자율주행차 사고 데이터 저장 및 암호화

5대 분야 Autonomous Driving • Function Security • 기술분야명 사고기록 플랫폼
담당 센터 모빌리티플랫폼 • 연구자 신대교

Security

개념

자율 주행 차량의 사고 시점 전·후 일정시간동안 차량의 내·외부 영상 및 음성, 서라운드 센서, V2X 통신, IVN을 통한 차량 상태 등 다양한 정보를 저장 및 암호화 하는 기술

개발 내용

기술내용

자율주행 Level 2, 3단계 수준의 ADR 플랫폼 및 프로토타입 개발
- 자동차 전·후 영상 정보, 내·외부 네트워크 트래픽 정보 수집
- 센서 정보 기반 사고 여부 판단기술

ADR 저장 데이터의 무결성/조작방지 및 암·복호화 기술

차별성

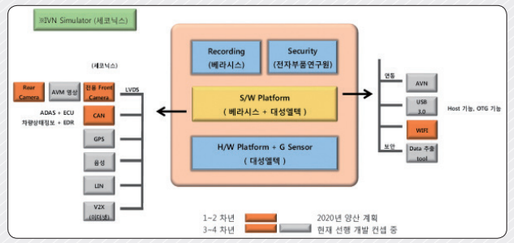
본 과제에서 개발 예정인 ADR 플랫폼 탑재를 위해 실제 모델 차량의 선정과 국내 메이저 제조사와의 후속 차량 공동개발에 대한 연구를 진행 중

현재 출시 예정인 차량과 자율주행 차량을 위한 ADR을 동시에 개발하는 두 트랙 진행으로 상용화와 첨단 기술 개발을 동시에 추진

해외주요기관

독일 Escript社(CycurHSM, CycurCORE)

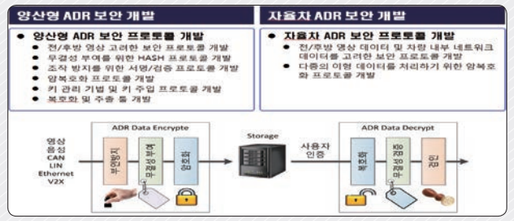
개발 내용



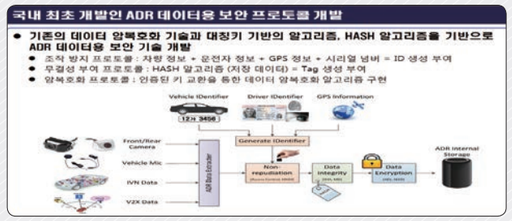
자율 차량용 ADR 아키텍쳐

자율주행 Level 3 이상에서 자율차 ADR 연차별 목표

연구원 보유(개발) 핵심기술



양산형 및 자율차용 ADR 보안개발



국내최초 ADR 데이터용 보안 프로토콜

연구원 보유(개발) 핵심기술

KETI 핵심기술

실시간 영상 데이터 보안 및 조작 방지, 무결성 프로토콜 개발을 위한 HASH 및 암·복호화 기술

고속 보안 프로토콜, 운전자 임의 영상 조작 방지, 사고 기록 정보의 무결성 부여 기술
- 전방 FHD 영상(30 fps)과 후방 HD 영상을 15ms이내 실시간 보안 적용 기술
- 차량 CAN 내부 네트워크 보안을 위한 OTP(One-Time Password) 기반 하드웨어보안모듈(HSM)을 활용한 경량 보안 알고리즘 기술

차별성

현재 상용화된 경쟁 기술이 없음

* 기존 상용차용 EDR(Event Data Recoder)은 국제규정(IEEE1616, SAE J1698 등)에서 정한 규격에 따라 제조 및 판매되고 있으나 자율주행에서 요구하는 서라운드 센서 데이터, 다채널 영상 데이터, V2X 통신 데이터 등의 정보 기록에는 한계

관련기술 보유 IP

대칭키 알고리즘을 이용한 경량 암·복호화 방법 및 시스템(국내/출원/2015)

OTP를 이용한 차량 내부 네크워크 보안 방법 및 시스템(국내/등록/2017)

Business Model

- **차량용 ADR (보안 S/W 및 프로토콜)**
  - 탑승자 검지, 운전자 감시(졸음, 시선이동 등), 제스처 입력 등 차량 제어용 디바이스 UI 기술에 적용
- **수요 예상 기업**
  - 자동차 제조 기업, 차량 부품제조 기업

관련 연구 분야

Core Technology	Related Technology		
	차량 제어보안	차량번호 인식	주행기록
 자율주행차 사고 데이터 저장 및 암호화 정보통신미디어/모빌리티플랫폼 신대교	OTP기반의 HSM 타입 차량 인증/보안/예지보전 플랫폼 정보통신미디어/모빌리티플랫폼 신대교	고속주행 차량번호 인식 일체형 임베디드 플랫폼 정보통신미디어/콘텐츠응용 박세호	차량 운행기록 장치 및 운전성향 분석 알고리즘 정보통신미디어/모빌리티플랫폼 이선영

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년11월01일
(11) 등록번호 10-1792341
(24) 등록일자 2017년10월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 12/40* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
H04L 9/0863 (2013.01)
(21) 출원번호 10-2015-0143267
(22) 출원일자 2015년10월14일
심사청구일자 2016년04월01일
(65) 공개번호 10-2017-0043778
(43) 공개일자 2017년04월24일
(56) 선행기술조사문헌
KR1020120137729 A*
KR1020030087874 A*
A. Menezes 외 2명, Handbook of Applied Cryptography, Chapter. 1,10, CRC Press (1996)*
KR1020060062641 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
전자부품연구원
경기도 성남시 분당구 새나리로 25 (야탑동)
(72) 발명자
신대교
경기도 성남시 분당구 양현로 138, 808동 902호
임기택
경기도 수원시 영통구 청명로 132, 331동 803호
(뒷면에 계속)
(74) 대리인
남충우

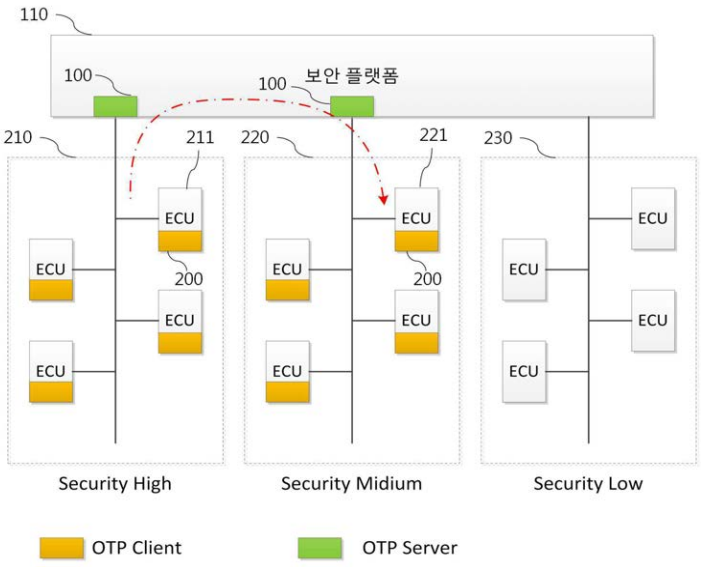
전체 청구항 수 : 총 5 항 심사관 : 양종필

(54) 발명의 명칭 **OTP를 이용한 차량 내부 네크워크 보안 방법 및 시스템**

(57) 요 약

OTP를 이용한 차량 내부 네크워크 보안 방법 및 시스템이 제공된다. 본 발명의 일 실시예에 따른 차량 네트워크는, 데이터에 비밀키를 이용하여 생성한 인증 코드를 부가하여 전송하는 컨트롤 유닛 및 인증 코드를 이용하여 컨트롤 유닛을 인증하는 인증부를 포함한다. 이에 의해, 차량 내부 네트워크의 보안 기능이 추가되어, 차량 네트워크의 해킹에 의한 위험과 피해를 미연에 방지할 수 있게 된다.

대 표 도 - 도1



(52) CPC특허분류
H04L 2012/40215 (2013.01)
(72) 발명자
윤상훈
경기도 성남시 분당구 판교로 393, 208동 102호
정한균
경기도 용인시 기흥구 사은로126번길 10, 112동 101호
진성근
경기도 성남시 중원구 광명로264번길 8, 201호

이 발명을 지원한 국가연구개발사업
과제고유번호 1615006851
부처명 국토교통부/해양부
연구관리전문기관 국토교통과학기술진흥원
연구사업명 건설교통기술연구개발사업
연구과제명 위성항법기반 교통인프라 기술개발
기 여 율 1/1
주관기관 한국항공우주연구원
연구기간 2014.05.12 ~ 2015.10.11

명 세 서

청구범위

청구항 1

차량 네트워크 시스템에 있어서,

보유하고 있는 비밀키를 이용하여 생성한 인증 코드를 데이터에 부가하여 제2 컨트롤 유닛에 전송하는 제1 컨트롤 유닛; 및

보유하고 있는 상기 제1 컨트롤 유닛의 비밀키와 상기 인증 코드를 이용하여 상기 제1 컨트롤 유닛을 인증하는 인증부;를 포함하고,

상기 차량 네트워크 시스템을 구성하는 컨트롤 유닛들은,

다수의 보안 등급 중 하나가 부여되며,

상기 제1 컨트롤 유닛은,

특정 보안 등급이 부여되고,

부여된 보안 등급의 종류에 따라, 상기 데이터에 상기 인증 코드를 부가하여 전송하는 주기가 결정되며,

상기 인증부는,

상기 제1 컨트롤 유닛으로부터 식별 정보를 수신하고, 수신한 식별 정보를 서버에 전송하면서 상기 제1 컨트롤 유닛의 비밀키를 요청하여 획득하고,

상기 서버는,

컨트롤 유닛들의 식별 정보들과 비밀키들을 매칭하여 보유하고 있어, 상기 인증부가 요청한 상기 제1 컨트롤 유닛의 식별 정보에 매칭된 상기 제1 컨트롤 유닛의 비밀키를 상기 인증부에 전송하는 것을 특징으로 하는 차량 네트워크 시스템.

청구항 2

청구항 1에 있어서,

상기 인증부는,

상기 제1 컨트롤 유닛이 인증된 컨트롤 유닛으로 판명되면, 상기 데이터의 목적지인 상기 제2 컨트롤 유닛에 상기 데이터를 처리할 것을 명령하는 것을 특징으로 하는 차량 네트워크 시스템.

청구항 3

청구항 2에 있어서,

상기 인증부는,

상기 제1 컨트롤 유닛이 인증되지 않은 컨트롤 유닛으로 판명되면, 상기 제2 컨트롤 유닛에 상기 데이터를 폐기하도록 명령하는 것을 특징으로 하는 차량 네트워크 시스템.

청구항 4

청구항 1에 있어서,

상기 제1 컨트롤 유닛은,

시간 정보 및 이벤트 정보 중 적어도 하나와 상기 비밀키를 이용하여 상기 인증 코드를 생성하는 하드웨어로 구현된 클라이언트를 이용하여, 상기 인증 코드를 생성하고,

상기 인증부는,

시간 정보 및 이벤트 정보 중 적어도 하나와 상기 제1 컨트롤 유닛의 비밀키를 이용하여 상기 인증 코드를 생성하여, 상기 제1 컨트롤 유닛으로부터 수신한 인증 코드와 비교하는 하드웨어로 구현된 서버를 이용하여, 상기 인증 코드를 검증하는 것을 특징으로 하는 차량 네트워크 시스템.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

차량 네트워크 시스템의 보안 방법에 있어서,

상기 차량 네트워크 시스템을 구성하는 제1 컨트롤 유닛이, 보유하고 있는 비밀키를 이용하여 생성한 인증 코드를 데이터에 부가하여 제2 컨트롤 유닛에 전송하는 단계; 및

상기 차량 네트워크 시스템에 마련된 인증부가, 보유하고 있는 상기 제1 컨트롤 유닛의 비밀키와 상기 인증 코드를 이용하여 상기 제1 컨트롤 유닛을 인증하는 단계;를 포함하고,

상기 차량 네트워크 시스템을 구성하는 컨트롤 유닛들은,

다수의 보안 등급 중 하나가 부여되며,

상기 제1 컨트롤 유닛은,

특정 보안 등급이 부여되고,

부여된 보안 등급의 종류에 따라, 상기 데이터에 상기 인증 코드를 부가하여 전송하는 주기가 결정되며,

상기 인증부는,

상기 제1 컨트롤 유닛으로부터 식별 정보를 수신하고, 수신한 식별 정보를 서버에 전송하면서 상기 제1 컨트롤 유닛의 비밀키를 요청하여 획득하고,

상기 서버는,

컨트롤 유닛들의 식별 정보들과 비밀키들을 매칭하여 보유하고 있어, 상기 인증부가 요청한 상기 제1 컨트롤 유닛의 식별 정보에 매칭된 상기 제1 컨트롤 유닛의 비밀키를 상기 인증부에 전송하는 것을 특징으로 하는 차량 네트워크 시스템의 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 차량 네크워크에 관한 것으로, 더욱 상세하게는 차량 내부 네크워크를 보안하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 기존의 차량 내부 네트워크는 보안과 관련한 별도의 장치나 프로토콜이 없어, 해킹에 취약한 구조이다.

[0003] IoT의 폭발적인 증가와 더불어 보안에 대한 공격도 많아질 것으로 예상되며, 특히, 자동차에 대한 해킹은 경제적, 사회적으로 매우 심각하며 치명적인 결과를 초래하게 된다. 실제로, 자동차에 대한 보안은 외부에서 시도되는 해킹에 무력한 모습을 보이고 있다.

[0004] 2013년 8월 해커 컨퍼런스에서 닌텐도의 휴대용 게임기로 2010년형 토요타 프리우스와 포드 이스케이프 해킹 시범을 보였다. 악성앱을 내려받은 스마트폰을 감염하고, 무선 통신망을 통해 차안에서 앱을 구동하여, '가속', 엔진 폐쇄', 'RPM 조작', '핸들 제어', '주행 중 흔들림'을 유발하였다.

[0005] 전기차 생산업체인 테슬라의 경우 2014년 16일 전자기기 보안 콘퍼런스에서 자사의 차량을 해킹하는 데에 성공하면 1만 달러를 지급하겠다고 선언한 후 하루 만에 중국인 해커에게 해킹당하여 수모를 당했다.

[0006] 이에 따라, 스마트키 해킹, CAN 데이터 해킹 등을 통한 자동차 보안 피해가 발생 가능할 것으로 예상되는 바, 이를 방지하기 위한 보안 기술의 마련이 시급하다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, 해킹에 강건하도록 차량 내부 네트워크를 보안하는 방법 및 시스템을 제공함에 있다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른, 차량 네트워크는, 데이터에 비밀키를 이용하여 생성한 인증 코드를 부가하여 전송하는 컨트롤 유닛; 및 상기 인증 코드를 이용하여 상기 컨트롤 유닛을 인증하는 인증부;를 포함한다.

[0009] 그리고, 상기 인증부는, 상기 컨트롤 유닛이 인증된 컨트롤 유닛으로 판명되면, 상기 데이터의 목적지 컨트롤 유닛에 상기 데이터를 처리할 것을 명령할 수 있다.

[0010] 또한, 상기 인증부는, 상기 컨트롤 유닛이 인증되지 않은 컨트롤 유닛으로 판명되면, 상기 데이터의 목적지 컨트롤 유닛에 상기 데이터를 폐기하도록 명령할 수 있다.

[0011] 그리고, 상기 컨트롤 유닛은, 시간 정보 및 이벤트 정보 중 적어도 하나와 상기 비밀키를 이용하여 상기 인증 코드를 생성하는 하드웨어로 구현된 클라이언트를 이용하여, 상기 인증 코드를 생성하고, 상기 인증부는, 시간 정보 및 이벤트 정보 중 적어도 하나와 상기 비밀키를 이용하여 상기 인증 코드를 생성하여, 상기 컨트롤 유닛으로부터 수신한 인증 코드와 비교하는 하드웨어로 구현된 서버를 이용하여, 상기 인증 코드를 검증할 수 있다.

[0012] 또한, 차량 네트워크를 구성하는 컨트롤 유닛들은, 다수의 보안 등급 중 하나가 부여되며, 상기 컨트롤 유닛은, 특정 보안 등급이 부여될 수 있다.

[0013] 그리고, 상기 컨트롤 유닛은, 보안 등급의 종류에 따라, 상기 데이터에 상기 인증 코드를 부가하여 전송하는 주기가 결정될 수 있다.

[0014] 그리고, 상기 인증부는, 상기 컨트롤 유닛으로부터 식별 정보를 수신하고, 수신한 식별 정보를 이용하여 서버로부터 상기 비밀키를 획득할 수 있다.

[0015] 한편, 본 발명의 다른 실시예에 따른, 차량 네트워크의 보안 방법은, 상기 차량 네트워크를 구성하는 컨트롤 유닛이, 데이터에 비밀키를 이용하여 생성한 인증 코드를 부가하여 전송하는 단계; 및 상기 차량 네트워크에 마련된 인증부가, 상기 인증 코드를 이용하여 상기 컨트롤 유닛을 인증하는 단계;를 포함한다.

발명의 효과

[0016] 이상 설명한 바와 같이, 본 발명의 실시예들에 따르면, 차량 내부 네트워크의 보안 기능이 추가되어, 차량 네트워크의 해킹에 의한 위험과 피해를 미연에 방지할 수 있게 된다.

[0017] 특히, 본 발명의 실시예들에 따르면, 차량 내부 네트워크의 고속 통신에 최적인 보안/인증이 가능하고, 보안 등급에 따른 차등적인 효율적 운용이 가능해진다.

도면의 간단한 설명

[0018] 도 1은 본 발명의 일 실시예에 따른 차량 내부 네트워크를 도시한 도면,

도 2는 OTP 클라이언트의 설명에 제공되는 도면,

도 3은 OTP 클라이언트의 상세 블럭도,

도 4는 차량 네트워크 데이터인 CAN 데이터의 후단에 OTP가 부가된 메시지 포맷,

도 5는 OTP 서버의 상세 블럭도,

도 6은 ECU에 대한 인증이 수행되는 절차를 도식적으로 나타낸 도면, 그리고,

도 7은 OTP 서버와 OTP 클라이언트가 동일한 비밀키를 공유하게 되는 과정의 설명에 제공되는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 발명의 실시예에서는, OTP(One Time Password)를 이용하여 차량 내부 ECU(Electronic Control Unit)들 간의 통신 보안을 강화하는 방법을 제시한다.

[0020] 이를 위해, 먼저 차량 내부 네트워크를 구성하는 ECU들을 보안 등급 별로 분류하고, 보안이 요구되는 등급에 포함된 ECU들에 대해서는 자신의 비밀키로 생성한 OTP를 데이터의 후단에 부가하여 전송하도록 한다.

[0021] 그리고, 차량 내부 네트워크의 보안 플랫폼은 자신이 보유하고 있는 ECU의 비밀키로 OTP를 생성하고, 생성한 OTP와 ECU로부터 수신한 데이터에 부가되어 있는 OTP를 비교하여, ECU를 인증한다.

[0022] 인증된(검증된 또는 정당한) ECU에 의해 생성/전송된 데이터로 판명된 경우, 목적지 ECU는 데이터를 통해 지시/요청하는 동작을 수행한다.

[0023] 하지만, 인증되지 않은 ECU에 의해 생성/전송된 데이터는 폐기되며, 목적지 ECU가 데이터를 통해 지시/요청하는 동작(해킹 동작)을 수행하지 않는다. 나아가, 보안 플랫폼은, 차량 내부 네트워크에 인증되지 않은 ECU가 포함되어 있음을 사용자(운전자)에게 안내하고, 관리자(이를 테면 AS 센터)에게 원격으로 알람 한다.

[0024] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0025] 도 1은 본 발명의 일 실시예에 따른 차량 내부 네트워크를 도시한 도면이다. 본 발명의 실시예에 따른 차량 내부 네트워크는, 도 1에 도시된 바와 같이, 보안 플랫폼(110)과 다수의 ECU들을 포함하여 구축된다.

[0026] 또한, 도 1에 도시된 바와 같이, ECU들은 보안 등급 별로 분류되어 있다. 구체적으로, 1) 운전자의 안전에 매우 중대한 영향을 줄 수 있는 ECU들(이를 테면, 차량 운전/제어와 관련한 ECU들)은 "Security High"로 분류되고, 2) 운전자의 안전에 영향을 줄 수 있는 ECU들(이를 테면, 차량 상태 모니터링과 관련한 ECU들)은 "Security Medium"으로 분류되고, 3) 운전자의 안전과 관련 없는 ECU들(이를 테면, 멀티 미디어 시스템을 위한 ECU들)은 "Security Low"로 분류된다.

[0027] "Security High" 그룹(210)에 포함된 ECU들과 "Security Medium" 그룹(220)에 포함된 ECU들은, 데이터를 전송할 때 후단에 OTP를 부가하여야 한다. 이에, 이 그룹들(210,220)에 포함된 ECU들은 OTP 클라이언트(200)가 부가된다.

[0028] 도 2에 도시된 바와 같이, OTP 클라이언트(200)는 ECU와 별도의 하드웨어로 구성한다. 이하에서, OTP 클라이언트(200)에 대해, 도 3을 참조하여 상세히 설명한다.

[0029] 도 3은 OTP 클라이언트(200)의 상세 블럭도이다. OTP 클라이언트(200)는, 도 3에 도시된 바와 같이, OTP 생성 모듈(200a), 시간 타이머(200b) 및 이벤트 카운터(200c)를 포함하고, 비밀키(200d)를 저장하고 있다.

[0030] OTP 생성 모듈(200a)은 시간 타이머(200b)에서 생성된 시간 정보와 이벤트 카운터(200c)에서 생성된 이벤트 정보와 함께 비밀키(200d)를 입력으로 하여, OTP를 생성하는 회로이다.

[0031] ECU는 OTP 생성 모듈(200a)에 의해 생성된 OTP를 자신의 데이터 후단에 부가하여 전송한다. 도 4에는 차량 네

트워크 데이터인 CAN 데이터의 후단에 OTP가 부가된 메시지 포맷을 나타내었다.

[0032] ECU들은 동일 그룹에 포함된 ECU에 데이터를 전송할 수 있음은 물론, 다른 그룹에 포함된 ECU에 데이터를 전송할 수도 있다. 즉, 도 1에 도시된 바와 같이, "Security High" 그룹(210)에 포함된 ECU(211)가 "Security Medium" 그룹(220)에 포함된 ECU(221)로 데이터를 전송하는 것이 가능하다.

[0033] 보안이 요구되는 그룹들(210, 220)에 포함된 ECU에서 전송된 데이터에 대해서는, 보안 플랫폼(110)의 OTP 서버(100)가 인증 절차를 수행하여, 인증된 ECU에 의해 생성/전송된 데이터인지 그렇지 않은지 판단하는 인증 수단으로 기능한다.

[0034] 이하에서, OTP 서버(100)에 대해, 도 5를 참조하여 상세히 설명한다. 도 5는 OTP 서버(100)의 상세 블럭도이다. OTP 서버(100)는, 도 5에 도시된 바와 같이, OTP 생성 모듈(100a), 시간 타이머(100b), 이벤트 카운터(100c) 및 OTP 비교기(100e)를 포함하고, 비밀키 테이블(100d)를 저장하고 있다.

[0035] OTP 생성 모듈(100a)은 시간 타이머(100b)에서 생성된 시간 정보, 이벤트 카운터(100c)에서 생성된 이벤트 정보와 함께 비밀키 테이블(100d)에 저장된 비밀키를 이용하여 OTP를 생성하는 회로이다. 이용되는 비밀키는, 비밀키 테이블(100d)에 저장된 비밀키들 중 인증하고자 하는 ECU의 비밀키이다.

[0036] OTP 비교기(100e)는 OTP 생성 모듈(100a)에서 생성된 OTP와 ECU로부터 수신된 데이터에 부가되어 있는 OTP를 비교하여, ECU 인증 절차를 수행한다. 도 6에는 보안 플랫폼(110)의 OTP 서버(100)에 의해 ECU에 대한 인증이 수행되는 절차를 도식적으로 나타내었다.

[0037] OTP 비교기(100e)에 의해 OTP가 동일한 것으로 판명되면, 보안 플랫폼(110)은 인증된 ECU로부터 데이터 생성/전송이 이루어진 것으로 취급하여, 목적지 ECU에 데이터를 처리할 것을 명령한다.

[0038] 하지만, OTP 비교기(100e)에 의해 OTP가 상이한 것으로 판명되면, 보안 플랫폼(110)은 인증되지 않은 ECU로부터 데이터 생성/전송이 이루어진 것으로 취급하여, 목적지 ECU에 데이터를 처리하지 말고 폐기할 것을 명령한다. 또한, 보안 플랫폼(110)은 알람을 발생시켜 사용자(운전자)로 하여금 운전을 중단할 것을 알리고, 관리자(원격 AS 센터)에게도 원격으로 해킹 사실을 통보한다.

[0039] OTP 서버(100)와 OTP 클라이언트(200)에 의한 OTP 생성에는 시간 정보와 이벤트 정보를 이용하는 것을 상정하였으나, 예시적인 것에 불과하다. 즉, 시간 정보와 이벤트 정보 중 하나만을 이용하여 OTP를 생성하는 것이 가능함은 물론, 그 밖의 다른 정보를 이용하는 것도 가능하다.

[0040] 이하에서, OTP 서버(100)와 OTP 클라이언트(200)가 동일한 비밀키를 공유하게 되는 과정에 대해, 도 7을 참조하여 상세히 설명한다. 도 7에서는 추가/교체로 인해 ECU(211)가 차량 네트워크에 편입된 상황에서, 보안 플랫폼(110)의 OTP 서버(100)가 ECU(211)에 부착/연결된 OTP 클라이언트(200)와 동일한 비밀키를 확보하는 과정을 나타내었다.

[0041] 도 7에 도시된 바와 같이, 차량 네트워크에 새로이 편입된 ECU(211)가 "Security High" 그룹(210)이나 "Security Medium" 그룹(220)에 포함되어야 할 ECU로 판명되면, 보안 플랫폼(110)은 ECU(211)에 S/N(Serial Number)을 요청한다.

[0042] 이후, 보안 플랫폼(110)은 ECU(211)로부터 수신한 S/N을 키 발급 서버(300)에 전송하면서 비밀키를 요청한다. 키 발급 서버(300)는 인증된 (정품의) ECU들의 비밀키들을 S/N들에 매칭하여 보유하고 있다.

[0043] 따라서, 키 발급 서버(300)는 보안 플랫폼(110)으로부터 수신한 S/N에 매칭되어 있는 비밀키를 보안 플랫폼(110)에 전송하며, 보안 플랫폼(110)은 수신한 비밀키를 OTP 서버(100)에 전달한다.

[0044] 키 발급 서버(300)와 보안 플랫폼(110) 간의 통신은 보안이 적용된 네트워크를 통해 이루어지도록 한다.

[0045] 위 과정은, 차량 출고 후에 ECU가 추가/교체된 경우에 한하여 적용된다. 차량 출고시에는, 차량에 장착된 ECU들 각각에 대한 비밀키들을 OTP 서버(100)에 저장한 상태로 출고한다.

[0046] 지금까지, OTP를 이용한 차량 내부 네크워크 보안에 대해 바람직한 실시예를 들어 상세히 설명하였다.

[0047] OTP는 비밀키를 이용하여 생성한 인증 코드의 일 예로 언급한 것이다. 따라서, OTP는 다른 종류의 비밀키 기반 인증 코드로 대체 가능하다. 비밀키 방식의 암호화는, 공개키&개인키 방식에 비해, 알고리즘이 간단하여 속도가 빠르며 클라이언트와 서버를 하드웨어로 구현할 수 있도록 하여 준다.

[0048] 한편, ECU들에 의한 OTP 부가는 모든 데이터에 대해 하는 것이 가장 바람직하지만, 오버헤드 감소를 위해 주기

적으로 수행할 수도 있다. 이때, 부가 주기는 보안 등급에 따라 결정할 수 있다. 예를 들어, 보안 등급이 높은 ECU는 데이터 10개 마다 OTP를 부가하고, 보안 등급이 중간인 ECU는 데이터 100개 마다 OTP를 부가하도록 구현하는 것이 가능하다.

[0049] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

[0050] 100 : OTP 서버

200 : OTP 클라이언트

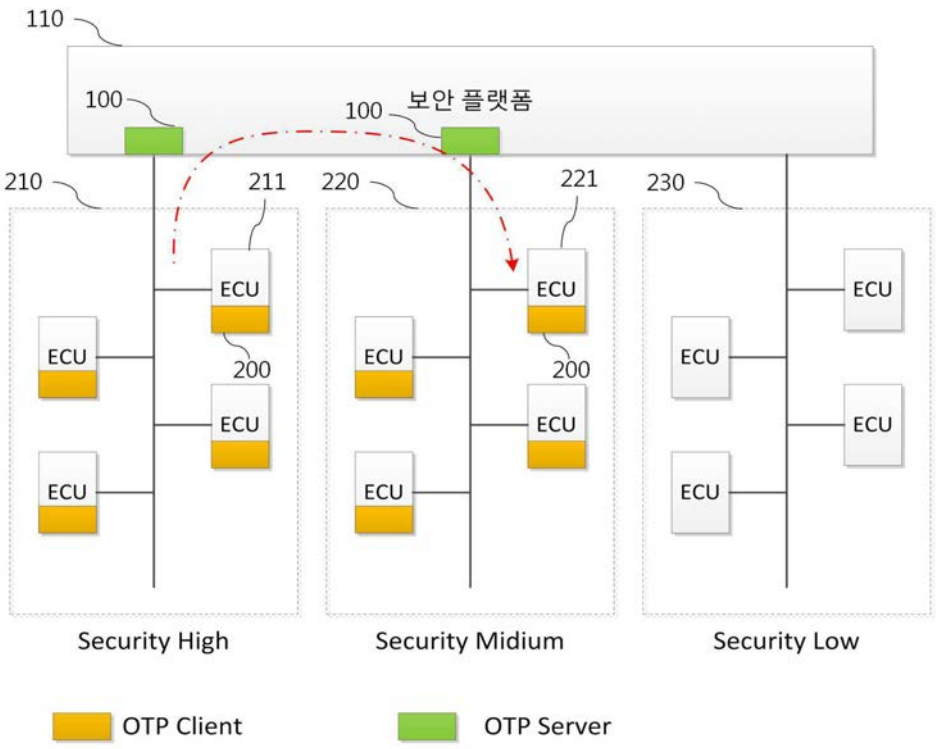
110 : 보안 플랫폼

211, 212, 221 : ECU

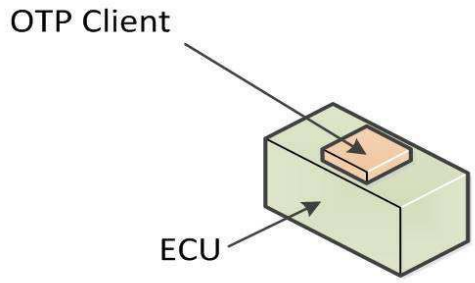
300 : 키 발급 서버

도면

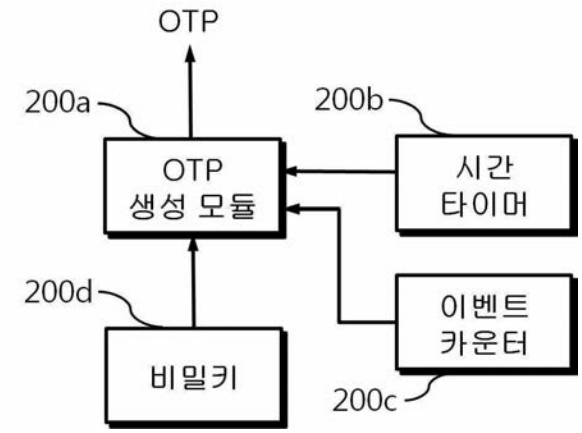
도면1



도면2

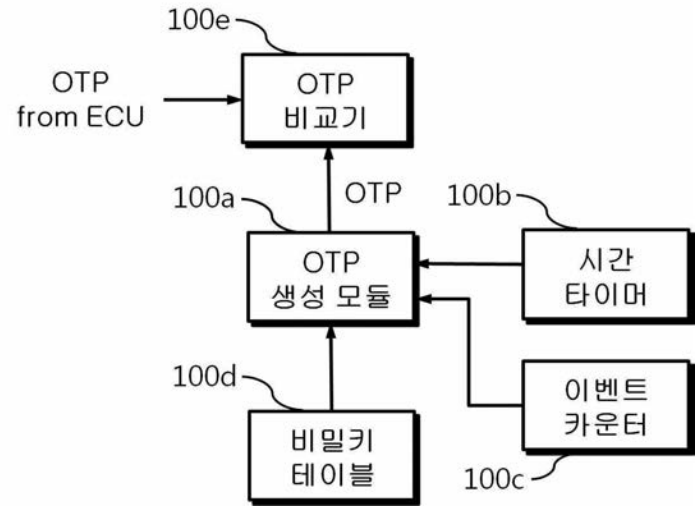


도면3

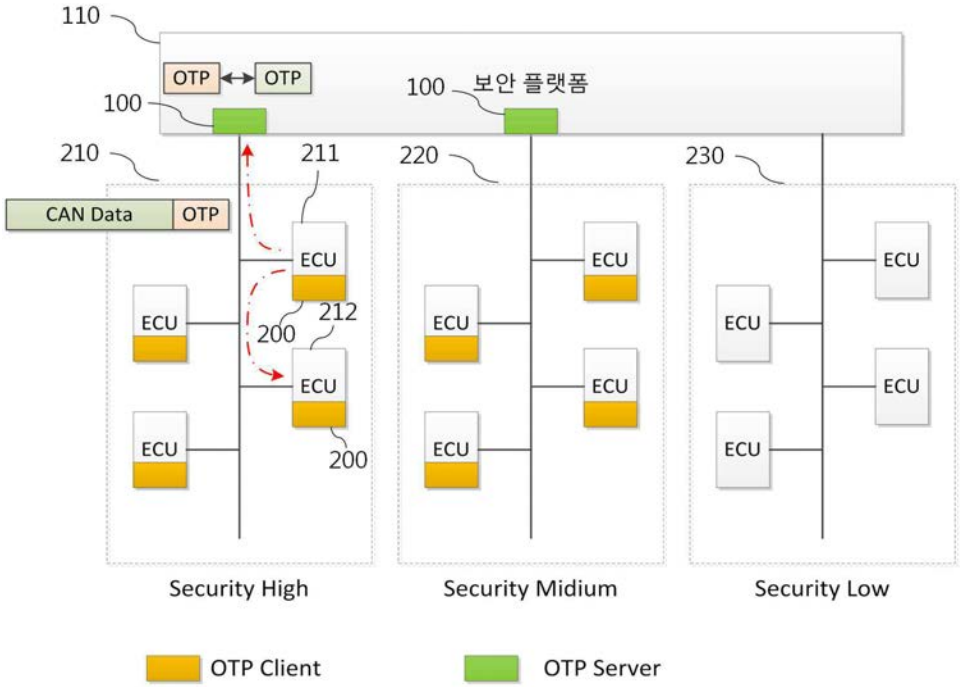


도면4

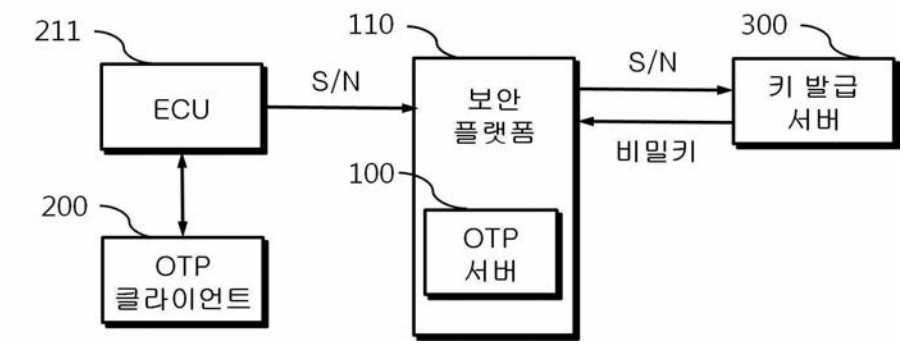
도면5



도면6


110
OTP
OTP
100
100
보안 플랫폼
210
211
220
230
CAN Data
OTP
ECU
ECU
ECU
212
200
ECU
ECU
ECU
ECU
ECU
ECU
ECU
ECU
ECU
200
Security High
Security Midium
Security Low
OTP Client
OTP Server

도면7


211
ECU
S/N
110
보안
플랫폼
S/N
비밀키
300
키 발급
서버
200
OTP
클라이언트
100
OTP
서버

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0077003
(43) 공개일자 2017년07월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/0625 (2013.01)
(21) 출원번호 10-2015-0187021
(22) 출원일자 2015년12월27일
심사청구일자 없음

(71) 출원인
전자부품연구원
경기도 성남시 분당구 새나리로 25 (야탑동)
(72) 발명자
신대교
경기도 성남시 분당구 양현로 138 , 808동 902호
윤상훈
경기도 성남시 분당구 판교로 393, 208동 102호
(뒷면에 계속)
(74) 대리인
남충우

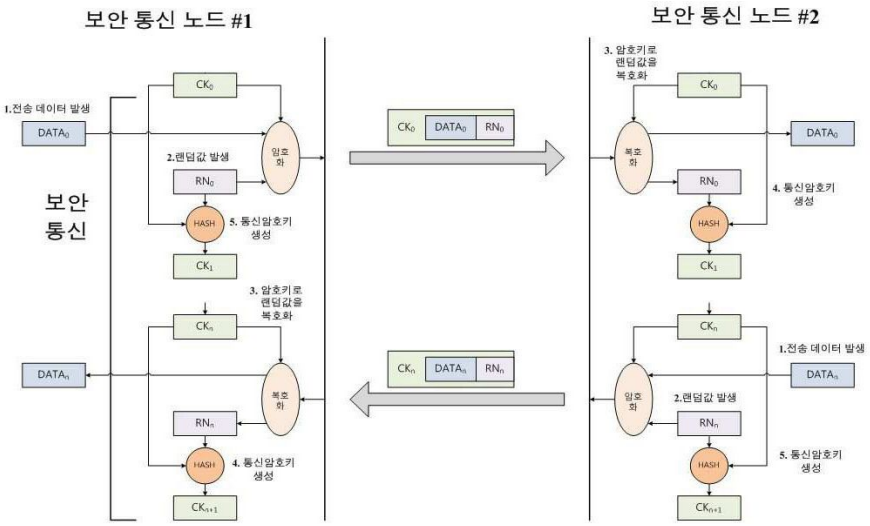
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **대칭키 알고리즘을 이용한 경량 암복호화 방법 및 시스템**

(57) 요 약

대칭키 알고리즘을 이용한 경량 암복호화 방법 및 시스템이 제공된다. 본 발명의 실시예에 따른 암복호화 방법은, 최초 랜덤값을 생성하여, 보유하고 있는 대칭키로 암호화하여 전달하고, 최초 랜덤값과 대칭키를 해쉬 알고리즘에 대입하여 최초 통신 암호키를 생성한다. 이에 의해, IoT 디바이스와 차량의 ECU와 같이 저성능 프로세서 환경에서도, 보안이 강화된 경량 암복호화가 가능해진다.

대 표 도



(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/0869 (2013.01)
(72) 발명자
정한균
경기도 성남시 분당구 느티로 22, 에이-1325호
최광호
경기도 의왕시 내손로 13, 115동 1702호

이 발명을 지원한 국가연구개발사업
과제고유번호 1711026385
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신기술인력양성
연구과제명 산학연 연계형 SW-SoC 융합 고급인력양성
기 여 율 1/1
주관기관 전자부품연구원
연구기간 2015.01.01 ~ 2015.12.31

명 세 서

청구범위

청구항 1

제1 노드가, 최초 랜덤값을 생성하는 단계;

상기 제1 노드가, 상기 최초 랜덤값을 보유하고 있는 대칭키로 암호화하여 제2 노드에 전달하는 단계;

상기 제1 노드가, 상기 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 단계;를 포함하는 것을 특징으로 하는 암복호화 방법.

청구항 2

청구항 1에 있어서,

제2 노드가, 암호화된 최초 랜덤값을 상기 제1 노드로부터 수신하는 단계;

상기 제2 노드가, 상기 암호화된 최초 랜덤값을 보유하고 있는 대칭키로 복호화하는 단계;

상기 제2 노드가, 복호화된 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 단계;를 더 포함하는 것을 특징으로 하는 암복호화 방법.

청구항 3

청구항 2에 있어서,

제1 랜덤값을 생성하는 단계;

상기 제1 랜덤값과 제1 데이터를 상기 최초 통신 암호키로 암호화하여 상기 제1 노드에 전달하는 단계;

상기 제1 랜덤값과 상기 최초 통신 암호키를 상기 해쉬 알고리즘에 대입하여, 제1 통신 암호키를 생성하는 단계;를 더 포함하는 것을 특징으로 하는 암복호화 방법.

청구항 4

청구항 3에 있어서,

상기 제2 노드가, 암호화된 제1 랜덤값과 제1 데이터를 상기 제1 노드로부터 수신하는 단계;

상기 제2 노드가, 상기 암호화된 제1 랜덤값과 제1 데이터를 상기 최초 통신 암호키로 복호화하는 단계;

상기 제2 노드가, 복호화된 제1 랜덤값과 상기 최초 통신 암호키를 해쉬 알고리즘에 대입하여, 제1 통신 암호키를 생성하는 단계;를 더 포함하는 것을 특징으로 하는 암복호화 방법.

청구항 5

청구항 2에 있어서,

상기 제1 노드가, 데이터를 통신하는 과정에서 상기 최초 통신 암호키로부터 순차적으로 생성되는 통신 암호키들 중 일부와 상기 최초 통신 암호키를 보유하는 단계;를 더 포함하는 것을 특징으로 하는 암복호화 방법.

청구항 6

최초 랜덤값을 생성하여, 보유하고 있는 대칭키로 암호화하여 전송하고, 상기 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여 최초 통신 암호키를 생성하는 제1 노드; 및

상기 제1 노드로부터 암호화된 최초 랜덤값을 수신하여, 보유하고 있는 대칭키로 복호화하고, 복호화된 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 제2 노드;를 포함하는 것을 특징으로 하는 암복호화 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 암복호화 기술에 관한 것으로, 더욱 상세하게는 IoT나 차량 등과 같이 CPU의 프로세싱 능력이 높지 않은 응용 분야를 위한 암복호화 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 현재 차량이나 IoT를 위하여 개발하고 있는 암복호화 방식은 비대칭키 방식이다. 비대칭키 암복호화 방식은, 도 1에 도시된 바와 같이, 공개키와 개인키로 구성된 1쌍의 키를 이용한 암호화 방식이다.

[0003] 비대칭키 암복호화 방식은, 키의 분배가 용이하고 인증, 전자서명에 이용가능하다. 비대칭키 암복호화 방식은, 공개키를 인증하기 위한 인증서 발급 때문에 네트워크에 연결이 필요하며, 공개키와 개인키를 생성하는 알고리즘 때문에 고성능의 프로세싱 CPU가 필요하다.

[0004] 따라서, 저성능의 프로세싱 파워를 가진 IoT나 외부 네트워크와 연결이 용이하지 않은 차량 환경에 적용하기에는 어렵다. IoT와 차량의 보안에 대한 필요성이 높아지고 있는바, 이를 해결하기 위한 방안의 모색이 요청된다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 상기와 같은 문제점을 해결하기 위하여 안출된 것으로서, 본 발명의 목적은, IoT 디바이스와 차량의 ECU와 같이 저성능 프로세서 환경에 적합하며, 보안이 강화된 경량 암복호화 방법 및 시스템을 제공함에 있다.

과제의 해결 수단

[0006] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른, 암복호화 방법은, 제1 노드가, 최초 랜덤값을 생성하는 단계; 상기 제1 노드가, 상기 최초 랜덤값을 보유하고 있는 대칭키로 암호화하여 제2 노드에 전달하는 단계; 및 상기 제1 노드가, 상기 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 단계;를 포함한다.

[0007] 그리고, 본 발명의 일 실시예에 따른 암복호화 방법은, 제2 노드가, 암호화된 최초 랜덤값을 상기 제1 노드로부터 수신하는 단계; 상기 제2 노드가, 상기 암호화된 최초 랜덤값을 보유하고 있는 대칭키로 복호화하는 단계; 상기 제2 노드가, 복호화된 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 단계;를 더 포함할 수 있다.

[0008] 또한, 본 발명의 일 실시예에 따른 암복호화 방법은, 제1 랜덤값을 생성하는 단계; 상기 제1 랜덤값과 제1 데이터를 상기 최초 통신 암호키로 암호화하여 상기 제1 노드에 전달하는 단계; 상기 제1 랜덤값과 상기 최초 통신 암호키를 상기 해쉬 알고리즘에 대입하여, 제1 통신 암호키를 생성하는 단계;를 더 포함할 수 있다.

[0009] 그리고, 본 발명의 일 실시예에 따른 암복호화 방법은, 상기 제2 노드가, 암호화된 제1 랜덤값과 제1 데이터를 상기 제1 노드로부터 수신하는 단계; 상기 제2 노드가, 상기 암호화된 제1 랜덤값과 제1 데이터를 상기 최초 통신 암호키로 복호화하는 단계; 상기 제2 노드가, 복호화된 제1 랜덤값과 상기 최초 통신 암호키를 해쉬 알고리즘에 대입하여, 제1 통신 암호키를 생성하는 단계;를 더 포함할 수 있다.

[0010] 또한, 본 발명의 일 실시예에 따른 암복호화 방법은, 상기 제1 노드가, 데이터를 통신하는 과정에서 상기 최초 통신 암호키로부터 순차적으로 생성되는 통신 암호키들 중 일부와 상기 최초 통신 암호키를 보유하는 단계;를

더 포함할 수 있다.

[0011] 한편, 본 발명의 다른 실시예에 따른, 암복호화 시스템은, 최초 랜덤값을 생성하여, 보유하고 있는 대칭키로 암호화하여 전송하고, 상기 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여 최초 통신 암호키를 생성하는 제1 노드; 및 상기 제1 노드로부터 암호화된 최초 랜덤값을 수신하여, 보유하고 있는 대칭키로 복호화하고, 복호화된 최초 랜덤값과 상기 대칭키를 해쉬 알고리즘에 대입하여, 최초 통신 암호키를 생성하는 제2 노드;를 포함한다.

발명의 효과

[0012] 이상 설명한 바와 같이, 본 발명의 실시예들에 따르면, IoT 디바이스와 차량의 ECU와 같이 저성능 프로세서 환경에서도, 보안이 강화된 경량 암복호화가 가능해진다.

[0013] 또한, 본 발명의 실시예들에 따르면, 보안상의 이유로 네트워크에 연결하는 것이 부적절한 차량의 ECU에 대해, 최선의 암복호화 방법 및 시스템을 제공할 수 있게 된다.

도면의 간단한 설명

[0014] 도 1은 비대칭키 암복호화 알고리즘을 나타낸 도면,

도 2는 대칭키 암복호화 알고리즘을 나타낸 도면,

도 3은 본 발명의 일 실시예에 따른 경량 암복호화 방법에 있어서, 최초 통신 암호키를 생성하는 과정의 설명에 제공되는 도면,

도 4는 본 발명의 일 실시예에 따른 경량 암복호화 방법에 있어서, 데이터 전송을 위한 통신 암호키를 생성하는 과정의 설명에 제공되는 도면,

도 5는 데이터 유실에 대비한 보안 통신 노드의 통신 암호키 보유의 설명에 제공되는 도면, 그리고,

도 6은 본 발명의 실시예에 따른 경량 암복호화 방법이 적용가능한 차량 네트워크를 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0016] 본 발명의 실시예에서는, 대칭키 알고리즘을 이용한 경량 암복호화 방법 및 시스템을 제시한다.

[0017] IoT 디바이스나 차량의 ECU와 같이 프로세서의 능력이 높지 않은 경우나 차량의 ECU와 같이 보안상의 이유로 외부 네트워크에 연결할 수 없거나 연결하는 것이 부적합한 경우, 본 발명의 실시예에 따른 암복호화 방법 및 시스템이 매우 유용하다.

[0018] 도 2는 대칭키 암복호화 알고리즘을 나타낸 도면이다. 도 2에 도시된 바와 같이, 대칭키 암복호화 알고리즘은, 암호화키와 복호화키가 동일하다. 송신자와 수신자는 동일한 대칭키를 이용하여 암호화된 통신을 사용한다.

[0019] 대칭키 암복호화 알고리즘은, 간단하게 암복호화가 가능하다. 대칭키 암복호화 알고리즘은, 비밀키의 주입과 보관이 중요하며, 비밀키가 노출될 경우에 더 이상 암복호화를 진행할 수 없다는 단점이 있다.

[0020] 이를 보완하기 위해, 본 발명의 실시예에서는, 대칭키 암복호화 알고리즘을 이용하되, 매 통신마다 새로운 통신 암호키를 생성하여 이용함으로써, 보안을 강화한다.

[0021] 도 3은 본 발명의 일 실시예에 따른 경량 암복호화 방법에 있어서, 최초 통신 암호키를 생성하는 과정의 설명에 제공되는 도면이다.

[0022] 본 발명의 실시예에 따른 경량 암복호화 통신은, 미리 대칭키를 나누어 보유한 2개의 보안 통신 노드들이 서로를 인증하고 최초 통신 암호키를 생성하는 절차로 시작한다.

[0023] 구체적으로, 도 3에 도시된 바와 같이, 보안 통신 노드 #1이, 1) 랜덤값(RN_{int})을 발생시키고, 2) 랜덤값(RN_{init})을 보유하고 있는 대칭키(SK)로 암호화하여 보안 통신 노드 #2에 전달한다.

[0024] 그러면, 보안 통신 노드 #2는, 3) 보안 통신 노드 #1로부터 수신한 암호화된 랜덤값(RN_{init})을 보유하고 있는 대

칭키(SK)로 복호화하여 랜덤값(RN_{init})을 확보한다.

[0025] 다음, 보안 통신 노드 #2는, 4) 복호화한 랜덤값(RN_{init})과 대칭키(SK)를 해쉬 알고리즘에 대입하여, 데이터 통신에 사용할 최초 통신 암호키(CK_0)를 생성하고 보관한다.

[0026] 마찬가지로, 보안 통신 노드 #1도, 5) 랜덤값(RN_{init})과 대칭키(SK)를 해쉬 알고리즘에 대입하여, 데이터 통신에 사용할 최초 통신 암호키(CK_0)를 생성하고 보관한다.

[0027] 도 3에서는, 보안 통신 노드 #1이 랜덤값(RN_{init})을 발생시켜 통신을 개시하는 것을 상정하였으나, 예시적인 것에 불과하다. 보안 통신 노드 #2에 의해 통신이 개시되는 것도 가능하다.

[0028] 어느 경우이던, 보안 통신 노드 #1과 보안 통신 노드 #2는 모두 대칭키(SK)로부터 생성한 최초 통신 암호키(CK_0)을 공유하게 된다.

[0029] 이후 통신 시도 시마다, 보안 통신 노드 #1과 보안 통신 노드 #2는 새로운 통신 암호키를 생성하여 암복호화 통신을 시도한다. 이 과정에 대해 도 4를 참조하여 상세히 설명한다.

[0030] 도 4는 본 발명의 일 실시예에 따른 경량 암복호화 방법에 있어서, 데이터 전송을 위한 통신 암호키를 생성하는 과정의 설명에 제공되는 도면이다.

[0031] 도 4에 도시된 바와 같이, 1) 전송할 데이터($DATA_0$)가 발생한 보안 통신 노드 #1은, 2) 랜덤값(RN_0)을 발생시키고, 전송할 데이터($DATA_0$)와 랜덤값(RN_0)을 최초 통신 암호키(CK_0)로 암호화하여 보안 통신 노드 #2에 전송한다.

[0032] 그러면, 보안 통신 노드 #2는, 3) 보유하고 있는 최초 통신 암호키(CK_0)로 데이터($DATA_0$)와 랜덤값(RN_0)을 복호화하고, 4) 복호화된 랜덤값(RN_0)과 최초 통신 암호키(CK_0)를 해쉬 알고리즘에 대입하여 다음에 사용할 통신 암호키(CK_1)를 생성하여 보관한다.

[0033] 마찬가지로, 보안 통신 노드 #1도, 5) 랜덤값(RN_0)과 최초 통신 암호키(CK_0)를 해쉬 알고리즘에 대입하여 다음에 사용할 통신 암호키(CK_1)를 생성하여 보관한다.

[0034] 이에 의해, 보안 통신 노드 #1과 보안 통신 노드 #2는 모두 최초 통신 암호키(CK_0)로부터 생성한 통신 암호키(CK_1)을 공유하게 된다.

[0035] 이후, 전송할 데이터가 발생한 보안 통신 노드 #1 또는 보안 통신 노드 #2에 의해 통신이 개시되고, 통신이 완료되면 보안 통신 노드 #1과 보안 통신 노드 #2는 모두 통신 암호키(CK_1)로부터 생성한 통신 암호키(CK_2)를 공유하게 된다.

[0036] 도 4에는, n+1회의 통신이 이루어져, 보안 통신 노드 #1과 보안 통신 노드 #2가 통신 암호키(CK_{n+1})를 공유하고 있는 상황을 도시하였다.

[0037] 한편, 전송된 데이터가 유실되면, 보안 통신 노드 #1과 보안 통신 노드 #2는 통신 암호키를 공유할 수 없어, 데이터 복호화에 실패하게 된다. 이를 위해, 보안 통신 노드 #1과 보안 통신 노드 #2는 과거에 생성&사용하였던 통신 암호키들도 일정량을 보유한다.

[0038] 이에, 데이터 복호화에 실패한 수신 노드가 송신 노드에게 복호 실패를 통보하면, 송신 노드는 바로 이전에 생성&사용하였던 통신 암호키로 데이터를 암호화하여 다시 전송한다.

[0039] 만약, 전송된 데이터의 유실이 2회이면, 수신 노드는 다시 전송된 데이터에 대해서도 복호화에 실패한다. 이 경우, 송신 노드는 그 이전에 생성&사용하였던 통신 암호키로 데이터를 다시 암호화하여 다시 전송한다.

[0040] 데이터 유실에 의해 통신 암호키의 공유가 불가능해지는 사태를 방지하기 위해, 도 5에 도시된 바와 같이, 보안 통신 노드 #1과 보안 통신 노드 #2는 최근 생성한 8개의 통신 암호키(CK_{n+1}~CK_{n-6})와 최초 통신 암호키(CK_0)를 보유한다.

[0041] 최초 통신 암호키(CK_0)를 보유하는 것은 8회 이상의 데이터 유실이 발생한 경우를 대비하기 위해 8개 이상의 통

신 암호키를 보유하는 것을 회피하기 위함이다.

[0042] 이전의 통신 암호키들을 이용하여 통신하였음에도 불구하고, 8회 이상의 데이터 유실에 의해 복호화에 모두 실패한 경우, 송신 노드는 최초 통신 암호키(CK_0)로 데이터를 암호화하여 전송한다. 수신 노드는 최초 통신 암호키(CK_0)를 보유하고 있으므로, 데이터 복호화가 가능하다.

[0043] 도 6은 본 발명의 실시예에 따른 경량 암복호화 방법이 적용가능한 차량 네트워크를 예시하였다. 본 발명의 실시예에 따른 경량 암복호화 방법은, 차량 네트워크를 구성하는 다수의 ECU들 간의 보안 통신에 적용가능하다.

[0044] 또한, 본 발명의 실시예에 따른 경량 암복호화 방법은, IoT 디바이스들 간의 보안 통신에도 적용가능하다. 나아가, 그 밖의 다른 네트워크에서 노드들 간의 보안 통신에 대해, 본 발명의 기술적 사상이 제한 없이 폭넓게 적용가능하다.

[0045] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

[0046] SK : 대칭키

RN : 랜덤값

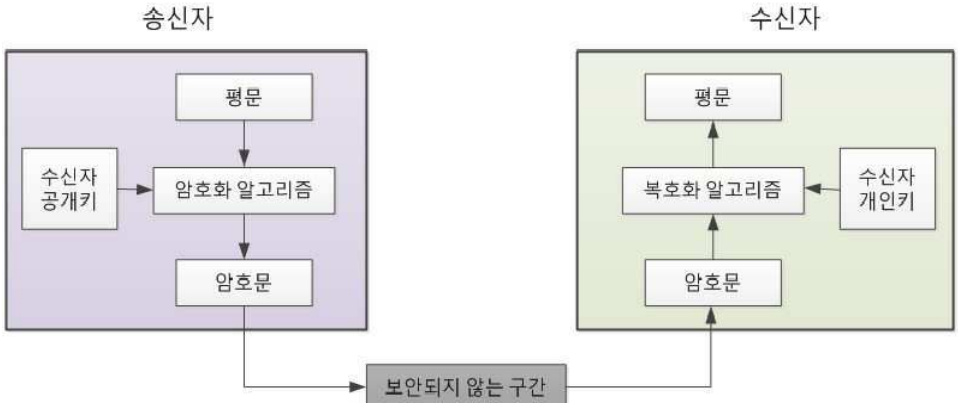
HASH : 해쉬 알고리즘

CK : 통신 암호키

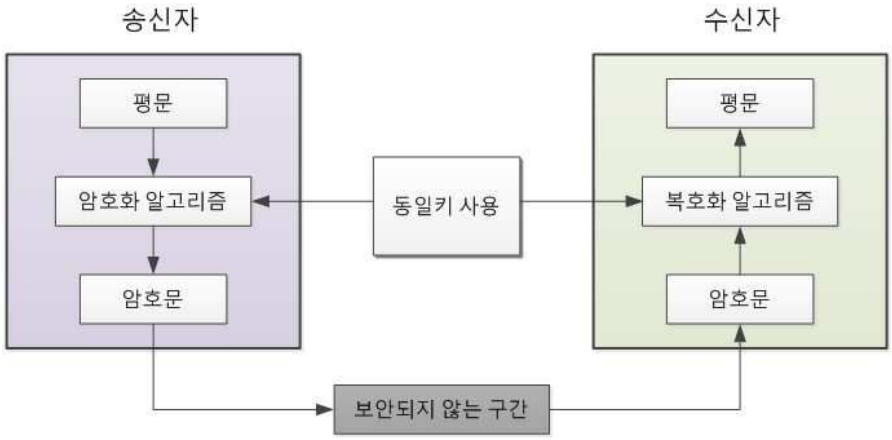
DATA : 전송 데이터

도면

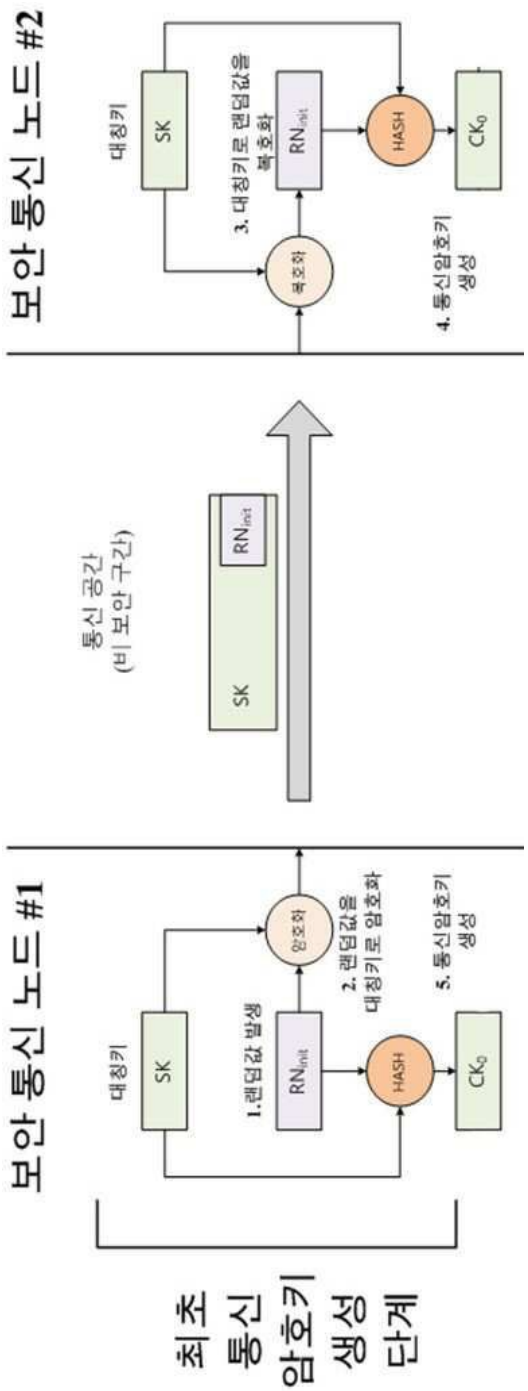
도면1



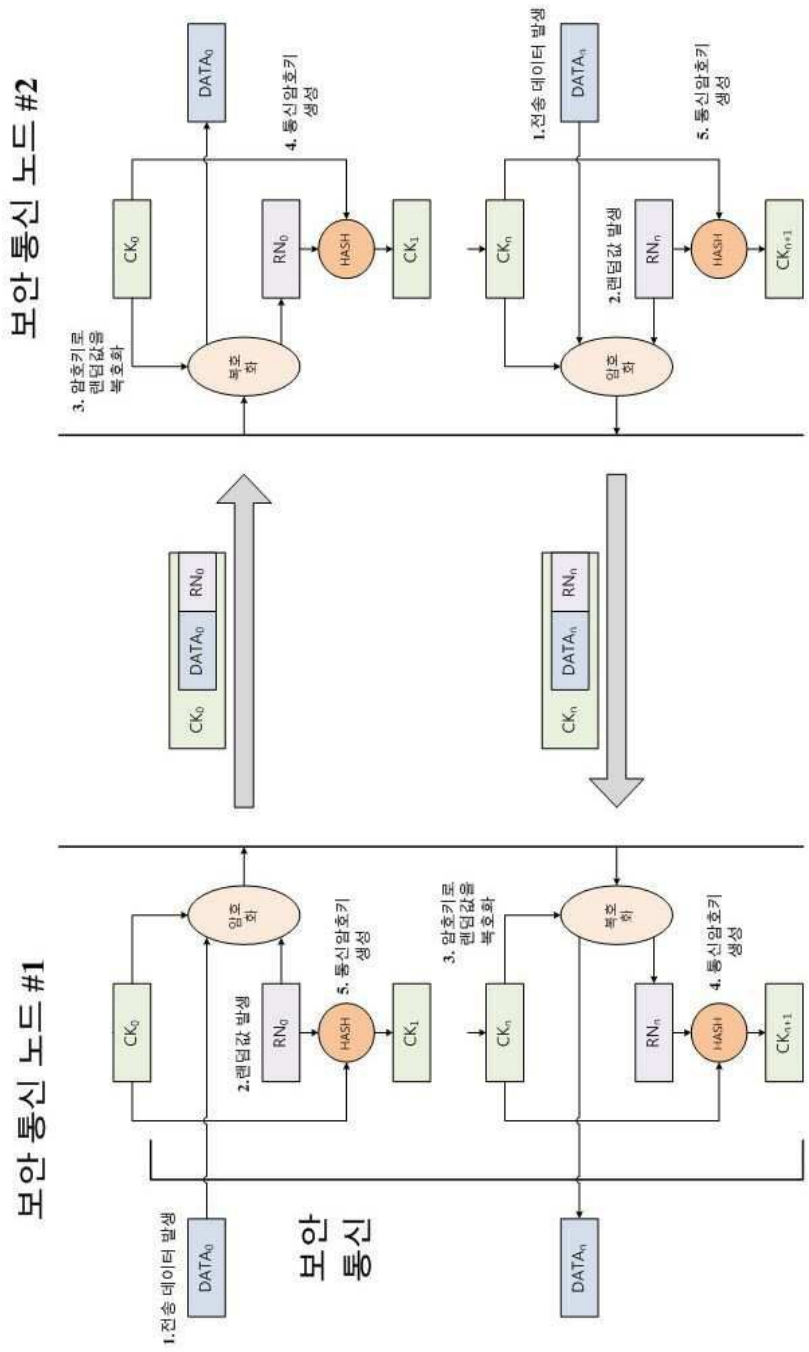
도면2



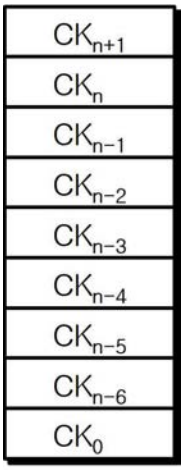
도면3


보안 통신 노드 #2
대칭키
SK
3. 대칭키로 랜덤값을 복호화
RNinit
HASH
CK0
복호화
4. 통신암호키 생성
통신 공간
(비 보안 구간)
SK
RNinit
보안 통신 노드 #1
대칭키
SK
1.랜덤값 발생
RNinit
암호화
2. 랜덤값을 대칭키로 암호화
HASH
CK0
3. 통신암호키 생성
최초 통신 암호키 생성 단계

도면4


보안 통신 노드 #2
보안 통신 노드 #1
보안 통신
1.전송 데이터 발생
2.랜덤값 발생
3. 암호키로 랜덤값을 복호화
4. 통신암호키 생성
5. 통신암호키 생성
암호화
복호화
HASH

도면5



도면6