



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0118293
(43) 공개일자 2014년10월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) H04B 13/00 (2006.01)
A61B 5/00 (2006.01)
(21) 출원번호 10-2013-0033918
(22) 출원일자 2013년03월28일
심사청구일자 없음

(71) 출원인
인텔렉추얼디스커버리 주식회사
서울특별시 강남구 삼성로 511, 10층 (삼성동, 골
든타워)
(72) 발명자
이동훈
서울 성북구 안암로 145, 미래융합기술관 612호
(안암동5가, 고려대학교이과대학)
최원석
서울 성북구 안암로 145, 로봇융합관 403호 (안암
동5가, 고려대학교이과대학)
이화성
서울 성북구 안암로 145, 로봇융합관 403호 (안암
동5가, 고려대학교이과대학)
(74) 대리인
특허법인엠에이피에스

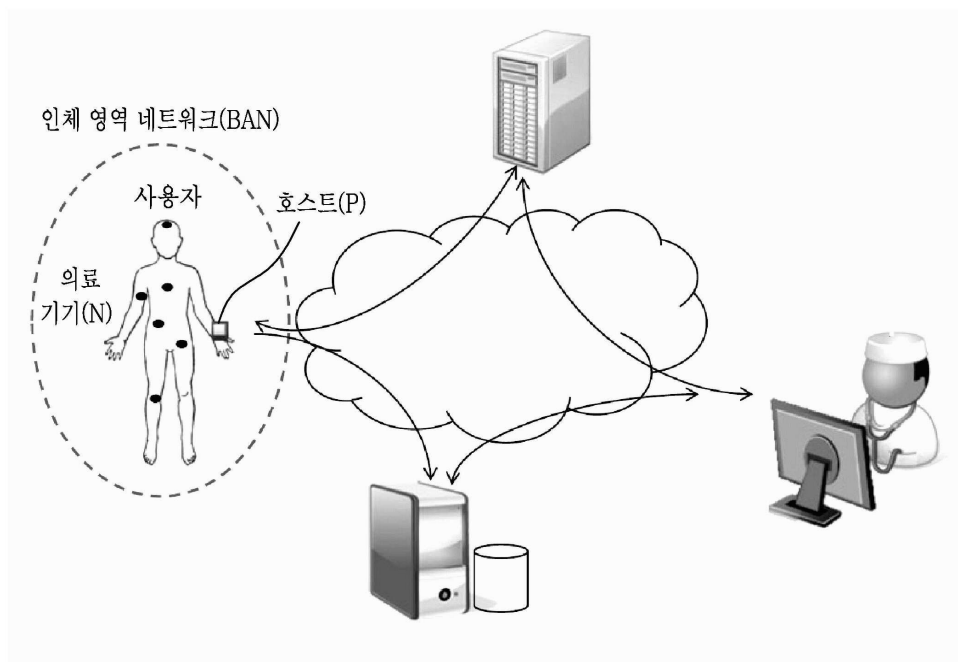
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 의료 기기 및 의료 기기의 생체 데이터를 이용한 데이터 교환 방법

(57) 요약

본 발명은 사용자의 신체에 이식되거나 부착되어 상기 사용자의 하나 이상의 생체 정보를 수집하여 의료 기기 호스트로 전송하고, 상기 의료 기기 호스트로부터 제어 정보를 수신하는 의료 기기이되, 상기 사용자의 특정 생체 정보를 상기 의료 기기 호스트와 동시에 센싱하여 세션키를 생성하고, 상기 세션키가 유효한 상태에 있는 동안, 상기 세션키로 암호화된 상기 생체 정보 또는 상기 제어 정보를 상기 의료 기기 호스트와 교환하되, 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 의료 기기를 제공한다.

대표도 - 도1



특허청구의 범위

청구항 1

의료 기기에 있어서,

사용자의 신체에 이식되거나 부착되어 상기 사용자의 하나 이상의 생체 정보를 수집하여 의료 기기 호스트로 전송하고, 상기 의료 기기 호스트로부터 제어 정보를 수신하는 의료 기기이되,

상기 사용자의 특정 생체 정보를 상기 의료 기기 호스트와 동시에 센싱하여 세션키를 생성하고,

상기 세션키가 유효한 상태에 있는 동안, 상기 세션키로 암호화된 상기 생체 정보 또는 상기 제어 정보를 상기 의료 기기 호스트와 교환하되,

상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 의료 기기.

청구항 2

제 1 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 혈당, 혈압, 체온, 맥박, 혈류량, 및 헤모글로빈 농도 중 하나 이상을 포함하는 의료 기기.

청구항 3

제 1 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 상기 특정 생체 정보의 엔트로피(entropy)에 따라 결정되는 측정 기간 동안 측정되는 의료 기기.

청구항 4

제 1 항에 있어서,

상기 세션키는 상기 의료 기기 및 상기 의료 기기 호스트가 일련의 데이터를 교환하는 세션(session)을 시작하기 전에 생성되며, 유효하지 않을 경우 재생성되는 의료 기기.

청구항 5

의료 기기 호스트에 있어서,

사용자의 신체에 이식되거나 부착되어 상기 사용자의 하나 이상의 생체 정보를 수집하는 의료 기기로부터 상기 하나 이상의 생체 정보를 취합하고, 상기 의료 기기에 제어 정보를 전송하는 의료 기기 호스트이되,

상기 사용자의 특정 생체 정보를 상기 의료 기기와 동시에 센싱하여 세션키를 생성하고,

상기 세션키가 유효한 상태에 있는 동안, 상기 세션키로 암호화된 상기 생체 정보 또는 상기 제어 정보를 상기 의료 기기와 교환하되,

상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 의료 기기 호스트.

청구항 6

제 1 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 혈당, 혈압, 체온, 맥박, 혈류량, 및 헤모글로빈 농도 중 하나 이상을 포함하는 의료 기기 호스트.

청구항 7

제 1 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 상기 특정 생체 정보의 엔트로피(entropy)에 따라 결정되는 측정 기간 동안 측정되는 의료 기기 호스트.

청구항 8

제 1 항에 있어서,

상기 세션키는 상기 의료 기기 및 상기 의료 기기 호스트가 일련의 데이터를 교환하는 세션(session)을 시작하기 전에 생성되며, 유효하지 않을 경우 재생성되는 의료 기기 호스트.

청구항 9

의료 기기의 의료 기기 호스트와의 데이터 교환 방법에 있어서,

상기 의료 기기가 상기 의료 기기 호스트와 동일한 시점에 사용자의 특정 생체 정보를 센싱하는 단계;

상기 의료 기기가 상기 센싱한 생체 정보를 사용하여 세션키를 산출하는 단계; 및

상기 의료 기기가 사용자의 생체 정보를 수집하여 상기 수집한 사용자의 생체 정보를 상기 세션키로 암호화하여 상기 의료 기기 호스트로 전송하는 단계;를 포함하되,

상기 세션키를 산출하는 단계는 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 단계;를 더 포함하는 데이터 교환 방법.

청구항 10

제 9 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 혈당, 혈압, 체온, 맥박, 혈류량, 및 헤모글로빈 농도 중 하나 이상을 포함하는 데이터 교환 방법.

청구항 11

제 9 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 상기 특정 생체 정보의 엔트로피(entropy)에 따라 결정되는 측정 기간 동안 측정되는 데이터 교환 방법.

청구항 12

제 9 항에 있어서,

상기 의료 기기가 상기 의료 기기 호스트가 자신의 세션키로 암호화하여 전송한 제어 정보를 자신의 세션키로 복호화하는 단계;를 포함하는 데이터 교환 방법.

청구항 13

의료 기기 호스트의 의료 기기와의 데이터 교환 방법에 있어서,

상기 의료 기기 호스트가 상기 의료 기기와 동일한 시점에 사용자의 특정 생체 정보를 센싱하는 단계;

상기 의료 기기 호스트가 상기 센싱한 생체 정보를 사용하여 세션키를 산출하는 단계; 및

상기 의료 기기 호스트가 제어 정보를 자신의 세션키로 암호화하여 상기 의료 기기로 전송하는 단계;를 포함하되,

상기 세션키를 산출하는 단계는 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 단계;를 더 포함하는 의료 기기 호스트의 데이터 교환 방법.

청구항 14

제 13 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 혈당, 혈압, 체온, 맥박, 혈류량, 및 헤모글로빈 농도 중 하나 이상을 포함하는 데이터 교환 방법.

청구항 15

제 13 항에 있어서,

상기 세션키 생성을 위해 센싱되는 상기 특정 생체 정보는 상기 특정 생체 정보의 엔트로피(entropy)에 따라 결정되는 측정 기간 동안 측정되는 데이터 교환 방법.

청구항 16

제 13 항에 있어서,

상기 의료 기기 호스트가 상기 의료 기기가 자신의 세션키로 암호화하여 전송한 상기 사용자의 생체 정보를 자신의 세션키로 복호화하는 단계;를 포함하는 데이터 교환 방법.

명세서

기술 분야

[0001] 본 발명은 의료 기기의 생체 데이터를 이용한 데이터 교환 방법에 관한 것이다.

배경 기술

[0002] 기술의 발달로 인하여 환자 신체 내부에 삽입되어 작동하는 이식형 의료기기 시장이 커지고 있다. 이식형 의료기기는 환자에게 이식되어 환자의 생체 정보를 측정하며, 필요에 따라 환자에게 이상 동작이 감지되는 경우 이에 적절한 동작을 하여 환자의 생명을 유지 하거나 통증을 완화시켜주는 기기이다.

[0003] 예를 들어, 환자의 가슴에 삽입되어 있는 이식형 체세동기는 심장 질환을 가지고 있는 환자에게 이식되어, 일상 생활 중 심장이 정지된 경우 이를 감지하여 강력한 전기적 충격을 가함으로써 심장이 정상적으로 움직이는 것을 도와준다.

[0004] 이식형 의료 기기는 주기적으로 환자의 상태를 센싱하고 센싱한 생체 정보를 의사 등의 의료서비스 제공자에게 전송한다. 의료 서비스 제공자는 환자의 건강 상태에 따라 이식형 의료 기기의 설정값을 변경시키는 등, 프로그래머 등의 외부 기기를 통하여 이식형 의료 기기를 제어할 수 있다.

[0005] 이식형 의료 기기와 외부 기기 사이에 교환되는 정보는 매우 중요하여 안전하게 보호되어야 한다. 예를 들어, 악의적인 공격자가 이식형 의료 기기의 설정값을 부적절한 값으로 변경하는 경우 환자의 생명까지 위협할 수 있기 때문이다.

[0006] 따라서 이식형 의료 기기와 외부 기기간에 안전하게 데이터를 교환할 수 있는 방법이 필요하다.

[0007] 이와 관련하여 한국특허 출원번호 제10-2010-0035298호("헬스케어용 의료 센서를 위한 암호화 방법 및 장치")에는 귀환 수열 및 비선형 함수를 사용하여 생성한 암호화 키를 사용하여, 의료 센서로부터 수집한 생체 신호를 입력받아 암호화하여 서버로 전송하면, 서버는 동일한 방식으로 생성한 암호화 키를 이용하여 복호화하는 구성이 개시되어 있다.

[0008] 또한, 한국특허 출원번호 제10-2010-7024615호("거리 기반 보안")에는 거리에 기반하여 기능을 수행하도록 요청하는 것을 허용할지 여부를 판단하는 구성이 개시되어 있다.

발명의 내용

해결하려는 과제

[0009] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 호스트와의 안전한 데이터 교환을 위한 암호화 키를 필요할 때마다 단순한 연산을 통해 생성하는 의료 기기를 제공하는 것이다.

과제의 해결 수단

- [0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 의료 기기는 사용자의 신체에 이식되거나 부착되어 상기 사용자의 하나 이상의 생체 정보를 수집하여 의료 기기 호스트로 전송하고, 상기 의료 기기 호스트로부터 제어 정보를 수신하는 의료 기기이되, 상기 사용자의 특정 생체 정보를 상기 의료 기기 호스트와 동시에 센싱하여 세션키를 생성하고, 상기 세션키가 유효한 상태에 있는 동안, 상기 세션키로 암호화된 상기 생체 정보 또는 상기 제어 정보를 상기 의료 기기 호스트와 교환하되, 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 것을 특징으로 한다.
- [0011] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 의료 기기 호스트는 사용자의 신체에 이식되거나 부착되어 상기 사용자의 하나 이상의 생체 정보를 수집하는 의료 기기로부터 상기 하나 이상의 생체 정보를 취합하고, 상기 의료 기기에 제어 정보를 전송하는 의료 기기 호스트이되, 상기 사용자의 특정 생체 정보를 상기 의료 기기와 동시에 센싱하여 세션키를 생성하고, 상기 세션키가 유효한 상태에 있는 동안, 상기 세션키로 암호화된 상기 생체 정보 또는 상기 제어 정보를 상기 의료 기기와 교환하되, 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 것을 특징으로 한다.
- [0012] 상기와 같은 목적을 달성하기 위한 본 발명의 제 3 측면에 따른 의료 기기의 의료 기기 호스트와의 데이터 교환 방법은 상기 의료 기기가 상기 의료 기기 호스트와 동일한 시점에 사용자의 특정 생체 정보를 센싱하는 단계; 상기 의료 기기가 상기 센싱한 생체 정보를 사용하여 세션키를 산출하는 단계; 및 상기 의료 기기가 사용자의 생체 정보를 수집하여 상기 수집한 사용자의 생체 정보를 상기 세션키로 암호화하여 상기 의료 기기 호스트로 전송하는 단계;를 포함하되, 상기 세션키를 산출하는 단계는 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 단계;를 더 포함하는 것을 특징으로 한다.
- [0013] 상기와 같은 목적을 달성하기 위한 본 발명의 제 4 측면에 따른 의료 기기 호스트의 의료 기기와의 데이터 교환 방법은 상기 의료 기기 호스트가 상기 의료 기기와 동일한 시점에 사용자의 특정 생체 정보를 센싱하는 단계; 상기 의료 기기 호스트가 상기 센싱한 생체 정보를 사용하여 세션키를 산출하는 단계; 및 상기 의료 기기 호스트가 제어 정보를 자신의 세션키로 암호화하여 상기 의료 기기호로 전송하는 단계;를 포함하되, 상기 세션키를 산출하는 단계는 상기 의료 기기와 상기 의료 기기 호스트가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시키는 단계;를 더 포함하는 것을 특징으로 한다.

발명의 효과

- [0014] 본 발명은 이식형 의료 기기에 있어, 호스트와의 안전한 데이터 교환을 위한 암호화 키를 필요할 때마다 단순한 연산을 통해 생성하는 효과를 얻는다.
- [0015] 의료 기기와 호스트는 동시에 각각 측정된 사용자의 생체 데이터를 사용하여 암호화 키를 생성하므로, 암호화 키를 미리 배포하지 않아도 된다.
- [0016] 암호화 키를 미리 배포하지 않아도 되므로, 의료 기기를 추가 이식하는 등의 이유로 암호화 키를 갱신해야 할 때의 노력이 적다. 더욱 중요하게는, 암호화 키사전에 저장하지 않으므로 암호화 키를 도난당할 위험이 없다. 또한, 호스트가 없을 때 호스트 이외의 다른 외부 기기를 사용하여도 신속하게 암호화 키를 생성하여 의료 세션을 시작할 수 있으므로, 응급 상황시 대처하기가 용이하다.
- [0017] 생체 데이터간 오차를 간단한 오차 정정 기법을 통해 보정하므로, 암호화 키를 생성하는 데 드는 연산 노력이 적어 의료 기기의 전력 소모를 줄일 수 있다. 따라서 제한된 배터리 자원을 가지고 있는 이식형 의료 기기의 수명 단축을 줄일 수 있다.

도면의 간단한 설명

- [0018] 도 1은 본 발명의 일실시예에 따른 의료 기기 및 호스트를 포함하는 신체 영역 네트워크의 구조를 도시함.
 도 2는 본 발명의 일실시예에 따른 의료 기기 및 호스트의 구조를 도시함.
 도 3은 본 발명의 일실시예에 따른 의료 기기의 구조를 도시함.

도 4는 종래의 의료 기기와 호스트간 인증 방법을 도시함.

도 5는 본 발명의 일실시예에 따른 의료 기기 및 호스트가 사용할 수 있는 생체 데이터를 도시함.

도 6은 본 발명의 일실시예에 따른 데이터 교환 방법의 흐름을 도시함.

발명을 실시하기 위한 구체적인 내용

- [0019] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [0020] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0021] 도 1은 본 발명의 일실시예에 따른 의료 기기 및 호스트를 포함하는 신체 영역 네트워크의 구조를 도시하고 있다.
- [0022] 도시되어 있는 바와 같이, 사용자의 신체에 이식되거나 부착되어 사용자의 하나 이상의 생체 정보를 수집하는 하나 이상의 의료 기기(N)는 신체 영역 네트워크(BAN: body area network)를 구성할 수 있다. 예를 들어, 각 의료 기기는 무선으로 서로 통신할 수 있다. 이러한 실시예를 특히 무선 신체 영역 네트워크(WBAN: wireless body area network)라고 부르며, 이는 인체에 부착 또는 삽입된 하나 이상의 센서 노드(N)들 간의 무선 통신으로 환자의 생체 정보를 획득하는 네트워크를 뜻한다.
- [0023] 이러한 네트워크에서 호스트(P)는 각 센서로부터 정보를 취합하는 대표 센서 노드는 베이스 스테이션(base station)일 수 있으며, 의료 기기(N)에 제어 정보를 전송하여 의료 기기(N)의 설정값 등을 제어한다. 이러한 의미에서 호스트(P)는 프로그래머(programmer)라고 불릴 수 있다. 또한, 이식형 의료 기기(N)가 신체의 내부에 삽입되어 동작하는 데 반해, 호스트(P)는 신체의 외부에 위치하므로, 외부 기기라고 부를 수도 있다.
- [0024] 일실시예에서 호스트(P)는 병원, 클리닉 등의 의료 센터와 연결되어, 신체 영역 네트워크를 구성하는 하나 이상의 의료 기기(N)로부터 취합한 생체 정보를 의료 센터로 전송할 수 있으며, 또한 의료 센터 의료진의 단말로부터 의료 기기(N)의 제어 정보를 수신하여 의료 기기(N)로 전달할 수 있다.
- [0025] 도 2는 본 발명의 일실시예에 따른 의료 기기 및 호스트의 구조를 도시하고 있다.
- [0026] 도시되어 있는 실시예에서, 의료 기기(N)와 호스트(P)는 각각 센싱 모듈 및 무선 통신 모듈을 가지고 있다. 각자의 센싱 모듈이 센싱한 생체 정보를 기반으로 세션키를 도출하며, 각자의 무선 통신 모듈을 통해 데이터를 교환한다. 교환하는 데이터에는 환자의 기본 정보, 및 전원을 켜고 끄는 등의 다양한 제어 정보가 포함되며, 이러한 데이터는 센싱한 생체 정보를 기반으로 도출한 세션키를 사용하여 암호화되어 교환된다.
- [0027] 전술한 바와 같이, 이식형 의료 기기와 외부 기기간에 교환되는 데이터는 환자의 건강에 치명적인 영향을 미칠 수 있는 매우 중요한 데이터이므로 안전하게 보호되어야 한다.
- [0028] 예를 들어, 도 3은 본 발명의 일실시예에 따른 의료 기기의 구조를 도시하고 있다.
- [0029] 본 발명의 일실시예에 따른 이식형 의료 기기(N)는 이식형 제세동기, 이식형 심장 박동기, 이식형 신경 자극기 등을 포함하나, 여기에 제한되지는 않는다.
- [0030] 도시되어 있는 본 발명의 일실시예에 따른 이식형 제세동기(N)는 포함되어 있는 배터리로부터 전원을 공급받으며, 심장의 생체 신호를 센싱할 수 있는 센싱 회로, 및 전극을 통해 심장에 자극을 가하기 위한 출력 회로를 포함하고 있다. 센싱 회로를 통해 자신이 이식되어 있는 환자의 심장이 정지하였음을 감지하고, 출력 회로를 통해 전극으로 강력한 전기 충격을 내보내어, 심장이 다시 정상적으로 움직이는 것을 도와준다.
- [0031] 이때, 전기 충격의 세기나 횟수 등의 설정값은 환자의 상태에 따라 달라져야 할 것이다. 환자의 상태에 맞지 않는 강도나 횟수는 오히려 환자의 생명을 위협하는 공격으로 사용될 수 있다.
- [0032] 따라서 호스트(P)로부터 이러한 제어 정보를 제공받을 때는 악의적인 공격자가 부적절한 설정값을 주입하지 않

도록 해야 한다. 마찬가지로 이식형 제세동기(N)가 호스트(P)로 전송하는 생체 정보가 악의적인 공격자에 의해 변경되어도, 의료진이 잘못된 정보에 근거한 잘못된 판단으로 호스트(P)에 부적절한 설정값을 이식형 제세동기(N)에 전송하도록 할 수 있으므로, 이식형 제세동기(N)가 호스트(P)로 전송하는 생체 정보도 안전하게 보호되어야 한다.

- [0033] 한편, 또한, 환자의 기본 호스트(P)가 없는 상황에서 심장이 정지했을 때의 응급 상황에서도 빠르게 대처할 수 있는 것이 바람직할 것이다. 예를 들어, 모든 기능을 포함하는 호스트(P)가 부피가 크고 무게가 많이 나가는 기기일 경우, 환자는 이를 휴대하기 곤란할 것이다. 대신 기본 기능만을 탑재하더라도 작고 가벼운 휴대 단말(P)을 소지하게 한다면, 의료 센터의 병실 이외의 공간에서도 환자의 심장 상태를 모니터링할 수 있다. 또한, 더 나아가, 환자가 응급 상황에서 자신의 휴대 단말(P)을 소지하고 있지 않더라도 다른 휴대 단말(P)을 사용하여 이식형 제세동기(N)를 제어할 수 있는 것이 바람직할 것이다.
- [0034] 따라서, 호스트(P)와 이식형 의료 기기(N)간의 일련의 데이터 교환을 통한 의료 세션(session)에 사용할 암호화 키, 즉, 세션키를 필요할 때마다 간단하게 생성하는 것이 바람직하다.
- [0035] 이에 따라, 본 발명의 일실시예에 따른 의료 기기(N)는 호스트(P)와의 안전한 데이터 교환을 위한 암호화 키, 즉, 세션키를 필요할 때마다 단순한 연산을 통해 생성한다. 의료 기기(N)와 호스트(P)는 동시에 각각 측정한 사용자의 생체 데이터를 사용하여 암호화 키를 생성하므로, 암호화 키를 미리 배포하지 않아도 된다.
- [0036] 암호화 키를 미리 배포하지 않아도 되므로, 의료 기기를 추가 이식하는 등의 이유로 암호화 키를 갱신해야 할 때의 노력이 적다. 더욱 중요하게는, 암호화 키를 사전에 저장하지 않으므로 암호화 키를 도난당할 위험이 없다. 또한, 호스트(P)가 없을 때 호스트(P) 이외의 다른 외부 기기(P)를 사용하여도 신속하게 암호화 키를 생성하여 의료 세션을 시작할 수 있으므로, 응급 상황시 대처하기가 용이하다.
- [0037] 이에 더해, 본 발명의 일실시예에 따른 의료 기기(N)는 생체 데이터간 오차를 간단한 오차 정정 기법을 통해 보정하므로, 암호화 키를 생성하는 데 드는 연산 노력이 적어, 의료 기기의 전력 소모를 줄일 수 있다. 따라서 제한된 배터리 자원을 가지고 있는 이식형 의료 기기의 수명 단축을 줄일 수 있다.
- [0038] 이하 본 발명의 장점을 종래 기술과 비교하여 좀더 설명한다.
- [0039] 도 4는 종래의 의료 기기와 호스트간 인증 방법을 도시하고 있다.
- [0040] 종래의 이식형 의료기기는 외부기기를 인증하는 방법으로 거리기반 인증 방법을 사용하고 있다. 거리 기반 인증 방법의 중요한 가정 사항은 환자의 이식형의료기기에 대하여 공격을 시도하는 공격자는 환자가 인지할 수 없는 거리에서 공격을 시도할 것이라는 것이다. 따라서, 도시된 실시예에서와 같이, 3~5m 등 소정의 범위 내에 있는 호스트는 정당한 호스트라고 판단한다.
- [0041] 하지만, 이러한 가정 사항에는 다음과 같은 2가지 문제점이 존재한다.
- [0042] 첫째, 자신의 이식형의료기기가 공격자로부터 공격받고 있다는 것을 인지한다고 하더라도 즉, 환자가 공격자를 직접 목격하였더라도 어떠한 대응도 할 수 없는 환자가 있을 수 있다.
- [0043] 둘째, 통신거리가 약 10m인 블루투스과 같은 근거리 통신기술을 사용한다고 하더라도, 확장 안테나를 사용하면 통신거리를 1~2km 확장시킬 수 있다. 이는 공격자가 환자로부터 멀리 떨어져도 이식형 의료기기의 공격이 가능함을 의미한다.
- [0044] 또한, 비밀키를 안전하게 공유하기 위해 사용할 수 있는 종래의 방법은 이식형 의료기기를 환자에 삽입하기 이전에 비밀키를 저장하는 방법 또는 공개키 암호시스템을 사용하여 인증서 기반의 키 공유 방법을 적용하는 방법 등이 있다. 하지만, 이러한 방법 모두 이식형 의료기기에는 부적절하다.
- [0045] 비밀키를 사전에 공유하는 첫번째 방법은 이식형 의료 기기가 비밀키를 저장해두고 해당 비밀키를 알고 있는 외부 기기하고만 통신을 하는 방법이다. 이 방법은 비밀키의 업데이트가 제한되며, 이식형 의료 기기가 직접 비밀키를 안전하게 관리해야 하기 때문에 리소스가 제한되는 이식형 의료기기에는 부적절하다.
- [0046] 두번째 방법은 공개키 기반 암호 시스템이 대칭키 암호 시스템이 비하여 연산량이 많다는 문제 때문에 부적절하다. 키 공유 시 배터리 소모가 커짐으로써 이식형 의료기기의 수명이 줄어들기 때문이다.
- [0047] 이에 반해, 전술한 바와 같이 본 발명은 간단하게 연산할 수 있는 세션키를 사용하여 의료 기기(N)와 호스트(P)간의 세션키가 유효한 기간 동안 행해지는 일련의 데이터 교환을 통해 의료 행위를 수행하므로, 안전하고 효

울적이며, 응급 상황에 좀더 신속하게 대처할 수 있다는 장점이 있다.

- [0048] 이러한 본발명의 장점은 의료 기기(N)와 호스트(P)가 동시에 각각 센싱한 사용자의 생체 데이터를 사용하여 세션키를 생성한다는 본발명의 특징에 의해 얻어지는 효과이다.
- [0049] 도 5는 본 발명의 일실시예에 따른 의료 기기 및 호스트가 사용할 수 있는 생체 데이터를 도시하고 있다.
- [0050] 사람의 맥박이나 혈당 등과 같은 생체 정보는 측정하는 매 시간마다 다양하게 변화한다. 이처럼 다양하게 변화하는 대표적 생체 정보로는 도면과 같은 것들이 있다.
- [0051] 이렇게 변화하는 생체 정보를 사용하여 생성한 난수는 미국 NIST의 난수 테스트(Randomness Test)를 통과함이 밝혀졌다. NIST의 난수 테스트를 통과하였다는 것은 암호화 통신을 위한 비밀키로 생체 정보를 사용하는 것이 가능함을 의미한다.
- [0052] 또한, 동일한 시간에 동일한 사람에게서 측정된다면 다른 위치에서 측정되었더라도 같은 생체 정보가 측정된다. 예를 들어, 사람의 맥박은 심장 근처에서 측정한 것과 손목에서 측정한 것이 거의 동일한 값으로 측정된다. 따라서, 이식형 의료 기기(N)와 호스트(P)가 동일한 시간에 동일한 사람에 대해 동일한 생체 정보를 측정하면 동일한 난수를 생성할 수 있다.
- [0053] 즉, 생체 정보는 사용자마다, 시간에 따라 상이하되, 부위별 오차는 작거나 오차를 극복할 수 있는 방안이 있으므로, 의료 기기(N)와 호스트(P)가 동시에 각각 센싱한 사용자의 생체 데이터를 사용하여 세션키를 생성하는 것이 가능하다.
- [0054] 이식형 의료 기기(N)와 호스트(P)가 각각 측정한 생체 정보에 약간의 오차가 발생하는 경우, 오류 정정(error correcting) 기법을 사용하여 조절할 수 있다.
- [0055] 예를 들어, 오류 정정 코드(error correcting code)를 사용한 퍼지 볼트(fuzzy vault) 기법을 사용하여 오차를 조절할 수 있다.
- [0056] 이러한 세션키는 AES와 등의 블록 암호 알고리즘을 이용한 암호화에 사용될 수 있다.
- [0057] 도 6은 본 발명의 일실시예에 따른 데이터 교환 방법의 흐름을 도시하고 있다.
- [0058] 일련의 암호화된 데이터 교환을 통해 의료 행위를 수행하는 세션(session)을 시작하기 전에, 의료 기기(N)와 호스트(P)가 사용자의 생체 정보를 동시에 센싱한다(S100). 의료 기기(N)와 의료 기기 호스트(P)가 각각 센싱한 생체 정보에 오차가 있는 경우, 오류 정정 기법을 사용하여 서로 일치시킨다.
- [0059] 의료 기기(N)와 호스트(P)가 각각 센싱한 생체 정보를 사용하여 세션키를 산출한다(S200).
- [0060] 세션 동안 의료 기기(N)가 센싱한 생체 정보를 자신의 세션키로 암호화하여 호스트(P)로 전송하면, 호스트(P)는 자신의 세션키로 이를 복호화하여 사용한다(S300).
- [0061] 세션 동안 호스트(P)가 의료 기기(N)로 설정값 세팅 등의 제어 정보를 자신의 세션키로 암호화하여 의료 기기로 전송하면, 의료 기기(N)는 자신의 세션키로 이를 복호화하여 사용한다(S400).
- [0062] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 매커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.
- [0063] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다. 본 발명의 일 실시예의 하나 이상의 구성 요소 또는 동작을 실시하기 위하여 사용될 수 있는 컴퓨터 시스템 아키텍처의 일례를 설명하면, 하드웨어 시스템은 프로세서, 캐쉬, 메모리 및 상술한 기능에 관련된 하나 이상의 소프트웨어 어플리케이션 및 드라이버를 포함할 수 있다.
- [0064] 추가적으로, 하드웨어 시스템은 고성능 입/출력(I/O) 버스 및 표준 I/O 버스를 포함한다. 호스트 브릿지는 프로

세서를 고성능 I/O 버스에 결합시키고, I/O 버스 브릿지는 버스들을 상호 결합시킨다. 시스템 메모리 및 네트워크/통신 인터페이스는 고성능 I/O 버스에 결합된다. 하드웨어 시스템은 비디오 메모리 및 그 비디오 메모리에 결합된 디스플레이 장치를 더 포함할 수 있다. 대용량 기억장치 및 I/O 포트는 표준 I/O 버스에 결합된다. 하드웨어 시스템은 키보드 및 포인팅 디바이스(pointing device), 그리고 표준 I/O 버스에 결합된 디스플레이 장치를 선택적으로 포함할 수 있다. 총괄적으로, 이러한 요소들은 넓은 범위의 컴퓨터 하드웨어 시스템을 표현하도록 의도되며, 인텔사에 의해 제조된 펜티엄 프로세서뿐만 아니라 다른 적절한 프로세서에 기반하는 범용 컴퓨터 시스템을 포함하나 이에 제한되지는 않는다.

[0065] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

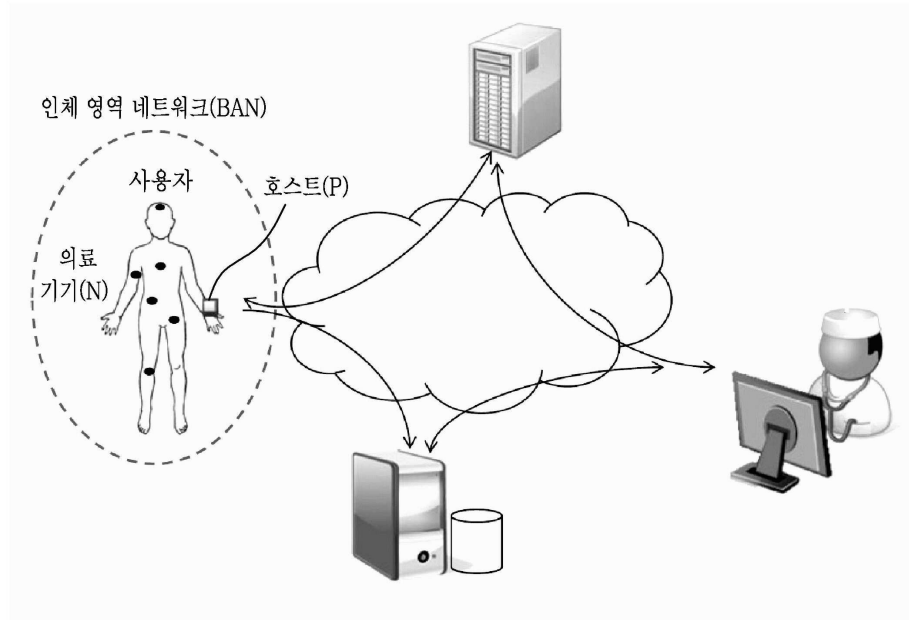
[0066] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

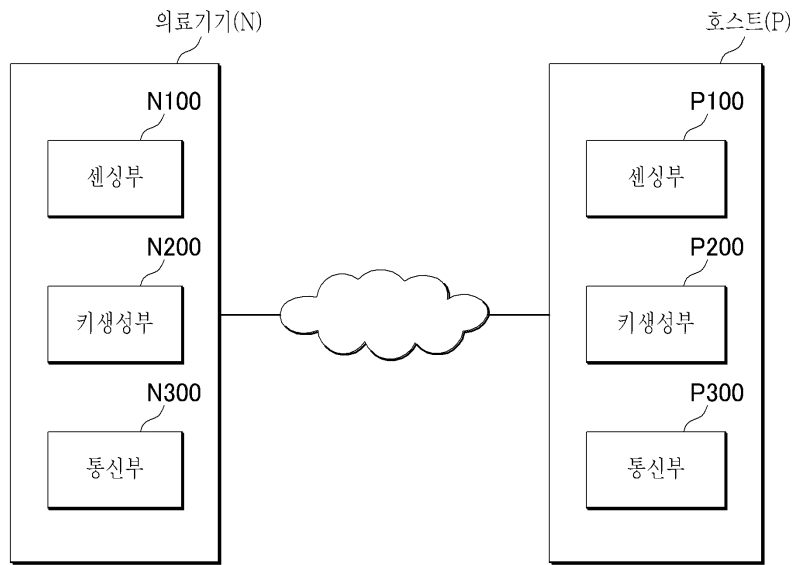
[0067] N: 의료 기기
P: 의료 기기 호스트

도면

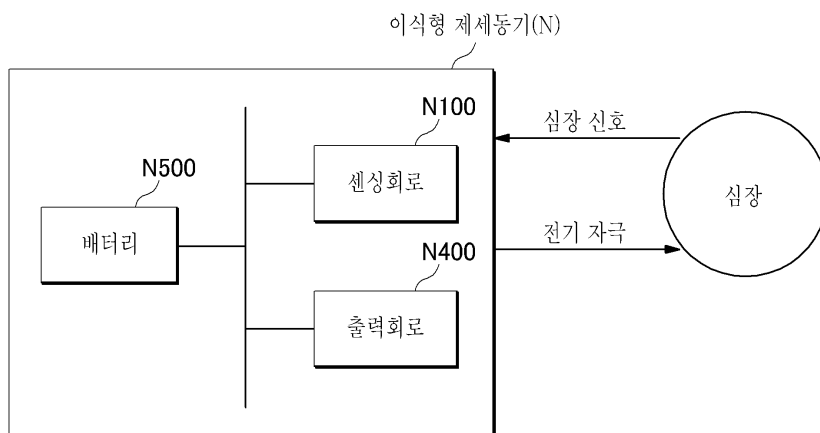
도면1



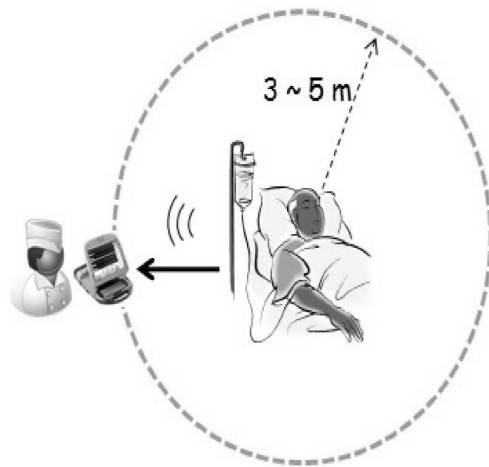
도면2



도면3



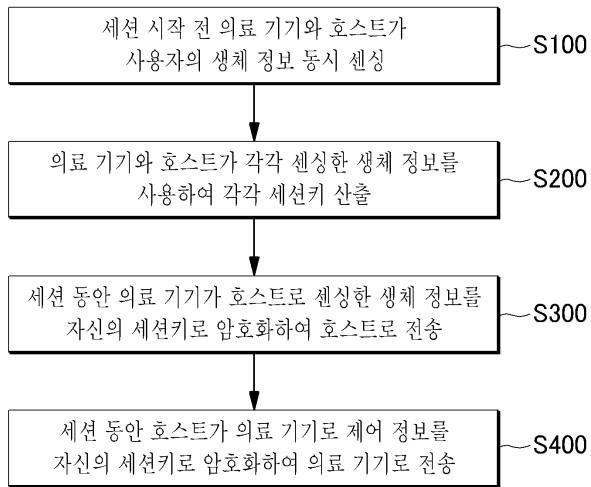
도면4



도면5

생체정보	범위
혈당 (Blood Glucose)	64-140mg/dL
혈압 (Blood Pressure)	120-160mmHg
체온 (Temperature)	97.0-105.0F
헤모글로빈 (Hemoglobin)	12.1-17.2g/dL
혈류량 (Blood Flow)	>0.9ABI <0.5ABI

도면6



专利名称(译)	使用医疗设备和医疗设备的生物特征数据进行数据交换的方法		
公开(公告)号	KR1020140118293A	公开(公告)日	2014-10-08
申请号	KR1020130033918	申请日	2013-03-28
[标]申请(专利权)人(译)	英迪股份有限公司		
申请(专利权)人(译)	英特尔公司沥永久发现		
当前申请(专利权)人(译)	英特尔公司沥永久发现		
[标]发明人	LEE DONG HOON 이동훈 CHOI WON SUK 최원석 LEE HWA SEONG 이화성		
发明人	이동훈 최원석 이화성		
IPC分类号	H04L9/06 H04B13/00 A61B5/00		
CPC分类号	H04L9/0861 A61B5/01 A61B5/02 H04B13/005 H04L2209/88		
外部链接	Espacenet		

摘要(译)

本发明提供一种医疗设备，其被移植或附着到用户的身体以收集用户的一个或多个生物信息，将生物信息传送到医疗设备的主机，并从主机接收控制信息。医疗器械医疗设备通过同时感测用户的特定生物信息与医疗设备的主机来生成会话密钥，并且在会话期间将与会话密钥或控制信息一起加密的生物信息与医疗设备的主机交换。密钥有效。如果医疗设备的主机和医疗设备分别具有感测到的生物信息的错误，则医疗设备通过使用纠错技术彼此匹配。

