(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년01월08일
(11) 등록번호 10-1583311
(24) 등록일자 2015년12월31일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2014-0113021
(22) 출원일자 2014년08월28일
심사청구일자 2014년08월28일
(56) 선행기술조사문헌
JP2012123614 A
KR100416894 B1
KR100407900 B1

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
최원석
서울 강북구 삼양로 256, 105동 501호 (미아동, 래미안미아1차아파트)
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
(74) 대리인
김등용

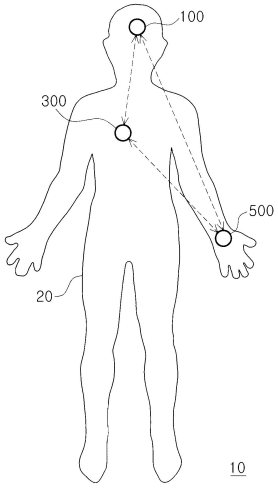
전체 청구항 수 : 총 9 항 심사관 : 문형섭

(54) 발명의 명칭 **키 교환 방법 및 바디 센서**

(57) 요 약

키 교환 방법이 개시된다. 상기 키 교환 방법은, 제1 바디 센서가 제2 바디 센서로 상기 제1 바디 센서의 ID와 상기 제2 바디 센서의 ID를 포함하는 키 교환 요청 메시지를 송신하는 단계, 상기 제1 바디 센서가 적어도 하나의 공유값을 생성하는 단계, 상기 제1 바디 센서가 미리 정해진 시간 구간 동안 인체의 생체정보를 측정하는 단계, 상기 제1 바디 센서가 회귀 분석을 통하여 측정된 생체정보로부터 생체정보 함수를 생성하는 단계, 상기 제1 바디 센서가 상기 적어도 하나의 공유값을 입력으로 하는 상기 생체정보 함수의 값을 이용하여 키를 생성하는 단계, 및 상기 제1 바디 센서가 생성된 키를 하나의 입력으로 하는 해시값을 상기 제2 바디 센서로 송신하는 단계를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 2013043620
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 원천기술개발사업
연구과제명 개인 프라이버시 보장 원격 접근기술(총괄:super mobile 구현을 위한 시스템 SW 원천기술 연구)
기 여 율 1/1
주관기관 성균관대학교
연구기간 2013.07.01 ~ 2014.06.30

명 세 서

청구범위

청구항 1

제1 바디 센서가 제2 바디 센서로 상기 제1 바디 센서의 ID(identification)와 상기 제2 바디 센서의 ID를 포함하는 키 교환 요청 메시지를 송신하는 단계;

상기 제1 바디 센서가, 상기 제2 바디 센서와 공유되는 적어도 하나의 공유값을 생성하는 단계;

상기 제1 바디 센서가 미리 정해진 시간 구간 동안 인체의 생체정보를 측정하는 단계;

상기 제1 바디 센서가 회귀 분석(Regression Analysis)을 통하여 측정된 생체정보로부터 생체정보 함수를 생성하는 단계;

상기 제1 바디 센서가 상기 적어도 하나의 공유값을 입력으로 하는 상기 생체정보 함수의 값을 이용하여 키를 생성하는 단계; 및

상기 제1 바디 센서가 생성된 키를 하나의 입력으로 하는 해시값을 상기 제2 바디 센서로 송신하는 단계를 포함하는 키 교환 방법.

청구항 2

제1항에 있어서,

상기 키 교환 방법은,

상기 제1 바디 센서가 상기 생성된 키와 상기 제2 바디 센서가 생성한 키가 동일함을 확인하는 확인 메시지를 상기 제2 바디 센서로부터 수신하는 단계를 더 포함하는 키 교환 방법.

청구항 3

제1항에 있어서,

상기 해시값은 상기 제1 바디 센서의 ID, 상기 제2 바디 센서의 ID, 및 상기 적어도 하나의 공유값 중 적어도 하나를 추가적인 입력으로 하는 해시값인, 키 교환 방법.

청구항 4

제1항에 있어서,

상기 생체정보 함수를 생성하는 단계는 정현파(sinusoidal wave) 함수를 모델로 이용하는 키 교환 방법.

청구항 5

제1항에 있어서,

상기 키를 생성하는 단계는,

상기 적어도 하나의 공유값들 각각을 입력으로 하는 다수의 생체정보 함수 값들에 배타적 논리합(exclusive OR) 연산을 수행하여 상기 키를 생성하는, 키 교환 방법.

청구항 6

제2 바디 센서로 제1 바디 센서의 ID와 상기 제2 바디 센서의 ID를 포함하는 키 교환 요청 메시지를 송신하고, 상기 제2 바디 센서와 공유되는 적어도 하나의 공유값을 생성하는 설정 모듈;

미리 정해진 시간 구간 동안 인체의 생체정보를 측정하는 측정 모듈;

회귀 분석을 통하여 측정된 생체정보로부터 생체정보 함수를 생성하는 회귀 분석 모듈; 및

상기 적어도 하나의 공유값을 입력으로 하는 상기 생체정보 함수의 값을 이용하여 키를 생성하고, 생성된 키를 하나의 입력으로 하는 해시값을 상기 제2 바디 센서로 송신하는 키 생성 모듈을 포함하는 바디 센서.

청구항 7

제6항에 있어서,

상기 키 생성 모듈은,

상기 생성된 키와 상기 제2 바디 센서가 생성한 키가 동일함을 확인하는 확인 메시지를 상기 제2 바디 센서로부터 수신하는 바디 센서.

청구항 8

제6항에 있어서,

상기 해시값은 상기 제1 바디 센서의 ID, 상기 제2 바디 센서의 ID, 및 상기 적어도 하나의 공유값 중 적어도 하나를 추가적인 입력으로 하는 해시값인, 바디 센서.

청구항 9

제6항에 있어서,

상기 키 생성 모듈은,

상기 적어도 하나의 공유값들 각각을 입력으로 하는 다수의 생체정보 함수 값들에 배타적 논리합 연산을 수행하여 상기 키를 생성하는, 바디 센서.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 키 교환 방법에 관한 것으로, 특히 인체의 생체정보를 이용하여 키를 생성하고, 생성된 키를 교환하는 키 교환 방법 및 바디 센서에 관한 것이다.

배 경 기 술

[0002] 건강에 대한 관심의 증가 및 고령화로 인하여, 최근 다양한 형태의 의료 서비스 및 의료 기기가 개발되고 있다. 특히, 환자 신체 내부에 삽입된 형태로 작동하는 이식형 의료 기기는 주기적으로 병원을 방문해야 하는 환자의 병원 방문 횟수를 줄여주거나 심장질환과 같이 갑작스런 몸 이상으로 인해 생명이 위협받는 응급 상황에서 즉각적인 대응을 가능케 할 수 있다.

[0003] 예컨대, 심장박동이 불규칙한 심장질환자는 이식형 페이스메이커를 자신의 가슴에 이식할 수 있다. 그리하여, 이식형 페이스메이커는 심장질환자에게서 불규칙한 심장 박동이 발생할 때 이를 감지하고, 심장박동이 정상이 될 수 있도록 도와준다. 이러한 이식형 의료 기기를 사용하는 환자의 수는 매년 증가하고 있으며 관련 시장 규모도 매년 성장하고 있다.

[0004] 현재 의료 목적으로 사용되고 있는 이식형 의료 기기는 향후 발전하여 의료 분야 뿐만 아니라, 휘트니스(Fitness), 게임 또는 군사 분야 등 다양한 분야에서 활용될 수 있을 것으로 예상된다.

[0005] 이처럼, 이식형 의료 기기를 포함하여 인체에 삽입 또는 부착되는 형태의 센서를 바디 센서(body sensor)라 한다. 바디 센서는 맥박, 혈당 등과 같은 생체정보 뿐만 아니라 사용자의 자세, 시선 등을 측정하여 다양한 애플리케이션에 활용하며, 현재도 다양한 애플리케이션이 지속적으로 개발되고 있는 추세이다. 또한, 향후에는 단일 바디 센서를 활용하는 것 뿐만 아니라 사용자 몸에 부착 또는 삽입된 형태인 다수의 바디 센서가 상호 데이터 교환을 통하여 사용자에게 맞춤화된 서비스를 제공할 수 있는 애플리케이션이 개발될 것으로 예상된다.

[0006] 그러나, 이러한 바디 센서가 측정한 정보가 노출된다면, 심각한 보안상의 문제가 발생할 수 있다. 바디 센서가 측정하는 정보는 사용자의 건강 상태 및 생활 패턴 등을 알 수 있는 매우 민감한 정보이기 때문이다. 따라서, 바디 센서에 적용 가능한 새로운 보안 기술이 필요한 실정이다.

[0007] 다수의 바디 센서들을 포함하는 바디 영역 네트워크(Body Area Networks; BANs)에 보안 기술을 적용하기 위해서

는 바디 센서 간에 키 교환(Key Agreement) 기술이 우선시 되어야 한다. 바디 센서 간에 안전한 키 교환을 통하여 향후 암호화 또는 인증이 가능하게 되기 때문이다. 하지만, 바디 영역 네트워크는 바디 센서들이 추가되거나 제거될 수 있다는 특징과 응급 상황을 고려한 키 관리 기술이 필요하다. 응급 상황을 고려한 키 관리 기술이란 사용자 자신만이 알고 있는 비밀 정보를 이용하여 바디 센서와 통신할 수 있다면, 사용자의 의식이 없는 응급 상황에서 응급 처치를 해주는 의료진이 정상적으로 바디 센서와 통신할 수 없다는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허 제10-1083429호

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적인 과제는 생체정보를 이용하여 생성된 키를 교환함으로써, 보안에 강한 키 교환 방법 및 바디 센서를 제공하는 것이다.

과제의 해결 수단

[0010] 본 발명의 일 실시 예에 따른 키 교환 방법은, 제1 바디 센서가 제2 바디 센서로 상기 제1 바디 센서의 ID와 상기 제2 바디 센서의 ID를 포함하는 키 교환 요청 메시지를 송신하는 단계, 상기 제1 바디 센서가 적어도 하나의 공유값을 생성하는 단계, 상기 제1 바디 센서가 미리 정해진 시간 구간 동안 인체의 생체정보를 측정하는 단계, 상기 제1 바디 센서가 회귀 분석을 통하여 측정된 생체정보로부터 생체정보 함수를 생성하는 단계, 상기 제1 바디 센서가 상기 적어도 하나의 공유값을 입력으로 하는 상기 생체정보 함수의 값을 이용하여 키를 생성하는 단계, 및 상기 제1 바디 센서가 생성된 키를 하나의 입력으로 하는 해시값을 상기 제2 바디 센서로 송신하는 단계를 포함한다.

[0011] 본 발명의 일 실시 예에 따른 바디 센서는, 제2 바디 센서로 제1 바디 센서의 ID와 상기 제2 바디 센서의 ID를 포함하는 키 교환 요청 메시지를 송신하고, 적어도 하나의 공유값을 생성하는 설정 모듈, 미리 정해진 시간 구간 동안 인체의 생체정보를 측정하는 측정 모듈, 회귀 분석을 통하여 측정된 생체정보로부터 생체정보 함수를 생성하는 회귀 분석 모듈, 및 상기 적어도 하나의 공유값을 입력으로 하는 상기 생체정보 함수의 값을 이용하여 키를 생성하고, 생성된 키를 하나의 입력으로 하는 해시값을 상기 제2 바디 센서로 송신하는 키 생성 모듈을 포함한다.

발명의 효과

[0012] 본 발명의 실시 예에 따른 키 교환 방법은 인체에 삽입되거나 부착된 센서만이 측정할 수 있는 생체정보를 이용하여 키를 생성하고 생성된 키를 교환함으로써, 생체정보가 제3자에게 노출되는 것을 차단할 수 있는 효과가 있다.

[0013] 또한, 본 발명의 실시 예에 따른 키 교환 방법은 상호 통신 없이 측정된 생체정보를 이용하여 키를 생성함으로써, 바디 센서 간의 통신량을 감소시켜 바디 센서의 전력 소모량을 최소화할 수 있다. 결과적으로, 바디 센서의 수명을 연장할 수 있는 효과가 있다.

도면의 간단한 설명

[0014] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 바디 영역 네트워크를 도시한다.

도 2는 도 1에 도시된 제1 바디 센서의 기능 블럭도이다.

도 3은 도 1에 도시된 바디 영역 네트워크에서 키를 교환하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0016] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0017] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0018] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0019] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0020] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0021] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0022] 도 1은 본 발명의 일 실시 예에 따른 바디 영역 네트워크를 도시한다.

[0023] 도 1을 참조하면, 바디 영역 네트워크(Body Area Networks; 10)는 다수의 센서 노드들, 즉 다수의 바디 센서들(100, 300, 및 500)을 포함한다. 도 1에는 3개의 바디 센서들만이 도시되어 있으나, 본 발명이 상기 바디 센서의 갯수에 제한되는 것은 아니며, 바디 영역 네트워크(10)에 새로운 바디 센서가 추가되거나 기존의 바디 센서가 제거됨에 따라, 상기 바디 센서의 갯수는 유동적으로 변화할 수 있다.

[0024] 바디 영역 네트워크(10)는 다수의 센서 노드들(100, 300, 및 500)이 인체(20)에 삽입되거나 부착되어 인체(20)의 생체정보나 인체(20)의 움직임 정보를 측정할 수 있다. 또한, 다수의 센서 노드들(100, 300, 및 500) 각각은 무선 통신 기술, 예컨대 블루투스(Bluetooth), 지그비(Zigbee), 와이파이(Wi-Fi) 등과 같은 무선 통신 기술을 이용하여 서로 통신할 수 있다. 실시 예에 따라 인체(20)는 사람이 아닌 동물을 의미할 수도 있다.

[0025] 실시 예에 따라, 제1 바디 센서(100), 제2 바디 센서(300), 및 제3 바디 센서(500) 중 적어도 하나는 제3자가 인체(20)에 삽입하거나 부착한 센서일 수 있다. 예컨대, 환자의 의식이 없는 상황과 같은 응급 상황이 발생했을 때, 의료진은 인체(20)에 바디 센서를 삽입하거나 부착함으로써, 나머지 바디 센서를 제어하거나 상기 나머지 바디 센서가 측정한 생체정보를 이용할 수 있다.

[0026] 또한, 본 발명에 의한 키 교환 방법 및 바디 센서는 동일한 시간에 동일한 인체(20)로부터 측정되는 생체정보는 매우 유사하다는 개념을 기반으로 한다.

[0027] 도 2는 도 1에 도시된 제1 바디 센서의 기능 블럭도이다.

[0028] 도 1과 도 2를 참조하면, 바디 영역 네트워크(10)에 포함된 다수의 바디 센서들(100, 300 및 500)은 동일한 기능을 수행할 수 있으므로, 제1 바디 센서(100)에 대해 설명하고, 나머지 바디 센서들에 대한 설명은 생략하기로 한다. 또한, 제1 바디 센서(100), 제2 바디 센서(300), 및 제3 바디 센서(500) 각각은 동일한 생체정보를 측정할 수 있다. 다만, 제1 바디 센서(100), 제2 바디 센서(300), 및 제3 바디 센서(500)는 각각의 고유한 기능, 예컨대 인슐린 펌핑(insulim pumping), 혈압(blood pressure) 측정, 근전도(electromyography; EMG) 측정, 심전도(electrocardiogram; ECG) 측정, 맥파(hotoplethysmography; PPG) 측정, 뇌파(electroencephalogram; EEG) 등을 수행할 수 있다.

[0029] 제1 바디 센서(100)는 설정 모듈(110), 측정 모듈(130), 회귀 분석 모듈(150), 및 키 생성 모듈(170)을 포함한다.

[0030] 설정 모듈(110)은 키 교환의 대상 바디 센서, 예컨대 제2 바디 센서(300)와 동일한 값을 공유하기 위한 동작을 수행할 수 있다. 구체적으로, 설정 모듈(110)은 키 교환 동작을 시작하기 위한 키 교환 요청 메시지를 송신할 수 있다. 상기 키 교환 요청 메시지는 키 교환을 희망하는 제1 바디 센서(100)의 ID(Identification)와 키 교환의 상대방인 제2 바디 센서(300)의 ID를 포함할 수 있다. 따라서, 상기 키 교환 요청 메시지의 송수신을 통하여 제1 바디 센서(100)와 제2 바디 센서(300) 사이의 키 교환 동작이 수행될 수 있다.

[0031] 키 생성 과정에서 이용되는 적어도 하나의 공유값을 생성하기 위해 제1 바디 센서(100)와 제2 바디 센서(300)는 동일한 값(d)을 공유할 필요가 있다. 이 때, 동일한 값(d)은 타임 스탬프(time stamp)나 카운터 값일 수 있다. 즉, 상기 동일한 값(d)은 상기 키 교환 요청 메시지를 송신한 시간, 상기 키 교환 요청 메시지를 수신한 시간, 또는 생체정보 측정을 시작하기 위한 시간을 의미할 수 있다. 또한, 제1 바디 센서(100)와 제2 바디 센서(300)는 미리 동기화된 타이머나 카운터를 포함할 수 있다. 또한, 초(second) 단위 또는 분(minute) 단위의 시간 측정이 이루어진다면, 제1 바디 센서(100)와 제2 바디 센서(300) 사이의 송수신 과정에서 발생하는 시간 불일치 문제를 해소할 수 있다.

[0032] 설정 모듈(110)은 상기 동일한 값(d)을 이용하여, 적어도 하나의 공유값을 생성할 수 있다. 상기 적어도 하나의 공유값은 다음 수학식 1을 이용하여 생성될 수 있다.

수학식 1

[0033] $$S=\{h^1(d),h^2(d),\cdots,h^N(d)\}$$

[0034] 상기 S는 공유값들의 집합을 의미하고, 상기 h()는 해쉬 함수를 의미할 수 있다. 상기 공유값들의 집합(S)은 N(N은 1 이상의 자연수)개의 공유값들, 즉 적어도 하나의 공유값을 포함할 수 있다. 상기와 같은 과정을 통하여, 제1 바디 센서(100)와 제2 바디 센서(300)는 상기 적어도 하나의 공유값(S)을 공유할 수 있다.

[0035] 측정 모듈(130)은 인체(20)의 생체정보를 측정할 수 있다. 상기 생체정보는 ECG 또는 PPG일 수 있다. 즉, 제1 바디 센서(100)와 제2 바디 센서(300)는 동일한 생체정보를 측정할 수 있어야 한다.

[0036] 구체적으로, 측정 모듈(130)은 미리 정해진 시간 구간(T) 동안 인체(20)의 생체정보를 측정하여 아래의 수학식 2와 같은 측정값을 생성할 수 있다.

수학식 2

[0037] $$\overline{v_1^k}=v^k+\epsilon_1^k$$

[0038] 상기 수학식 2에서 $\overline{v_1^k}$ 는 측정 모듈(130)에 의해서 시간 t=k(0<k<T)일 때 측정된 값이고, v^k 는 인체(20)의 고유한 생체정보이고, ϵ_1^k 는 노이즈(noise)를 의미한다. 또한, 상기 k는 미리 정해진 시간 구간(T)에

속하는 불연속된 다수의 값들일 수 있다. 또한, 동일한 인체(20)를 대상으로 동일한 시간에 측정이 이루어지더라도, 제1 바디 센서(100)의 측정 모듈(130)에 의해 측정된 값과 제2 바디 센서(300)의 측정 모듈에 의해 측정된 값은 상이할 수 있다. 제1 바디 센서(100)와 제2 바디 센서(300)의 측정 위치, 바디 센서의 고유한 특성 등이 상이하기 때문이다.

[0039] 회귀 분석 모듈(150)은 회귀 분석(Regression analysis) 기법을 이용하여, 측정 모듈(130)에 의해 측정된 측정값($\overline{v_1^k}$)으로부터 생체정보 값(v^k)을 생성할 수 있다. 상기 회귀 분석 기법은 샘플링된 측정값($\overline{v_1^k}$)으로부터 실제 생체정보 값(v^k)을 확률론적 방법으로 추측할 수 있는 도구이다. 즉, 회귀 분석 모듈(150)은 미리 정해진 시간 구간(T) 동안 측정된 샘플링 데이터($\{\overline{v_1^k} \mid 0 < k < T\}$)에 대하여 회귀 분석 기법을 이용하여 $\{v^k \mid 0 < k < T\}$ 를 추측할 수 있다.

[0040] 구체적으로, 회귀 분석 모듈(150)은 아래의 수학식 3과 같은 정현파(Sinusoidal wave) 함수를 모델 함수로 하여 생체정보를 모델링하고, 모델링된 생체정보 함수($f_1(t)$)를 생성할 수 있다.

수학식 3

[0041] $$f_1(t) = a \times sin(b \times t + c)$$

[0042] 수학식 1에서, a, b 및 c는 회귀 계수이다. 상기 회귀 계수들(a, b, 및 c)은 회귀 분석의 결과로써 도출될 수 있다.

[0043] 상기와 같이 회귀 분석 기법을 적용하면, 제1 바디 센서(100)와 제2 바디 센서(300)는 동일한 생체정보($\{v^k \mid 0 < k < T\}$)를 가질 수 있다. 또한, 상기 생체 정보는 인체(20)에 삽입되거나 부착되어 정당하게 인체(20)의 생체정보를 측정한 바디 센서만이 획득할 수 있다.

[0044] 키 생성 모듈(170)은 생체정보 함수($f_1(t)$)에 적어도 하나의 공유값(S)을 입력함으로써, 키(sk)를 생성할 수 있다. 상기 키(sk)는 아래의 수학식 4를 이용하여 생성될 수 있다.

수학식 4

[0045] $$sk = f_1(h^1(d)) \oplus f_2(h^2(d)) \oplus \cdots \oplus f_1(h^N(d))$$

[0046] 상기 수학식 3에서, 연산자 $\oplus$ 는 배타적 논리합(exclusive OR; XOR)을 의미하나, 본 발명이 이에 제한되는 것은 아니다. 실시 예에 따라, 상기 연산자($\oplus$)는 논리합(OR), 논리곱(AND) 등으로 구현될 수도 있다.

[0047] 또한, 키 생성 모듈(170)은 키(sk)를 입력으로 하는 해시 값을 생성하고 생성된 해시값을 제2 바디 센서(300)로 송신할 수 있다. 실시 예에 따라, 생성된 해시값은 제1 바디 센서(100)의 ID, 제2 바디 센서(300)의 ID, 및 적어도 하나의 공유값(S) 중 적어도 하나 이상을 추가적인 입력으로 하는 해시값일 수 있다. 이와 같이, 키(sk) 자체를 송신하는 것이 아닌 해시값을 송신함으로써 키(sk)가 노출되는 것을 방지할 수 있다.

[0048] 이 때, 상기 해시값을 수신한 제2 바디 센서(300)의 키 생성 모듈은 수신된 해시값과 제2 바디 센서(300)가 동일한 방식으로 생성한 해시값의 일치 여부를 확인한다. 제1 바디 센서(100)가 생성한 해시값과 제2 바디 센서

(300)가 생성한 해시값이 동일할 경우, 제2 바디 센서(300)의 키 생성 모듈은 상기 해시값들이 일치함을 확인하는 제1 확인 메시지를 제1 바디 센서(100)로 송신할 수 있다. 상기 확인 메시지는 제2 바디 센서(300)가 생성한 해시값일 수 있도 있다. 또한, 제1 바디 센서(100)가 생성한 해시값과 제2 바디 센서(300)가 생성한 해시값이 동일하지 않은 경우, 제2 바디 센서(300)의 키 생성 모듈은 상기 해시값들이 일치하지 않음을 확인하는 제2 확인 메시지를 제1 바디 센서(100)로 송신할 수도 있다.

[0049] 키 생성 모듈(170)이 상기 제1 확인 메시지를 수신한 경우, 제1 바디 센서(100)와 제2 바디 센서(300) 사이의 키 교환은 성공적으로 완료되고, 제1 바디 센서(100)와 제2 바디 센서(300)는 동일한 키(sk)를 안전하게 공유하게 된다. 키 생성 모듈(170)이 상기 제2 확인 메시지를 수신한 경우, 제1 바디 센서(100)와 제2 바디 센서(300) 사이의 키 교환은 종료되고, 공유값 설정 단계부터 재차 실행될 수 있다.

[0050] 도 2에 도시된 제1 바디 센서(100)의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0051] 또한, 본 명세서에서 모듈이라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 모듈은 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0052] 도 3은 도 1에 도시된 바디 영역 네트워크에서 키를 교환하는 방법을 설명하기 위한 흐름도이다.

[0053] 도 1 내지 도 3을 참조하면, 키 교환을 원하는 제1 바디 센서(100)는 키 교환을 요청하는 메시지인 키 교환 요청 메시지를 키 교환의 상대방인, 제2 바디 센서(300)로 송신한다(S110). 이 때, 상기 키 교환 요청 메시지는 제1 바디 센서(100)의 ID와 제2 바디 센서(300)의 ID를 포함할 수 있다.

[0054] 제1 바디 센서(100)와 제2 바디 센서(300)는 서로 공유된 동일한 값(d)을 이용하여, 적어도 하나의 공유값을 생성할 수 있다(S120). 즉, 제1 바디 센서(100)는 적어도 하나의 공유값을 포함하는 공유값들의 집합(S_1)을 생성하고, 제2 바디 센서(300)는 적어도 하나의 공유값을 포함하는 공유값들의 집합(S_2)을 생성할 수 있다. 이 때, 공유값들의 집합(S_1)과 공유값들의 집합(S_2)에는 동일한 공유값들이 포함되어 있다.

[0055] 제1 바디 센서(100)와 제2 바디 센서(300)는 인체(20)의 생체정보를 측정할 수 있다(S130). 또한, 제1 바디 센서(100)와 제2 바디 센서(300)는 각각 회귀 분석 기법을 이용하여, 생체정보 함수를 생성할 수 있다(S140). 즉 제1 바디 센서(100)는 제1 생체정보 함수($f_1(t)$)를 생성하고, 제2 바디 센서(300)는 제2 생체정보 함수($f_2(t)$)를 생성할 수 있다.

[0056] 제1 바디 센서(100)와 제2 바디 센서(300)는 생성된 생체정보 함수와 공유값들의 집합을 이용하여, 키를 생성할 수 있다(S150). 즉, 제1 바디 센서(100)는 공유값들의 집합(S_1)과 제1 생체정보 함수($f_1(t)$)를 이용하여 제1 키(sk_1)를 생성하고, 제2 바디 센서(300)는 공유값들의 집합(S_2)과 제2 생체정보 함수($f_2(t)$)를 이용하여 제2 키(sk_2)를 생성할 수 있다.

[0057] 또한, 제1 바디 센서(100)는 생성된 키(sk_1)를 제2 바디 센서(300)로 송신하고, 제1 바디 센서(100)가 생성한 키(sk_1)를 수신한 제2 바디 센서(300)는 제1 바디 센서(100)가 생성한 키(sk_1)와 제2 바디 센서(300)가 생성한 키(sk_2)의 일치 여부를 확인하고 확인 결과를 제1 바디 센서(100)로 송신함으로써, 키 확인 과정이 수행된다(S160). 이 때, 제1 바디 센서(100)가 생성한 키(sk_1)와 제2 바디 센서(300)가 생성한 키(sk_2)가 동일한 경우 키 교환은 성공적으로 완료되나, 동일하지 않은 경우 키 교환은 실패하게 된다. 즉, 제1 바디 센서(100)가 키의 동일함을 의미하는 메시지를 수신한 경우 키 교환은 성공적으로 완료되고, 키가 동일하지 않음을 의미하는 메시지를 수신한 경우 키 교환은 실패하게 된다. 키 교환이 성공적으로 완료되지 않은 경우, 키 교환 요청 메시지를 송신하는 단계가 재차 수행됨으로써, 키 교환이 재차 시도될 수 있다.

[0058] 상기와 같은 과정을 통하여 교환된 키는 암호화 또는 인증 과정에서 활용될 수 있다. 또한, 제1 바디 센서(100)가 의료진이 환자의 인체(20)에 삽입하거나 부착한 센서일 경우, 환자의 의식이 없는 상태에서도 제2 바디 센서(300)를 제어하거나 제2 바디 센서(300)가 측정한 생체정보를 수신하는 것이 가능하다. 또한, 인체(20)에 삽입되거나 부착되어 동일한 생체정보를 측정할 수 있는 바디 센서만이 키 교환을 할 수 있기 때문에, 환자의 생

체정보는 안전하게 보호될 수 있다.

[0059] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0060] 10 : 바디 영역 네트워크

20 : 인체

100 : 제1 바디 센서

110 : 설정 모듈

130 : 측정 모듈

150 : 회귀 분석 모듈

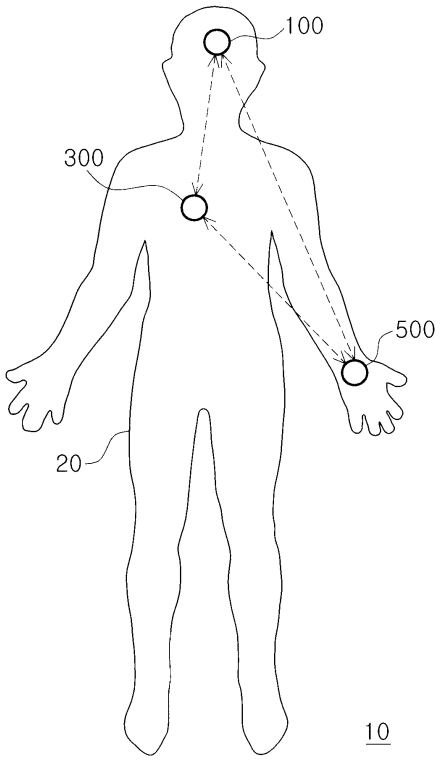
170 : 키 생성 모듈

300 : 제2 바디 센서

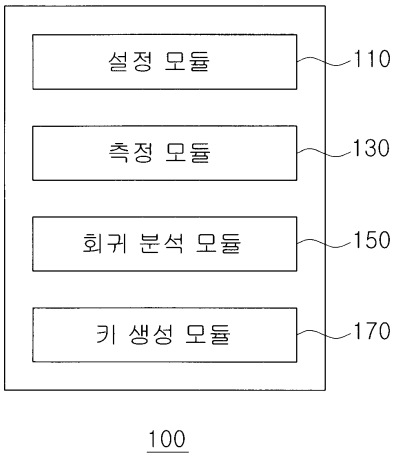
500 : 제3 바디 센서

도면

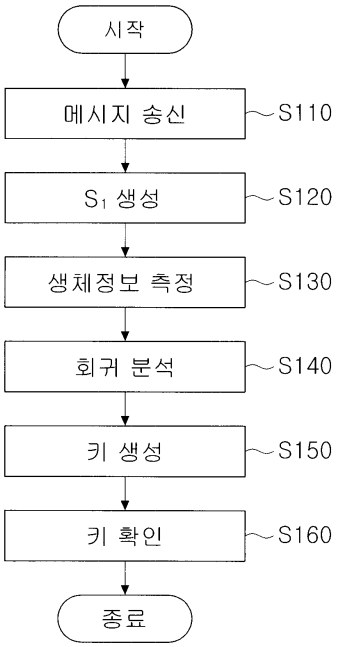
도면1



도면2


설정 모듈
110
측정 모듈
130
회귀 분석 모듈
150
키 생성 모듈
170
100

도면3


시작
메시지 송신
S110
S_1 생성
S120
생체정보 측정
S130
회귀 분석
S140
키 생성
S150
키 확인
S160
종료