시 위치정보 추적에 충분한 거리는 약 1M 이내에서 80% 정도 위치 추적율을 보이고 있다. 각 beacon node 는 정기적으로 무선 메시지를 발신한다. 무선통신 Mobile node는 beacon과 각 beacon node, 주파 수, power level를 위한 평균 received

signal strength(RSSI), 신호강도 같은 signature를 획득 한다. 각 beacon node는 주기적으로 주파수와 전달 power level의 범위에 무선 메시지를 발신한다. Mobile node는 beacon과 각 beacon node, 주파수, power level을 위한 평균 received signal strength (RSSI)같은 signature를 획득 한다. 무선, 모바일 통신 과정에서 환경에 적합한 경량암호 및 인증기술, 경량 키 관리 기술, 부 채널 공격방지 보안기술이 적용 되도록 한다.

5. 결 론

u-Healthcare용 ad hoc기반 센서 네트워크에서 의료 데이터의 유효성은 중요하기 때문에 통신 간섭에 의해 패킷이 손실되는 것을 최대한 방지하여 신뢰성 통신을 유지해야 한다. 스마트 센서는 컴퓨터 기술과의 결합에 의해서 센서기능을 대폭적으로 향상시킨 지능화된 센서이다. USN은 무선을 이용하여 스마트 센서들을 네트워크로 연결한다. OS는 tiny OS를 이용하고 무선 의료 센서와 PDA등의 디바이스를 사용한다. SOA 기반 보안 메커니즘을 확보하기 위해서 두 가지 접근 방법에 기초하는데 하나는 모델 기반으로 보안 패턴기반 유형을 개발하여 적용하는 것이며 이는 계층화된 보안 패턴의 맵을 설계하여 적용하는 것이다. 다른 하나는 보안기능을 별도의 분리 된 알고리즘으로 접근하는 방법이 아니라 정보 처리 기능 핵심 단계에서 취약점을 예방하는 기능 측면의 알고리즘을 적용하는 것이다. 기본적인 보안 메커니즘을 정보처리 기능구조와 동작에서 보안을 반영한다. 이 연구에서 제안된 센싱 보안 프레임워크 모델 대처방식이 현장의 의료정보 시스템 개발과정에서 참고자료로 활용되기를 기대한다.

참고문헌

[1] K.F. Akyildiz et al., “wirelesssensornetworks:asurvey”,Computernetworks,Vol.38,pp.393-422,March 2002.

[2] Perrig, A., Stankovic, J., and Wagner, D. 2004. Security in wireless sensor networks. Commun. ACM 47, 6 (Jun. 2004), 53-57.

[3] Sensor Networks for Medical Care, Victor Shnayder, Bor-rong Chen, Konrad Lorincz, Thaddeus R. F. Fulford-Jones, and Matt Welsh. Harvard University TechnicalReport TR-08-05,April2005.

[4] Sensor Networks for Emergency Response: Challenges and Opportunities, Konrad Lorincz, David Malan, Thaddeus R. F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoff Mainland, Steve Moulton, and Matt Welsh. In IEEE Pervasive Computing,SpecialIssueonPervasiveComputingforFirstResponse,Oct-Dec2004.

[5] A Portable, Low-Power, Wireless Two-Lead EKG System, Thaddeus R. F. Fulford-Jones, Gu-Yeon Wei, and Matt Welsh. In Proceedings of the 26th IEEE EMBS Annual International Conference, SanFrancisco, September2004

[6] CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, David Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. International Workshop on Wearable and Implantable Body Sensor Networks, April 2004.

[7] Lifeguard Overview, Stanford Lifeguard Website, Retrieved December 23,2004 URL: http://lifeguard.stanford.edu/lifeguard_flyer.pdf

[8] Biomedical telemedicine - CSCI E-170 January 11, 2005

[8] Healthwear:Medical Technology Becomes Wearable - 2004 IEEE

[9] Vital Positioning System Product Page, Medical Intelligence website, Retrieved December28,2004.

[저 자 소 개]

김 점 구 (Jeom goo Kim)

1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재 남서울대학교
컴퓨터학과 교수
IT융합연구소장

email : jgoo@nsu.ac.kr

노 시 춘 (SiChoon Noh)

1987년 : 고려대학교
경영정보학(석사)
2005년 : 경기대학교
정보보호기술(박사)
2002년 : KT 시스템보안부장
2004년 : KT 충청전산국장
2005년~현 재 : 남서울대학교
컴퓨터학과 교수
2011년~현 재 : 남서울대학교
IT융합연구소 연구위원

email : nsc321@nsu.ac.kr