(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0072721
(43) 공개일자 2020년06월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04B 13/00* (2006.01)
H04L 9/06 (2006.01) *H04L 9/30* (2006.01)
(52) CPC특허분류
H04L 9/3271 (2013.01)
H04B 13/005 (2013.01)
(21) 출원번호 10-2018-0160626
(22) 출원일자 2018년12월13일
심사청구일자 2018년12월13일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 아카데미로 119 (송도동)
(72) 발명자
전광길
인천광역시 연수구 경원대로119번길 21, 114동 904호(동춘동, 연수2차풍림아파트)
(74) 대리인
특허법인충정

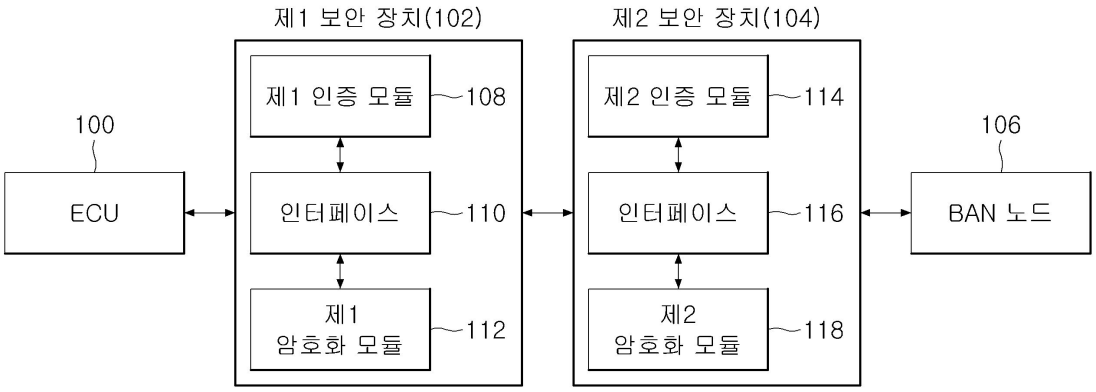
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치**

(57) 요 약

본 발명의 일 실시예에 의한 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치는, 상기 스마트 차량의 전자제어장치는 제1 보안 장치를 통해 데이터를 송수신하고, 상기 신체 영역 네트워크는 제2 보안 장치를 통해 데이터를 송수신하며, 상기 제1 보안 장치는, 제1 인증 모듈; 및 제1 암호화 모듈을 포함하고, 상기 제2 보안 장치는, 제2 인증 모듈; 및 제2 암호화 모듈을 포함하여, 저전력 소모, 작은 대기 시간 및 작은 자원 활용의 이점을 가지며, VAN 상황에서 적용되는 BAN을 위해 작동하는 새로운 보안 체계를 제공할 수 있다.

대 표 도



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/0877 (2013.01)
H04L 9/3066 (2013.01)
H04L 9/3236 (2013.01)
H04L 9/3263 (2013.01)
H04L 2209/84 (2013.01)

명 세 서

청구범위

청구항 1

신체 영역 네트워크(BAN: ban area network) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치에 있어서,

상기 스마트 차량의 전자제어장치는 제1 보안 장치를 통해 데이터를 송수신하고, 상기 신체 영역 네트워크는 제2 보안 장치를 통해 데이터를 송수신하며,

상기 제1 보안 장치는, 제1 인증 모듈; 및 제1 암호화 모듈을 포함하고,

상기 제2 보안 장치는, 제2 인증 모듈; 및 제2 암호화 모듈을 포함하며,

상기 제1 인증 모듈은, 상기 제2 보안 장치에 인증서를 요구하고, 상기 제2 보안 장치로부터 수신되는 인증서를 검증하며, 챌린지를 생성하고, 상기 제1 보안 장치와 상기 제2 보안 장치에만 알려진 비밀 키 및 상기 챌린지에 기반하여 응답을 생성하며, 상기 제2 보안 장치에 상기 챌린지를 전송하고 상기 제2 보안 장치로부터 수신되는 응답을 검증하여 상기 신체 영역 네트워크 노드의 인증 여부를 결정하며,

상기 제1 암호화 모듈은, 제1 개인 키에 기반하여 제1 공개 키를 생성하고 상기 제2 보안 장치와 공개 키를 교환하며, 상기 제1 개인 키와 상기 제2 보안 장치로부터 수신되는 제2 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 전자제어장치로부터 수신되는 데이터를 암호화하여 상기 제2 보안 장치로 전송하거나 상기 제2 보안 장치로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 전자제어장치로 전송하며,

상기 제2 인증 모듈은, 상기 제1 보안 장치로부터 인증서를 요구받는 경우, 상기 제1 보안 장치에 인증서를 전송하고, 상기 제1 보안 장치로부터 수신되는 상기 챌린지 및 상기 비밀 키에 기반하여 응답을 생성하여 생성된 응답을 상기 제1 보안 장치로 전송하며,

상기 제2 암호화 모듈은, 제2 개인 키에 기반하여 제2 공개 키를 생성하고 상기 제1 보안 장치와 공개 키를 교환하며, 상기 제2 개인 키와 상기 제1 보안 장치로부터 수신되는 제1 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 신체 영역 네트워크 노드로부터 수신되는 데이터를 암호화하여 상기 제1 보안 장치로 전송하거나 상기 제1 보안 장치로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 신체 영역 네트워크 노드로 전송하는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

청구항 2

청구항 1에 있어서,

상기 제1 인증 모듈은, 상기 제2 보안 장치로부터 수신된 응답이 상기 제1 인증 모듈에서 생성한 응답과 동일한 경우, 상기 신체 영역 네트워크 노드를 인증하는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

청구항 3

청구항 2에 있어서,

상기 응답은, 해시 기반 메시지 인증 코드(HMAC: hash-based message authentication code) 보안 해시 알고리즘(SHA: secure hash algorithm)-256에 기반하여 계산되고,

상기 제2 인증 모듈은, 상기 제1 보안 장치로부터 수신된 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 상기 응답으로서 생성하고,

상기 제1 인증 모듈은, 상기 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 상기 응답으로서 생성하는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

청구항 4

청구항 1에 있어서,

상기 챌린지는 상기 신체 영역 네트워크(BAN) 노드에서 수집한 생체 인식 데이터를 사용하여 생성되는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

청구항 5

청구항 4에 있어서,

상기 생체 인식 데이터는, 상기 신체 영역 네트워크 노드에 의해 획득되는 심전도 데이터, 심박수, 체온 및 혈압 중 적어도 하나를 포함하는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

청구항 6

청구항 1에 있어서,

상기 제1 암호화 모듈 및 상기 제2 암호화 모듈 각각은 타원곡선 암호화(ECC: Elliptic Curve Cryptography) 모듈 및 고급 암호화 표준(AES: Advanced Encryption Standard) 모듈을 포함하고,

상기 제1 암호화 모듈과 상기 제2 암호화 모듈 각각은 타원곡선 암호화 모듈을 이용하여, 타원곡선 디피-헬만(ECDH: Elliptic-Curve Diffie-Hellman) 키 동의 프로토콜에 기반하여 각각의 개인 키에 대응하는 공개 키를 생성하여 생성된 공개 키를 서로 교환하고,

상기 제1 암호화 모듈과 상기 제2 암호화 모듈 각각의 고급 암호화 표준(AES) 모듈은, 자신의 개인 키와 상대방으로부터 수신된 공개 키에 기반하여 AES에 따라 데이터를 암호화하기 위한 대칭 키를 생성하는, 신체 영역 네트워크(BAN: ban area networks) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 관한 것이다.

배 경 기 술

[0002] 교통 캐나다의 국가 충돌 데이터베이스(NCDB)가 발표한 "캐나다 자동차 교통 충돌 통계:2015"에서 보고된 것처럼 2015년 캐나다에서 교통 사고 사상자는 118,000명에 달했고, 1800명이 사망하고 161,000명이 다쳤다. 그러나 스마트 차량 시스템, IoT(Internet of Things) 및 진보된 센서의 개발을 통해 운전자가 운전할 때 운전자가 더 나은 의사 결정을 내릴 수 있도록 현대 기술이 점점 더 많이 적용될 수 있다.

[0003] 최근 몇 년 동안, 차량 영역 네트워크(VAN: Vehicle area network)는 스마트 차량의 통신 프로토콜을 정의하고 규제함으로써 거대한 학문 및 연구 관심을 끌었다. 결과적으로 지능형 애플리케이션을 위한 새로운 영역이 열리게 되었다. 보다 정확하게, 지능형 VAN은 네 가지 유형의 통신으로 구성된다.

[0004] 첫 번째는 차량 내부의 네트워크인 인트라-VAN 통신이다. 승객 또는 차량에 부착된 센서로부터 수집된 데이터는 이 네트워크 하에서 교환될 필요가 있다. 또한, 차량 대 차량 통신은 다양한 차량 간의 데이터 교환 네트워크이다. 셋째, 차량 대 광대역 클라우드의 통신은 클라우드와 차량 간의 데이터 교환 네트워크이다. 마지막으로, 차량과 도로 간 인프라 통신이 있는데, 차량이 스마트 신호등과 같은 지능형 인프라와 통신한다.

[0005] 인트라-VAN의 목표는 센서 또는 네트워크의 중앙 허브에서 수집한 정보를 제공하고 운전 중에 의사 결정을 용이하게 하는 것이다. 기존의 연구에서 [3]은 운전 중에 운전자의 육체적 행동 상태를 인식할 수 있도록 말하기 감정에 따라 졸린듯한 운전자 행동 상태를 분석하는 접근법을 제안했다. 또한, 당뇨병과 같은 만성 질환이 있는

운전자의 건강 상태는 사고 예방을 위해 센서의 도움을 받아 모니터링할 수 있다. 당뇨병의 경우 혈당이 위험 수준에 도달하면 운전자에게 통보를 받으며 사고는 예방된다. 그러나 자동차에 적합한 생체 센서가 부족한 것과 같은 VAN의 개발을 제한하는 몇 가지 과제가 있다.

[0006] 한편, 신체 영역 네트워크(BAN: Body Area Network)는 효율적이고 경제적이며 중단 없는 건강 상태 모니터링을 위한 요구 사항을 충족시키는 것으로 밝혀졌기 때문에 BAN의 발전이 급속히 증가하고 있다. BAN을 위해 설계된 센서를 사용하여 심전도(ECG), 심박수, 혈압과 같은 다양한 유형의 생체 데이터를 편리하고 비교적 정확하게 수집할 수 있다. 눈치챌 수 있듯이, VAN 내에서 언급된 문제 및 제한 중 일부는 BAN의 도움을 받아 해결할 수 있다. 이러한 이유로 BAN을 인트라-VAN 환경에 적용하면 운전자가 BAN 노드에서 수집한 생체 인식 데이터를 기반으로 건강 상태 관련 사고를 예방하고 운전 의사 결정을 개선하는 데 기여할 수 있다. 이 경우 스마트폰과 같은 기존의 BAN 허브 장치와 달리, 차량의 전자제어장치(ECU: electronic control unit)와 같은 중앙 내장형 시스템은 허브가 될 수 있는 가능성이 있는데, 노드에서 데이터를 수집하고 분석하여 운전자에게. 피드백을 제공한다.

[0007] BAN을 VAN에 적용하더라도 VAN의 기능이 향상되지만 보안 통신을 유지하는 것은 인간의 생체 인식 데이터가 비교적 사적이고 중요하기 때문에 조사해야 할 중요한 문제이다. 따라서, 저전력 소모, 작은 대기 시간 및 작은 자원 활용의 이점을 가지며, VAN 상황에서 적용되는 BAN을 위해 작동하는 새로운 보안 체계가 요구된다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) KR 10-2018-0121121 A

발명의 내용

해결하려는 과제

[0009] 본 발명이 해결하고자 하는 과제는 저전력 소모, 작은 대기 시간 및 작은 자원 활용의 이점을 가지며, VAN 상황에서 적용되는 BAN을 위해 작동하는 새로운 보안 체계를 제공할 수 있는 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치를 제공하는 것이다.

과제의 해결 수단

[0010] 상기 과제를 해결하기 위한 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치는,

[0011] 신체 영역 네트워크(BAN: ban area network) 노드와 스마트 차량의 전자제어장치(ECU: electronic control unit) 간의 데이터 통신을 위한 보안 장치에 있어서,

[0012] 상기 스마트 차량의 전자제어장치는 제1 보안 장치를 통해 데이터를 송수신하고, 상기 신체 영역 네트워크는 제2 보안 장치를 통해 데이터를 송수신하며,

[0013] 상기 제1 보안 장치는, 제1 인증 모듈; 및 제1 암호화 모듈을 포함하고,

[0014] 상기 제2 보안 장치는, 제2 인증 모듈; 및 제2 암호화 모듈을 포함하며,

[0015] 상기 제1 인증 모듈은, 상기 제2 보안 장치에 인증서를 요구하고, 상기 제2 보안 장치로부터 수신되는 인증서를 검증하며, 챌린지를 생성하고, 상기 제1 보안 장치와 상기 제2 보안 장치에만 알려진 비밀 키 및 상기 챌린지에 기반하여 응답을 생성하며, 상기 제2 보안 장치에 상기 챌린지를 전송하고 상기 제2 보안 장치로부터 수신되는 응답을 검증하여 상기 신체 영역 네트워크 노드의 인증 여부를 결정하며,

[0016] 상기 제1 암호화 모듈은, 제1 개인 키에 기반하여 제1 공개 키를 생성하고 상기 제2 보안 장치와 공개 키를 교환하며, 상기 제1 개인 키와 상기 제2 보안 장치로부터 수신되는 제2 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 전자제어장치로부터 수신되는 데이터를 암호화하여 상기 제2 보안 장치로 전송하거나 상기 제2 보안 장치로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 전자제어장치로 전송하며,

[0017] 상기 제2 인증 모듈은, 상기 제1 보안 장치로부터 인증서를 요구받는 경우, 상기 제1 보안 장치에 인증서를 전

송하고, 상기 제1 보안 장치로부터 수신되는 상기 챌린지 및 상기 비밀 키에 기반하여 응답을 생성하여 생성된 응답을 상기 제1 보안 장치로 전송하며,

[0018] 상기 제2 암호화 모듈은, 제2 개인 키에 기반하여 제2 공개 키를 생성하고 상기 제1 보안 장치와 공개 키를 교환하며, 상기 제2 개인 키와 상기 제1 보안 장치로부터 수신되는 제1 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 신체 영역 네트워크 노드로부터 수신되는 데이터를 암호화하여 상기 제1 보안 장치로 전송하거나 상기 제1 보안 장치로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 신체 영역 네트워크 노드로 전송한다.

[0019] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 제1 인증 모듈은, 상기 제2 보안 장치로부터 수신된 응답이 상기 제1 인증 모듈에서 생성한 응답과 동일한 경우, 상기 신체 영역 네트워크 노드를 인증할 수 있다.

[0020] 또한, 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 응답은, 해시 기반 메시지 인증 코드(HMAC: hash-based message authentication code) 보안 해시 알고리즘(SHA: secure hash algorithm)-256에 기반하여 계산되고,

[0021] 상기 제2 인증 모듈은, 상기 제1 보안 장치로부터 수신된 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 상기 응답으로서 생성하고,

[0022] 상기 제1 인증 모듈은, 상기 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 상기 응답으로서 생성할 수 있다.

[0023] 또한, 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 챌린지는 상기 신체 영역 네트워크(BAN) 노드에서 수집한 생체 인식 데이터를 사용하여 생성될 수 있다.

[0024] 또한, 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 생체 인식 데이터는, 상기 신체 영역 네트워크 노드에 의해 획득되는 심전도 데이터, 심박수, 체온 및 혈압 중 적어도 하나를 포함할 수 있다.

[0025] 또한, 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 제1 암호화 모듈 및 상기 제2 암호화 모듈 각각은 타원곡선 암호화(ECC: Elliptic Curve Cryptography) 모듈 및 고급 암호화 표준(AES: Advanced Encryption Standard) 모듈을 포함하고,

[0026] 상기 제1 암호화 모듈과 상기 제2 암호화 모듈 각각은 타원곡선 암호화 모듈을 이용하여, 타원곡선 디피-헬만(ECDH: Elliptic-Curve Diffie-Hellman) 키 동의 프로토콜에 기반하여 각각의 개인 키에 대응하는 공개 키를 생성하여 생성된 공개 키를 서로 교환하고,

[0027] 상기 제1 암호화 모듈과 상기 제2 암호화 모듈 각각의 고급 암호화 표준(AES) 모듈은, 자신의 개인 키와 상대방으로부터 수신된 공개 키에 기반하여 AES에 따라 데이터를 암호화하기 위한 대칭 키를 생성할 수 있다.

발명의 효과

[0028] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 의하면, 저전력 소모, 작은 대기 시간 및 작은 자원 활용의 이점을 가지며, VAN 상황에서 적용되는 BAN을 위해 작동하는 새로운 보안 체계를 제공할 수 있다.

[0029] 보다 구체적으로, 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치의 장점은 다음과 같다.

[0030] 첫째, BLE에 비해 연결 대기 시간이 짧다. 두 번째로, 동작 주파수는 10㎒로서 이는 상대적으로 낮으며, 또한 낮은 전력 소비를 초래한다. 셋째, 표준에 명시되고 위임된 인증 목적을 위한 인증서 유효성 확인 프로세스 외에도 HMAC-SHA256과 관련된 새로운 챌린지-응답 교환 방법이 제안되어 인증의 보안 수준을 향상시킨다. 넷째, 제안된 보안 체계는 하드웨어 자원 활용도가 상대적으로 낮다. 마지막으로 제안된 설계는 하드웨어로 구현된다. 소프트웨어 기반 보안 체계와 비교할 때, 하드웨어 기반 설계는 전력 소비가 낮고 동작 주파수의 유연성이 강하다.

도면의 간단한 설명

[0031] 도 1은 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치의 블록도.

도 2는 도 1에 도시된 보안 장치의 상세 블록도.

도 3은 ECU 보안 장치와 신체 영역 네트워크 노드 간의 보안 방식의 흐름을 도시한 도면.

도 4는 예시적인 SHA-256의 흐름도.

발명을 실시하기 위한 구체적인 내용

[0032] 본 발명의 목적, 특정한 장점들 및 신규한 특징들은 첨부된 도면들과 연관되어지는 이하의 상세한 설명과 바람직한 실시예들로부터 더욱 명백해질 것이다.

[0033] 이에 앞서 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이고 사전적인 의미로 해석되어서는 아니되며, 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있는 원칙에 입각하여 본 발명의 기술적 사상에 부합되는 의미와 개념으로 해석되어야 한다.

[0034] 본 명세서에서 각 도면의 구성요소들에 참조번호를 부가함에 있어서, 동일한 구성 요소들에 한해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 번호를 가지도록 하고 있음에 유의하여야 한다.

[0035] 또한, "제1", "제2", "일면", "타면" 등의 용어는, 하나의 구성요소를 다른 구성요소로부터 구별하기 위해 사용되는 것으로, 구성요소가 상기 용어들에 의해 제한되는 것은 아니다.

[0036] 이하, 본 발명을 설명함에 있어, 본 발명의 요지를 불필요하게 흐릴 수 있는 관련된 공지 기술에 대한 상세한 설명은 생략한다.

[0037] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시형태를 상세히 설명하기로 한다.

[0038] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치는, 인증 모듈, 암호화 모듈, 인증 및 암호화 모듈 간의 인터페이스, 보안 체계와의 인터페이스의 주요 하드웨어 모듈로 구성된다. 인증 모듈 및 암호화 모듈은 통신의 보안 수준에 따라 독립적으로 또는 함께 작동할 수 있다. 예를 들어, 통신 모듈의 보안 레벨이 레벨 2인 동안 인증 모듈과 암호화 모듈이 모두 활성화되고 협력된다.

[0039] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치는 도 1에 도시되어 있다. 도 2는 도 1에 도시된 제1 및 제2 보안 장치(102, 104)의 상세 블록도이고, 도 3은 그 동작 시퀀스를 도시한 것이다. 직렬 주변 인터페이스(SPI)는 제안된 보안 체계와 기존의 VAN 시스템 간의 연결을 설정하기 위한 보안 체계의 인터페이스로 활용되었다.

[0040] 도 1 및 도 2에 도시된 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치는, 신체 영역 네트워크(BAN: ban area network) 노드(106)와 스마트 차량의 전자제어장치(ECU: electronic control unit)(100) 간의 데이터 통신을 위한 보안 장치이다.

[0041] 도 1 및 도 2에 도시된 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에 있어서, 상기 스마트 차량의 전자제어장치(100)는 제1 보안 장치(102)를 통해 데이터를 송수신하고, 상기 신체 영역 네트워크 노드(106)는 제2 보안 장치(104)를 통해 데이터를 송수신한다.

[0042] 상기 제1 보안 장치(102)는, 제1 인증 모듈(108), 인터페이스(110) 및 제1 암호화 모듈(112)을 포함하고, 상기 제2 보안 장치(104)는, 제2 인증 모듈(114), 인터페이스(116) 및 제2 암호화 모듈(118)을 포함한다.

[0043] 상기 제1 인증 모듈(108)은, 상기 제2 보안 장치(104)에 인증서를 요구하고, 상기 제2 보안 장치(104)로부터 수신되는 인증서를 검증하며, 챌린지를 생성하고, 상기 제1 보안 장치(102)와 상기 제2 보안 장치(104)에만 알려진 비밀 키 및 상기 챌린지에 기반하여 응답을 생성하며, 상기 제2 보안 장치(104)에 상기 챌린지를 전송하고 상기 제2 보안 장치(104)로부터 수신되는 응답을 검증하여 상기 신체 영역 네트워크 노드(106)의 인증 여부를 결정한다.

[0044] 상기 제1 암호화 모듈(112)은, 제1 개인 키에 기반하여 제1 공개 키를 생성하고 상기 제2 보안 장치(104)와 공개 키를 교환하며, 상기 제1 개인 키와 상기 제2 보안 장치(104)로부터 수신되는 제2 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 전자제어장치(100)로부터 수신되는 데이터를 암호화하여 상기 제2 보안 장치(104)로 전송하거나 상기 제2 보안 장치(104)로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 전자제어장치(100)로 전송한다.

[0045] 상기 제2 인증 모듈(114)은, 상기 제1 보안 장치(102)로부터 인증서를 요구받는 경우, 상기 제1 보안 장치(102)에 인증서를 전송하고, 상기 제1 보안 장치(102)로부터 수신되는 상기 챌린지 및 상기 비밀 키에 기반하여 응답을 생성하여 생성된 응답을 상기 제1 보안 장치로 전송한다.

[0046] 상기 제2 암호화 모듈(118)은, 제2 개인 키에 기반하여 제2 공개 키를 생성하고 상기 제1 보안 장치(102)와 공개 키를 교환하며, 상기 제2 개인 키와 상기 제1 보안 장치(102)로부터 수신되는 제1 공개 키에 기반하여 대칭 키를 생성하고, 생성된 대칭 키를 사용하여 상기 신체 영역 네트워크 노드(106)로부터 수신되는 데이터를 암호화하여 상기 제1 보안 장치(102)로 전송하거나 상기 제1 보안 장치(102)로부터 수신되는 암호화된 데이터를 암호 해독하여 상기 신체 영역 네트워크 노드(106)로 전송한다.

[0047] 상기 제1 인증 모듈(108)은 상기 제2 보안 장치(104)로부터 수신된 응답이 상기 제1 인증 모듈(108)에서 생성한 응답과 동일한 경우, 상기 신체 영역 네트워크 노드(106)를 인증한다.

[0048] 상기 응답은, 해시 기반 메시지 인증 코드(HMAC: hash-based message authentication code) 보안 해시 알고리즘(SHA: secure hash algorithm)-256에 기반하여 계산되고, 상기 제2 인증 모듈(114)은, 상기 제1 보안 장치(102)로부터 수신된 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 응답으로서 생성하고, 상기 제1 인증 모듈(108)은, 상기 챌린지 및 상기 비밀 키를 결합하며, 결합된 값을 SHA-256 함수에 기반하여 출력된 HMAC 출력을 상기 응답으로서 생성한다.

[0049] 상기 챌린지는 상기 신체 영역 네트워크(BAN) 노드(106))에서 수집한 생체 인식 데이터를 사용하여 생성되고, 상기 생체 인식 데이터는, 상기 신체 영역 네트워크 노드(106)에 의해 획득되는 심전도 데이터, 심박수, 체온 및 혈압 중 적어도 하나를 포함한다.

[0050] 상기 제1 암호화 모듈(112) 및 상기 제2 암호화 모듈(118) 각각은, 타원곡선 암호화(ECC: Elliptic Curve Cryptography) 모듈(216) 및 고급 암호화 표준(AES: Advanced Encryption Standard) 모듈(222)을 포함하고, 상기 제1 암호화 모듈(112)과 상기 제2 암호화 모듈(118) 각각의 타원곡선 암호화 모듈(216)은, 타원곡선 디피-헬만(ECDH: Elliptic-Curve Diffie-Hellman) 키 동의 프로토콜에 기반하여 각각의 개인 키에 대응하는 공개 키를 생성하여 생성된 공개 키를 서로 교환하며, 상기 제1 암호화 모듈(112)과 상기 제2 암호화 모듈(118) 각각의 고급 암호화 표준(AES) 모듈(222)은, 자신의 개인 키와 상대방으로부터 수신된 공개 키에 기반하여 AES에 따라 데이터를 암호화하기 위한 대칭 키를 생성한다.

[0051] 한편, 도 2에 도시된 보안 장치는, 인증 모듈(200), 암호화 모듈(202), 인증 모듈과 암호화 모듈 간의 인터페이스(204), 및 보안 시스템의 인터페이스(206)를 포함한다.

[0052] 인증 모듈(200)은, HMAC-SHA256 모듈(212), 인증 모듈용 로직 제어 유닛(214), 인증서 및 비밀 키를 저장하기 위한 롬(208), 및 챌린지 및 응답을 저장하기 위한 램(210)을 포함한다.

[0053] 암호화 모듈(202)은, 타원곡선 암호화(ECC) 모듈(216), 데이터를 암호화하고 암호된 데이터를 암호 해독하기 위한 고급 암호화 표준(AES) 모듈(222), 매개 변수 관리부(218), 및 암호화 모듈용 로직 제어 유닛(220)을 포함한다.

[0055] **인증 모듈**

[0056] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에서 BAN 노드(106)를 인증하기 위한 인증 방법의 절차는, i) 인증서의 유효성 검증과, ii) 챌린지-응답 교환의 검증의 두 단계로 나눌 수 있다. 인증 방법의 순서는 도 3에 도시되어 있다.

[0058] 인증서 유효성 검증

[0059] 앞에서 설명한 것처럼 인증서 유효성 검증은 표준 IEEE 802.15.6에 지정된 절차이다. 그러나 표준 요구 사항을 달성하기 위한 여러 가지 방법이 있다. 본 발명의 일 실시예에서 인증서의 유효성 검증은 X.509 인증서와 관련이 있으며 여기서는 두 가지 작업이 수행된다.

[0060] 먼저, ECU(100)의 제1 보안 장치(102)는 BAN 노드(106)의 제2 보안 장치(104)로 노드 인증서를 요구한다(S300). BAN 노드(106)의 제2 보안 장치(104)는 인증서를 제1 보안 장치(102)로 전송한다(S302).

[0061] 둘째, 인증서는 ECU(100)의 제1 보안 장치(102)에 의해 검증된다(S303). 인증서는 X.509v3 표준을 따르며 인증서 체인은 여기에서 찾을 수 있고, 노드 인증서 서명은 ECU(100)의 제1 보안 장치(102)에 있는 다음 인증서의 공개 키를 사용하여 확인된다. 테스트 목적으로 사용된 인증서는 OpenSSL을 사용하여 자체 서명되고 생성되었다.

[0062] 유효성 검증은 RFC 5280에 명시된 대로 인증 경로 유효성 검증 알고리즘에 따라 수행된다. 인증서가 확인되면 인증서 보유 노드는 진성이다. 사용자 이름-암호 인증 동등에서 사용자 이름이 제공되었으며 신뢰할 수 있다. 챌린지-응답 인증 형태의 암호 보안 계층은 그 다음이고, 신원 확인이 필수적이지는 않지만, BAN 노드(106)에 대한 고유한 챌린지 응답을 명시적으로 연결하고 인증 시 이를 요구함으로써 시스템을 더욱 안전하게 보호한다.

[0064] 챌린지-응답 교환의 검증

[0065] 챌린지-응답 교환의 검증은 표준 IEEE 802.15.6에 명시되지 않은 추가적인 보안 절차이다. 그것은 세 단계로 세분화된다.

[0066] 처음에 제1 보안 장치(102)는 64비트 길이의 챌린지를 발행하여 노드 응답 요구와 함께 BAN 노드(106)의 제2 보안 장치(104)로 전송한다(S304). 챌린지는 임의의 비트 순서로 볼 수 있으며 심전도(ECG) 데이터, 심박수, 체온 또는 혈압과 같이 연결된 BAN 노드(106)에서 수집한 생체 인식 데이터를 사용하여 잠재적으로 생성된다. 챌린지는 그것이 처리되는 알려지지 않은 노드(106)의 제2 보안 장치(104)로 보내지고(S304), 제2 보안 장치(104)는 신뢰할 수 있는 ECU(100)의 제1 보안 장치(102)와 신뢰할 수 있는 BAN 노드(106)의 제2 보안 장치(104)에만 알려진 256비트 비밀 키 및 상기 제1 보안 장치(102)로부터 수신된 챌린지를 사용하여 256비트의 응답을 계산하여(S306). 노드 응답을 제1 보안 장치(102)로 전송한다(S308).

[0067] 제1 보안 장치(102)는 상기 비밀 키 및 상기 챌린지를 사용하여 응답을 계산하고 그것을 제2 보안 장치(102)로부터 수신된 응답과 비교하여 응답을 검증한다(S310).

[0068] 응답을 계산하려면 해시 기반 메시지 인증 코드(HMAC: hash-based message authentication code)가 필요하다. HMAC는 암호화 해시 기능을 기반으로 하는 안전한 절차이다. 이 경우 사용되는 해시 함수는 보안 해시 알고리즘(SHA: Secure Hash Algorithm)-256이지만 다른 해시 함수로 업데이트될 수 있다. 기본 해시 기능에서 발견된 모든 취약점은 본질적으로 메시지 인증 코드의 약점이 된다. 이런 이유로 함수는 충돌과 같은 공격에 내성이 필요하다.

[0069] 즉, 해시 함수는 무한히 많은 임의의 입력 집합을 일반적으로 더 작지만 여전히 고정된 출력 집합에 매핑하여 작동한다. 이 출력 세트는 절차적으로 생성되지만 입력과 많이 다르므로 다시 추적할 수 없다. 충돌은 두 입력이 똑같은 출력을 줄 수 있을 때 발생하며, 생일 문제로도 알려져 있다. 이것은 실수로 발생할 가능성은 극히 적지만, 해시 함수의 결함으로 인해 충돌을 감지하고 의도적으로 메시지를 위조할 수 있다.

[0070] MD5 나 SHA-1과 같은 대중적인 함수는 Carnegie Mellon University의 Software Engineering Institute와 암스테르담과 Google의 CWI Institute에서 볼 수 있듯이 안전하지 않은 것으로 결정되었다. 이러한 이유로 해시 함수 SHA-256이 본 발명의 일 실시예에 의한 보안 장치의 인증 모듈에 사용되었으므로 더 안전한 대안으로 간주된다.

[0071] HMAC 절차는 메시지(m)와 비밀 키(k)의 두 입력을 결합하고, 해시 함수(H)를 사용하여 HMAC(m, k) 출력을 생성하는 방식으로 작동한다. 해시 함수는 두 번 실행되며 HMAC의 기능 블록이고, 모듈러 2 연산(XOR) 및 연결이 추가된다. 절차는 수학식 1과 같다. $\oplus$와 |는 각각 XOR과 연결을 나타낸다.

[0072] 본 발명의 일 실시예에 의한 보안 장치에서, 상기 HMAC 절차에서 사용되는 메시지(m)는 제1 보안 장치(102)에서 생성된 챌린지이다. 상기 제1 보안 장치(102)에서 생성된 챌린지는 상기 제2 보안 장치(104)로 전송되므로, 상기 제1 보안 장치(102)와 상기 제2 보안 장치(104)는 각각 상기 챌린지를 HMAC 절차의 메시지(m)로 간주하여 비

밀 키(k)와 결합한 후 HMAC 출력을 생성한다.

수학식 1

[0073] $$HMAC(m,k) = H((k \oplus opad)|H((k \oplus ipad)|m))$$

[0074] ipad 및 opad는 내부 및 외부 패딩 상수이며, 해시 블록 크기의 길이로 확장되는, 반복값인 $0 \times 5c5c \ldots$ 및 $0 \times 3636 \ldots$ 으로 구성된다. 유사한 전처리가 키에 대해 수행되며 이것은 더 짧다; 그것은 오른쪽이 0으로 채워져 해시 블록 크기의 길이와 일치시킨다. 키가 더 길면 해시 함수는 키 길이를 올바른 길이로 줄이기 위해 키 자체에 대해 세 번 실행된다. 도시된 바와 같이, 전처리된 키는 초기에 내부 패딩과 XOR 처리되고, 그 출력은 메시지와 연결되며, 이들은 모두 해싱된다. 사전 처리된 키는 외부 패딩과 XOR되고 앞에서 설명한 해시의 출력과 연결된다. 연결의 출력이 다시 해싱되고 이번 해시 함수의 출력이 최종 출력이 된다.

[0075] 언급한 바와 같이, 임의의 해시 함수가 H 블록을 구현하는데 사용될 수 있으며, 이 경우에 그것은 SHA-256이다. SHA-256의 절차는 도 4에 간략히 설명되어 있다.

[0076] SHA-256은 처음 8개의 소수인 2 내지 19의 제곱근의 소수부의 처음 32비트와 함께, 8개의 변수인 해시 변수 H_0 내지 H_7을 초기화함으로써 시작된다(S400). 변수 H는 해시 출력을 저장하는 데 사용된다. 64개의 상수(k_0 내지 k_{63})로 배열 k를 초기화하는 또 다른 초기화가 이어진다(S400). 이 상수는 라운드(round) 상수라고도 하며 처음 64개의 소수(2 내지 311)의 입방근의 소수부의 처음 32비트이다.

[0077] 초기화 후 해시 입력에 대해 일부 사전 처리가 수행된다(S400). 우선 단일 '1' 비트가 끝에 추가된다. 그런 다음 L+1+K+64가 512의 배수가 되도록 다수의 '0' 비트들이 추가되는데, L은 입력의 길이, 1은 '1' 비트, K는 부가되는 '0' 비트들의 수이다. 이 작업이 끝나면, 길이 L은 64-비트 빅-엔디안(big-endian) 정수로서 끝에 추가되므로, 총 길이가 512의 배수가 된다. 따라서 메시지는 512비트의 청크(chunks)로 나뉘며, 다음 절차는 변수 H를 이용하여 각 청크에 대해 반복하고, 모든 반복마다 변수 H에 다시 가산한다. 분명히 해시 입력이 상대적으로 작으면, 함수는 하나의 청크에 대해서만 실행될 것이다.

[0078] 입력 청크 처리가 종료되는지가 판단되고(S402), 입력 청크 처리가 종료되지 않은 경우, 모든 청크에 대해, 배열 w를 만들어서 채운다(S406). 이 배열은 메시지 스케줄 배열(message schedule array)이라고도 하며 라운드 상수 배열과 마찬가지로 64개의 32 비트 요소들을 포함한다. 배열을 채우기 위해 청크는 16개의 32-비트 서브 청크들로 나뉘며, 메시지 스케줄 배열의 처음 16개 요소인 w_0 내지 w_{15}로 복사된다. 나머지 48개의 요소들에 대해, 수학식 2는 이들이 어떻게 채워지는지 보여준다. ROR은 오른쪽으로 회전하는 것을 나타낸다. 즉, 드롭된 비트들은 왼쪽에 생성된 공간에 배치되는 반면, SHR은 오른쪽으로 시프트하는 것을 나타내는데, 즉, 삭제된 비트는 폐기되고 생성된 공간은 '0' 비트로 채워진다.

수학식 2

[0079] $$w_i = w_{i-16} + w_{i-7} + S_0 + S_1$$

수학식 3

[0080] $$S_0 = (w_{i-15}\ ROR\ 7) \oplus (w_{i-15}\ ROR\ 18) \oplus (w_{i-15}\ SHR\ 3)$$
$$S_1 = (w_{i-2}\ ROR\ 17) \oplus (w_{i-2}\ ROR\ 19) \oplus (w_{i-2}\ SHR\ 10)$$

[0081] 다음 단계는 해시 변수 H_0 내지 H_7에서 발견된 내용을 가지고 8개의 임시 작업 변수 a 내지 h를 초기화한다

(S406).

[0082] 모든 메시지 스케줄 어레이 요소들에 대해 동작이 수행되었는지가 판단되고(S408), 모든 메시지 스케줄 어레이 요소들에 대해 동작이 수행되지 않은 경우, 메시지 스케줄 배열(총 64개)의 모든 요소에 대해 압축 함수가 실행된다(S410). 이것은 임시 작업 변수를 조작할 것이다. 이 함수의 알고리즘은 수학식 4 내지 수학식 6과 같다.

수학식 4

[0083]
$$h = g,\ g = f,\ f = e,\ e = d + T_1$$
$$d = c,\ c = b,\ b = a,\ a = T_1 + T_2$$

수학식 5

[0084]
$$T_1 = h + S_1 + ch + k_i + w_i$$
$$T_2 = S_0 + maj$$

수학식 6

[0085]
$$S_1 = (e\ ROR\ 6) \oplus (e\ ROR\ 11) \oplus (e\ ROR\ 25)$$
$$ch = (e\ \&\ f) \oplus (\bar{e}\ \&\ g)$$
$$S_0 = (a\ ROR\ 2) \oplus (a\ ROR\ 13) \oplus (a\ ROR\ 22)$$
$$maj = (a\ \&\ b) \oplus (a\ \&\ c) \oplus (b\ \&\ c)$$

[0086] 볼 수 있듯이, 압축 함수는 i에 의존하는데, 그것은 라운드 상수(k_i)와 메시지 스케줄(w_i) 배열의 요소이다. 압축 함수 다음에는, 작업 변수들이 해시 변수들에 다시 추가되어 그들의 값을 업데이트한다. 이 과정은 더 이상 처리할 청크가 없을 때까지 반복되고, 모든 입력 청크에 대한 처리가 종료된 경우, 그 시점에서 해시의 출력은 수학식 7에 나타난 것처럼 해시 변수들이 서로 단순히 추가된다(S404).

수학식 7

[0087]
$$H = H_1 | H_2 | H_3 | H_4 | H_5 | H_6 | H_7$$

[0089] **암호화 모듈**

[0090] ECC가 본 발명의 일 실시예에 의한 보안 장치의 암호화 모듈(112, 118)의 암호화 방법으로 활용되었다.

[0091] ECC는 효율적인 암호화 방법이다; 그것은 훨씬 더 짧은 키 크기를 사용하여 다른 공개 키 암호화 방법과 동일한 보안 수준을 달성할 수 있다는 것이 입증되었다. 이 때문에 저전력 소모, 낮은 처리 지연, 낮은 메모리 소비 등의 장점을 지닌 ECC는 표준 암호화 방식인 IEEE 802.15.6 표준에 의해 채택되었다.

[0092] ECC는 Rivest, Shamir, Adelman(RSA) 및 디지털 서명 알고리즘(DSA: Digital Signature Algorithm) 시스템에 비해 더 강력한 보안을 제공하는 대체 공개 키 시스템으로 제안되었다. 더 강력한 보안 암호화가 필요한 이유는 기존의 RSA 및 DSA에서 정수 분해 문제와 이산 대수가 지수함수적인 것보다 더 적게 시간이 걸린다는 것이다.

계산 능력이 증가함에 따라, 충분한 안전을 제공하기 위해서는 점점 더 중요한 요소가 필요하다. 예를 들어, National Standard Institute of Technology(NIST)에 의해 설정된 표준에서 1024비트 길이의 키를 선택하는 것이 좋다.

[0093] 이와 대조적으로 ECC의 보안은 주로 ECDLP(Elliptic Curve Discrete Logarithm Problem)의 명백한 난해함을 기반으로 한다. 타원 곡선 E(Fq), 베이스 포인트 P∈E(Fq) 및 차수 k가 주어지면, 유한 필드 Fq에 정의된 포인트-승산으로 타원 곡선상의 다른 점을 계산하기 쉽다.

수학식 8

[0094]
$$Q = k \cdot P = \underbrace{P + P + \cdots + P}_{k\ times} \in E(F_q)$$

[0095] 여기서 k는 개인 키로 사용될 수 있고 Q는 공개 키로 사용될 수 있다.

[0096] ECC에 대한 기본 공격은 이러한 정수가 존재한다는 조건하에 이 두 주어진 포인트 P와 Q에서 개인 키로 사용되는 차수 k를 계산하는 것이다. 그러나 가장 효율적인 일반 알고리즘조차도 계산하기에 엄청나게 복잡할 것이다(차수 계산은 키 크기에 지수적이다).

[0097] 결과적으로 기존의 기술에 비해 ECC의 주요 매력은 기본적인 난해한 수학적 문제를 해결하는 최상의 알고리즘인 ECDLP가 ECC에서 완전히 지수적으로 소요된다는 것이다. 160비트 키를 가진 ECC 공개 키 시스템은 1024비트 키를 가진 기존의 RSA 및 DSA 시스템과 동일한 수준의 보안을 제공한다는 것이 입증되었다. ECC에 대한 하위-지수적 공격이 없으므로 처리 능력, 저장 공간, 대역폭 및 전력이 잠재적으로 감소한다. 이러한 장점으로 인해 ECC는 스마트폰 및 IoT 장치와 같이 제한된 장치에 적합한 암호화 기술 후보가 된다.

[0098] 한편, AES는 NIST에 의해 선택된 이전의 데이터 암호화 표준(DES: Data Encryption Standard)과 비교하여 더 강력한 대칭 키 알고리즘이다.

[0099] 본 발명의 일 실시예에 의한 신체 영역 네트워크 노드와 스마트 차량의 전자제어장치 간의 데이터 통신을 위한 보안 장치에서는 ECC와 AES 기법을 결합하여 보안 체계에서 강력하고 효율적인 암호화 기법을 구현한다. 이 방식에서 ECC 모듈은 ECDH(Elliptic-Curve Diffie-Hellman) 키 동의 프로토콜을 기반으로 공개 키를 생성 및 변경한다. 보안 채널을 사용하여, 공개 키가 생성되고 양쪽 통신 종단 사이에서 교환되며 AES 모듈에 의해 수행되는 것처럼 보다 빠른 대칭 암호화가 수행된다. 제안된 암호화 모듈의 하드웨어 구조는 도 2의 오른쪽에 나와있다.

[0100] 암호화 모듈(202)의 암호화 절차는 다음과 같이 설명된다. 처음에는 임의의 개인 키가 k1 및 k2로 표시된 두 통신 종단들, 즉 제1 보안 장치(102)의 제1 암호화 모듈(112)과 제2 보안 장치(104)의 제2 암호화 모듈(118)에서 각각 생성된다(도 3의 S312, S314). ECC 모듈(216)을 사용하여 양측은 공개 키를 다음과 같이 계산한다(도 3의 S312, S314).

수학식 9

[0101]
$$Q_1 = k_1 * P$$

수학식 10

[0102]
$$Q_2 = k_2 * P$$

[0103] 여기서 P는 타원 곡선에 미리 정의된 기점이다. 곱셈 연산자는 타원 곡선에 정의된 포인트 곱셈이다. ECC 암호화의 안전성은 ECDLP에 의해 보증된다; Q와 P로부터 k를 계산하는 것은 정말로 어렵다. ECDH 프로토콜에

따르면, 공개 키 Q1과 Q2는 양측 간에 공유된다(도 3의 S316).

[0104] 마지막으로, 대칭 키는 수학식 11과 같이 생성되는데(도 3의 S318, S320), 이것은 AES에서 일반 텍스트를 암호화하고 해독하는 데 사용할 수 있다. ECDH 기반 키 동의는 전체 인증 절차 이전에 한 번만 처리된다.

수학식 11

[0105]
$$
\begin{aligned}
K &= k_1 * Q_2 \\
&= k_1 * (k_2 * P) \\
&= k_1 * k_2 * P \\
&= k_2 * (k_1 * P) \\
&= k_2 * Q_1
\end{aligned}
$$

[0106] AES 모듈(222)의 경우, 카운터 작동 모드(AES-CTR)가 선택된다. 그 이유 중 하나는 AES-CTR이 블록 암호화에서 강력한 안전성을 제공한다는 것이다. 다른 이유는 암호화와 암호 해독이 BAN의 저전력 요구 사항에 중요한 동일한 하드웨어 모듈을 공유할 수 있기 때문이다.

[0107] 도 3의 중간 부분은 암호화 설정 단계의 순서를 보여준다. 그 후에 BAN 노드(106)와 ECU(100) 간의 통신이, 제1 보안 장치(102)와 제2 보안 장치(104에 의해 보안화된다.

[0109] **FPGA에서 본 발명의 일 실시예에 의한 보안 장치의 보안 체계 평가**

[0110] 본 발명의 일 실시예에 의한 보안 장치의 보안 체계는 Verilog 및 VHDL로 구현되었다. 이는 Altera Arria 10 FPGA(10AS066N3F40E2SG)로 평가되었다. 표 1은 최종 구현 보고서를 보여준다.

표 1

[0111]

FPGA	Altera Arria 10 (10AS066N3F40E2SG)
ALMs	7341/251,680 (2.92%)
Registers	14,743/1,006,720 (1.46%)
Memory	1,007,616/43,642,880 (2.31%)
Operating frequency	10 MHz
Maximum frequency	106.18 MHz
Power consumption	61.86 mW
Connection time	2.7 ms

[0112] 본 발명의 일 실시예에 의한 보안 장치의 보안 체계는 시험 합성 분석으로 평가되었는데, 클록 제약을 위반하지 않으면서 106.18㎒의 높은 작동 주파수가 달성되었다. 그러나 BAN과 VAN이 작동하는 상황을 고려할 때 10㎒의 작동 주파수로 충분하다고 판명되었다. 이 결정에는 두 가지 중요한 이유가 있다. 첫째, BLE(Bluetooth Low Energy)와 비교할 때 BAN은 초당 수천 번 노드에서 생체 인식 데이터를 요청할 필요가 없으므로 훨씬 더 낮은 속도로 데이터를 교환한다. 둘째, 제안된 설계의 지연 시간은 BAN의 요구 조건을 충족시키는 10㎒의 주파수에서 작동하는 경우에도 BLE의 연결 시간에 가깝다. 따라서 동작 주파수는 전형적인 경우로 최종 합성을 위한 10㎒로 결정되며, 소비 전력을 최적화할 때 시범적인 것과는 다르다. 제안된 설계의 자원 활용도는 적응형 논리 모듈(ALM), 레지스터 및 메모리 측면에서 설명된다. 총 자원 중 백분율 또한 표 1에 나와 있다.

[0113] 앞서 설명한 바와 같이, 제안된 보안 체계의 인증 모듈과 암호화 모듈은 통신의 보안 수준에 따라 독립적으로 또는 함께 동작할 수 있다. 즉, 일부 상황에서는 단 하나의 모듈만 작동하기 때문에 위에 표시된 코어 전원보다

훨씬 적은 전력 소모가 발생한다.

[0114] 인증 모듈 및 암호화 모듈의 자원 활용도 및 대기 시간은 표 2에 설명되어 있다. 강조해야 할 한 가지 점은 표 2에 표시된 암호화 모듈의 대기 시간이 암호화 설정 단계의 ECC 키 생성 기간이며, 이 특정 대기 시간은 한 번만 발생한다. 이후 암호화 설정 단계의 대기 시간은 각 데이터 프레임의 AES 키 계산 기간의 대기 시간으로 0.01ms이다. 한편, 보안 체계의 동작 주파수에 따른 최대 처리량은 11.85Mbps이다.

표 2

[0115]

Module	ALMs	Registers	Memory	Latency(ms)
Authentication module	1529 (0.61%)	2048 (0.20%)	16,384 (0.04%)	0.95
Encryption module	5812 (2.31%)	12,695 (1.26%)	991,232 (2.27%)	1.75

[0116] 최종 합성 결과는 제안된 보안 체계가 BAN 및 내부 VAN 모두에 대해 저전력, 짧은 대기 시간 및 작은 하드웨어 비용의 요구 사항을 충족함을 보여준다. 한편, 설계의 동작 주파수는 BAN과 VAN이 적용되는 상황에서 요구되는 것보다 훨씬 낮은 전력 소비를 달성하도록 최적화되었으며 회로의 대기 시간은 여전히 요구 사항을 충족시킨다.

[0117] 이전에 제시되었듯이, 제안된 보안 체계의 장점은 다음과 같이 요약될 수 있다. 첫째, BLE에 비해 연결 대기 시간이 짧다. 두 번째로, 동작 주파수는 10㎒로서 이는 상대적으로 낮으며, 또한 낮은 전력 소비를 초래한다. 셋째, 표준에 명시되고 위임된 인증 목적을 위한 인증서 유효성 확인 프로세스 외에도 HMAC-SHA256과 관련된 새로운 챌린지-응답 교환 방법이 제안되어 인증의 보안 수준을 향상시킨다. 넷째, 제안된 보안 체계는 하드웨어 자원 활용도가 상대적으로 낮다. 마지막으로 제안된 설계는 하드웨어로 구현된다. 소프트웨어 기반 보안 체계와 비교할 때, 하드웨어 기반 설계는 전력 소비가 낮고 동작 주파수의 유연성이 강하다.

[0118] 이상 본 발명을 구체적인 실시예를 통하여 상세하게 설명하였으나, 이는 본 발명을 구체적으로 설명하기 위한 것으로, 본 발명은 이에 한정되지 않으며, 본 발명의 기술적 사상 내에서 당 분야의 통상의 지식을 가진 자에 의해 그 변형이나 개량이 가능함은 명백하다고 할 것이다.

[0119] 본 발명의 단순한 변형 내지 변경은 모두 본 발명의 영역에 속하는 것으로, 본 발명의 구체적인 보호 범위는 첨부된 청구범위에 의하여 명확해질 것이다.

부호의 설명

[0120] 100 : ECU 102 : 제1 보안 장치

104 : 제2 보안 장치 106 : BAN 노드

108 : 제1 인증 모듈 110 : 인터페이스

112 : 제1 암호화 모듈 114 : 제2 인증 모듈

116 : 인터페이스 118 : 제2 암호화 모듈

200 : 인증 모듈 202 : 암호화 모듈

204 : 인증 모듈과 암호화 모듈 간의 인터페이스

206 : 보안 시스템의 인터페이스

208 : 롬 210 : 램

212 : HMAC-SHA256 모듈 214 : 인증 모듈용 로직 제어 유닛

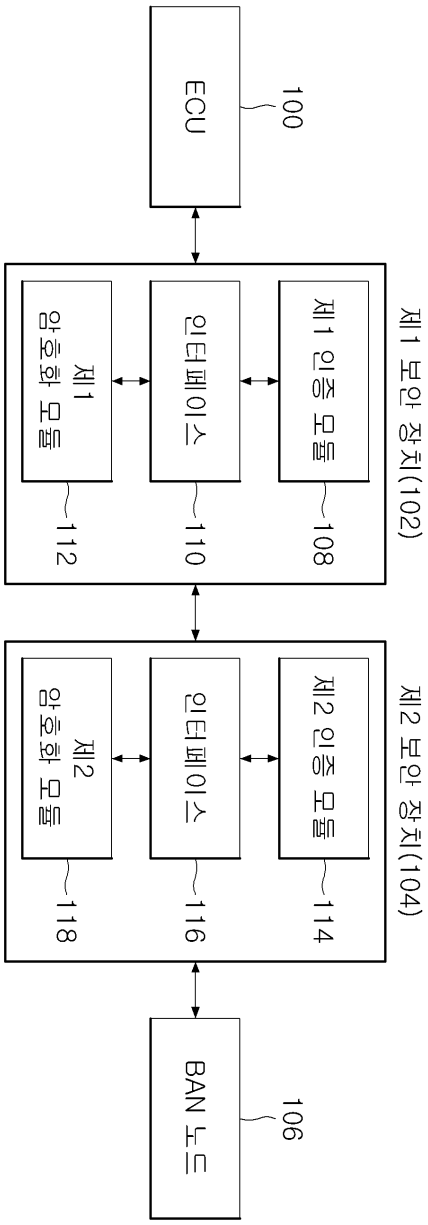
216 : ECC 모듈 218 : 매개 변수 관리부

220 : 암호화 모듈용 로직 제어 유닛

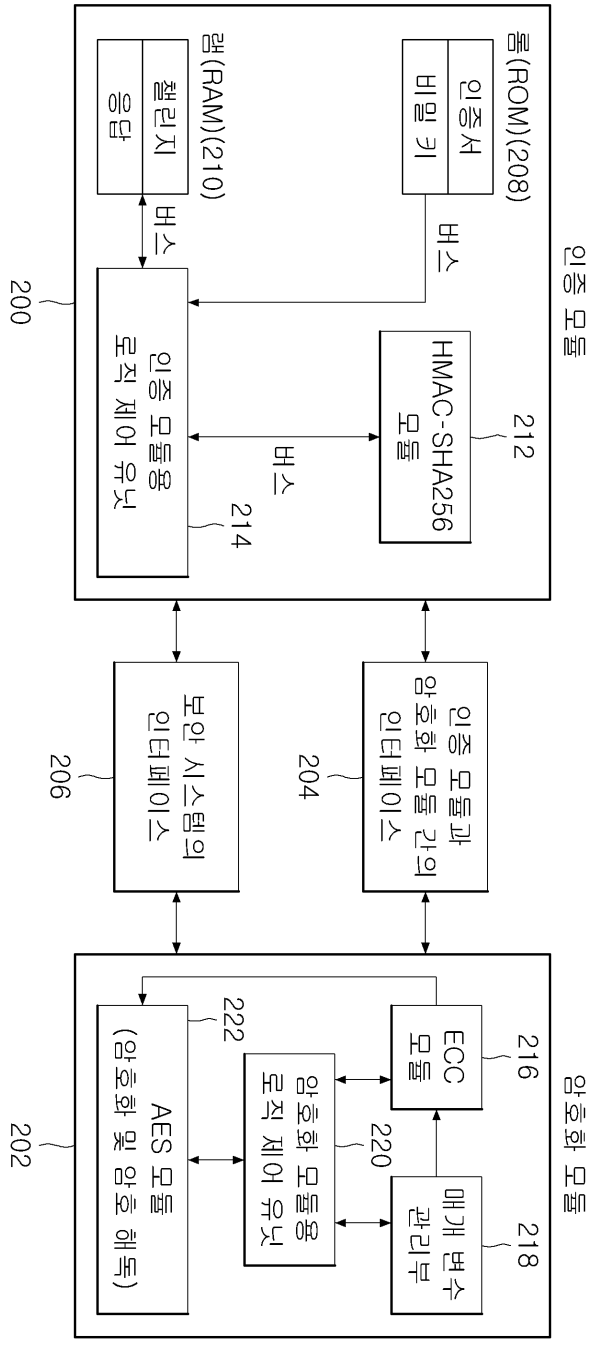
222 : AES 모듈

도면

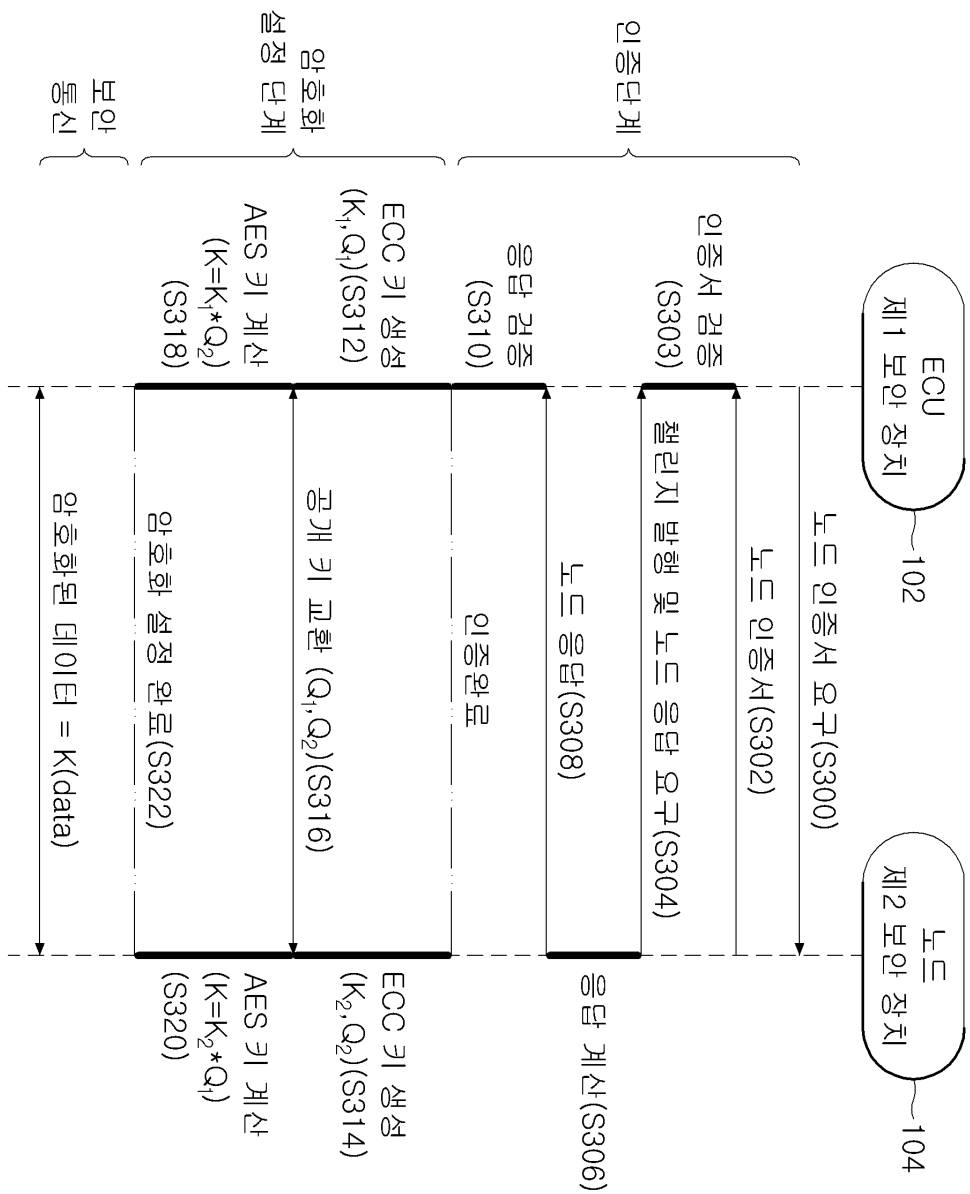
도면1


ECU
100
제1 보안 장치(102)
제1 인증 모듈
108
인터페이스
110
제1 암호화 모듈
112
제2 보안 장치(104)
제2 인증 모듈
114
인터페이스
116
제2 암호화 모듈
118
BAN 노드
106

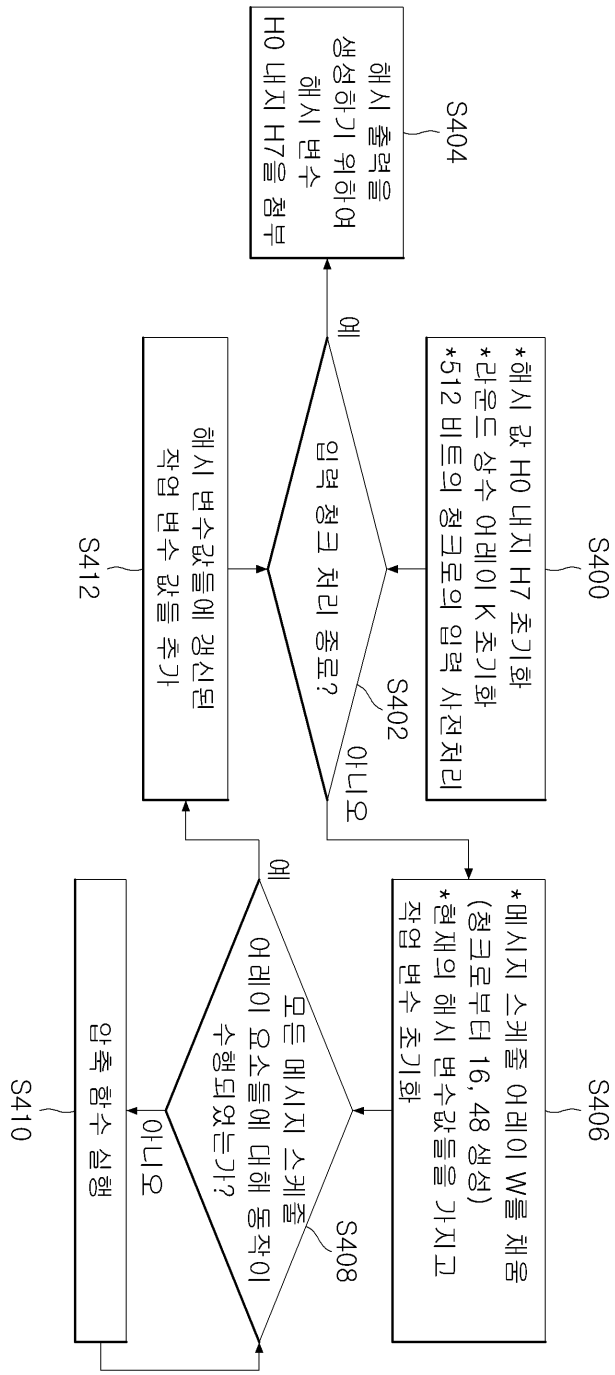
도면2


인증 모듈
롬(ROM)(208)
인증서
비밀 키
램(RAM)(210)
챌린지
응답
버스
버스
200
인증 모듈용
로직 제어 유닛
214
HMAC-SHA256
모듈
212
보안 시스템의
인터페이스
206
인증 모듈과
암호화 모듈 간의
인터페이스
204
암호화 모듈
ECC
모듈
216
AES 모듈
(암호화 및 암호 해독)
222
암호화 모듈용
로직 제어 유닛
220
매개 변수
관리부
218
202

도면3


ECU
제1 보안 장치
102
노드
제2 보안 장치
104
노드 인증서 요구(S300)
노드 인증서(S302)
인증서 검증
(S303)
챌린지 발행 및 노드 응답 요구(S304)
노드 응답(S308)
응답 계산(S306)
응답 검증
(S310)
인증완료
ECC 키 생성
(K_1,Q_1)(S312)
공개 키 교환 (Q_1,Q_2)(S316)
ECC 키 생성
(K_2,Q_2)(S314)
AES 키 계산
($K=K_1*Q_2$)
(S318)
암호화 설정 완료(S322)
AES 키 계산
($K=K_2*Q_1$)
(S320)
암호화된 데이터 = K(data)
인증단계
암호화
설정 단계
보안
통신

도면4


*해시 값 H0 내지 H7 초기화
*라운드 상수 어레이 K 초기화
*512 비트의 청크로의 입력 사전처리
S400
*메시지 스케줄 어레이 W를 채움
(청크로부터 16, 48 생성)
*현재의 해시 변수값들을 가지고
작업 변수 초기화
S406
모든 메시지 스케줄
어레이 요소들에 대해 동작이
수행되었는가?
S408
예
아니오
압축 함수 실행
S410
입력 청크 처리 종료?
S402
예
아니오
해시 변수값들에 갱신된
작업 변수 값들 추가
S412
해시 출력을
생성하기 위하여
해시 변수
H0 내지 H7을 첨부
S404