(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0069376
(43) 공개일자 2025년05월19일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2021.01) *G06F 21/32* (2013.01)
G06F 9/30 (2018.01) *H04L 9/06* (2006.01)
H04L 9/32 (2006.01) *H04W 12/00* (2021.01)
H04W 12/041 (2021.01) *H04W 12/71* (2021.01)
H04W 84/18 (2009.01)
(52) CPC특허분류
H04W 12/06 (2021.01)
G06F 21/32 (2013.01)
(21) 출원번호 10-2024-0060810
(22) 출원일자 2024년05월08일
심사청구일자 2024년05월08일
(30) 우선권주장
1020230155336 2023년11월10일 대한민국(KR)

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웰 카운티2단지)
(74) 대리인
특허법인충정

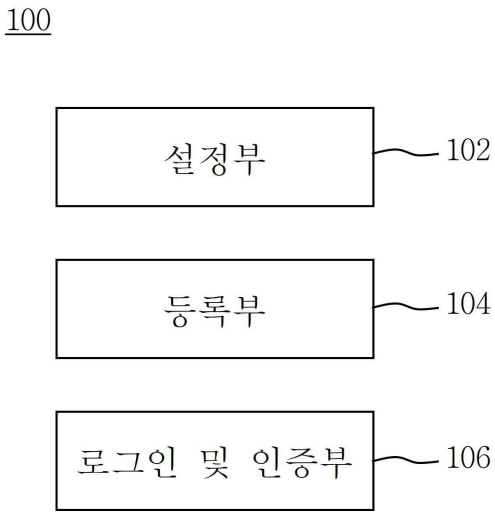
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **지능형 센서 기반 사용자 생체 인증을 위한 향상된 무선 통신 시스템 및 방법**

(57) 요 약

본 발명의 실시예는 복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템으로서, 상기 무선 센서 네트워크의 센서에 ID를 할당하는 설정부; 사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록부; 및 상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증부;를 포함하고, 상기 인증부는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

대 표 도 - 도2



(52) CPC특허분류
G06F 9/30029 (2013.01)
H04L 9/065 (2013.01)
H04L 9/3231 (2013.01)
H04W 12/009 (2021.01)
H04W 12/041 (2021.01)
H04W 12/71 (2021.01)
H04W 84/18 (2013.01)

명 세 서

청구범위

청구항 1

복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템으로서,

상기 무선 센서 네트워크의 센서에 ID를 할당하는 설정부;

사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록부; 및

상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증부;를 포함하고,

상기 인증부는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 2

제1항에 있어서,

상기 설정부는,

상기 센서에 상기 게이트웨이 노드의 비밀키(K_{GN})를 할당하여, 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)가 상기 비밀키(K_{GN})와 함께 센서 ID의 해시가 되도록 하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 3

제1항에 있어서,

상기 등록부는,

상기 사용자의 ID 및 패스워드를 선택하고, 소정의 상기 센서에 상기 사용자의 생체 인식을 각인하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 4

제3항에 있어서,

상기 등록부는, 상기 퍼지 추출기를 이용하여 랜덤 생체 인식 키 및 비-비밀 값을 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 5

제4항에 있어서,

상기 랜덤 생체 인식 키 및 상기 비-비밀 값은 Gen(BIO) = 〈R, P〉 이고, 상기 R 및 상기 패스워드의 해시를 계산하여 상기 사용자의 생체 인식 기반의 패스워드(HPWi)를 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

(여기에서, Gen(.)은 퍼지 생성 함수, BIO는 사용자의 생체 인식, R은 랜덤 생체 인식 키, P는 퍼지 추출기에 의해 생성된 비-비밀 값임)

청구항 6

제2항에 있어서,

상기 등록부는,

상기 센서의 등록을 위해서 상기 센서의 ID(ID_{SN}) 및 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)를 상기 게이트웨이 노드로 전송하고,

상기 게이트웨이 노드는 상기 비밀키(K_{GN})를 사용하여 상기 센서의 ID(ID_{SN})의 해시로서 SID*를 계산하고,

상기 SID*와 상기 SID가 일치하면 상기 센서를 등록하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 7

제5항에 있어서,

상기 로그인 및 인증부는,

상기 사용자가 생체 인식을 입력하고,

상기 퍼지 추출기의 재생 함수를 계산하여 랜덤 생체 인식 키 R = Rep〈BIO, P〉를 재생성하고,

상기 R을 이용하여 상기 생체 인식 기반의 패스워드(HPWi)를 HPWi*로 계산하고,

상기 생체 인식 기반의 패스워드(HPWi)와 상기 HPWi*가 일치하면 상기 사용자를 정당한 사용자로 인식하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 8

제3항에 있어서,

상기 사용자 생체 인증 무선 통신 시스템은 패스워드 변경부를 더 포함하고, 상기 패스워드 변경부는,

상기 퍼지 추출기의 생성 함수를 이용하여 상기 사용자 생체 인식의 비-비밀 값 P 및 랜덤 생체 인식 키 R을 계산하고,

상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 패스워드의 해시를 HPWi*로 계산하고,

상기 패스워드와 상기 HPWi*가 일치하면, 상기 사용자가 새로운 패스워드를 입력하고,

상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 새로운 패스워드의 해시를 계산하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템.

청구항 9

복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크의 센서에 ID를 할당하는 설정 단계;

사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록 단계; 및

상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증 단계;를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법으로서,

상기 인증 단계는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 10

제9항에 있어서,

상기 설정 단계는,

상기 센서에 상기 게이트웨이 노드의 비밀키(K_{GN})를 할당하여, 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)가 상기 비밀키(K_{GN})와 함께 센서 ID의 해시가 되도록 하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 11

제9항에 있어서,

상기 등록 단계는,

상기 사용자의 ID 및 패스워드를 선택하고, 소정의 상기 센서에 상기 사용자의 생체 인식을 각인하는 것을 포함하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 12

제11항에 있어서,

상기 등록 단계는, 상기 퍼지 추출기를 이용하여 랜덤 생체 인식 키 및 비-비밀 값을 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 13

제12항에 있어서,

상기 랜덤 생체 인식 키 및 상기 비-비밀 값은 Gen(BIO) = 〈R, P〉 이고, 상기 R 및 상기 패스워드의 해시를 계산하여 상기 사용자의 생체 인식 기반의 패스워드(HPWi)를 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

(여기에서, Gen(.)은 퍼지 생성 함수, BIO는 사용자의 생체 인식, R은 랜덤 생체 인식 키, P는 퍼지 추출기에 의해 생성된 비-비밀 값임)

청구항 14

제10항에 있어서,

상기 등록 단계는,

상기 센서의 등록을 위해서 상기 센서의 ID(ID_{SN}) 및 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)를 상기 게이트웨이 노드로 전송하고,

상기 게이트웨이 노드는 상기 비밀키(K_{GN})를 사용하여 상기 센서의 ID(ID_{SN})의 해시로서 SID*를 계산하고,

상기 SID*와 상기 SID가 일치하면 상기 센서를 등록하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 15

제13항에 있어서,

상기 로그인 및 인증 단계는,

상기 사용자가 생체 인식을 입력하고,

상기 퍼지 추출기의 재생 함수를 계산하여 랜덤 생체 인식 키 R = Rep〈BIO, P〉를 재생성하고,

상기 R을 이용하여 상기 생체 인식 기반의 패스워드(HPWi)를 HPWi*로 계산하고,

상기 생체 인식 기반의 패스워드(HPWi)와 상기 HPWi*가 일치하면 상기 사용자를 정당한 사용자로 인식하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

청구항 16

제11항에 있어서,

상기 사용자 생체 인증 무선 통신 방법은 패스워드 변경 단계를 더 포함하고, 상기 패스워드 변경 단계는,

상기 퍼지 추출기의 생성 함수를 이용하여 상기 사용자 생체 인식의 비-비밀 값 P 및 랜덤 생체 인식 키 R을 계산하고,

상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 패스워드의 해시를 HPWi*로 계산하고,

상기 패스워드와 상기 HPWi*가 일치하면, 상기 사용자가 새로운 패스워드를 입력하고,

상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 새로운 패스워드의 해시를 계산하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 지능형 센서 기반 사용자 생체 인증을 위한 향상된 무선 통신 시스템 및 방법에 관한 것으로서, 더욱 상세하게는 사용자의 생체 인식(biometrics)에 기반한 경량 및 보안 인증 프로토콜을 이용하여 무선 센서 네트워크에서 무선 통신을 하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 애드 혹(Ad hoc) 네트워크 장치는 에너지, 저장 및 프로세싱을 위한 리소스가 제한되어 있다. 또한, 기존의 보안 솔루션은 매우 작은 센서 노드에는 적합하지 않다. 대칭형 암호 방식은 공개 키 암호 방식보다 더 많은 에너지를 소비하는 반면, 공개 키 암호 방식은 자원 집약적이어서 무선 네트워크에 적합하지 않다.

[0003] 또한, 대칭형 암호 방식에는 키(key) 관리 문제가 있다. 다양한 인증 메커니즘이 설계되었지만 거의 모두 복잡하거나 안전하지 않다. 더 적은 리소스 소비로 네트워크 보안을 개선하려면 더 진보되고 가벼운 솔루션을 개발할 필요가 있다.

[0004] 무선 센서 네트워크(wireless sensor network, WSN)에서 센서 노드는 주로 전장(battlefield), 감시(surveillance), 공항 또는 중요한 건물과 같은 안전하지 않은 장소에 배치되기 때문에 무선 센서 네트워크 애플리케이션에서 보안은 필수적이다. 이러한 네트워크의 데이터는 센서 노드를 통해 개방된 공간으로 무선으로 전송되므로, 제3자가 신호를 가로챌 가능성이 있어 네트워크에 주요 위협이 된다.

발명의 내용

해결하려는 과제

[0005] 이와 같은 문제점을 해결하기 위하여, 본 발명은 무선 센서 네트워크에 대한 안전한 사용자 인증 시스템과 방법을 제공하는데 그 목적이 있다.

과제의 해결 수단

[0006] 본 발명의 실시예는, 복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템으로서, 상기 무선 센서 네트워크의 센서에 ID를 할당하는 설정부; 사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록부; 및 상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증부;를 포함하고, 상기 인증부는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0007] 본 발명의 실시예는, 상기 설정부는, 상기 센서에 상기 게이트웨이 노드의 비밀키(K_{GN})를 할당하여, 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)가 상기 비밀키(K_{GN})와 함께 센서 ID의 해시가 되도록 하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0008] 본 발명의 실시예는, 상기 등록부는, 상기 사용자의 ID 및 패스워드를 선택하고, 소정의 상기 센서에 상기 사용자의 생체 인식을 각인하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0009] 본 발명의 실시예는, 상기 등록부는, 상기 퍼지 추출기를 이용하여 랜덤 생체 인식 키 및 비-비밀 값을 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0010] 본 발명의 실시예는, 상기 랜덤 생체 인식 키 및 상기 비-비밀 값은 Gen(BIO) = 〈R, P〉이고, 상기 R 및 상기 패스워드의 해시를 계산하여 상기 사용자의 생체 인식 기반의 패스워드(HPWi)를 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다. (여기에서, Gen(.)은 퍼지 생성 함수, BIO는 사용자의 생체 인식, R은 랜덤 생체 인식 키, P는 퍼지 추출기에 의해 생성된 비-비밀 값임)

[0011] 본 발명의 실시예는, 상기 등록부는, 상기 센서의 등록을 위해서 상기 센서의 ID(ID_{SN}) 및 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)를 상기 게이트웨이 노드로 전송하고, 상기 게이트웨이 노드는 상기 비밀키(K_{GN})를 사용하여 상기 센서의 ID(ID_{SN})의 해시로서 SID*를 계산하고, 상기 SID*와 상기 SID가 일치하면 상기 센서를 등록하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0012] 본 발명의 실시예는, 상기 로그인 및 인증부는, 상기 사용자가 생체 인식을 입력하고, 상기 퍼지 추출기의 재생함수를 계산하여 랜덤 생체 인식 키 R = Rep〈BIO, P〉를 재생성하고, 상기 R을 이용하여 상기 생체 인식 기반의 패스워드(HPWi)를 HPWi*로 계산하고, 상기 생체 인식 기반의 패스워드(HPWi)와 상기 HPWi*가 일치하면 상기 사용자를 정당한 사용자로 인식하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0013] 본 발명의 실시예는, 상기 사용자 생체 인증 무선 통신 시스템은 패스워드 변경부를 더 포함하고, 상기 패스워드 변경부는, 상기 퍼지 추출기의 생성 함수를 이용하여 상기 사용자 생체 인식의 비-비밀 값 P 및 랜덤 생체 인식 키 R을 계산하고, 상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 패스워드의 해시를 HPWi*로 계산하고, 상기 패스워드와 상기 HPWi*가 일치하면, 상기 사용자가 새로운 패스워드를 입력하고, 상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 새로운 패스워드의 해시를 계산하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 제공한다.

[0014] 본 발명의 실시예는, 복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크의 센서에 ID를 할당하는 설정 단계; 사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록 단계; 및 상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증 단계;를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법으로서, 상기 인증 단계는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0015] 본 발명의 실시예는, 상기 설정 단계는, 상기 센서에 상기 게이트웨이 노드의 비밀키(K_{GN})를 할당하여, 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)가 상기 비밀키(K_{GN})와 함께 센서 ID의 해시가 되도록 하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0016] 본 발명의 실시예는, 상기 등록 단계는, 상기 사용자의 ID 및 패스워드를 선택하고, 소정의 상기 센서에 상기 사용자의 생체 인식을 각인하는 것을 포함하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0017] 본 발명의 실시예는, 상기 등록 단계는, 상기 퍼지 추출기를 이용하여 랜덤 생체 인식 키 및 비-비밀 값을 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0018] 본 발명의 실시예는, 상기 랜덤 생체 인식 키 및 상기 비-비밀 값은 Gen(BIO) = 〈R, P〉이고, 상기 R 및 상기 패스워드의 해시를 계산하여 상기 사용자의 생체 인식 기반의 패스워드(HPWi)를 생성하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다. (여기에서, Gen(.)은 퍼지 생성 함수, BIO는 사용자의 생체 인식, R은 랜덤 생체 인식 키, P는 퍼지 추출기에 의해 생성된 비-비밀 값임)

[0019] 본 발명의 실시예는, 상기 등록 단계는, 상기 센서의 등록을 위해서 상기 센서의 ID(ID_{SN}) 및 상기 게이트웨이 노드에 대한 상기 센서의 ID(SID)를 상기 게이트웨이 노드로 전송하고, 상기 게이트웨이 노드는 상기 비밀키(K_{GN})를 사용하여 상기 센서의 ID(ID_{SN})의 해시로서 SID*를 계산하고, 상기 SID*와 상기 SID가 일치하면 상기 센서를 등록하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0020] 본 발명의 실시예는, 상기 로그인 및 인증 단계는, 상기 사용자가 생체 인식을 입력하고, 상기 퍼지 추출기의 재생 함수를 계산하여 랜덤 생체 인식 키 R = Rep〈BIO, P〉를 재생성하고, 상기 R을 이용하여 상기 생체 인식 기반의 패스워드(HPWi)를 HPWi*로 계산하고, 상기 생체 인식 기반의 패스워드(HPWi)와 상기 HPWi*가 일치하면

상기 사용자를 정당한 사용자로 인식하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

[0021] 본 발명의 실시예는, 상기 사용자 생체 인증 무선 통신 방법은 패스워드 변경 단계를 더 포함하고, 상기 패스워드 변경 단계는, 상기 퍼지 추출기의 생성 함수를 이용하여 상기 사용자 생체 인식의 비-비밀 값 P 및 랜덤 생체 인식 키 R을 계산하고, 상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 패스워드의 해시를 HPWi*로 계산하고, 상기 패스워드와 상기 HPWi*가 일치하면, 상기 사용자가 새로운 패스워드를 입력하고, 상기 랜덤 생체 인식 키 R로 XoR 연산된 상기 새로운 패스워드의 해시를 계산하는, 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법을 제공한다.

발명의 효과

[0022] 본 발명의 실시예는 계산 비용과 통신 오버헤드를 감소시킬 수 있다.

[0023] 또한, 본 발명의 실시예는 다양한 공격에 의한 영향을 줄여 무선 센서 네트워크를 안전하게 보호할 수 있다.

[0024] 또한, 본 발명의 실시예는 노드와 사용자 간의 통신이 데이터 패킷의 인증, 무결성, 가용성을 보장할 수 있도록 가볍고 덜 복잡한 인증 프로토콜을 설계할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크를 개략적으로 나타내는 도면이다.

도 2는 본 발명의 실시예에 따른 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 개략적으로 나타내는 도면이다.

도 3은 해시 함수가 단방향 함수 특성을 갖는 단방향 해시 함수를 나타내는 도면이다.

도 4는 퍼지 추출기의 메커니즘을 나타내는 도면이다.

도 5는 XOR 게이트를 나타내는 도면이다.

도 6은 본 발명의 실시예에 따른 BUAKA 방식의 사용자 등록 단계를 나타내는 도면이다.

도 7은 본 발명의 실시예에 따른 BUAKA 방식의 센서 등록 단계를 나타내는 도면이다.

도 8은 본 발명의 실시예에 따른 BUAKA 방식의 로그인 및 인증 단계를 나타내는 도면이다.

도 9는 본 발명의 실시예에 따른 BUAKA 방식의 패스워드 업데이트를 나타내는 도면이다.

도 10은 AVISPA Span 인증 도구를 나타내는 도면이다.

도 11은 AVISPA 도구의 작업 흐름도이다.

도 12는 사용자 측에서의 계산 복잡도 비교를 나타내는 도면이다.

도 13은 게이트웨이 노드 측에 대한 계산 복잡도 비교를 나타내는 도면이다.

도 14는 센서 측에서 계산 복잡도 비교를 나타내는 도면이다.

도 15는 전체적인 계산 복잡도 비교를 나타내는 도면이다.

도 16은 도 12 내지 도 14를 종합하여 계산 복잡도 비교를 나타내는 도면이다.

도 17은 본 발명의 실시예에 따른 BUAKA 방식의 개선된 비율을 나타내는 도면이다.

도 18은 통신 오버헤드의 비교를 나타내는 도면이다.

도 19는 OFMC 시뮬레이션의 결과를 나타내는 도면이다.

도 20은 CL-AtSe 시뮬레이션의 결과를 나타내는 도면이다.

도 21은 본 발명의 실시예에 따른 지능형 센서 기반의 사용자 생체 인증 무선 통신 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 이하, 첨부된 도면을 참조하여 본 명세서에 개시된 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0027] 본 설명에서, "포함", "구비" 또는 "구성"과 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0028] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0029] 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0030] 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않으며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0031] 또한, 본 명세서 전체에 걸쳐 인용된 논문의 개시 내용은 그 전체로서 본 명세서에 참조로 삽입되어 본 출원이 속하는 기술 분야의 수준 및 본 출원의 내용이 보다 명확하게 설명된다.

[0032] 아래에서는, 본 발명의 실시예에 대하여 도면을 참조하여 상세히 설명한다.

[0033] 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 개략적으로 나타내는 도면이다.

[0034] 무선 통신 기술은 의료, 국방, 농업, 산업 분야로부터 시작하여 다양한 응용 프로그램을 제공하는 주요 역할을 한다. 무선 센서 네트워크(WSN)는 이전의 인프라 구조를 통해 통신하거나 인프라 없이 통신하는 노드 그룹으로 정의할 수 있다.

[0035] 단일 센서 노드는 마이크로프로세서, 제한된 스토리지, 배터리 리소스를 포함한다. 이러한 네트워크의 주요 목적은 많은 양의 데이터를 수집하며, 중요한 이벤트를 식별하고, 그에 따라 대응하는 것이다. 무선 센서 네트워크는 다수의 센서 노드(Sensor Node), 싱크 노드(Sink Node) 또는 게이트웨이 노드(Gateway Node, GN 또는 GWN), 및 기지국(Base Station, BS)으로 구성된다.

[0036] 게이트웨이 노드(GN)는 네트워크와 실제 세계 사이의 커뮤니케이터 역할을 하므로 일반 센서 노드에 비해 추가적인 리소스를 가지고 있다. 센서 노드는 동작, 온도, 소리, 압력, 진동 및 공기 품질과 같은 주변 환경의 실시간 데이터를 모니터링하고 수립하도록 설계되었다.

[0037] 따라서, 데이터는 여러 노드를 통해 게이트웨이 노드(GN)에 전달되며 무선 연결을 통해 최종 사용자와 통신한다. 어떤 노드들은 일반적으로 불리한 환경 조건에 대해 제안되는 무작위 방식(비결정적 방식)으로 배치되는 반면, 다른 노드들은 결정적 방식으로 배치된다. 노드의 배치는 노드 연결성, 커버리지 영역, 에너지 사용률과 같은 몇 가지 중요한 요소를 고려하여 이루어진다.

[0038] 무선 센서 네트워크가 해당 지역에 배치되면, 그 안의 마이크로 프로세서가 노드 간 통신을 자동으로 시작하여 네트워크를 형성하고 무선 센서 네트워크 범위 내에서 노드 간에 데이터를 전송한다. 이러한 무선 센서 네트워크의 특성으로 인해 모든 위치에 무선 센서 네트워크의 배치를 허용한다.

[0039] 무선 센서 네트워크는 전통적인 유선 네트워크에 비해 다양한 이점을 가지고 있지만 데이터 통신, 제한된 배터리 자원, 로컬리제이션(Localization), 확장성, 로드 밸런싱(Load Balancing) 및 보안과 관련된 몇 가지 문제가 여전히 존재한다. 이러한 문제는 센서 노드의 성능에 영향을 미치며 데이터 지연, 처리 복잡도(processing complexity), 오버헤드, 지연 시간, 낮은 처리량, 노드 고갈(node depletion) 및 데이터 위반(data breach)으로 이어진다.

[0040] 무선 센서 네트워크 노드는 보안이 없으면 쉽게 손상된다. 센서 노드는 라우팅 정보 스푸핑(Spoofing)이나 변조, 민감한 정보 수집, 싱크홀 공격(Sinkhole Attack), 시빌 공격(Sybil Attack), 서비스 거부(DoS) 공격,

트래픽 분석, 모니터링 및 도청 등 다양한 공격에 취약하다.

[0041] 싱크홀 공격에서는 노드가 손상되고 가짜 광고 및 가짜 라우팅 업데이트를 사용하여 네트워크 트래픽을 공격한다. 시빌 공격에서는 공격자가 많은 수의 가명 ID를 생성하고 서비스를 파괴한다. DoS 공격에서는 공격자가 네트워크 리소스를 사용할 수 없도록 만들려고 한다.

[0042] 애플리케이션마다 다른 보안 요구 사항이 있으며 이러한 요구 사항이 충족되지 않으면 공격에 더 취약해진다. 이러한 공격은 외부 또는 내부 공격, 능동 또는 수동 공격 등 여러 가지 방식으로 분류할 수 있다. 외부 공격은 무선 센서 네트워크의 원격 및 개방 영역에 기인하는 반면, 내부 공격은 애플리케이션 유형에 따라 다르다. 공격은 능동 및 수동 공격으로도 나눌 수 있다. 능동 공격에서는 공격자가 메시지 내용을 수정하는 반면, 수동 공격에서는 공격자가 메시지를 관찰하기만 한다.

[0043] 무선 센서 네트워크에 대해 다양한 인증 방식이 개발되었지만, 실질적으로 기존의 인증 방식은 모두 데이터 통신을 위해 사용자와 센서 노드를 인증하기 위해 더 많은 계산 능력과 리소스를 소모한다. 센서들은 매우 낮은 연산 처리 능력을 갖는데, 이는 장치들이 작고 리소스의 수가 제한적이기 때문이다.

[0044] 그 결과, 장치들은 다양한 보안 메커니즘을 구현할 수 없게 된다. 일부 인증 방식은 센서의 리소스를 제한하는 특성을 가지고 있다. 그러나 경량 방식을 개발하기 위해 이러한 방식은 센서 보안을 희생하게 된다.

[0045] 따라서 무선 센서 네트워크에서 리소스 효율성과 보안 표준 사이의 균형을 맞출 수 있는 경량 인증 방식이 필요하게 된다. 따라서, 본 발명의 실시예에서는 경량 인증 프로토콜에 대한 요구 사항을 충족시키기 위해 사용자의 생체 인식(biometrics)에 기반한 경량 및 보안 인증 프로토콜을 제공한다.

[0046] 도 2는 본 발명의 실시예에 따른 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템을 개략적으로 나타내는 도면이다.

[0047] 도 2를 참조하면, 복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 시스템(100)은, 무선 센서 네트워크의 센서에 ID를 할당하는 설정부(102); 사용자의 생체 정보 및 센서를 게이트웨이 노드에 등록하는 등록부(104); 및 사용자의 생체 인식을 이용하여 무선 센서 네트워크에 로그인하고, 게이트웨이 노드가 사용자의 생체 정보 및 센서를 인증하는 로그인 및 인증부(106);를 포함한다. 이때, 로그인 및 인증부(106)는 퍼지 추출기를 이용하여 생체 인식을 생성 및 재생하며, 퍼지 추출기는 해시 함수를 사용할 수 있다.

[0048] 무선 통신 시스템(100)은 패스워드 변경부를 더 포함할 수 있다. 패스워드 변경부는, 퍼지 추출기의 생성 함수를 이용하여 사용자 생체 인식의 비-비밀 값 P 및 랜덤 생체 인식 키 R을 계산하고, 랜덤 생체 인식 키 R로 XoR 연산된 패스워드의 해시를 HPWi*로 계산하고, 패스워드와 HPWi*가 일치하면 사용자가 새로운 패스워드를 입력하고, 랜덤 생체 인식 키 R로 XoR 연산된 새로운 패스워드의 해시를 계산할 수 있다.

[0049] 본 발명의 실시예에서는 센서와 사용자 모두 통신을 위한 3-방향 핸드셰이크(3-way handshake)를 설정하기 전에 게이트웨이 노드(GN)에 등록할 수 있다. 기존의 인증 방식과 달리 본 발명의 실시예에 따른 BUAKA(Biometric based User Authentication and Key Agreement)에서는 퍼지 추출기(Fuzzy extractor)를 사용하여 사용자 인증을 위해 생체 인식을 생성하고 재생할 수 있다.

[0050] 본 발명의 실시예는 기존 접근 방식의 단점을 해결하기 위해 설계된 AKA(Authentication and Key Agreement) 방식을 계승한다.

[0051] 본 발명의 실시예는 기존 인증 방식을 단순화하는 동시에 무선 센서 네트워크에 대한 보다 최근의 일반적인 보안 위협을 포착하는 것을 목표로 한다.

[0052] 본 발명의 실시예에 따른 인증 방식은 설정 단계(setup phase), 등록 단계(registration phase), 로그인 및 인증 단계(authentication phase), 패스워드 변경 단계의 4단계로 구분된다.

[0053] 설정 단계는 센서 노드의 사전 배치 단계로 간주될 수 있다. 배치 전에 시스템 관리자는 설정 단계에서 각각의 모든 센서에 대해 ID를 선택하고 할당한다. 설정 단계에서는 모든 신규 노드와 기존 노드가 게이트웨이 노드(GN)의 ID를 갖도록 한다. 게이트웨이 노드는 통신을 위해 노드와 사용자를 추가로 연결한다.

[0054] 등록 단계에서는 사용자와 센서가 게이트웨이 노드에 등록된다. 사용자는 생체 인식 등록을 위해 퍼지 추출기를 사용하고, 생성된 생체 인식 값은 스마트 카드에 저장된다. 사용자가 로그인하면, 사용자의 스마트 카드에 저장된 생체 인식을 사용자의 현재 생체 인식과 비교한다. 이 네 가지 단계는 서로 연결되어 집합적인 과정을 수행

하고 네트워크 보안을 향상시킬 수 있다.

[0056] 1. 단방향 해시 함수(One way hash function)

[0057] 입력의 크기가 임의적이고 고정되지 않고 생성된 출력이 항상 고정된 길이의 이진 시퀀스인 압축 함수를 단방향 해시 함수 h(.)이라고 한다. 단방향은 출력 문자열에서 원래 입력 텍스트를 추출하는 것이 계산상 불가능하다는 것을 의미한다.

[0058] 다른 방식에서는, 해시 함수는 보낸 사람을 인증하고 메시지의 무결성을 검사하는 데 사용된다. 강력한 해시 함수는 동일한 해시 값을 가지는 두 개의 문자열을 찾기 어렵게 만든다. 일반적으로 해시 함수는 128비트의 해시 값을 생성한다. B = h(A)와 같이 입력 A의 해시가 B이면 $B = h^{-1}(A)$를 결정하는 것은 거의 불가능하다.

[0059] 도 3은 해시 함수가 단방향 함수 특성을 갖는 단방향 해시 함수를 나타내는 도면이다.

[0060] 해시 함수를 역으로 하는 것은 계산상 불가능하다. 또한, 해시 함수는 충돌 방지(collision-free)의 특징을 갖는다. 즉, 두 개의 개별 입력(input)이 동일한 해시 출력(hash output) 결과를 생성할 수 없고, 또한 매우 빠르다. 해시 계산 속도가 매우 빠른 특징을 갖는다.

[0062] 2. 퍼지 추출기(Fuzzy extractor)

[0063] 기존의 해싱 출력(hashing output)은 항상 고유하며, 입력이 약간만 달라도 완전히 별개의 출력을 생성할 수 있다. 생체 정보(biometric information)는 데이터 수집 과정에서 다양한 소리와 왜곡에 취약하여 원래의 생체 인식을 재생하는 것이 불가능하다는 것을 유념해야 한다.

[0064] 이러한 문제를 피하기 위해 퍼지 추출기 접근법이 제안된다. 거의 동일한 노이즈 입력 소스에 대해 동일한 출력 키를 생성하기 위해 퍼지 추출기가 사용된다. 입력 소스는 사용자의 생체 인식이 될 수 있으며, 퍼지 추출기는 생성된 사용자의 생체 데이터에서 생체 템플릿을 키로 사용하여 사용자가 인증할 수 있도록 한다. 퍼지 추출기는 생성(generate)과 재생(reproduce) 두 가지 방법을 채택한다.

[0065] 도 4는 퍼지 추출기의 메커니즘을 나타내는 도면이다.

[0066] - 생성(generate): 사용자의 생체 데이터(biometric data)를 이용하여 Gen(Bio) = 〈R, P〉와 같이 랜덤 키(random key) r 및 비-비밀 값(non-secret value) p를 생성한다.

[0067] - 재생(reproduce): 이 함수는 비-비밀 값 p를 사용하여 R = Rep 〈Bio', P〉와 같이 거의 동일한 생체 인식(biometrics)의 랜덤 키 r을 재생한다.

[0068] 도 4는 거의 동일한 노이즈 입력 소스에 대한 출력 키(output key)를 생성하는 데 사용되는 퍼지 추출기를 보여준다. 입력 소스(생체 인식)가 사용자 및 퍼지 추출기에 사용되고 사용자를 인증할 수 있게 하는 반면, 인증은 생성된 사용자의 생체 데이터에서 생체 템플릿(biometric template)을 키(key)로 사용하여 적용된다.

[0070] 3. 비트별 XOR 연산(Bitwise XOR operation)

[0071] 배타적 OR(exclusive OR)은 비트 패턴(bit pattern)에 대해 작용하는 이진 연산이다. 크기가 같은 2비트 쌍의 각각의 쌍에 대해 XOR을 수행한다. 두 비트가 같다면, 즉 둘 다 0이거나 1인 경우에는 결과값으로 0을 산출한다. 다른 비트 패턴에서는 결과적으로 항상 1을 반환한다. 비트 연산은 매우 간단하기 때문에 일반적으로 많은 산술 연산보다 빠른 특징을 갖는다.

[0072] 도 5는 XOR 게이트를 나타내는 도면이다.

[0073] 도 5는 비트 패턴에 대한 논리 XOR(logical XOR) 게이트 연산을 보여준다. 플로우 다이어그램은 XOR 연산이 2비트 쌍을 취하고, 두 쌍이 동일하면 모두 0 또는 1이라는 것을 명확하게 보여주고 있다.

[0075] 4. BUAKA의 작동

[0076] 본 발명의 실시예에 따른 프로토콜인 BUAKA(Biometric based User Authentication and Key Agreement)에 대하여 자세히 설명한다. 본 발명의 실시예에 따른 BUAKA 방식은 사용자 생체 인식과 사용자 비밀 암호의 해시(Hash)와 함께 퍼지 추출기(fuzzy extractor) 알고리즘의 사용자 세부 정보를 숨긴다. 모든 통신 메시지는 해시 함수, 연접 함수(concatenated function) 또는 XOR 함수의 결과이다. 이러한 방식으로, 평문(plain text)이 드러나게 하기 위해 메시지를 가로채는 위험을 쉽게 방지할 수 있다.

[0077] 본 발명의 실시예에 따른 BUAKA 프로토콜은 설정 단계, 등록 단계, 로그인 및 인증 단계, 패스워드 변경 단계의 4단계로 구성된다.

[0078] 등록 단계는 사용자 등록 및 센서 등록을 더 포함할 수 있다. 또한, 본 발명의 실시예에 따른 방식은 주로 세 개의 개체(entity), 즉 사용자, 게이트웨이 노드, 센서 노드에 기반한다.

[0079] 사용자는 자신의 생체 정보(biometric information)에 대해 퍼지 추출기를 사용하므로, 등록, 로그인 및 인증에 자신의 생체 정보를 사용할 수 있다. 로그인 및 인증 단계에서, 성공적인 로그인의 완료 직후에 인증이 시작된다. 게이트웨이 노드의 목적은 데이터 전송을 위해 센서와 사용자 사이에 보안 세션을 절충(negotiation)하고 설정하는 것이다.

[0080] 게이트웨이 노드는 세션을 시작하기 전에 센서와 사용자 모두를 인증한다. 패스워드 갱신 단계는 사용자가 스마트 카드에서 자신의 정보를 변경할 수 있도록 한다. 프로토콜을 더 잘 이해하기 위해 표 1은 BUAKA의 프로토콜에서 사용되는 표기법을 보여준다.

표 1

[0081]

Symbol	Description
U	User
GN	Gateway node
SN	Sensor node
IDi	User’s ID
ID_{GN}	GN’s ID
ID_{SN}	Sensor node’s ID
PWi	User’s selected password
Bio	User’s biometric info
HPWi	User’s biometric based password
HIDi	User’s anonymous ID
Gen(.)	Fuzzy generator function
Rep(.)	Fuzzy reproduction function
SC	Smart card
K_{GN}	Gateway node’s secret key
SID	sensor identity w.r.t GN
SKij	Session key between user and sensor
R	Random key of Biometric
P	Non-secret value of Biometric
Ri	Random number generated for IDi
Rg	Random number of GN
Ti	Time stamps
ΔT	Maximum transmission delay
h(.)	Secure one-way hashing function
||	Concatenation
⊕	Bitwise XOR

[0082] 4.1. 설정 단계(setup phase)

[0083] 이 단계에서는 등록 요청을 송신하고 올바른 응답을 수신할 수 있도록, 무선 센서 네트워크를 배치하기 전에 센서가 게이트웨이 노드에 대한 정보를 포함하고 있는지 확인한다. 배치 전에 시스템 관리자(system administrator, SA)는 각 센서에 ID를 선택하고 할당한다. 시스템 관리자는 또한 센서에 게이트웨이 노드의 비

밀키(secret key)(K_{GN})를 할당하여 게이트웨이 노드에 대한 센서 ID(SID)가 K_{GN}과 함께 센서 ID의 해시가 되도록 한다.

[0084] $SID = h(ID_{SN} || K_{GN})$

[0085] SID는 모든 센서 노드의 메모리에 저장된다. 또한, 사용자는 모든 센서 ID_{SN}에 대해 알고 있다.

[0087] 4.2. 등록 단계(Registration phase)

[0088] 도 6은 본 발명의 실시예에 따른 BUAKA 방식의 사용자 등록 단계를 나타내는 도면이다.

[0089] 등록 단계에서는 사용자 및 센서를 GN에 등록하는 것을 다룬다. 또한, 등록 단계에서는 센서에 저장된 데이터에 접근하기 위해 매번 사용자가 로그인할 수 있는 스마트 카드를 생성한다. 본 발명의 실시예에 따른 등록 단계는 사용자 등록과 센서 등록의 두 부분으로 구성된다. 도 6은 사용자 등록의 4단계를 보여준다.

[0090] <사용자 등록 단계>

[0091] 단계 1: 사용자는 먼저 자신의 ID(identity) IDi와 패스워드 PWi를 선택한 다음 특정 디바이스의 센서에 생체 인식 BIO를 각인시킨다. 그 다음 디바이스는 퍼지 추출기의 생성 기능을 사용하여, $Gen(BIO) = \langle R, P \rangle$와 같은 랜덤 생체 인식 키(biometric key) 및 비-비밀 값(non-secret value)을 생성한다. 여기서 R은 생체 인식의 랜덤 키이고 P는 퍼지 추출기에 의해 생성된 비-비밀 값이다.

[0092] 단계 2: 사용자는 랜덤 키 R과 패스워드 PWi의 해시를 HPWi로 계산한다. 이것이 사용자의 생체 인식 기반 패스워드(biometric based password)가 된다.

[0093] 단계 3: 사용자는 임의의 Ri를 선택하고, 랜덤 Ri와 사용자 ID IDi의 해시를 HIDi로 계산한다. 이 단계는 게이트웨이 노드와 센서들에 대한 사용자의 익명성을 보장한다.

[0094] 단계 4: 사용자는 게이트웨이 노드에 대한 등록 요청으로 해시 ID HIDi와 생체 정보 기반 패스워드 HPWi를 전송한다.

[0095] 단계 5: HIDi와 HPWi를 요청 메시지(request message)로 수신한 후 게이트웨이 노드는 랜덤키 Rg를 선택하고 스마트카드 값에 대한 2개의 파라미터를 계산한다. 이 두 개의 파라미터를 Ai와 Bi라고 표시한다. Ai는 게이트웨이 노드 키 K_{GN}과 연접된(concatenated) 랜덤 키 Rg의 해시로 계산된다.

[0096] 그리고 그 XoR을 HPWi로 가져온다. 다른 파라미터 Bi는 K_{GN}과 연접된 HIDi의 해시로 계산된다. 그 결과값이 HPWi와 HIDi의 해시값과 XoR 연산된다. 게이트웨이 노드는 메모리에 Ai와 Bi를 랜덤 Rg와 함께 저장한다. 게이트웨이 노드는 스마트카드 SC로서 Ai와 Bi를 보낸다.

[0097] 단계 6: 스마트카드 SC를 수신한 사용자는 이를 HIDi, HPWi, PWi, PWi, Pi와 함께 스마트카드로서 메모리에 저장한다.

[0098] <센서 등록>

[0099] 도 7은 본 발명의 실시예에 따른 BUAKA 방식의 센서 등록 단계를 나타내는 도면이다.

[0100] 센서 등록 단계의 상세한 설명은 다음과 같다.

[0101] 단계 1: 센서 등록을 위해, 센서는 자신의 ID를 ID_{SN}으로서, 게이트웨이 노드에 대한 센서 ID를 SID로서 게이트웨이 노드로 전송한다.

[0102] 단계 2: 게이트웨이 노드는 K_{GN}을 사용하여 ID_{SN}의 해시로서 SID*를 다시 계산한다. 그리고 그들이 일치하는지를 확인한다. SID* = SID와 일치하면 센서가 정당하므로 등록한다.

[0103] 단계 3: 게이트웨이 노트는 SID*를 응답으로 센서로 다시 전송한다.

[0104] <로그인 및 인증>

[0105] 도 8은 본 발명의 실시예에 따른 BUAKA 방식의 로그인 및 인증 단계를 나타내는 도면이다.

[0106] 도 8은 로그인 및 인증 단계의 14단계를 보여준다.

[0107] 단계 1: 로그인을 위해 사용자는 자신의 스마트카드 SC를 생체 인식(biometrics) BIO와 함께 센서 특정 장치(sensor-specific device)에 입력한다. 사용자측의 센서 특정 장치는 퍼지 추출기의 재생 함수(Reproduce function)를 계산하여 R= Rep 〈BIO, P〉와 같은 BIO의 랜덤 키 R을 재생성한다.

[0108] 그리고 나서, 재생성된 R(regenerated R)에 연접된(concatenated) PWi의 해시와 같은 장치에 의해 생체 인식 기반 패스워드가 HPWi*로 계산된다. 그리고, HPWi*가 스마트카드 SC에서 공제된 HPWi와 동일한지 확인한다. 만약 동일하다면 사용자는 정당한 사용자(legitimate user)이다.

[0109] 단계 2: 사용자측 센서 장치는 해시를 취함으로써 게이트웨이 노드에 대한 메시지를 M_1과 M_2로 계산한다. M1은 사용자가 통신하고자 하는 센서 ID ID_{SN}의 해시와 스마트카드의 Bi 파라미터로 계산된다. 그 다음 R_1과 T_1을 XoR 연산한다. 여기서 R_1은 사용자에 의해 생성된 난수(random number)이고 T_1은 타임스탬프(timestamp)이다. 또한, M_2를 ID_{SN}과 R_1이 연접된 Bi의 해시로 계산한다.

[0110] 단계 3: 사용자는 자신의 로그인 정보로서 HIDi, UPB, M_1, M_2를 게이트웨이 노드로 전송한다.

[0111] 단계 4: 로그인 메시지 수신 시, GN은 Bi*를 K_{GN}과 연접된 HIDi의 해시로 계산하고 나서, 사용자 생체 인식 기반 암호 UPB와 함께 XoR 연산을 한다.

[0112] 단계 5: 게이트웨이 노드는 메시지 M_1로부터 난수 R_1을 추론하여 계산한다. 또한, 게이트웨이 노드는 $T_2-T_1 \leq \Delta T$에 의해 타임스탬프의 최신성(freshness)를 확인한다. 여기서 T_2는 새로운 타임스탬프이다.

[0113] 단계 6: 게이트웨이 노드는 M_2*를 ID 센서와 난수 R_1이 연접된 Bi*의 해시로 계산하여 M_2를 인증한다. 그리고 그들이 동등한지 아닌지를 확인한다. 만약 로그인 요청의 M_2* = M_2이면 사용자는 유효(valid)하다.

[0114] 단계 7: 게이트웨이 노드는 센서 노드의 ID와 함께 센서 ID의 해시와 키 게이트웨이 노드를 연접(concatenate)하여 Mj를 계산한다. 또한 Mj를 갖는 SID의 해시와 같은 센서 노드에 대한 메시지 M_3 및 M_4를 계산한다. M_4는 SID 및 R_2와 연접된 Mj의 해시로 계산된다.

[0115] 단계 8: 게이트웨이 노드는 M3와 M_4를 센서로 전송한다.

[0116] 단계 9: 메시지 수신 시 센서는 Mj*를 센서 노드의 ID를 갖는 SID의 해시로 계산한다.

[0117] 그리고 또한 M3로부터 난수 R2를 추론하여 난수 R2를 계산한다. 센서는 T3-T2 ≤ ΔT에 의해 타임스탬프의 최신성을 확인한다. 여기서 T3는 새로운 타임스탬프이다.

[0118] 단계 10: 센서는 SID 및 R2와 연접된 Mj의 해시를 계산하여 M4*를 인증한다. 그리고, M4* = M4인지 확인한다. 만약 동일하다면 센서는 세션 키(session key)를 SKij = h(SID || Mj || R_2)로 계산한다.

[0119] 단계 11: 센서는 Mj*와 R2를 갖는 세션 키 SKij의 해시와 같은 메시지 M5를 계산한다. 그 결과 값은 타임스탬프 T3와 함께 XoR 연산된다. 센서는 M5를 게이트웨이 노드로 전송한다.

[0120] 단계 12: 센서로부터 메시지를 수신하면, 게이트웨이 노드는 SKij*를 SKij = h(SID || Mj || R_2)로 계산한다

[0121] 그러면 게이트웨이 노드는 M5로부터 T3를 도출하고, T4-T3 < ΔT와 같은 타임스탬프의 최신성을 확인한다

[0122] 단계 13: 게이트웨이 노드는 Mj를 갖는 세션 키의 해시와 랜덤 R2를 계산하여 M5를 인증한다. 그리고 그들이 동일한지 아닌지를 확인한다. 만약 M5* = M5이면, 게이트웨이 노드는 통신하고자 하는 센서 사용자의 ID를 갖는 HIDi의 해시와 같은 사용자 HIDnew의 새로운 ID를 계산한다. 그리고 HIDnew로 XoR 연산된 Ai와 Bi의 연접값(concatenated value)으로 M6를 추가로 계산한다. 또한 Skij와 T4로 XoR 연산된 IDSN을 갖는 M6의 해시와 같은 M7을 계산한다. 여기서 T4는 새로운 타임스탬프이다. 게이트웨이 노드는 M6와 M7을 사용자에게 보낸다.

[0123] 단계 14: 게이트웨이 노드로부터 메시지를 수신한 사용자는 M7에서 T4를 도출하고, T5-T4 < ΔT로 최신성을 확인한다. 그리고 나서 사용자는 통신하고자 하는 센서 사용자의 ID를 갖는 HIDi의 해시로 HIDnew*를 계산한다. 또한, HIDnew로 XoR 연산된 Ai와 Bi의 연접값(concatenated value)으로 M6*를 계산하고, M6* = M6인지 확인한

다. 만약 M6* = M6이면 아래 식을 계산한다.

[0124] $SKij = h(M6 \,||\, IDSN) \oplus M7 \oplus T4$

[0125] 이와 같이 3자 간의 핸드셰이크(handshake)가 성공하고, 세션 키 SKij가 설정된다. 사용자, 게이트웨이 노드 및 센서는 성공적으로 상호 인증된다.

[0126] 도 9는 본 발명의 실시예에 따른 BUAKA 방식의 패스워드 업데이트를 나타내는 도면이다.

[0127] <패스워드 업데이트 단계>

[0128] 이 단계는 사용자의 패스워드 PWi와 같은 사용자의 로그인 정보의 패스워드 갱신에 관한 것이다. 사용자가 패스워드를 업데이트할 때, 사용자는 아래에 나열된 단계를 따른다.

[0129] 단계 1: 사용자는 자신의 ID인 IDi와 이전 패스워드 PWi를 입력하고 생체 인식 BIO를 각인한다. 또한 센서 특정 장치에 스마트카드 SC를 삽입한다.

[0130] 단계 2: 센서 특정 장치는 퍼지 추출기의 생성 함수(generate function)를 이용하여 생체 인식 키(biometric key)를 계산한다. 생성 함수는 사용자 생체 인식의 비-비밀 값 P와 랜덤 키 R을 반환한다. 이후 랜덤 키 R로 XoR 연산된 사용자의 패스워드 PWi의 해시를 HPWi*로 계산하고 HPWi* = HPWi인지 확인한다. 만약 HPWi* = HPWi라면 사용자는 유효(valid)하다.

[0131] 단계 3: 장치는 사용자에게 새로운 패스워드 PW*i를 입력하도록 요청한 다음 랜덤 R로 XoR 연산된 새로운 패스워드 PW*i의 해시를 HPWi*로 계산한다.

[0132] 단계 4: 사용자는 HID와 새로운 패스워드 HPWi*를 게이트웨이 노드로 보낸다. 그런 다음 게이트웨이 노드는 게이트웨이 노드 키 K_{GN}과 연접된 랜덤 키 Rg의 해시와 같은 스마트 카드 SC의 파라미터를 다시 계산한다. 그런 다음 HPWi*와 함께 XoR 연산을 수행한다.

[0133] 다른 파라미터 Bi는 K_{GN}과 연접된 HIDi의 해시로 계산된다. 결과값은 HPWi*와 HIDi의 해시로 XoR 연산된다. 게이트웨이 노드는 메모리에 Ai와 Bi를 랜덤 Rg와 함께 저장한다. 게이트웨이 노드는 메모리에 사용자의 스마트카드 값을 업데이트한다.

[0134] 단계 5: 게이트웨이 노드는 업데이트된 스마트 카드 값을 사용자에게 전송한다.

[0135] 단계 6: 사용자는 업데이트된 스마트카드를 HIDi, HPWi, PWi, PWi, Pi와 함께 자신의 메모리에 스마트카드 값으로 저장한다.

[0137] 5. 결과 및 성과분석

[0138] 본 발명의 실시예에 따른 BUAKA 방식의 성능을 분석하고 기존의 여러 해시 기반 방식과 비교한다. 비교는 계산 비용(computational cost)과 통신 오버헤드(communication overhead)를 기반으로 한다.

[0139] 본 발명의 실시예에 따른 BUAKA 방식은 주로 퍼지 추출기, 해시 연산, XOR 및 연접(Concatenation)의 4가지 연산을 기반으로 한다. XOR 및 연접 함수는 어셈블리 수준 연산(assembly level operation)이며 처리 시간이 거의 소요되지 않는다.

[0140] 따라서 생체 인식 해시(biometric hash)의 추가와 단방향 해시 연산(one-way hash operation)의 감소에 대해 성능을 분석한다. 사용자와 게이트웨이 노드는 센서에 비해 더 큰 리소스를 가지고 있으므로 큰 지연 없이 쉽게 기능을 수행할 수 있다.

[0141] 사용자는 게이트웨이 노드에 직접 로그인 요청을 전송하고, 게이트웨이 노드는 메시지와 사용자의 정당성(legitimacy)을 추가로 인증하고 사용자와 센서 사이에 세션 키를 설정하기 위해 메시지를 센서에 전송한다. 본 발명의 실시예에 따른 BUAKA 방식에서, T_{FE}는 하나의 퍼지 추출기의 Gen(.) 또는 Rep(.) 연산을 수행하는 데 필요한 시간을 나타내고, T_h는 단방향 해시 연산을 위한 시간으로 간주한다.

[0142] ID의 길이는 128비트, 난수의 길이 128비트, 타임스탬프의 길이는 24비트이다. 해시 함수(SHA-256)에 의해 생성된 메시지는 256비트를 기반으로 한다. 또한 퍼지 추출기들은 경량 해시 연산(lightweight hash operation)을

기반으로 개발되었기 때문에 하나의 퍼지 추출기 연산을 실행하는 데 필요한 시간은 하나의 해시 함수에 필요한 시간과 동일하다고 가정한다.

[0143] 따라서 $T_{FE} \fallingdotseq T_H$로 결론내릴 수 있다. 암호 함수의 정확한 실행 시간을 추정하기 위해 JPBC(Java Pairing Based Cryptography) 라이브러리를 사용하여 계산한다. 이 시스템은 윈도우 10 운영체제, CPU 3.2GHz를 기반으로 하며, RAM은 4.0GB이다. 연산은 1,000번의 실행을 기반으로 수행된 후 산술 평균을 사용하여 밀리초(ms) 단위의 평균 시간을 계산한다.

[0144] 퍼지 추출기와 해시 연산의 실행 시간은 동일하다. 해시의 실행 시간을 0.0359ms으로 계산한다. 이 값을 사용하여 본 발명의 실시예에 따른 BUAKA 방식의 계산 비용을 계산하였다.

[0145] 지난 몇 년간 무선 센서 네트워크를 효율적이고 안전하며 경량화하기 위해 서로 다른 암호화 기반 프로토콜이 제안되었다. 그러나 한편으로 제안된 거의 모든 방식은 따라야 할 몇 가지 제약과 한계가 있다. 무선 센서 네트워크에 영향을 미치는 여러 요인들이 존재하여 해당 네트워크에서 사용되는 프로토콜의 성능에 영향을 준다. 또한 키 또는 데이터 패킷의 크기와 같이 많은 요인들이 암호화 프로토콜에 영향을 준다.

[0146] 다음은 본 발명의 실시예에 따른 프로토콜에 대한 몇 가지 가정이다.

[0147] i) 네트워크의 노드는 정적이다.

[0148] ii) 모든 노드의 계산 용량(computational capacity)과 통신 용량(communication capacity)은 동일하다.

[0149] iii) 프로토콜에 의해 생성된 모든 메시지는 안전하지 않은 채널을 통해 전송된다.

[0150] iv) 난수와 타임스탬프는 충분히 강력하며 다항식 시간 범위(polynomial time bound) 내에서 이 값들을 추측하는 것은 계산적으로 어렵다.

[0152] 5.1. 공격 모델(Attack model)

[0153] 기존 방식의 분석과 본 발명의 실시예에 따른 방식의 구현 과정에서 형성된 다음과 같은 가정을 고려하였다. 공격 모델은 보안 분석(security analysis)에 사용되며, 적(adversary)으로 여겨지는 네트워크의 특정 센서 노드로 표현된다. 이들은 네트워크에서 사용되는 비밀 암호키를 가진 노드로 메시지를 전송할 수 있다.

[0154] - 공격자(attacker)는 안전하지 않은 채널을 통해 교환된 메시지를 가로챌 수 있다.

[0155] - 공격자는 공개 채널(public channel)을 통해 전송된 메시지 구성 요소를 수정하거나 삭제할 수 있다.

[0156] - 공격자는 스마트 카드 정보를 추출하고 메모리에 저장된 비밀 크리덴셜(credential)을 추출할 수 있다.

[0157] - 공격자는 센서 노드를 손상시킬 수 있으며 저장된 파라미터의 모든 정보를 추출할 수 있다.

[0158] 경량 인증 프로토콜(lightweight authentication protocol)에 대한 요건을 충족시키기 위해, 본 발명의 실시예에서는 사용자의 생체 인식에 기초한 경량이고 안전한 인증 프로토콜을 개시한다. 통신을 위한 3-방향 핸드셰이크를 설정하기 전에 센서와 사용자 모두 게이트웨이 노드에 등록한다.

[0159] 종래의 인증 방식과 달리, 본 발명의 실시예에서는 퍼지 추출기를 사용하여 사용자 인증을 위한 생체 인식을 생성(generate)하고 재생(reproduce)할 수 있다. 입력이 약간 달라지는 경우 종래의 해시 함수는 다른 결과를 생성한다. 생체 정보(biometric information)는 데이터 캡처(data capture) 중에 수많은 교란(disturbance)에 민감하므로 해시 값은 항상 다른 결과를 생성한다.

[0160] 이를 방지하기 위해 생체 인식에서 난수와 비-비밀 키 값을 추출하는 데 퍼지 추출기가 사용된다. 본 발명의 실시예에 따른 경량 인증 방식은 참조논문 Lu et al (Y. Lu, L. Li, H. Peng, and Y.J.S. Yang, "An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks," vol. 16, no. 6, p. 837, 2016.)의 AKA 방식을 계승하며, 이 논문의 접근 방식의 단점을 해결하도록 설계되었다.

[0161] AVISPA(Automated Validation of Internet Security Protocols and Applications)는 본 발명의 실시예에 따른 인증 방식을 구현하기 위해 사용된 시뮬레이션 도구이다. 또한, 다양한 내부자 및 외부자 공격에 대한 프로토콜의 보안을 증명하는 데 사용되었다. 보안 목표가 만족스러운지 여부를 분석하기 위해 그 결과를 추출하였다.

AVISPA는 암호화 프로토콜에 대한 자동 안전 검사를 수행하는 도구이다.

[0162] 개체(entity) 인증 및 데이터의 보안을 확인하고, 여러 유형의 공격에 대한 예방을 검증하는 데 AVISPA이 사용된다. AVISPA는 구현을 위해 특정 고급 언어(high-level language)를 사용하는 푸시 버튼(push-button) 도구이다. 이 고급 언어가 HLPSL(High-Level Protocol Specification Language)이다.

[0163] HLPSL는 각기 다른 공격 모델, 기본적인 암호화 기법, 다양한 복잡 보안 속성에 대해 서로 다른 사양을 가지고 있다. HLPSL에서 사용하는 기본 용어로는 Roles, Text, Nat, Hash_func 등이 있다.

[0164] 도 10은 AVISPA Span 인증 도구를 나타내는 도면으로서, AVISPA SPAN 도구의 스크린샷을 보여준다.

[0165] 개체 간의 통신은 HLPSL을 사용할 때 항상 동기화된다. HLPSL을 사용하여 프로토콜을 모델링할 때, 미리 작성된 다른 규칙이 AVISPA 도구의 백엔드 분석기에 의해 프로토콜에 적용되는 IF(Intermediate Format)으로 변환된다. IF의 프로토콜은 공격이 발견될 때까지 여러 번 실행되거나 반대로 공격이 발견되지 않으면 안전한 것으로 간주된다.

[0166] HLPSL에서는 시스템의 동작을 상태(state)라고 한다. 상태는 시스템이 언제 변경될 필요가 있는지, 다시 시작할 필요가 있는지 등 시스템의 전환(transition)을 알려주는 다양한 변수를 가지고 있다. 이 변수들은 역할(role)이라고 불리는 통신 개체들이 소유한다. 프로세스를 시작하거나 종료하는 것은 서로 다른 역할로 간주된다.

[0167] 도 11은 AVISPA 도구의 작업 흐름도이다.

[0168] AVISPA는 백엔드에 처리를 위한 네 개의 버튼을 가지고 있다. 이 버튼들은 다음과 같이 명명된다.

[0169] - OFMC(On-the-fly-model-Checker)

[0170] OFMC 모델은 IF에 의해 분류된 전환 상태(transition state)를 검사하여 프로토콜 위조(protocol falsification) 및 제한된 인증(bounded verification)을 수행한다. 이는 프로토콜에 대해 많은 정확하고 철저한 상징적 기법(symbolic technique)을 구현한다. 유형화(typed) 및 비유형화(untyped)된 프로토콜 모델을 지원하며 다양한 암호화 수학 연산을 지원한다.

[0171] - CL-Atse (Constraint-Logic-based Attack Searcher)

[0172] CL-Atse는 일부 효율적인 모델링 알고리즘 및 리던던시 제어 전략(redundancy control strategy)과 함께 제약 조건 해결 전략(constraint solving strategy)을 사용한다. 암호 연산자의 대수적 속성을 처리하기 위해 모듈화되고 확장 가능하도록 설계된다. 유형 결함(type flaw)을 식별하고 메시지 연접(message concatenation)의 실행 시간을 관리한다.

[0173] - SATMC (SAT-based-Model-Checker)

[0174] SATMC는 보안 원칙의 심각한 위반을 반영하는 상태 집합 및 초기 상태와 같은 IF 지정 전환 연결(IF specified transition connection)의 제한된 언롤링(restricted unrolling)을 설명하는 명제 공식을 생성한다. 명제 공식은 이후 SAT 해독기(solver)에 로드되고, 발견된 모델은 다시 공격으로 변환된다.

[0175] - TA4SP(Tree-Automata-based-on-Automatic-Approximations-for-the-Analysis-of-Security-Protocols)

[0176] TA4SP는 표준 트리 언어(standard tree language)와 리라이팅(rewriting)을 사용하여 비밀성 측면에서 침입자 정보를 추정한다. TA4SP는 프로토콜에 결함이 있는지(과소 근사화로 인해) 또는 거의 모든 수의 세션에서 안전한지(과다 근사화로 인해)를 결정한다. 본 발명의 실시예에 따른 방식의 시뮬레이션을 위해, 실행 테스트 및 제한된 수의 세션 모델 검사를 위해 OFMC 및 CL-Atse 백엔드가 선택된다.

[0178] 5.2. 성능 파라미터

[0179] 본 발명의 실시예에 따른 알고리즘의 효율성과 보안 성능을 분석하기 위해 다음과 같은 성능 파라미터를 사용한다.

[0180] - 계산 비용 (Computational cost)

[0181] - 통신 오버헤드 (Communication overhead)

[0182] 또한 프로토콜 분석을 위해 네트워크에서 사용자와 게이트웨이 노드, 게이트웨이 노드와 센서 노드 사이의 통신

시 오버헤드를 측정했다.

[0183] 표 2는 BUAKA 방식의 성능 파라미터를 보여준다.

표 2

[0184]

성능 파라미터	설명
계산 비용	계산 비용은 시뮬레이션을 하는 동안 각 단계를 실행하는 시간의 양으로 정의된다. 본 발명의 실시예에 따른 모델의 시간을 추정하기 위해서, 시뮬레이션 실행 시간을 추정하기 위한 하드웨어나 시뮬레이션 도구에서 실행되는 것이 요구된다.
통신 오버헤드	통신 오버헤드는 하나의 노드에서 다른 노드로 전송될 총 패킷 수로 정의된다.

[0185] 5.3. 계산 비용 분석

[0186] 계산 비용에서, 본 발명의 실시예에 따른 프로토콜은 관련된 수학적 단계를 기반으로 분석된다. 비용은 암호 프리미티브(cryptographic primitive)의 실행에 필요한 시간으로 정의되는 것을 의미한다.

[0187] 등록 단계와 인증 단계에 걸쳐 다양한 연산을 수행하는 데 소요되는 시간을 계산 비용이라고 한다. 계산 비용을 위해, 사용자, 게이트웨이 노드 및 센서 사이의 연산 수를 살펴본다.

[0188] 참조논문(Y. Lu, L. Li, H. Peng, and Y.J.S. Yang, "An energy efficient mutual authentication and key agreement scheme preserving anonymity for wireless sensor networks," vol. 16, no. 6, p. 837, 2016.)의 인증 방식은 다중 대칭 암호 연산, 해시 연산 및 XoR 함수를 포함하기 때문에 계산 비용이 높다. 따라서, 모든 연산을 결합하면 참조논문의 방식이 매우 복잡해진다. 본 발명의 실시예에 따른 모델의 시간을 추정하기 위해서는 시뮬레이션 실행 시간을 추정하는 것이 필요하다.

[0189] 이하에서, 다른 방식과 관련된 BUAKA 방식의 계산 비용을 계산하여 비교한다. 분석하기 위해 사용한 파라미터는 T_H와 T_{FE}이다. XOR 연산과 연접(Concatenation) 연산의 실행 시간은 하드웨어 수준의 연산이고 무시할 수 있는 시간이 소요되기 때문에 포함되지 않는다. 또한, XOR 연산에는 메모리 연산이 포함되지 않는다.

[0190] 도 12는 사용자 측에서의 계산 복잡도(computational complexity) 비교를 나타내는 도면이다.

[0191] 사용자는 퍼지 추출기의 4개의 해시와 1개의 GEN(.), 1개의 REP(.) 함수를 실행하며, 그 경과 시간은 $4T_H+2T_{FE}$이다. 사용자의 계산 복잡도는 BUAKA가 다른 두 방식보다 훨씬 낮다. BUAKA의 값은 사용자 측에서 0.2154ms이며, 이는 다른 두 방식과 현저한 차이를 나타낸다.

[0192] 도 13은 게이트웨이 노드 측에 대한 계산 복잡도 비교를 나타내는 도면이다.

[0193] 게이트웨이 노드 측의 계산 복잡도는 SLUA-WSN 방식이 다른 두 방식보다 낮다. BUAKA의 값은 0.3949ms로서 AKA 방식보다는 낮지만 SLUA-WSN 방식보다는 0.1795ms 더 걸린다.

[0194] 도 14는 센서 측의 계산 복잡도 비교를 나타내는 도면이다.

[0195] 센서의 계산 복잡도는 BUAKA 방식이 다른 두 방식 보다 상당히 낮다. BUAKA 방식의 계산 비용은 센서의 경우 0.1077ms이다.

[0196] 도 15는 전체적인 계산 복잡도 비교를 나타내는 도면이고, 도 16은 도 12 내지 도 14를 종합하여 계산 복잡도 비교를 나타내는 도면이다.

[0197] 이는 BUAKA의 복잡도 비율(complexity rate)이 AKA 대비 0.5704ms 만큼 작고, SLUA-WSN 대비 1.471 ms 만큼 작다는 것을 증명한다.

[0198] 이상과 같이, 본 발명의 실시예에 따른 BUAKA 프로토콜이 가장 낮은 계산 비용을 나타낸다는 것을 알 수 있는데, 이는 프로토콜에 사용된 해시 연산 수가 가장 작기 때문이다. 본 발명의 실시예에 따른 BUAKA 방식은 어떤 종류의 대칭 연산도 포함하지 않으므로 다른 방식에 비해 더 나은 성능과 더 빠른 인증을 나타낸다.

[0199] BUAKA는 사용자 및 게이트웨이 노드 측에서 최대 기능을 수행하고, 낮은 리소스를 가진 센서에서 더 적은 연산을 수행한다. 표 3은 본 발명의 실시예에 따른 BUAKA 방식의 계산 비용을 다른 방식과 비교하여 보여준다. 결과

적으로 BUAKA 방식은 더 효율적인 계산 비용을 제공한다.

표 3

[0200]

Schemes	사용자	센서	게이트웨이 노드	합계	계산 비용
AKA	$7T_H$ +$2T_{SYM}$	$4T_H$ + $2T_{SYM}$	$11T_H$ + $3T_{SYM}$	$22T_H$ + $7T_{SYM}$	2.0183 ms
SLUA-WSN	$11T_H$ +$1T_{SYM}$	$11T_H$	$6T_H$	$28T_H$ + $1T_{SYM}$	1.1807 ms
BUAKA	$4T_H$ + 2F	$3T_H$	$11T_H$	$18T_H$ +2F	0.718 ms

[0201] 표 4는 다른 두 방식에 대해 본 발명의 실시예에 따른 BUAKA 방식의 개선된 백분율을 보여준다.

표 4

[0203]

	AKA	SLUA-WSN
Improved value	1.3633	0.4627
Improved percentage	65%	39%

[0204] 결과는 BUAKA가 AKA 방식에 비해 65% 더 나은 계산 결과를 보여준다. BUAKA의 계산 복잡도는 AKA의 방식보다 1.3633 낮다. 또한 BUAKA 계산 복잡도를 SLUA-WSN과 비교하면, 0.4627 감소한 39%의 효과적인 결과를 보여준다.

[0205] 도 17은 BUAKA 방식의 개선된 비율을 나타내는 도면이다.

[0206] 도 17은 다른 두 방식에 대해 본 발명의 실시예에 따른 BUAKA 방식의 개선된 비율을 보여준다. 그 결과는 본 발명의 실시예에 따른 BUAKA의 계산 복잡도가 AKA의 방식보다 1.3633 낮고 SLUA-WSN의 방식보다 0.4627 낮은 것을 보여준다.

[0208] 5.4 통신 오버헤드 분석

[0209] 도 18은 통신 오버헤드의 비교를 나타내는 도면이다.

[0210] 통신 중에 전송되는 총 패킷 수를 통신 오버헤드라고 한다. 통신 오버헤드에 대해, 사용자, 게이트웨이 노드(GN) 및 센서 사이의 메시지 전송과 관련된 연산의 수를 살펴본다.

[0211] 통신 오버헤드는 등록 단계와 인증 단계 동안 채널을 통해 전송되는 비트 수이다. 다른 방식과 관련된 BUAKA 방식의 통신 오버헤드를 계산하고 비교한다. BUAKA 방식에서 사용되는 기본 연산은 해시 함수와 퍼지 추출기이고, 파라미터는 사용자, 센서 및 게이트웨이 노드의 아이덴티티, 해시 함수의 메시지 다이제스트(message digest), 타임스탬프, 랜덤 논스(nonce) 및 스마트 카드 파라미터를 포함한다. 통신 오버헤드를 평가하기 위해, 해시 함수의 메시지 다이제스트와 퍼지 추출기의 결과가 모두 각각 256비트를 나타내고, 타임스탬프는 24비트를 나타내고, 랜덤 논스(nonce) 또한 24비트를 나타낸다고 가정한다.

[0212] BUAKA 방식의 통신 파라미터는 (ID_U, $h(PW_U \oplus R)$, ID_{SN}, ID_{GN}, R, P, M1, M2, M3, M4, M5, M6, M7) = 128 * 5 + 256 * 8 = 3200이다. 이 파라미터들은 BUAKA 방식의 구성 요소(building block)이다. 표 5에 통신 오버헤드의 비교 결과가 나타나 있다. 따라서, BUAKA 방식은 도 17과 같이 더 효율적인 통신 오버헤드를 갖는다.

표 5

[0214]

Schemes	통신 오버헤드
BUAKA	2688 bits
AKA	3328 bits

SLUA-WSN	3680 bits

[0215] 표 6은 본 발명의 실시예에 따른 BUAKA 방식이 기존 인증 방식에 비해 전송 오버헤드가 가장 적은 것을 보여준다.

표 6

[0217]

보안 속성	BUAKA	AKA	SLUA-WSN
Masquerade Attack	✓	✓	✓
Eavesdropping Attack	✓	✓	X
User ImpersonationAttack	✓	✓	X
Node ImpersonationAttack	✓	✓	X
Anonymity	✓	✓	X
Untraceability	✓	✓	✓
Stolen Smartcard Attack	✓	X	X
Loss Smart card attack	✓	X	X
Perfect Forward Secrecy	✓	X	✓

[0218] 도 18은 본 발명의 실시예가 기존 방식에 비해 통신 오버헤드가 낮아 센서 노드의 수명 향상에 도움이 될 것임을 추가로 나타낸다. 따라서 본 발명의 실시예에 따른 메커니즘은 무선 센서 네트워크에 쉽게 배치될 수 있다.

[0220] 5.5. BUAKA의 비공식 보안(Informal security) 분석

[0221] 아래에서는 BUAKA 방식에 대한 비공식적인 보안 분석을 제시한다. 또한 잘 알려진 보안 공격에 대한 본 발명의 실시예에 따른 프로토콜의 복원력(resilience)을 측정하고, 기존의 다른 방식과 보안 특징을 비교한다.

[0222] <위장 공격 (Masquerade attack)>

[0223] 공격자는 안전하지 않은 매체를 통해 전송된 메시지를 가로채어 이 공격에서 진정한 사용자로 위장하려고 시도한다. 그러나 공격자는 본 발명의 실시예에 따른 BUAKA 방식에서 요청 메시지 <HIDi, HPWi>를 적절하게 생성할 수 없다.

[0224] 공격자는 또한 사용자의 실제 ID인 IDi를 모르기 때문에 요청 메시지를 계산할 수 없다. 사용자의 IDi는 난수 Ru로 해시되므로 되돌릴 수 없고 캡처될 수 없다. 또한 공격자는 사용자의 생체 인식 BIO를 예측할 수 없으며, 그 결과 퍼지 추출기의 생성 함수를 사용하여 R을 생성할 수 없다. 따라서 BUAKA는 위장 공격에 강하다.

[0225] <도청 공격 (Eavesdropping Attack)>

[0226] 공격자는 안전하지 않은 채널을 통해 전송된 모든 메시지를 도청할 수 있다. 공격자는 센서에서 게이트웨이 노드로 전송되는 메시지 〈 M5 〉와 게이트웨이 노드에서 센서로 전송되는 메시지 〈 M3, M4 〉를 수집한다. BUAKA 방식에서 세션 키 SKij는 SKij = h(SID || Mj || R_2)로 계산된다. SID와 Mj는 암호 해시 함수에 의해 보호되므로, 공격자는 도청된 파라미터로부터 Mj = h(h(SID) || IDSN) 및 SID = h($I_{DS}N$ || K_{GN})를 계산할 수 없다. 따라서, BUAKA는 도청 공격에 강하다.

[0227] <사칭 공격 (Impersonation Attack)>

[0228] 공격자는 사용자 〈 HIDi, HPWi, M1, M2 〉의 로그인 요청을 가로챌 수 있다. 공격자는 M1을 갖게 되지만, 다시 로그인하기 위해서는 새로운 타임스탬프 Tnew로 M1을 다시 계산해야 하는데, 이것은 HPWi를 알지 못하면 불가능

하다. HPWi는 복제할 수 없는 사용자의 생체 인식 기반 패스워드다.

[0229] 따라서, 공격자는 HPWi를 알지 못하면 M1을 계산할 수 없다. 또한, M2 메시지는 단방향 해시이기 때문에 공격자는 M2 메시지로부터 사용자의 정보를 얻을 수 없다. 만약 공격자가 센서 노드로부터 메시지 SID를 가로챈다면, SID는 게이트웨이 노드의 비밀키로 해시되었기 때문에 그 값을 계산할 수 없다. 따라서, BUAKA는 사용자 및 센서 사칭 공격에 강하다.

[0230] <익명성과 추적 불가능성 (Anonymity and Untraceability)>

[0231] 공격자가 비보안 채널을 통해 전송된 통신을 도청하여 〈 M1, M2 〉를 캡처했다고 가정한다. 여기에서 M1= h(Bi || ID_{SN}) ⊕ R1 ⊕ T1 및 M2= h(Bi || ID_{SN} || R1)이다.

[0232] 전송된 메시지에는 사용자, 센서 및 게이트웨이 노드의 개인 정보가 없다. 또한, 센서 ID는 검색될 수 없는 다른 파라미터들로 해시된다. 따라서, BUAKA 방식은 익명성을 유지한다. 또한, 모든 전송된 파라미터들은 고유성(uniqueness)을 위해 난수들과 타임스탬프들로 채워진다. 따라서, BUAKA 방식에서 추적 불가능성이 유지된다.

[0233] <도난/분실된 스마트카드 공격 (Stolen/Lost Smart Card Attack)>

[0234] 공격자가 등록된 사용자의 분실/도난된 스마트카드 SC = 〈 A, B, HIDi, HPWi, PWi, PWi, Pi 〉를 복구(recover)했다고 가정한다.

[0235] 분석을 통해 공격자는 A, B, HIDi, HPWi, PWi, PWi, Pi 등 모든 비밀 정보를 추출할 수 있다. Pi를 제외한 스마트 카드에 저장된 모든 값은 해시 함수와 다른 파라미터들의 조합이다. 따라서 이러한 파라미터들을 생성하기 위해서는 사용자의 실제 ID, 패스워드, 생체 인식이 필요하다.

[0236] 생체 인식을 위조하는 것은 불가능하므로 이러한 값들을 재생성하는 것은 거의 불가능하다. 또한 공격자는 퍼지 추출기 때문에 계산된 값을 인증할 수 없을 것이다. 따라서 BUAKA 기법은 도난 및 분실된 스마트 카드 공격에 강하다.

[0237] <완전 순방향 비밀성 (Perfect Forward Secrecy)>

[0238] 세션 키 SKij가 공격자에 의해 손상되었다고 가정한다. 사용자와 노드들 사이의 이전 또는 이후의 세션들은 이 세션 키에 의해 드러나지 않아야 한다. SKij가 SKij = h(SID || Mj || R_2)로 계산되므로, Mj = h(h(SID) || ID_{SN}) 및 SID = h(ID_{SN} || K_{GN})는 공격자에 의해 계산될 수 없다.

[0239] 또한 어떠한 추가적인 비밀 파라미터도 노출시키지 않으며, 모든 파라미터는 난수와 타임스탬프를 사용하여 파라미터들을 계산하는 해시 함수로 바인딩된다. 결과적으로 BUAKA 방식은 완벽한 순방향 비밀 특성을 유지한다. 표 6은 BUAKA 방식과 다른 방식의 보안 속성 비교를 보여준다.

[0241] 5.6. AVISPA-SPAN을 이용한 공식 보안 검증

[0242] 이하에서는 널리 정형화된 보안 인증 도구인 AVISPA 도구를 사용하여 본 발명의 실시예에 따른 프로토콜을 시뮬레이션한다. 이 도구를 사용하여 프로토콜이 안전한지 안전하지 않은지를 판단할 수 있다.

[0244] 5.6.1 본 발명의 실시에에 따른 프로토콜 HLPSL 사양

[0245] 본 발명의 실시예에 따른 BUAKA 프로토콜의 시뮬레이션에 대해 설명한다.

[0246] AVISPA는 푸시버튼(push-button) 도구로, 구현을 위해 특정 고급 언어를 사용한다. 이 고급 언어가 HLPSL(High-Level Protocol Specification Language)이다. 시뮬레이션은 역할(role), 세션, 환경(environment)을 기반으로 한다. BUAKA는 사용자, 게이트웨이 노드, 센서에 대한 세 가지 기본 역할을 가지고 있다. HLPSL 사양에는 비밀(secret), 위트니스(witness), 요청(request)이라는 용어가 포함되어 있다.

[0247] 다음 문장은 주로 HLSPL 코드에서 사용된다.

[0248] - 비밀((PWi), sp1, (US)): 오직 사용자만이 이 패스워드 정보를 가지고 있다는 것을 의미한다. 게이트웨이 노드와 센서 노드는 이 정보에 접근할 수 없으므로 익명성을 준수할 수 있다.

[0249] - 비밀((HPWi), sp2, (US, GN)): 해시 암호는 사용자와 게이트웨이 노드에만 알려져 있으므로 비밀이며 센서 노드에서는 액세스할 수 없다.

[0250] - 위트니스 (US, GN, ua_ga_ni, R1'): 위트니스는 에이전트 사용자 US와 게이트웨이 노드가 R1'을 인증 식별자(authentication identifier) ua_ga_ni의 값으로 사용하여 프로토콜을 실행하고자 함을 보여준다.

[0252] 5.7. AVISPA 시뮬레이션 결과

[0253] AVISPA(Automated Validation of Internet Security Protocols and Applications) 시뮬레이션 도구는 본 발명의 실시예에 따른 프로토콜이 중간자(man-in-the-middle) 및 재생(replay) 공격에 대해 안전하다는 것을 보여준다.

[0254] 프로토콜이 안전한지 여부를 결정하기 위해 AVISPA 시뮬레이션 도구는 HLPSL를 사용한다. HLPSL 코드는 4개의 백엔드 모델 중 하나에 입력된다. BUAKA 프로토콜의 AVISPA 시뮬레이션 결과는 OFMC(On-the-Fly-Model Check)와 CL-AtSe(Constraint-Logic-Based Attack Searcher) 두 가지 백엔드 모드를 사용하여 입증된다.

[0255] OFMC 모델은 공격을 빠르게 탐지하여 프로토콜을 검증하는 데 사용된다. OFMC에서, 침입자는 프로토콜의 효율적인 위조(falsification)를 증명하기 위해 제한된 수의 세션에서 제한되지 않은 수의 메시지를 생성한다.

[0256] CL-AtSe 모드는 프로토콜 IF(Intermediate File) 파일을 프로토콜 공격 및 취약성을 식별하는데 사용되는 일련의 제약 조건으로 변환한다. CL-AtSe 및 OFMC 모드는 모두 재생 및 MITM 공격에 대해 프로토콜을 검사하며, 그 결과 요약은 프로토콜이 안전하다는 것을 보여준다. 4352 노드를 방문하기 위한 OFMC의 검색 시간은 62.54초이고, 7개 상태를 분석하기 위한 CL-AtSe의 변환 시간은 1.29초이다.

[0257] 도 19는 OFMC 시뮬레이션의 결과를 나타내는 도면이고, 도 20은 CL-AtSe 시뮬레이션의 결과를 나타내는 도면이다.

[0258] 도 19와 도 20은 AVISPA-SPAN에서 BUAKA 프로토콜 구현 결과를 보여준다.

[0259] 그 결과의 첫 번째 섹션의 제목은 Summary이며 프로토콜의 보안 상태, 즉 안전 여부를 결정한다. CL-AtSe의 결과는 프로토콜이 안전하므로 분석할 수 있지만 공격자가 도달할 수 없는 7개의 상태가 있음을 보여준다.

[0260] 도 21은 본 발명의 실시예에 따른 지능형 센서 기반의 사용자 생체 인증 무선 통신 방법의 순서도를 나타내는 도면이다.

[0261] 도 21을 참조하면, 본 발명의 실시예에 따른 지능형 센서 기반의 무선 센서 네트워크에 대한 사용자 생체 인증 무선 통신 방법은, 복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크의 센서에 ID를 할당하는 설정 단계(S100); 사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록 단계(S102); 및 상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증 단계(S104);를 포함한다. 이때, 상기 인증 단계는 퍼지 추출기를 이용하여 상기 생체 인식을 생성 및 재생하며, 상기 퍼지 추출기는 해시 함수를 사용할 수 있다. 도 1 내지 도 20에서 설명한 내용과 중복된 부분은 설명을 생략한다.

[0262] 본 발명의 실시예에서는 경량 인증 암호화 방식에 대하여 기존의 완전 순방향 비밀성, 익명성, 분실된 스마트카드 공격을 자원 효율적인 방식으로 해결하는 개선된 인증 방식을 설계하였다. 인증 알고리즘을 설계하기 위해 본 발명의 실시예에서는 시뮬레이션을 수행하였으며, 보안 및 에너지 효율성을 평가하기 위해 그 결과를 분석하였다.

[0263] 본 발명의 실시예에서는 BUAKA(Biometric based User Authentication and Key Agreement)라는 생체 인식 및 스마트카드 기반의 경량 및 안전한 사용자 인증 방식을 제안한다.

[0264] 이 방식은 사용자의 생체 인식을 생성하고 재생하는 퍼지 추출기를 기반으로 하며, 퍼지 추출기는 사용자 암호와 더욱 결합하여 보안을 강화한다. 사용자는 통신 전에 게이트웨이 노드 및 센서 노드에서 사용자 인증을 한다. BUAKA 방식의 성능을 평가하기 위해 비공식 보안 분석을 고려하고 AVISPA-Span 도구를 사용하여 공식 인증한다.

[0265] 본 발명의 실시예는 계산 요구 사항에 유리한 결과를 보였고, 재생 공격과 중간자 공격과 같은 공격에 성공적으로 저항함으로써 전체 성능과 보안을 향상시켰다. 계산 복잡도 및 통신 시간도 계산되었으며, 이는 기존 방식에

비해 본 발명의 실시예가 현저히 개선되었다는 것을 보여준다.

[0266] 따라서 본 발명의 실시예는 계산 복잡도 및 통신 오버헤드를 향상시킨다. 본 발명의 실시예는 사물 인터넷(IoT), 스마트 그리드 및 지능형 교통 시스템과 같은 다른 스마트 네트워크에서도 구현될 수 있다. 본 발명의 실시예는 보안과 관련된 연결 끊김(dis-connectivity), 간섭(interference), 로드 밸런싱(load balancing)과 같은 향후 네트워크의 다른 과제를 고려할 수 있다.

[0267] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

[0268] 100: 사용자 생체 인증 무선 통신 시스템

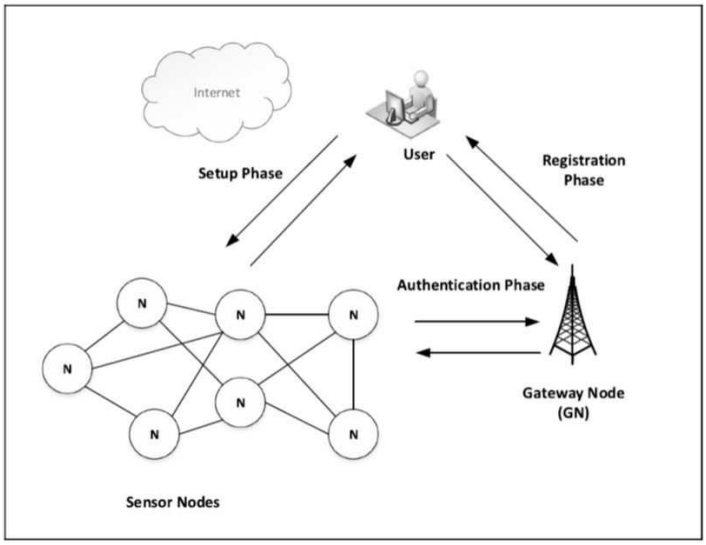
102: 설정부

104: 등록부

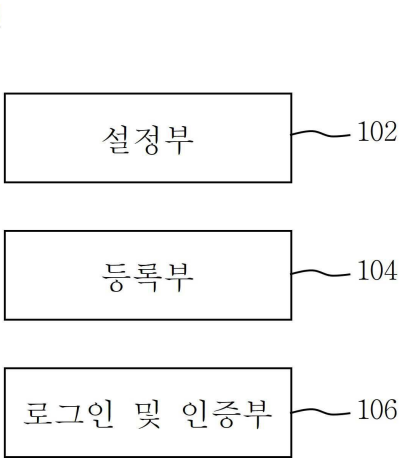
106: 로그인 및 인증부

도면

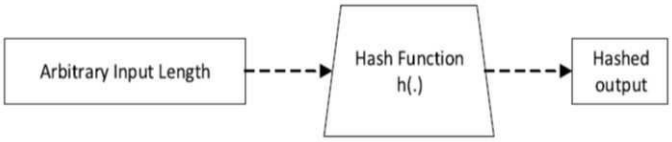
도면1



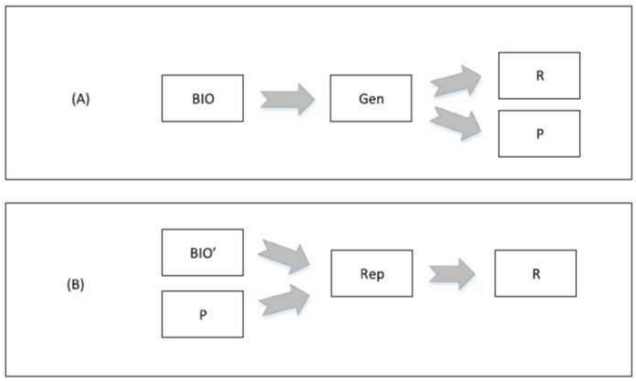
도면2



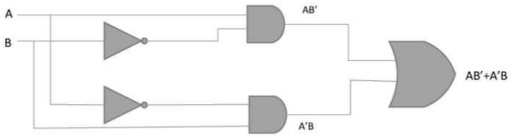
도면3



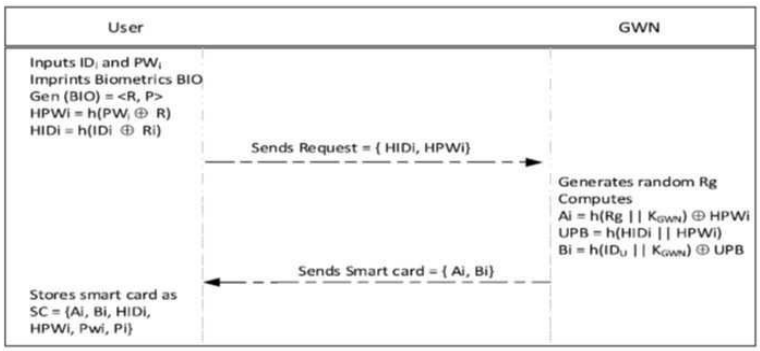
도면4



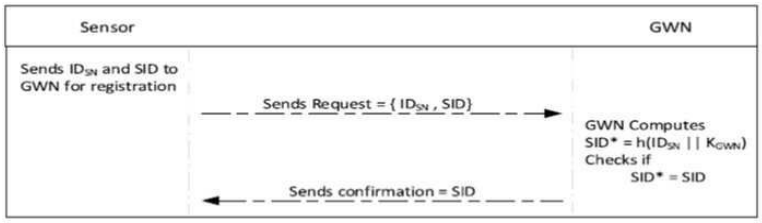
도면5



도면6



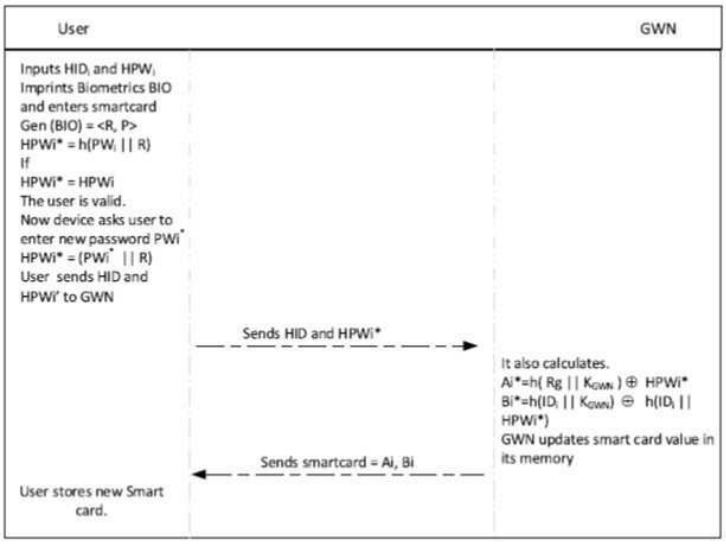
도면7



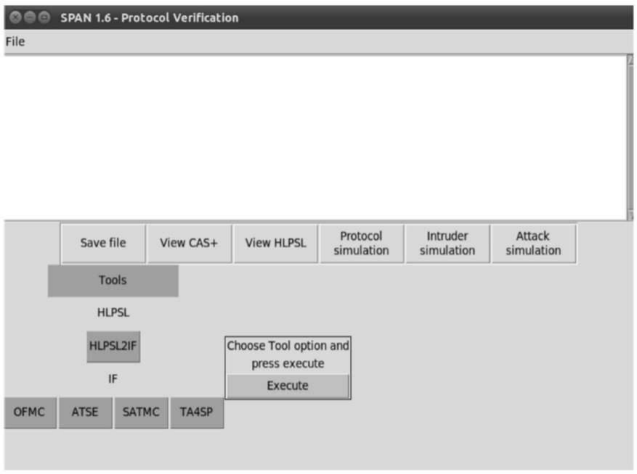
도면8


User
GWN
Sensor
Sends M1 and M2 to GWN
Sends M3 and M4 to Sensor
Sends M5 to GWN
Sends M6 and M7 to GWN
handshake among three-party is successful, and they established a session key SKj. User, GWN and Sensor are mutually authenticated successfully

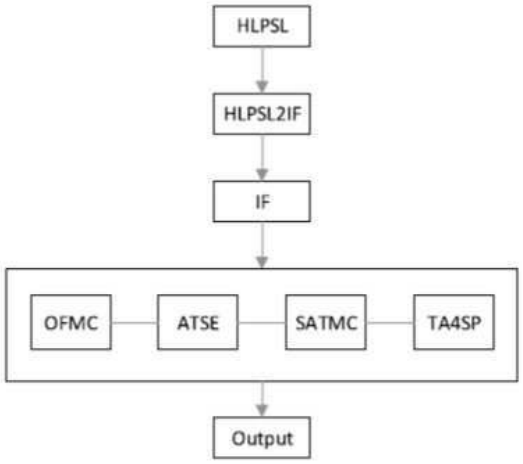
도면9


User
GWN
Inputs HIDi and HPWi
Imprints Biometrics BIO and enters smartcard
Gen (BIO) = <R, P>
HPWi* = h(PWi || R)
If
HPWi* = HPWi
The user is valid.
Now device asks user to enter new password PWi*
HPWi* = (PWi* || R)
User sends HID and HPWi' to GWN
Sends HID and HPWi*
It also calculates.
Ai*=h(Rg || KGWN) ⊕ HPWi*
Bi*=h(IDi || KGWN) ⊖ h(IDi || HPWi*)
GWN updates smart card value in its memory
Sends smartcard = Ai, Bi
User stores new Smart card.

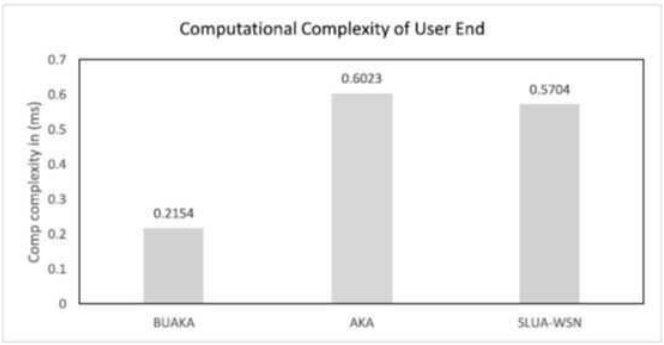
도면10



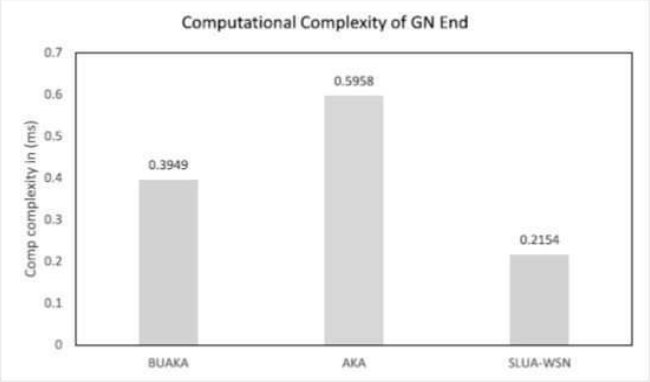
도면11



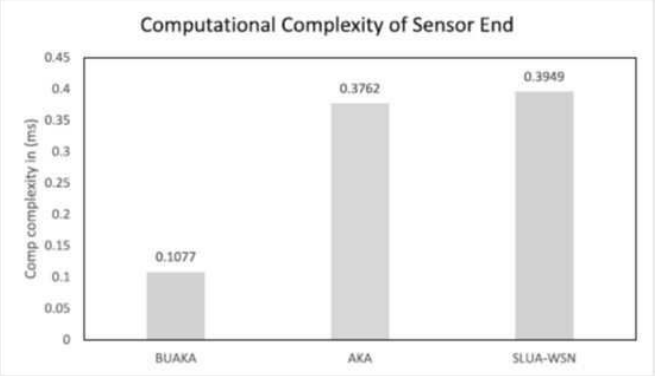
도면12



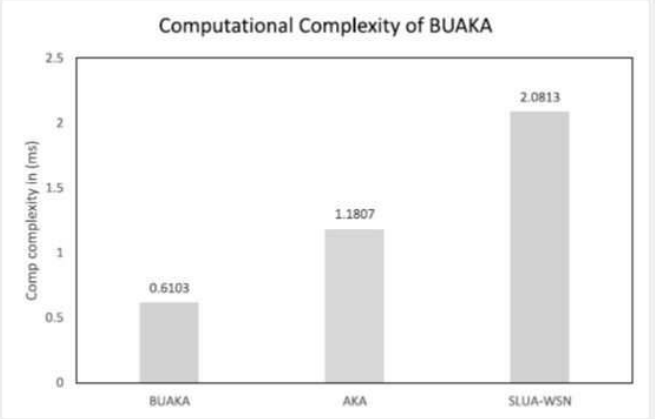
도면13



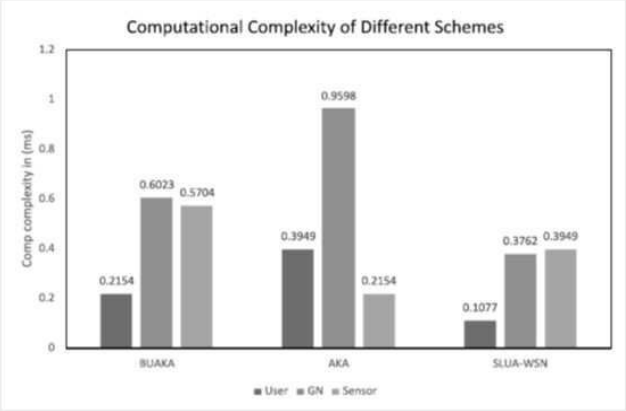
도면14



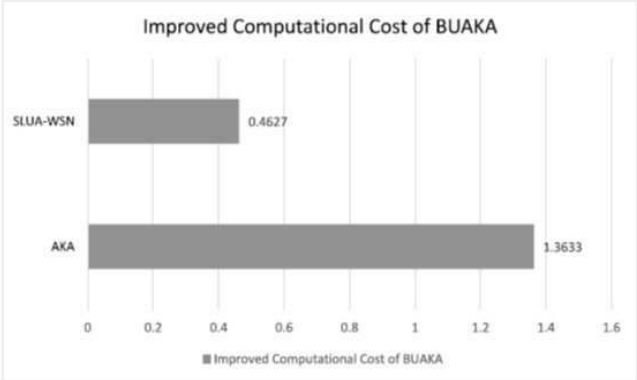
도면15



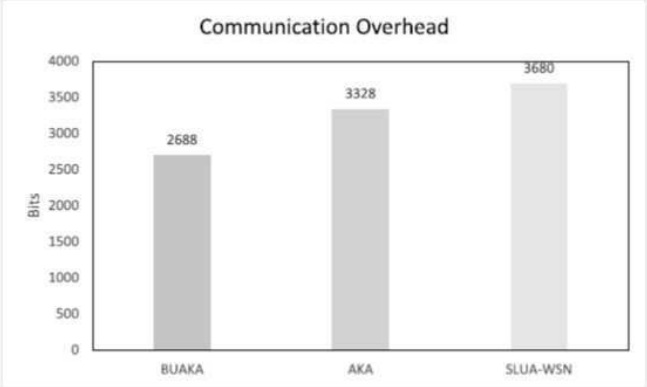
도면16



도면17



도면18



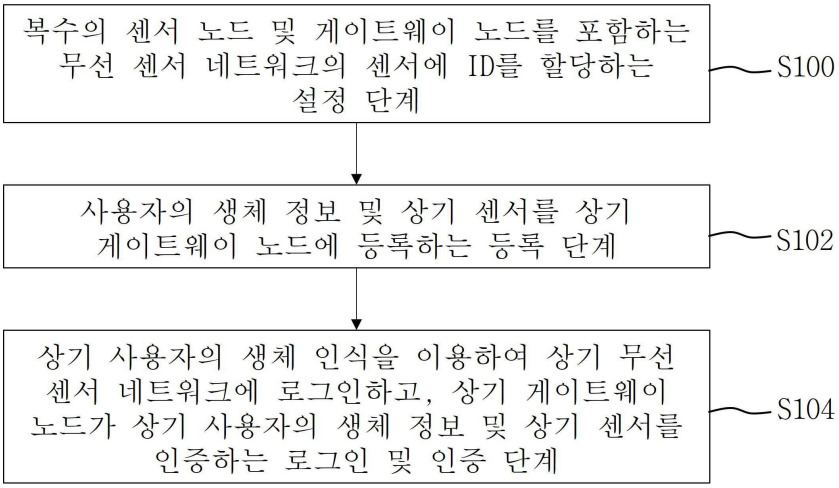
도면19

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/newBUAKA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 62.54s
  visitedNodes: 4352 nodes
  depth: 9 plies
```

도면20

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  UNTYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/newBUAKA.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 7 states
  Reachable  : 0 states
  Translation: 1.29 seconds
  Computation: 0.00 seconds
```

도면21


복수의 센서 노드 및 게이트웨이 노드를 포함하는 무선 센서 네트워크의 센서에 ID를 할당하는 설정 단계
S100
사용자의 생체 정보 및 상기 센서를 상기 게이트웨이 노드에 등록하는 등록 단계
S102
상기 사용자의 생체 인식을 이용하여 상기 무선 센서 네트워크에 로그인하고, 상기 게이트웨이 노드가 상기 사용자의 생체 정보 및 상기 센서를 인증하는 로그인 및 인증 단계
S104