(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0021157
(43) 공개일자 2013년03월05일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/14* (2006.01)
(21) 출원번호 10-2011-0083515
(22) 출원일자 2011년08월22일
심사청구일자 2011년08월22일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가 1
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침3단지 아파트 1404호 (내수동)
조효진
서울특별시 동대문구 안암로22길 25 (제기동)
(뒷면에 계속)
(74) 대리인
특허법인충현

전체 청구항 수 : 총 11 항

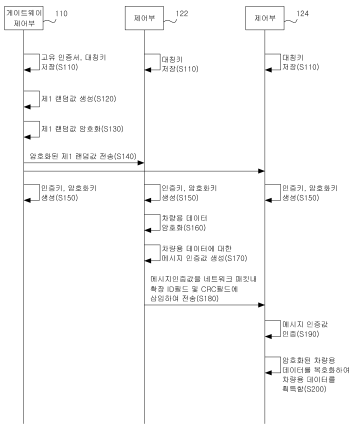
(54) 발명의 명칭 **차량용 데이터의 인증 및 획득 방법 및 시스템**

(57) 요 약

본 발명은 차량용 데이터의 인증 및 획득 방법 및 시스템에 관한 것으로, 보다 구체적으로는 차량 내 구비되는 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 상호 송수신하는 차량용 데이터의 인증 및 획득 방법은 게이트웨이 제어부가 고유 인증서를 저장하고, 상기 게이트웨이 제어부 및 상기 차량 내 구비되는 적어도 하나의 제어부가 상호 동일한 대칭키를 저장하는 대칭키저장단계; 상기 게이트웨이 제어부가 제1랜덤값을 생성하고, 생성한 상기 제1랜덤값을 상기 대칭키를 이용하여 암호화하고, 암호화된 상기 제1랜덤값을 상기 차량 내 구비되는 적어도 하나의 제어부로 전송하며, 상기 게이트웨이 제어부 및 암호화된 상기 제1랜덤값을 수신한 상기 제어부가 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하는 대칭키교환단계; 상기 제어부가 전송하고자 하는 상기 차량용 데이터를 암호화하고, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송하는 데이터전송단계; 및 상기 네트워크 패킷을 수신한 제어부가 상기 네트워크 패킷 내 상기 메시지인증값을 상기 인증키를 이용하여 인증한 후, 암호화된 차량용 데이터를 상기 암호화키를 이용하여 복호화한 후 상기 차량용 데이터를 획득하는 데이터수신단계;를 포함한다.

이러한 구성에 의해, 본 발명의 차량용 데이터의 인증 및 획득 방법 및 시스템은 차량 내 제어부간의 네트워크를 통한 차량용 데이터 송수신 시, 상기 차량용 데이터의 인증값을 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 나누어 삽입한 후 네트워크 통신을 수행함으로써, 차량용 데이터에 대한 인증값을 차량 내 제어부로 효율적으로 송수신할 수 있는 효과가 있다.

대 표 도 - 도1



(72) 발명자

우사무엘

서울특별시 송파구 오금로53길 7, 명산주택 403호 (거여동)

조아람

서울특별시 노원구 섬밭로 123, 3단지 아파트 301동 1507호 (공릉동)

이 발명을 지원한 국가연구개발사업

과제고유번호	KI002113201103100110013918KI002113201103
부처명	한국산업기술평가관리원
연구사업명	산업원천기술개발사업
연구과제명	Car-헬스케어 보안 기술개발
주관기관	고려대학교 산학협력단
연구기간	2011.03.01 ~ 2012.02.29

특허청구의 범위

청구항 1

차량 내 구비되는 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 상호 송수신하는 차량용 데이터의 인증 및 획득 방법에 있어서,

게이트웨이 제어부가 고유 인증서를 저장하고, 상기 게이트웨이 제어부 및 상기 차량 내 구비되는 적어도 하나의 제어부가 상호 동일한 대칭키를 저장하는 대칭키저장단계;

상기 게이트웨이 제어부가 제1랜덤값을 생성하고, 생성한 상기 제1랜덤값을 상기 대칭키를 이용하여 암호화하고, 암호화된 상기 제1랜덤값을 상기 차량 내 구비되는 적어도 하나의 제어부로 전송하며, 상기 게이트웨이 제어부 및 암호화된 상기 제1랜덤값을 수신한 상기 제어부가 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하는 대칭키교환단계;

상기 제어부가 전송하고자 하는 상기 차량용 데이터를 암호화하고, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송하는 데이터전송단계; 및

상기 네트워크 패킷을 수신한 제어부가 상기 네트워크 패킷 내 상기 메시지인증값을 상기 인증키를 이용하여 인증한 후, 암호화된 차량용 데이터를 상기 암호화키를 이용하여 복호화한 후 상기 차량용 데이터를 획득하는 데이터수신단계;

를 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 2

제1항에 있어서,

상기 데이터전송단계는

상기 제어부가 상기 메시지인증값을 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 각각 나누어 삽입하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 3

제1항에 있어서,

상기 데이터전송단계는

상기 차량용 데이터를 전송하고자 하는 상기 제어부가 기저장된 자신의 카운터값을 초기화한 후 해시하여, 해시한 값을 상기 차량용 데이터와 배타적연산을 수행하고, 이에 따라 가공메시지를 생성한 후, 생성된 가공메시지를 상기 암호화키를 이용하여 암호화하는 메시지암호화과정;

상기 제어부가 상기 인증키를 이용하여 암호화된 상기 가공메시지에 대한 메시지인증값을 생성하는 메시지인증값생성과정; 및

상기 제어부가 상기 메시지인증값을 상기 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 동일한 크기로 각각 나누어 삽입하고, 암호화된 상기 가공메시지를 포함하는 상기 네트워크 패킷을 차량 내 네트워크를 통해 전송하는 데이터전송과정;

을 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 4

제1항에 있어서,

상기 데이터수신단계는

상기 네트워크 패킷을 수신한 제어부가 상기 인증키를 이용하여 수신한 네트워크 패킷 내 포함된 메시지인증값을 인증하는 인증과정;

상기 제어부가 상기 네트워크 패킷 내 포함된 암호화된 가공메시지를 상기 암호화키를 이용하여 복호화하는 가공메시지복호화과정; 및

상기 제어부가 기저장된 카운터값을 해시한 후, 해시한 값과 복호화된 가공메시지간에 배타적연산을 수행하여 차량용 데이터를 획득하는 데이터획득과정;

을 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 5

제1항에 있어서,

상기 대칭키저장단계는

정비진단부가 자신의 고유 인증서를 저장하는 것을 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 6

제5항에 있어서,

상기 대칭키교환단계 수행 후 상기 데이터전송단계 수행 전,

상기 게이트웨이 제어부 및 정비진단부가 기저장된 고유 인증서를 상호 교환하고, 상기 게이트웨이 제어부가 상기 인증키 및 암호화키를 암호화하여 상기 정비진단부로 전송하는 키전송단계;

를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 7

제6항에 있어서,

상기 데이터수신단계는

상기 네트워크 패킷을 수신한 상기 정비진단부가 상기 네트워크 패킷 내 상기 메시지인증값을 상기 인증키를 이용하여 인증한 후, 암호화된 상기 차량용 데이터를 상기 암호화키를 이용하여 복호화하여 상기 차량용 데이터를 획득하는 것을 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 따른 방법을 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체.

청구항 9

차량 내 구비되는 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 상호 송수신하는 차량용 데이터의 인증 및 획득 시스템에 있어서,

고유의 인증서와 및 대칭키를 저장하고, 제1랜덤값을 생성하며, 상기 대칭키를 이용하여 상기 제1랜덤값을 암호화하고, 암호화된 상기 제1랜덤값을 전송하며, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하는 게이트웨이 제어부; 및

상기 대칭키를 저장하고, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하고, 상기 차량용 데이터를 암호화한 후, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송하며, 상기 네트워크 패킷 내 상기 메시지인증값을 인증한 후, 암호화된 차량용 데이터를 복호화하여 상기 차량용 데이터를 획득하는 적어도 하나의 제어부;

를 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 시스템.

청구항 10

제9항에 있어서,

상기 제어부는

상기 메시지인증값을 상기 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 각각 나누어 삽입하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 시스템.

청구항 11

제9항에 있어서,

고유의 인증서를 저장하고, 저장한 상기 고유의 인증서를 상기 게이트웨이 제어부와 상호 교환하며, 상기 게이트웨이 제어부로부터 암호화된 상기 인증키와 암호화키를 수신하고, 상기 제어부로부터 상기 네트워크 패킷을 수신한 후, 수신한 상기 인증키 및 암호화키를 이용하여 수신한 상기 네트워크 패킷 내 차량용 데이터를 획득하는 정비진단부;

를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 차량용 데이터의 인증 및 획득 방법 및 시스템에 관한 것으로, 특히 차량 내 구비되는 적어도 하나의 제어부간 상호 송수신되는 차량용 데이터를 용이하게 인증하고, 획득할 수 있는 차량용 데이터의 인증 및 획득 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 최근 들어, IT기술의 급속한 발전에 따라, 자동차분야는 현재 기술의 안전성, 편의성, 정보성에 중점을 두고 발전하고 있는 추세이다. 이러한 추세에 따라 차량 내 전자제어장치인 ECU(Electronic Control Unit)의 구비가 점차 증가되고 있다. 이러한 ECU는 엔진구동, 제동장치, 조향장치, 에어백과 같은 안전장치, 오디오 또는 에어컨과 같은 편의장치 등을 제어하는 제어장치를 말한다. 이처럼, 다양한 부분에서 사용되는 다수의 ECU는 차량의 내부에서 사용되는 프로토콜을 이용하여 상호간 통신을 수행한다. 이때, 사용되는 프로토콜은 CAN(Controller Area Network), LIN(Local Interconnect Network), FlexRay, MOST(Media Oriented Systems Transport)가 있으며, 이중에서도 CAN 프로토콜이 차량에서 주로 사용되고 있다. 이러한 CAN 프로토콜은 한 쌍의 꼬임선으로 구성됨에 따라, 물리적인 특징으로 인하여 외부 전자파나 노이즈에 강한 장점을 가질 뿐만 아니라, 브로드캐스트 통신방식을 사용하므로 차량 환경에 매우 적합한 특징을 갖는다.

[0003] 하지만 이러한 CAN 프로토콜을 이용한 통신방식은 브로드캐스트 통신을 사용하기 때문에, 외부에서 네트워크를

도청하기가 용이하고, 송수신되는 메시지를 인증할 수 있는 체계가 없다는 문제점이 있다. 뿐만 아니라, 상기 CAN 프로토콜은 송수신되는 메시지를 암호화하지 않기 때문에, 상기 메시지가 송수신과정에서 위조 또는 변조되는 것을 방지하기 어려우며, 외부 공격자가 도청하여 획득한 메시지를 그대로 ECU로 재전송하는 메시지 재전송 공격 또한 방지하기 어려운 문제점이 발생했다.

[0004] 이와 같은 문제점을 해결하고자 메시지인증코드(MAC, Message Authetication Code)를 사용함으로써, 네트워크를 통해 송수신되는 메시지를 보호하고 있다.

[0005] 하지만, 이처럼 메시지인증코드를 사용하여 메시지를 보호하는 경우, 상기 메시지의 프레임 내 사용가능한 여분의 프레임이 없으며, 상기 메시지를 암호화하는 경우, 차량정비소 내 진단장비가 암호화된 상기 메시지로부터 차량 내 각 ECU가 획득한 차량용 데이터를 획득하여 차량의 상태를 용이하게 파악하기 어렵다는 문제점이 발생했다.

[0006] 상술한 바와 같이, 차량용 데이터의 인증 및 획득에 대한 선행기술을 살펴보면 다음과 같다.

[0007] 선행기술 1은 한국공개특허공보 제2008-0023056호(2008.03.12)로서, 차량 진단 정보 송신장치 및 그 방법에 관한 것이다. 이러한 선행기술 1은 차량의 전자제어유닛(ECU)으로부터 각종 부품의 상태정보를 수집하고, 수집한 상태정보를 기초로 차량의 이상 상태 여부를 파악하며, 라디오 주파수 송신부는 파악된 이상 상태 여부를 차량 내에 탑재된 라디오의 수신 주파수 전 범위에 대하여 전송함으로써, 차량 진단정보를 운전자에게 알려준다.

[0008] 또한, 선행기술 2는 한국공개특허공보 제2003-0039180호(2003.05.17)로서, 자동차의 고장상태 진단장치에 관한 것이다. 이러한 선행기술 2는 자동차의 ECU와 연결되는 커넥터를 통하여 자동차의 고장정보를 입력받아 처리하는 주제어부와, 상기 커넥터를 통하여 입력되는 각종 데이터를 저장하는 메모리부와, 상기 메모리부에 저장된 데이터를 연산하여 고장 상태에 따른 신호를 출력하는 출력부와, 상기 각 부분에 전원을 공급하는 전원부를 포함하여 자동차의 고장 데이터를 제공한다.

발명의 내용

해결하려는 과제

[0009] 상기와 같은 종래 기술의 문제점을 해결하기 위해, 본 발명은 차량 내 구비되는 다수의 제어부간의 네트워크 통신 시, 송수신 되는 차량용 데이터의 인증 및 획득을 용이하게 수행하는 차량용 데이터의 인증 및 획득 방법 및 시스템을 제공하고자 한다.

과제의 해결 수단

[0010] 위와 같은 과제를 해결하기 위한 본 발명의 한 실시 예에 따른 차량 내 구비되는 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 상호 송수신하는 차량용 데이터의 인증 및 획득 방법은 게이트웨이 제어부가 고유 인증서를 저장하고, 상기 게이트웨이 제어부 및 상기 차량 내 구비되는 적어도 하나의 제어부가 상호 동일한 대칭키를 저장하는 대칭키저장단계; 상기 게이트웨이 제어부가 제1랜덤값을 생성하고, 생성한 상기 제1랜덤값을 상기 대칭키를 이용하여 암호화하고, 암호화된 상기 제1랜덤값을 상기 차량 내 구비되는 적어도 하나의 제어부로 전송하며, 상기 게이트웨이 제어부 및 암호화된 상기 제1랜덤값을 수신한 상기 제어부가 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하는 대칭키교환단계; 상기 제어부가 전송하고자 하는 상기 차량용 데이터를 암호화하고, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송하는 데이터전송단계; 및 상기 네트워크 패킷을 수신한 제어부가 상기 네트워크 패킷 내 상기 메시지인증값을 상기 인증키를 이용하여 인증한 후, 암호화된 차량용 데이터를 상기 암호화키를 이용하여 복호화한 후 상기 차량용 데이터를 획득하는 데이터수신단계;를 포함하는 것을 특징으로 한다.

[0011] 보다 바람직하게는 상기 제어부가 상기 메시지인증값을 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 각각 나누어 삽입하는 데이터전송단계를 포함할 수 있다.

[0012] 보다 바람직하게는 상기 차량용 데이터를 전송하고자 하는 상기 제어부가 기저장된 자신의 카운터값을 초기화한 후 해시하여, 해시한 값을 상기 차량용 데이터와 배타적연산을 수행하고, 이에 따라 가공메시지를 생성한 후,

생성된 가공메시지를 상기 암호화키를 이용하여 암호화하는 메시지암호화과정; 상기 제어부가 상기 인증키를 이용하여 암호화된 상기 가공메시지에 대한 메시지인증값을 생성하는 메시지인증값생성과정; 및 상기 제어부가 상기 메시지인증값을 상기 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 동일한 크기로 각각 나누어 삽입하고, 암호화된 상기 가공메시지를 포함하는 상기 네트워크 패킷을 차량 내 네트워크를 통해 전송하는 데이터전송과정;을 포함하는 데이터전송단계를 포함할 수 있다.

[0013] 보다 바람직하게는 상기 네트워크 패킷을 수신한 제어부가 상기 인증키를 이용하여 수신한 네트워크 패킷 내 포함된 메시지인증값을 인증하는 인증과정; 상기 제어부가 상기 네트워크 패킷 내 포함된 암호화된 가공메시지를 상기 암호화키를 이용하여 복호화하는 가공메시지복호화과정; 및 상기 제어부가 기저장된 카운터값을 해시한 후, 해시한 값과 복호화된 가공메시지간에 배타적연산을 수행하여 차량용 데이터를 획득하는 데이터획득과정;을 포함하는 데이터수신단계를 포함할 수 있다.

[0014] 특히, 정비진단부가 자신의 고유 인증서를 저장하는 것을 더 포함하는 대칭키저장단계를 포함할 수 있다.

[0015] 보다 바람직하게는 상기 대칭키교환단계 수행 후 상기 데이터전송단계 수행 전, 상기 게이트웨이 제어부 및 정비진단부가 기저장된 고유 인증서를 상호 교환하고, 상기 게이트웨이 제어부가 상기 인증키 및 암호화키를 암호화하여 상기 정비진단부로 전송하는 키전송단계;를 더 포함할 수 있다.

[0016] 특히, 상기 네트워크 패킷을 수신한 상기 정비진단부가 상기 네트워크 패킷 내 상기 메시지인증값을 상기 인증키를 이용하여 인증한 후, 암호화된 상기 차량용 데이터를 상기 암호화키를 이용하여 복호화하여 상기 차량용 데이터를 획득하는 것을 더 포함하는 데이터수신단계를 포함할 수 있다.

[0017] 위와 같은 과제를 해결하기 위한 본 발명의 다른 실시 예에 따른 차량 내 구비되는 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 상호 송수신하는 차량용 데이터의 인증 및 획득 시스템은 고유의 인증서와 및 대칭키를 저장하고, 제1랜덤값을 생성하며, 상기 대칭키를 이용하여 상기 제1랜덤값을 암호화하고, 암호화된 상기 제1랜덤값을 전송하며, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하는 게이트웨이 제어부; 및 상기 대칭키를 저장하고, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하고, 상기 차량용 데이터를 암호화한 후, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송하며, 상기 네트워크 패킷 내 상기 메시지인증값을 인증한 후, 암호화된 차량용 데이터를 복호화하여 상기 차량용 데이터를 획득하는 적어도 하나의 제어부;를 포함하는 것을 특징으로 한다.

[0018] 특히, 상기 메시지인증값을 상기 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 각각 나누어 삽입하는 제어부를 포함할 수 있다.

[0019] 보다 바람직하게는 고유의 인증서를 저장하고, 저장한 상기 고유의 인증서를 상기 게이트웨이 제어부와 상호 교환하며, 상기 게이트웨이 제어부로부터 암호화된 상기 인증키와 암호화키를 수신하고, 상기 제어부로부터 상기 네트워크 패킷을 수신한 후, 수신한 상기 인증키 및 암호화키를 이용하여 수신한 상기 네트워크 패킷 내 차량용 데이터를 획득하는 정비진단부;를 더 포함할 수 있다.

발명의 효과

[0020] 본 발명의 차량용 데이터의 인증 및 획득 방법 및 시스템은 차량 내 제어부간의 네트워크를 통한 차량용 데이터 송수신 시, 상기 차량용 데이터의 인증값을 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 나누어 삽입한 후 네트워크 통신을 수행함으로써, 차량용 데이터에 대한 인증값을 차량 내 제어부로 효율적으로 송수신할 수 있는 효과가 있다.

[0021] 또한 차량용 데이터의 인증 및 획득 방법 및 시스템은 제어부가 네트워크를 통한 차량용 데이터의 송수신 시, 메시지인증값을 이용하여 상기 차량용 데이터를 인증함에 따라, 상기 차량용 데이터의 위변조를 방지할 수 있는 효과가 있다.

[0022] 더불어, 차량용 데이터의 인증 및 획득 방법 및 시스템은 차량의 외부에 위치하는 차량정비를 위한 정비진단부가 상기 제어부가 전송한 차량용 데이터를 수신하고, 상기 제어부와 공유하는 암호화키를 이용하여 암호화된 차량용 데이터를 용이하게 복호화함에 따라, 상기 차량의 외부에 존재하는 정비진단부가 별도의 장치없이 상기 차

량에 대한 차량용 데이터를 용이하게 획득하여, 상기 차량의 상태를 파악할 수 있는 효과가 있다.

도면의 간단한 설명

[0023] 도 1은 본 발명의 일 실시 예에 따른 차량용 데이터의 인증 및 획득 방법의 순서도이다.

도 2는 본 발명의 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 방법의 순서도이다.

도 3은 도 1 내지 도 2에서 사용되는 네트워크 패킷 구조를 나타낸 도면이다.

도 4는 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템의 블록도이다.

도 5는 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0024] 이하, 본 발명을 바람직한 실시 예와 첨부한 도면을 참고로 하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되는 것은 아니다.

[0025] 이하, 도 1을 참조하여, 본 발명의 차량용 데이터의 인증 및 획득 방법에 대하여 자세히 살펴보도록 한다.

[0026] 도 1은 본 발명의 일 실시 예에 따른 차량용 데이터의 인증 및 획득 방법의 순서도이다.

[0027] 도 1에 도시된 바와 같이, 본 발명의 차량용 데이터의 인증 및 획득 방법은 먼저, 게이트웨어 제어부(110)가 공인된 인증기관으로부터 발급받은 자신의 고유 인증서 및 해당 네트워크에 포함되는 모든 제어부와 공유하기 위한 대칭키 sk를 저장하며, 또한 차량 내 구비되는 모든 제어부(122, 124 …)가 상기 게이트웨이 제어부(110)가 저장한 대칭키 sk와 동일한 대칭키 sk를 각각 저장한다(S110).

[0028] 이어서, 상기 게이트웨이 제어부(110)는 추후 인증키 및 암호화키 생성 시 사용되는 제1랜덤값을 생성하고(S120), 앞서 기저장한 상기 대칭키 sk를 이용하여 상기 제1랜덤값을 암호화한다(S130). 이후, 상기 게이트웨이 제어부(110)는 암호화된 상기 제1랜덤값을 차량용 네트워크 내 연결된 모든 제어부(122, 124 …)로 전송한다(S140). 이때, 사용되는 상기 네트워크는 CAN(Controller Area Network), LIN(Local Interconnect Network), FlexRay, MOST(Media Oriented Systems Transport) 프로토콜을 사용하는 네트워크 중 하나일 수 있다.

[0029] 이후, 상기 암호화된 제1랜덤값을 수신한 상기 모든 제어부(122, 124 …) 및 상기 게이트웨이 제어부(110)는 상기 암호화된 제1랜덤값을 기저장한 대칭키 sk를 이용하여 복호화하고, 복호화된 상기 제1랜덤값을 이용하여 향후, 차량용 데이터의 인증 시 사용되는 인증키 AK 및 암호화키 EK를 각각 생성한다(S150).

[0030] 이어서, 자신이 획득한 차량용 데이터를 다른 제어부(124 …)로 전송하고자 하는 제어부(122)가 전송하고자 하는 차량용 데이터를 암호화한다(S160). 이러한 차량용 데이터의 암호화과정을 보다 자세히 살펴보면, 상기 차량용 데이터를 전송하고자 하는 제어부(122)가 자신의 카운터값 Count을 먼저 초기화한 후, 초기화된 자신의 카운터값을 해시하여 해시한 값 H(Count)을 생성한다. 이후, 상기 제어부(122)는 전송하고자 하는 차량용 데이터 m를 상기 해시한값과 배타적연산(Xor)을 수행하여 가공메시지 rm를 생성하고, 앞서 생성한 암호화키 EK를 이용하여 상기 가공메시지를 암호화한다.

[0031] 이어서, 상기 제어부(122)는 앞서 생성한 인증키 AK를 이용하여 상기 가공메시지 rm를 포함하는 네트워크 패킷에 대한 32bit 크기를 갖는 메시지인증값을 생성한다(S170). 이와 같이 생성된 상기 메시지인증값을 상기 네트워크 패킷 내 프레임 중 확장 ID필드 및 CRC필드에 각각 16bit씩 동일한 크기로 나누어 삽입한다. 이와 같이, 상기 메시지인증값이 확장 ID필드 및 CRC필드에 삽입된 상기 네트워크 패킷을 다른 제어부(124)로 전송한다(S180).

[0032] 이와 같이, 상기 가공메시지를 암호화하고, 상기 메시지인증값을 생성한 제어부(122)는 자신의 카운터 값 Count에 1을 증가시킨다.

[0033] 이와 같이, 상기 네트워크 패킷을 수신한 제어부(124)는 수신한 네트워크 패킷 내 ID필드를 확인한 후, 앞서 생성한 인증키 AK를 사용하여 상기 네트워크 패킷 내 포함된 메시지인증값을 인증한다(S190).

[0034] 이와 같이, 상기 메시지인증값의 인증이 완료되면, 상기 제어부(124)는 수신한 네트워크 패킷 내 암호화된 차량

용 데이터를 앞서 생성한 대칭키 sk를 이용해 복호화하여 가공메시지 rm를 획득하고, 획득한 상기 가공메시지 rm를 상기 제어부(124)의 카운터값 Count을 해시한 값 H(Count)과 배타적연산(Xor)을 수행하여 차량용 메시지 m를 획득한다(S200).

[0035] 이처럼, 차량용 데이터를 획득한 상기 제어부(124)는 자신의 카운터값 Count을 1을 증가시키고, 복호화된 상기 차량용데이터를 용이하게 확인한다.

[0036] 또는 상술한 바와 달리, 차량의 내부에 구비되는 제어부로 다른 제어부가 획득한 차량용 데이터가 전송되는 것이 아닌, 상기 차량의 외부에 존재하는 정비진단부로 상기 차량용 데이터를 전송하는 경우에 대하여 도 2를 참조하여 살펴보도록 한다.

[0037] 도 2는 본 발명의 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 방법의 순서도이다.

[0038] 도 2에 도시된 바와 같이, 본 발명의 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 방법은 먼저, 게이트웨이 제어부(210)와 차량용 데이터를 전송하고자 하는 제어부(222)간 수행되는 인증키 AK 및 암호화키 EK 생성 과정은 도 1을 통해 설명한 바와 동일하게 수행되므로, 이에 대한 설명은 생략하기로 한다.

[0039] 상기 게이트웨이 제어부(210) 및 제어부(222)가 인증키 AK 및 암호화키 EK를 생성한 후, 정비진단부(230)가 상기 게이트웨이 제어부(210)로 차량용 데이터의 전송을 요청한다(S260).

[0040] 이에 따라, 상기 게이트웨이 제어부(210)는 제2랜덤값을 생성하고, 암호화 생성그룹 내 제너레이터값을 생성한 후, 상기 제2랜덤값 및 제너레이터값에 대하여, 기저장된 자신의 서명키를 이용해 서명을 수행하고, 서명된 제2랜덤값 및 제너레이터값과, 자신의 고유한 인증서를 상기 정비진단부(230)로 전송한다.

[0041] 상기 게이트웨이 제어부(210)의 인증서를 수신한 상기 정비진단부(230)는 수신한 게이트웨이 제어부(210)의 인증서에 대한 유효성을 검증하고, 상기 게이트웨이 제어부(210)가 서명한 서명에 대하여 검증을 수행한다.

[0042] 이후, 상기 정비진단부(230)는 제3랜덤값을 생성하고, 상기 제2랜덤값, 제3랜덤값 및 제너레이터값을 포함하는 그룹세션키를 생성한다. 이에 따라, 상기 정비진단부(230)는 상기 제2랜덤값 및 제너레이터값과, 상기 제3랜덤값 및 제너레이터값에 대하여 자신의 서명키를 이용해 서명을 수행하고, 서명이 완료된 상기 제2랜덤값 및 제너레이터값과, 상기 제3랜덤값 및 제너레이터값과, 자신의 고유한 인증서를 상기 게이트웨이 제어부(210)로 전송한다(S280).

[0043] 이후, 상기 게이트웨이 제어부(210)는 상기 정비진단부(230)로부터 수신한 인증서에 대한 유효성을 검증한 후, 상기 제2랜덤값 및 제너레이터값과, 상기 제3랜덤값 및 제너레이터값에 대한 서명을 검증한다. 이에 따라, 상기 게이트웨이 제어부(210)는 상기 서명에 대한 검증을 완료한 후, 상기 제2랜덤값, 제3랜덤값 및 제너레이터값을 포함하는 그룹세션키를 생성한다.

[0044] 이에 따라, 상기 게이트웨이 제어부(210)는 생성한 그룹세션키를 이용하여 앞서 생성한 인증키 AK 및 암호화키 EK를 암호화한 후(S290), 이를 상기 정비진단부(230)로 전송한다(S300).

[0045] 이후, 상기 정비진단부(230)는 앞서 자신이 생성한 그룹세션키를 이용하여 상기 게이트웨이 제어부(210)로부터 수신한 암호화된 인증키 AK 및 암호화키 EK를 복호화하여, 인증키 및 암호화키를 획득한다(S310).

[0046] 이어서, 차량용 데이터를 송신하고자 하는 제어부(222)는 앞서 상기 도 1을 통해 기술한 바와 같이, 상기 차량용 데이터를 암호화하고, 상기 차량용 데이터를 포함하는 네트워크 패킷에 대한 메시지인증값을 생성한 후(S330), 생성한 메시지인증값을 전송하고자 하는 네트워크 패킷 내 확장 ID필드 및 CRC필드에 삽입하여 정비진단부(230)로 전송한다(S340).

[0047] 이와 같이, 상기 제어부(222)로부터 전송된 네트워크 패킷을 수신한 정비진단부(230)는 수신한 네트워크 패킷 내 ID필드를 확인한 후, 앞서 생성한 인증키를 사용하여 상기 네트워크 패킷 내 포함된 메시지인증값을 인증한다(S350).

[0048] 이와 같이, 상기 정비진단부(230)가 상기 메시지인증값의 인증을 완료하면, 수신한 네트워크 패킷 내 암호화된 차량용 데이터를 앞서 생성한 대칭키를 이용해 복호화하여, 가공메시지 rm를 획득하고, 획득한 상기 가공메시지 rm를, 상기 정비진단부(230)의 자신의 카운터값 count을 해시한 값 H(Count)과 배타적연산(Xor)을 수행하여 차량용 데이터 m를 획득한다(S360).

[0049] 이처럼, 차량용 데이터를 획득한 상기 정비진단부(230)는 자신의 카운터값 Count을 1을 증가시키고, 획득한 상

기 차량용데이터에 대한 분석을 수행한다.

[0050] 결국, 차량의 외부에 존재하는 정비진단부(230)가 차량 내부에 구비되는 제어부(222)로부터 차량용 프로토콜을 사용하는 네트워크 내 통신을 통해 차량용 데이터를 전송받아, 이를 용이하게 분석할 수 있도록 한다.

[0051] 또한, 이러한 차량용 데이터의 인증 및 획득 방법은 컴퓨터로 실행하기 위한 프로그램이 기록된 컴퓨터 판독가능 기록매체에 저장될 수 있다. 이때, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0052] 이하, 도 3을 참조하여 송수신되는 네트워크 패킷의 구조에 대하여 보다 자세히 살펴보도록 한다.

[0053] 도 3은 도 1 내지 도 2에서 사용되는 네트워크 패킷 구조를 나타낸 도면이다.

[0054] 도 3에 도시된 바와 같이, 자신이 획득한 차량용 데이터를 전송하고자 하는 제어부가 상기 차량용 데이터를 포함하는 가공메시지를 암호화키를 이용하여 암호화함으로써, 32bit 크기를 갖는 메시지인증값을 생성한다.

[0055] 상기 제어부는 이와 같이 생성한 메시지인증값을 전송하고자 하는 네트워크 패킷 내 18비트의 크기를 갖는 확장ID필드 중 16비트에 일부를 삽입하고, 나머지 16비트는 CRC필드에 삽입한 후, 상기 메시지인증값이 삽입된 상기 네트워크 패킷을 전송하고자 하는 제어부 또는 정비진단부로 전송한다.

[0056] 이에 따라, 제어부가 전송하고자 하는 차량용 데이터에 대한 메시지인증값이 전송되는 네트워크 패킷 내 프레임에 삽입되어 전송됨에 따라, 상기 네트워크 패킷을 효율적으로 사용할 수 있다.

[0057] 도 4는 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템의 블록도이다.

[0058] 도 4에 도시된 바와 같이, 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템은 게이트웨이 제어부(110) 및 적어도 하나의 제어부(122, 124 126, 128 …)를 포함한다.

[0059] 게이트웨이 제어부(110)는 고유의 인증서와 및 대칭키를 저장하고, 제1랜덤값을 생성하며, 상기 대칭키를 이용하여 상기 제1랜덤값을 암호화하고, 암호화된 상기 제1랜덤값을 전송하며, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성한다.

[0060] 제어부(122)는 상기 게이트웨이 제어부(110)가 저장한 대칭키와 동일한 대칭키를 저장하고, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하고, 상기 차량용 데이터를 암호화한 후, 상기 인증키를 이용하여 암호화된 차량용 데이터에 대한 메시지인증값을 생성하고, 상기 메시지인증값을 네트워크 패킷 내 적어도 하나의 필드에 삽입하여 전송한다. 이때, 상기 제어부(122)는 상기 메시지인증값을 상기 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 동일한 크기로 각각 나누어 삽입한 후, 전송하는 것이 바람직하다.

[0061] 또한 상기 제어부(122)로부터 네트워크 패킷을 수신한 다른 제어부(124, 126, 128)는 상기 게이트웨이 제어부(110)가 저장한 대칭키와 동일한 대칭키를 저장하고, 암호화된 상기 제1랜덤값에 기초하여 차량용 데이터를 암호화하기 위한 인증키 및 암호화키를 생성하며, 상기 네트워크 패킷 내 상기 메시지인증값을 인증한 후, 암호화된 차량용 데이터를 복호화하여 상기 차량용 데이터를 획득한다.

[0062] 이와 같이, 차량용 데이터를 전송하거나, 수신하는 제어부(122, 124, 126, 128)는 그 상황에 따라 차량용 데이터의 전송과 수신이 상호 변경가능한 것은 당연하다.

[0063] 또는 이외에도, 제어부가 상기 차량용 데이터를 차량의 외부에 존재하는 정비진단부로 전송하는 경우도 발생한다.

[0064] 도 5는 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템의 블록도이다.

[0065] 도 5에 도시된 바와 같이, 본 발명의 또 다른 실시 예에 따른 차량용 데이터의 인증 및 획득 시스템은 앞서 도 4를 통해 설명한 게이트웨이 제어부(210)와 제어부(222, 224, 226, 228) 외에 정비진단부(230)를 더 포함한다.

[0066] 상기 게이트웨이 제어부(210) 및 차량용 데이터를 전송하는 제어부(222)에 대한 설명은 앞서 도 4를 통해 설명한 바와 동일하므로, 그 설명을 생략하도록 하며, 이하에서는 정비진단부(230)에 대하여 설명하도록 한다.

[0067] 정비진단부(230)는 자신의 고유 인증서를 저장하고, 저장한 상기 고유의 인증서를 상기 게이트웨이 제어부(210)와 상호 교환하며, 상기 게이트웨이 제어부(210)로부터 암호화된 상기 인증키와 암호화키를 수신하고, 제어부(222)로부터 상기 네트워크 패킷을 수신한 후, 수신한 상기 인증키 및 암호화키를 이용하여 수신한 상기 네트워크 패킷 내 차량용 데이터를 획득한다.

[0068] 이와 같이, 상기 정비진단부(230)가 차량의 내외부에 구비되는 위치와 상관없이 동일한 프로토콜을 통해 네트워크 통신을 수행한다면, 상기 정비진단부(230)는 차량용 데이터를 용이하게 획득할 수 있다.

[0069] 본 발명의 차량용 데이터의 인증 및 획득 방법 및 시스템은 차량 내 제어부간의 네트워크를 통한 차량용 데이터 송수신 시, 상기 차량용 데이터의 인증값을 네트워크 패킷 내 확장ID 필드 및 CRC 필드에 나누어 삽입한 후 네트워크 통신을 수행함으로써, 차량용 데이터에 대한 인증값을 차량 내 제어부로 효율적으로 송수신할 수 있는 효과가 있다.

[0070] 또한 차량용 데이터의 인증 및 획득 방법 및 시스템은 제어부가 네트워크를 통한 차량용 데이터의 송수신 시, 메시지인증값을 이용하여 상기 차량용 데이터를 인증함에 따라, 상기 차량용 데이터의 위변조를 방지할 수 있는 효과가 있다.

[0071] 더불어, 차량용 데이터의 인증 및 획득 방법 및 시스템은 차량의 외부에 위치하는 차량정비를 위한 정비진단부가 상기 제어부가 전송한 차량용 데이터를 수신하고, 상기 제어부와 공유하는 암호화키를 이용하여 암호화된 차량용 데이터를 용이하게 복호화함에 따라, 상기 차량의 외부에 존재하는 정비진단부가 별도의 장치없이 상기 차량에 대한 차량용 데이터를 용이하게 획득하여, 상기 차량의 상태를 파악할 수 있는 효과가 있다.

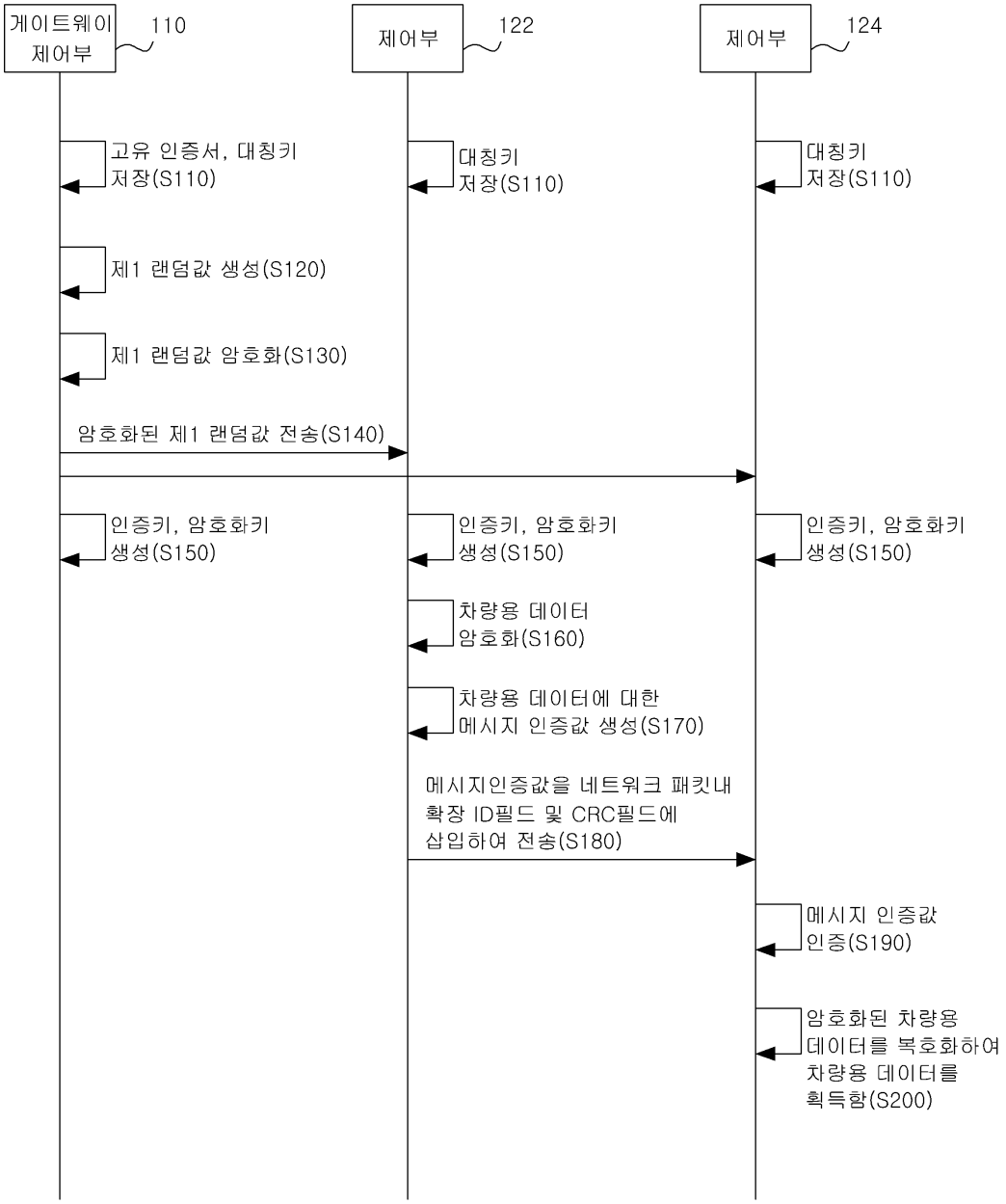
[0072] 상기에서는 본 발명의 바람직한 실시 예에 대하여 설명하였지만, 본 발명은 이에 한정되는 것이 아니고 본 발명의 기술 사상 범위 내에서 여러 가지로 변형하여 실시하는 것이 가능하고 이 또한 첨부된 특허청구범위에 속하는 것은 당연하다.

부호의 설명

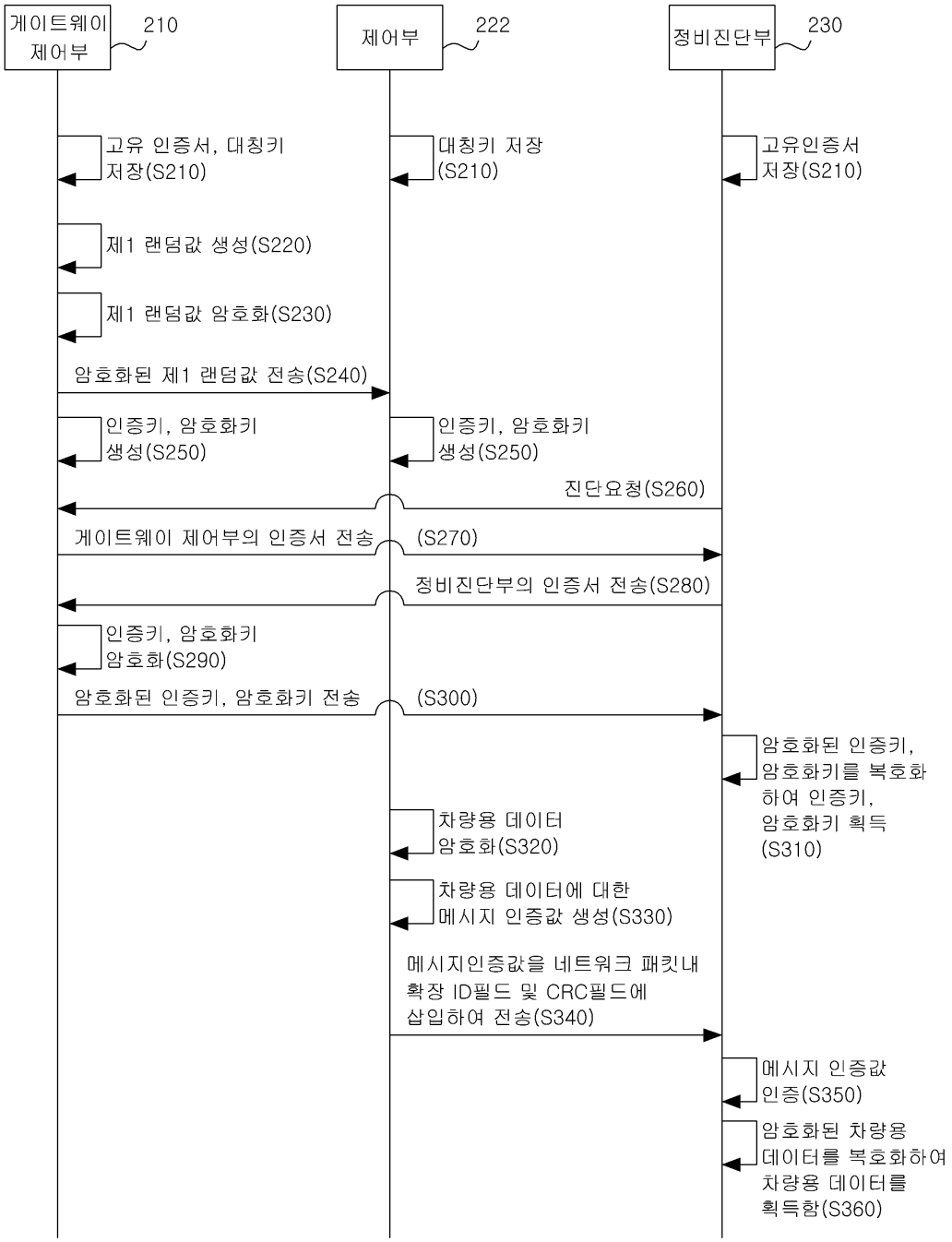
[0073] 110: 게이트웨이 제어부 122, 124, 126, 128: 제어부

도면

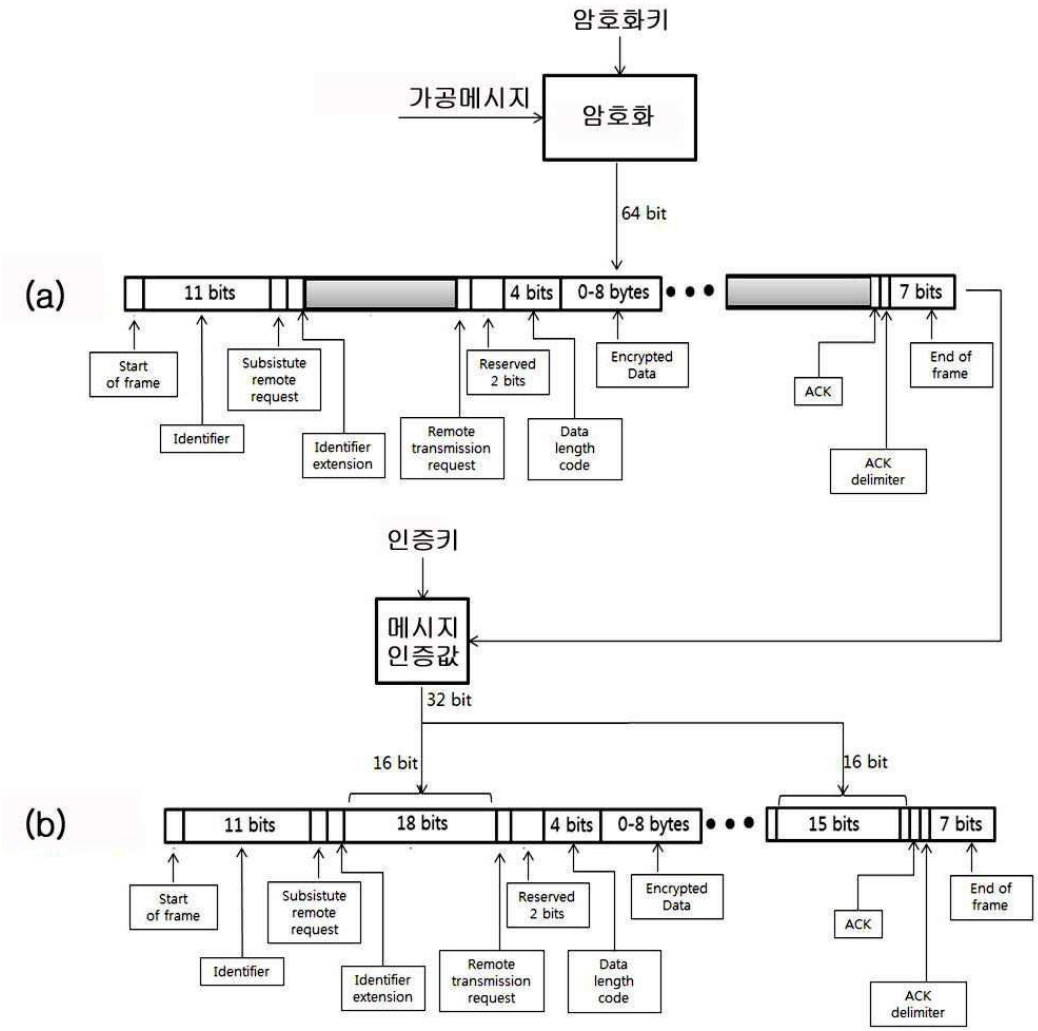
도면1


게이트웨이 제어부
110
제어부
122
제어부
124
고유 인증서, 대칭키 저장(S110)
대칭키 저장(S110)
대칭키 저장(S110)
제1 랜덤값 생성(S120)
제1 랜덤값 암호화(S130)
암호화된 제1 랜덤값 전송(S140)
인증키, 암호화키 생성(S150)
인증키, 암호화키 생성(S150)
인증키, 암호화키 생성(S150)
차량용 데이터 암호화(S160)
차량용 데이터에 대한 메시지 인증값 생성(S170)
메시지인증값을 네트워크 패킷내 확장 ID필드 및 CRC필드에 삽입하여 전송(S180)
메시지 인증값 인증(S190)
암호화된 차량용 데이터를 복호화하여 차량용 데이터를 획득함(S200)

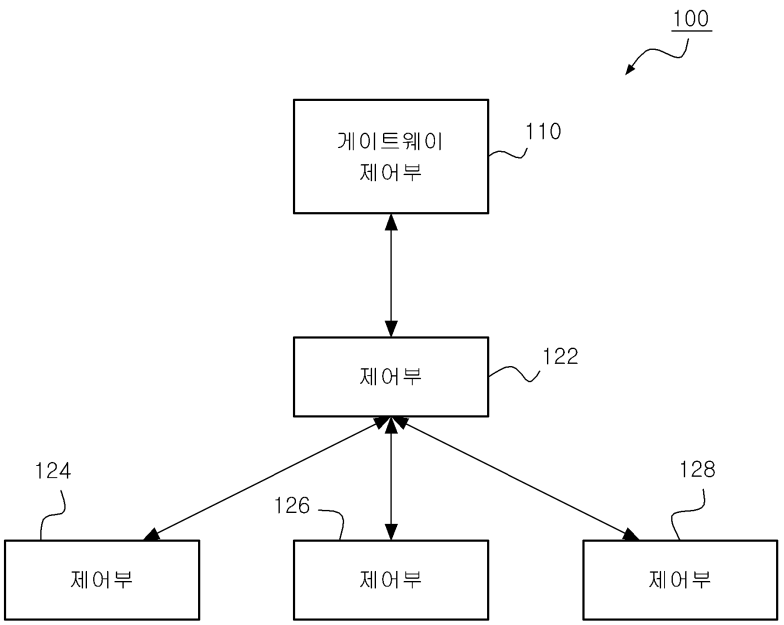
도면2


게이트웨이 제어부
210
제어부
222
정비진단부
230
고유 인증서, 대칭키 저장(S210)
대칭키 저장 (S210)
고유인증서 저장(S210)
제1 랜덤값 생성(S220)
제1 랜덤값 암호화(S230)
암호화된 제1 랜덤값 전송(S240)
인증키, 암호화키 생성(S250)
인증키, 암호화키 생성(S250)
진단요청(S260)
게이트웨이 제어부의 인증서 전송
(S270)
정비진단부의 인증서 전송(S280)
인증키, 암호화키 암호화(S290)
암호화된 인증키, 암호화키 전송
(S300)
암호화된 인증키, 암호화키를 복호화하여 인증키, 암호화키 획득 (S310)
차량용 데이터 암호화(S320)
차량용 데이터에 대한 메시지 인증값 생성(S330)
메시지인증값을 네트워크 패킷내 확장 ID필드 및 CRC필드에 삽입하여 전송(S340)
메시지 인증값 인증(S350)
암호화된 차량용 데이터를 복호화하여 차량용 데이터를 획득함(S360)

도면3


암호화키
가공메시지
암호화
64 bit
(a)
11 bits
4 bits
0-8 bytes
7 bits
Start of frame
Subsistute remote request
Identifier
Identifier extension
Reserved 2 bits
Remote transmission request
Data length code
Encrypted Data
ACK
ACK delimiter
End of frame
인증키
메시지 인증값
32 bit
16 bit
16 bit
(b)
11 bits
18 bits
4 bits
0-8 bytes
15 bits
7 bits
Start of frame
Subsistute remote request
Identifier
Identifier extension
Reserved 2 bits
Remote transmission request
Data length code
Encrypted Data
ACK
ACK delimiter
End of frame

도면4


100
게이트웨이 제어부
110
제어부
122
124
126
128
제어부
제어부
제어부

도면5