체내 삽입장치간 동기화를 위한 환자 인증 프로토콜

정윤수* · 김용태**

Patient Authentication Protocol for Synchronization between Implantable Medical Device

Yoon-Su Jeong* · Yong-Tae Kim**

본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.

요 약

최근 IT 기술과 의료기술이 접목된 유헬스케어 서비스 중 불치병을 갖고 있는 환자에게 의료 서비스를 제공하는 체내삽입장치 기술이 각광을 받고 있다. 그러나 체내삽입장치 기술은 환자의 생체정보를 무선구간에서 제3자에게 쉽게 유출되어 악용될 수 있는 보안문제가 나타나고 있다. 본 논문에서는 환자와 병원관계자간 동기화를 통해 환자와 병원관계자가 서로 생성한 랜덤값과 인증서버가 생성한 랜덤값을 이용하여 환자와 병원관계자를 인증하는 인증 프로토콜을 제안한다. 특히, 제안 프로토콜은 환자와 병원관계자가 사전에 인증서버에 등록된 정보를 이용하여 생성한 보안 정보를 세션키 생성과정에 이용함으로써 인증서버에게 허락받지 못한 제3자의 접근을 차단함으로써 안정성을 높이고 있다.

ABSTRACT

Among U-healthcare services adapting the latest IT technique and medical technique, a body-injecting device technique providing medical service to a patient who has incurable disease. But the body-injecting device technique can be easily exposed during wireless section to the third person and it can be used illegally. This paper proposes certification protocol which certifies a patient and hospital staff using random number created by certification server and a patient with hospital staff by synchronization. Specially, the proposed protocol uses security information created by information registered in certification server previously by a patient and hospital staff so that in keeps from accessing of third person who didn't get approval. And it gives more stability.

키 워드

체내삽입장치, 키 분배, 프로토콜, 이산대수

Key word

Implantable Device, Key Distribution, Protocol, Discrete Logarithm Problem

* 정회원 : 목원대학교 정보통신공학과 교수 (제1저자, bukmunro@gmail.com)

접수일자 : 2012. 07. 30

** 정회원 : 한남대학교 멀티미디어학부 교수 (교신저자)

심사완료일자 : 2012. 08. 21

I. 서 론

IT 기술이 의료기술에 접목되면서 의료서비스는 불치병(심장병, 당뇨병, 심근경색 등)을 갖고 있는 환자의 신체에 센서들을 부착하여 언제, 어디서나 의료 서비스를 지원받을 수 있다[1]. 그러나, 환자에게 부착된 센서는 무선 구간을 통해 병원관계자(의사, 간호사, 약사 등)에게 전달되기 때문에 제3자에게 환자의 생체정보가 노출될 수 있다[2]. 이러한 보안 문제를 해결하기 위해서 많은 연구자들이 체내삽입장치와 관련된 보안 연구를 활발하게 수행하고 있지만 현재까지 현실에 적합한 연구 성과가 나타나고 있지 않은 실정이다.

불치병 환자에게 사용되는 체내삽입장치(심장 페이스메이커나 제세동기와 같은 장치)는 환자의 생명과 개인정보가 직접적으로 연관되어 있어 제3자로부터 공격(reply 공격, Man-in-the-Middle 공격 등)을 받을 경우 쉽게 환자 정보가 노출될 수 있는 문제가 있다[3].

최근 연구에서는 환자 신체에 부착된 체내삽입장치에서 발생하는 생체정보의 안전성을 높이기 위해서 체내삽입장치를 구성하는 의료장비들에게 키 분배 프로토콜을 통해 사전에 암호키를 분배하고 있다[4]. 그러나, 환자들이 체내삽입장치를 많이 사용하면서 환자의 생체정보를 병원관계자에게 전달할 때 발생하는 지연 및 보안 문제 등으로 인하여 생체정보의 안전성을 보장할 수 못하고 있다. 만약 제3자가 환자와 병원관계자 사이에서 reply 공격과 man-in-the-middle 공격 등을 수행할 경우 보안위협이 쉽게 발생할 수 있다[5].

본 논문에서는 유헬스케어 환경에서 체내삽입장치를 부착한 환자의 생체정보를 안전하게 병원관계자에 전달하기 위한 인증 프로토콜을 제안한다. 제안 프로토콜은 환자와 병원관계자간 동기화를 유지하기 위해서 환자와 병원관계자가 서로 생성한 랜덤 수를 조합하여 보안 정보를 사용한다. 특히, 제안 프로토콜은 보안 정보의 안전성을 이산대수문제를 이용하여 생성함으로써, 관리자로부터 접근 허가가 승인된 환자나 병원관계자의 정보 이외의 허가받지 않은 정보에 대해서 제 3자가 쉽게 접근하지 못하도록 하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어 환경의 체내삽입장치 및 보안 요구사항에 대해서 알아본다. 3장에서는 이산대수문제 기반의 환자와 병원관계자간 동기화를 유지하기 위한 키를 생성하는

인증 프로토콜을 제안하고, 4장에서는 유헬스케어 환경에서 발생하기 쉬운 보안 공격유형에 대해서 안전성과 효율성을 평가하고, 마지막으로 5장에서 결론을 맺는다.

II. 관련 연구

2.1. 유헬스케어 서비스

유헬스케어 서비스는 기존 의료 서비스에 유·무선 온라인 네트워크를 적용하여 전자적 의료정보 및 진료 예약관리 등을 진화시킴으로써 환자의 상태를 언제 어디서나 수집, 처리, 전달, 관리 할 수 있는 의료서비스를 의미한다[3].

그림 1. 유헬스케어 시스템의 구조
Fig. 1 Structure of u-Healthcare System

그림 1은 유헬스케어 서비스에 대한 개념도이다[6]. 그림 1에서 환자와 병원관계자 사이에서 유헬스케어 서비스를 구성하는 일반적인 항목은 센싱, 모니터링, 분석 및 피드백 등으로 구성된다. 센싱과정은 가정 환경에서 환자 자신의 상태를 혈압, 당뇨, 심전도, 체지방 분석 등의 정보를 인터넷을 통해 유헬스케어 서비스 센터에 전달한다. 모니터링 과정은 이동형 측정기기를 사용하여 가정에 있는 환경처럼 환자의 상태를 24시간 모니터링하여 문제가 발생할 경우 바로 탐지한다. 분석 및 피드백 과정은 의사가 환자의 상태정보를 분석하여 유헬스케어 서비스 센터를 통해 처방을 한다.

2.2. 유헬스케어 환경의 체내삽입장치

체내삽입장치를 부착한 환자는 유·무선 온라인 네트워크를 통해 환자의 생체정보를 병원관계자(의사, 간호사, 약사 등)에게 전달함으로써 병원관계자는 환자의

표 1. 헬스케어 센서의 개발 동향용어 정의
Table. 1 Notation Definition of Development Review in u-Healthcare Sensor

활동영역	주요 애플리케이션		개발 기업
예방	유해 인자 감지	환경 오염 물질 감지, 세균·바이러스 등 병원성 미생물 감지 등	Applied Enzyme Technology, BioDot, Ercon, Institute of Bioscience 등
	건강 증진 및 관리	혈당·혈압 측정기, 체중·체지방 측정기, 운동량 측정기 등	Omron, Roche Diagnostics, Johnson & Johnson Medical 등
진단	현장 진단	혈당 검사, 임신 테스트, 약물 남용 검사, 감염 질환(조류독감, 식중독균 등) 검사 등	Biozyme Laboratories, Dupont, Roche Diagnostics, 나노엔텍, 바이오메드랩 등
	임상 검사	암 검사, 감염 질환(AIDS 등) 검사, 각종 임상 화학 검사(혈액, 대·소변, 타액) 등	
모니터링	환자 모니터링	혈압·혈당·맥박 산소 측정기, 심전계 등	CE Healthcare, Philips, Siemens, Cardiac Science, Medtronic, SmartPill 등
	고령자 모니터링	동작·활동량 감지 가능한 모션 센서, 웨어러블 모니터링 솔루션 등	CE Healthcare, Intel, 비트컴퓨터 등

참고문헌 : LG Business Insight 2009. 4 [7]

상태를 언제, 어디서나 수집, 처리, 전달, 관리할 수 있다. [3].

표 1은 LG 비즈니스에서 2009년 유헬스케어 서비스의 활동영역을 예방, 진단, 모니터링 등으로 구분하여 기업들이 헬스케어 센서를 활용하고 있는 주요 애플리케이션과 개발 기업들을 조사한 결과이다. [표 1]의 결과처럼 체내삽입장치를 사용하고 있는 유헬스케어 서비스는 현재까지 센서와 통신·의료 인프라 간 연계가 부족, 기술적 한계, 고비용, 소비자 친화적인 ‘Easy-to-USE’ 시스템의 부재 등의 문제점이 나타나고 있다[7].

2.3. 기존 연구분석

체내 삽입장치를 사용하는 환자의 증가는 체내삽입장치에 대한 보안 연구를 수행하는 연구자의 연구동기가 되었다. T. Denning et. al[8]는 체내삽입장치의 안전성을 향상시키기 위해서 응급상황에서 체내삽입장치의 물리적 환경의 속성 정보를 이용한 fail-open 개념을 제안하였다. [8]에서 제안한 fail-open 개념은 공격자가 체내삽입장치에 접근을 시도할 경우 발생할 수 있는 새로운 보안 위협을 소개하고 있다. 센서를 이용한 환경에서는 전파방해(jamming)와 관련된 스푸핑 공격을 예방하기 위한 연구가 활발히 진행되고 있다[9,10,11]. 그러나 센서를 부착한 체내삽입장치에서는 전파방해와 관련된 보안 공격에 대한 보안 연구가 미약하다. 체내삽입장치

에서는 하드웨어 제약과 밴드(band) 규정 때문에 anti 전파방해 전략[12]과 직접 시퀀스 확산 스펙트럼 변조(Direct-Sequence Spread Spectrum Modulation)를 적용할 수 없다. [5]에서는 단순한 ECG 신호상에서 추출된 FFT(Fast Fourier Transform)의 계수가 키로 사용된다. 그러나 [5]에서는 입력 샘플들을 통하여 키를 생성하는데 요구되는 기본적인 엔트로피 비트를 가지고 키를 생성하는데 충분한 엔트로피를 얻을 수 있는지에 대한 엄격한 실험을 하지 못하고 있다. 그리고 [13]은 해쉬 후에 키를 평가하고 있기 때문에 논리적으로 정확하지 않다. Poon et. al.[11]는 ECG와 PPG (photoplethysmogram) 신호 구현에 [5]를 적용하였다.

III. 체내삽입장치를 위한 키 관리 프로토콜

이 절에서는 체내삽입형 장치를 부착한 환자의 생체 정보를 안전하게 전달하기 위한 인증 프로토콜을 제안한다.

3.1. 개요

체내삽입장치를 부착한 환자가 병원관계자(의사/간호사/약사 등)와 통신하기 위해서 인증서로부터 전달받

은 익명의 인식자 $AID(Anonymous\ Identity)$ 와 랜덤수 $R = \{x_1, x_2, \dots, x_{\phi(n)}\}$ 을 이용하여 세션키를 생성하기 위한 환경을 그림 2에서 보여주고 있다.

그림 2. 제안 프로토콜의 환경
Fig. 2 Environment of Proposed Protocol

그림 2에서 환자와 병원관계자는 생체정보를 송·수신하기 전에 인증서버로부터 랜덤수의 집합 R 을 전달받아야 한다. 이 때, 병원관계자가 전달받은 랜덤수의 집합 R 은 환자와 동일한 랜덤수의 집합이며 환자마다 다르다. 만약 제3자가 불법적으로 인증서버나 환자의 체내 삽입장치에 접근하여 생체정보를 수집하려할 경우 관리자는 세션키를 이용하여 불법적 접근을 제어할 수 있다. 이 때, 세션키는 환자의 체내삽입장치와 병원관계자 간 서로 송·수신되는 생체정보의 동기화 기능을 수행한다.

3.2. 용어 정의

표 2는 제안된 프로토콜에서 사용하는 용어에 대한 설명이다.

표 2. 용어 정의
Table. 2 Definition of Terminology

용어	정의
ID	사용자 인식자
AID	익명의 인식자
p, q	숫수
SI	서로 소인 p, q 를 이용한 보안 인식자
R	인증서버의 랜덤수 집합
$x_1, x_2, \dots, x_n$	랜덤수 집합 R 의 원소

HR	병원관계자의 랜덤수
n	원소의 갯수
$\parallel$	XOR 연산
$h()$	해쉬 함수

3.3. 키 관리 프로토콜

환자와 병원관계자간 생체정보를 안전하게 송·수신하기 위해서는 환자의 병원관계자가 서로 공유할 수 있는 세션키가 필요하다. 제안 프로토콜은 사전단계, 키생성단계, 키검증단계 등 3단계로 구성된다.

3.3.1. 사전단계

이 단계는 환자와 병원관계자간에 생체정보의 전송 및 갱신을 위한 키 생성을 위한 사전 정보를 인증서버에 전달하는 단계이다. 환자는 인증서버에게 환자의 인식자 *ID* 관리자를 통해 인증서버에게 환자의 인식자를 전송한다. 인증서버는 전송된 환자의 인식자 *ID*를 해쉬함수 $h()$ 에 적용하여 익명의 인식자 *AID*를 생성한다.

$$AID = h(ID) \quad \text{식 (1)}$$

관리자는 병원관계자에게 환자의 생체정보에 접근하기 위한 인식자와 병원관계자가 생성한 랜덤수 HR 을 인증서버에게 전달한다. 전달된 정보 중 병원관계자의 랜덤수 HR 은 식 (2)처럼 환자의 익명 인식자 AID 와 XOR하여 해쉬한 결과를 S 로 대체한다.

$$S = h(AID \parallel HR) \quad \text{식 (2)}$$

인증서버는 인증서버가 생성한 숫자 n 과 함께 환자
에게 AID 와 S 를 함께 전달하고 병원관계자에게는 n
과 S 를 전달한다.

3.3.2. 키 생성단계

이 단계는 인증서버가 환자와 병원관계자 사이에서 환자의 생체정보를 안전하게 전달하기 위한 세션키를 생성하는 단계이다. 관리자는 환자와 병원관계자간의 동기화를 유지하기 위해서 환자와 병원관계자가 임의로 선택한 서로 소인 숫수 p 와 q 를 요청하여 식 (3)을 생성한 후 인증서버에 저장한다.

$$SI = \prod_{i=1, j=1}^n p_i q_j \quad \text{식 (3)}$$

식 (3)은 환자와 병원관계자 사이에서 송 · 수신되는 정보가 제3자에게 유출되지 않도록 키 생성단계에서 만들어진 보안정보로써, 인증서버에 의해 환자와 병원관계자의 동기화를 유지하기 위해 사용된다. 식 (3)이 생성된 이후 인증서버는 인증서버가 생성한 랜덤 수의 집합 R 을 식 (4)처럼 생성한다.

$$R = \{x_1, x_2, \dots, x_{\Phi(n)}\} \quad \text{식 (4)}$$

여기에서, $\Phi(n)$ 은 n 에 서로 소인 n 보다 작은 양의 정수의 개수를 의미한다. 만약 n 이 숫수라면 $\Phi(n) = n-1$ 이 된다.

인증서버는 모듈러 n 상에서 S 를 식 (4)의 각 원소에 곱하여 식 (5)와 같은 정보 중에서 세션키를 선택한다.

$$M = \{(Sx_1 \bmod n), (Sx_2 \bmod n), \dots, (Sx_{\Phi(n)} \bmod n)\} \quad \text{식 (5)}$$

식 (5)에서 S 는 n 과 서로 소이고 x_i 는 n 과 서로 소가 되기 때문에 Sx_i 도 n 과 서로 소가 된다. 이와 같이 식 (5)의 M 은 n 과 서로 소인 n 보다 작은 정수들로 구성된다. M 에서 중복되는 정보들은 존재하지 않는다. 만약 식 (6)과 같은 결과가 나타난다면 그때는 x_i 와 x_j 가 같은 결과값이 된다.

$$Sx_i \bmod n = Sx_j \bmod n \quad \text{식 (6)}$$

인증서버는 세션키 M 을 환자와 병원관계자에게 전달한다.

3.3.3. 키 검증단계

이 단계는 환자와 병원관계자 사이에서 환자의 생체 정보를 송 · 수신하기 위한 세션키를 검증하는 단계이다. 환자는 인증서버로부터 전달받은 정보를 이용하여 식 (7)~식(10)처럼 세션키를 추출하여 인증서버가 발급한 세션키가 맞는지 검증과정을 수행한다.

$$M = \prod_{i=1}^{\Phi(n)} (Sx_i \bmod n) = \prod_{i=1}^{\Phi(n)} x_i \quad \text{식 (7)}$$

$$\prod_{i=1}^{\Phi(n)} ax_i \equiv \prod_{i=1}^{\Phi(n)} x_i \pmod{n} \quad \text{식 (8)}$$

$$S^{\Phi(n)} + \left[\prod_{i=1}^{\Phi(n)} x_i \right] \equiv \prod_{i=1}^{\Phi(n)} x_i \pmod{n} \quad \text{식 (9)}$$

$$S^{\Phi(n)} \equiv 1 \pmod{n} \quad \text{식 (10)}$$

병원관계자는 S 를 도출하여 병원관계자의 랜덤수 HR 을 식 (11)에 XOR하여 환자의 익명 인식자 AID 를 추출한다.

$$AID' = h(AID \parallel HR) \parallel HR \quad \text{식 (11)}$$

병원관계자는 관리자를 통해 환자의 익명 인식자 AID 를 전달받아 식 (11)에서 생성한 AID' 를 식 (12)처럼 비교 검증한다.

$$AID = AID' \quad \text{식 (12)}$$

환자는 병원관계자가 수행한 식 (11)~식 (12)과정과 동일한 방법으로 식 (13)~식 (14)처럼 병원관계자의 랜덤수 HR 을 비교검증한다.

$$HR' = h(AID \parallel HR) \parallel AID \quad \text{식 (13)}$$

$$HR = HR' \quad \text{식 (14)}$$

환자와 병원관계자는 생성된 세션키 M 을 사용하여 병원관계자에게 환화하자의 생체정보를 암호하여 전달함으로써 환자와 병원관계자의 무결성을 보장받는다.

IV. 평 가

4.1. 재사용 공격

병원관계자가 환자의 생체정보를 요청하기 위해서

는 우선 병원관계자가 합법적인지를 검사해야 한다. 제안 프로토콜에서는 병원관계자가 인증서버에게 인증 정보를 전달하여 합법적인 사용자인지를 판별하고 있다. 특히, 제3자는 체내삽입장치의 재사용 공격을 통하여 환자의 생체정보를 불법적으로 수집할 수 있기 때문에 제안 프로토콜에서는 사전에 등록된 환자와 병원관계자의 랜덤수를 $M = \{(Sx_1 \bmod n), (Sx_2 \bmod n), \dots, (Sx_{\phi(n)} \bmod n)\}$ 처럼 인증서버가 생성한 랜덤 수의 집합 $R = \{x_1, x_2, \dots, x_{\phi(n)}\}$ 의 정보와 각각 곱하여 세션키를 생성함으로써 제3자에게 도청되더라도 안정성을 보장 받게 된다.

환자와 병원관계자는 관리자로부터 전달받은 M 의 정보 중에서 임의의 한 개 원소를 추출하여 세션키로 사용하면서 S 정보를 구성하고 있는 AID 와 HR 를 환자와 병원관계자가 서로 검증하기 때문에 재사용 공격에 안전하다.

4.2. 스푸핑 공격

제안 프로토콜에서는 제3자가 병원관계자의 시리얼 번호 HR 를 이용하여 HR' 을 생성할 경우 환자의 실제 인식자 ID 와 환자가 생성한 숫자 p 를 알지 못하기 때문에 제3자는 SI 와 S 정보를 유추하지 못한다. 또한, 제3자가 환자의 익명 인식자 AID 를 유추하기 위한 환자의 인식자 ID 를 알지 못한 상태에서 관리자를 통해 인증서버에 전달되는 정보는 이전 세션동안 도청한 정보를 대신 전송하게 된다. 그러나 인증서버는 SI 와 함께 세션키 M 을 결정하는 AID 와 HR 를 서로 비교하여 환자와 병원관계자를 동기화 시키기 때문에 제3자의 공격을 막을 수 있다.

4.3. 정보노출방지

제안 프로토콜에서는 병원관계자가 환자의 생체정보를 요청할때마다 병원관계자는 랜덤수 HR 를 생성하고 환자의 익명의 인식자 AID 를 해쉬함수 $h()$ 에 적용한다. 또한, 환자와 병원관계자의 동기화를 위해 병원관계자가 환자의 생체정보를 요청할 때마다 환자와 병원관계자가 선택한 서로 소인 p 와 q 를 매번 생성하여 SI 정보를 생성한다. 만약 제3자에 의해 환자의 생체 정보가 노출될 경우 제3자는 환자의 생체정보를 획득하기 위해 인증서버로부터 환자의 병원관계자의 정보를 획득

하여야 하지만 제안 프로토콜에서는 제3자가 불법적으로 유추할 수 없도록 세션키 M 을 생성하여 환자의 생체정보노출을 사전에 예방한다.

4.4. 프라이버시 예방(Privacy Protection)

제안 프로토콜은 환자의 생체 정보를 수집하기 전에 인증서버에게 환자와 병원관계자의 인증 정보를 사전에 등록하여 병원관계자가 환자의 생체정보에 접근할 경우 접근 여부를 판별할 수 있도록 하여 환자의 프라이버시를 안전하게 예방할 수 있도록 한다. 제안 프로토콜에서는 사전에 등록된 정보를 이용하여 세션키를 생성하여 환자, 관리자, 병원관계자가 서로 독립적으로 세션키를 공유할 수 있도록 함으로써 제3자가 불법적으로 키를 공유하려고 시도하더라도 키를 유출할 수 있는 정보를 추출하지 못하기 때문에 세션키를 생성할 수 없다. 또한, 환자와 병원관계자가 각각 사전에 랜덤 값을 생성하여 인증서버에 등록할 때 환자와 병원관계자의 랜덤 값으로 해쉬한 S 와 환자와 병원관계자간의 동기화를 유지하기 위해서 환자와 병원관계자가 임의로 선택한 서로 소인 p, q 를 매 세션마다 생성하여 보안 정보 SI 로 관리하기 때문에 제3자가 공유된 세션키를 유추하기가 어렵다. 만약 제3자가 세션키를 유추하더라도 독립적으로 서로 공유된 세션키를 모두 추출하지는 못하고, 환자의 인식자 ID 를 해쉬함수 $h()$ 에 적용하여 익명의 인식자 AID 를 생성하기 때문에 공격자가 특정 환자를 식별할 수 없어 환자의 프라이버시를 제공한다.

4.5. 환자 익명성

제안 프로토콜에서는 체내삽입장치를 부착한 환자의 인식자 ID 를 인증서버에 전달하여 인증서버가 해쉬함수 $h()$ 에 적용하여 익명의 인식자 AID 를 환자에게 전달하여 사용하기 때문에 공격자가 체내삽입장치의 생체정보를 불법적으로 추출하려고 하더라도 환자 자신이 생성한 ID 를 추측할 수 없기 때문에 환자의 익명성을 제공한다.

V. 결 론

최근 불치병을 갖고 있는 환자에게 센서를 부착하여 의료서비스를 제공하는 체내삽입장치 기술이 증가하

고 있다. 그러나 무선 구간에서 환자의 생체정보를 불법적으로 악용하는 보안 피해도 급증하고 있는 추세이다. 본 논문에서는 체내삽입장치를 부착한 환자의 생체정보를 안전하게 병원관계자에게 전달할 수 있도록 환자와 병원관계자간 동기화를 통해 환자와 병원관계자를 인증할 수 있는 인증 프로토콜을 제안하였다. 제안된 프로토콜은 환자와 병원관계자를 동기화하기 위해서 환자와 병원관계자가 생성한 랜덤값을 인증서버에 등록하여 인증서버가 생성한 랜덤값과 조합하여 인증정보를 생성함으로써 인증서버에 승인받지 못한 제3자의 접근을 사전에 차단함으로써 보안성을 높였다. 향후 연구로 본 연구에서 조사된 결과를 기반으로 체내 삽입장치에 실제 적용하여 효율성 평가를 수행할 계획이다.

참고문헌

- [1] Y. S. Jeong(2012), "RFID-based Authentication Protocol for Implantable Medical Device", The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 141-146.
- [2] Y. S. Jeong and S. H. Lee(2012), "u-Healthcare Service Authentication Protocol based on RFID Technology", The Journal Of Digital Policy & Management, Vol. 10, No. 2, pp. 153-160.
- [3] 정윤수, 이상호(2012), "상태정보에 따른 체내삽입형 장치를 부착한 유-헬스케어 환자의 프라이버시 보호 프로토콜", 한국통신학회논문지 제37권 제4호(융합기술), pp. 277-353
- [4] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta(2010), "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", Vol. 14, No. 1, pp. 60-68.
- [5] S. Cherukuri, K. Venkatasubramanian, and S. Gupta(2003), "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body", International conference on Parallel Processing Workshops.

- [6] 이봉근, 정윤수, 이상호, "u-헬스케어 환경에서 환자의 무결성을 보장하는 RFID 보안 프로토콜", 한국정보통신학회논문지, 제16권 3호, pp. 13-19, 2012년 3월.
- [7] 고은지(2009), "헬스케어 혁명을 선도하는 스마트 센서", LG Business Insight, pp. 37-44.
- [8] T. Denning, K. Fu, and T. Kohno(2008), "Absence makes the heart grow fonder: new directions for implantable medical device security", In HotSec.
- [9] L. Sang and A. Arora(2008), "Capabilities of low-power wireless jammers", Technical Report OSU-CISRC-5/08-TR24, Ohio State Univ.
- [10] I. Martinovic, P. Pichota, and J. Schmitt(2009), "Jamming for good: a fresh approach to authentic communication in WSNs", In Wisec.
- [11] C. Poon, Y. Zhang, and S. Bao(2006), "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health", IEEE Communications Magazine, 44(4):73-81.
- [12] M. Strasser, C. Popper, S. Capkun, and M. Galaj(2008), "Jamming-resistant key establishment using uncoordinated frequency hopping", In IEEE Symposium on Security and Privacy.

저자소개

정윤수(Yoon-Su Jeong)

1998. 청주대학교 전자계산학과 학사

2000. 충북대학교 대학원 전자계산학과 석사

2008. 충북대학교 대학원 전자계산학과 박사

2008.3 ~ 2009.8 충북대 및 한남대 시간강사

2009.9 ~ 2012.2 한남대학교 산업기술연구소 전임연구원

2012.3 ~ 현재 목원대학교 정보통신공학과 교수

※ 관심분야: IPTV, 정보보호, 암호이론, Network Security, 유 · 무선통신보안

김용태 (Yong-Tae Kim)

1984. 한남대학교 계산통계학과
학사.

1988. 숭실대학교 전자계산학과
석사.

2008. 충북대학교 전자계산학과 박사.

2002. 12. ~2006.2 (주)가림정보기술 이사

2010. 8 ~ 현재 한남대학교 멀티미디어 학부 교수

※ 관심분야: 모바일 웹서비스, 정보보호, 센서 웹,
모바일 통신보안