(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0024117
(43) 공개일자 2015년03월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2013-0101171
(22) 출원일자 2013년08월26일
심사청구일자 2013년08월26일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)
조효진
서울 동대문구 안암로22길 25, (제기동)
우사무엘
서울 송파구 오금로53길 7, 403호 (거여동)
(74) 대리인
특허법인충현

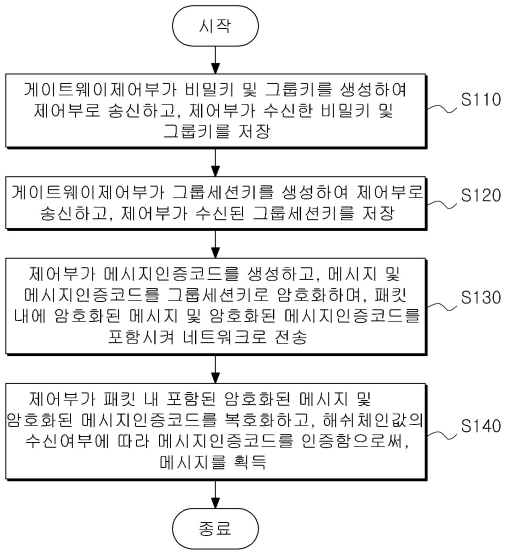
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **차량용 데이터의 인증 및 획득 방법**

(57) 요 약

차량용 데이터의 인증 및 획득 방법에 관한 것으로서, 게이트웨이제어부가 메시지의 인증에 사용되는 비밀키 및 키 암호화에 사용되는 그룹키를 생성하여 제어부로 송신하고, 제어부가 게이트웨이제어부로부터 수신된 비밀키 및 그룹키를 저장하고, 게이트웨이제어부가 그룹세션키를 생성하여 제어부로 송신하고, 제어부가 게이트웨이제어부로부터 수신된 그룹세션키를 저장하고, 제어부가 송신하고자 하는 메시지의 인증에 필요한 메시지인증코드를 생성하고, 송신하고자 하는 메시지 및 메시지인증코드를 그룹세션키로 암호화하며, 송신하고자 하는 패킷 내 암호화된 메시지 및 암호화된 메시지인증코드를 포함시켜 네트워크로 송신하며, 패킷을 수신한 제어부는 패킷 내 포함된 암호화된 메시지 및 암호화된 메시지인증코드를 복호화하고, 메시지에 대한 처리를 결정하는 해쉬체인값의 수신 여부에 따라 복호화된 메시지인증코드를 인증함으로써, 메시지를 획득한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 G01201303010003
부처명 지식경제부
연구관리전문기관 한국산업기술평가관리원
연구사업명 산업원천기술개발사업
연구과제명 Car-헬스케어 보안 기술개발
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2013.03.01 ~ 2014.02.28

특허청구의 범위

청구항 1

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

게이트웨이제어부가 메시지의 인증 사용되는 비밀키 및 키 암호화에 사용되는 그룹키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 비밀키 및 상기 그룹키를 저장하는 단계;

상기 게이트웨이제어부가 그룹세션키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 그룹세션키를 저장하는 단계;

상기 제어부가 송신하고자 하는 메시지의 인증에 필요한 메시지인증코드(Message Authentication Code)를 생성하고, 송신하고자 하는 메시지 및 상기 메시지인증코드를 상기 그룹세션키로 암호화하며, 송신하고자 하는 패킷 내 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 포함시켜 네트워크로 송신하는 단계; 및

상기 패킷을 수신한 제어부는 상기 패킷 내 포함된 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 복호화하고, 상기 메시지에 대한 처리를 결정하는 해쉬체인(hash chain)값의 수신 여부에 따라 상기 복호화된 메시지인증코드를 인증함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 2

제 1 항에 있어서,

상기 비밀키 및 상기 그룹키를 저장하는 단계 수행 전,

상기 게이트웨이제어부가 인증서를 상기 제어부에 전송하고, 상기 제어부는 수신된 인증서를 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 3

제 1 항에 있어서,

상기 비밀키 및 상기 그룹키를 저장하는 단계는,

상기 게이트웨이제어부 및 상기 제어부가 상기 메시지에 대한 인증을 나타내는 카운터의 초기값을 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 4

제 1 항에 있어서,

상기 네트워크는,

CAN(Controller Area Network) 프로토콜을 사용하며, 브로드캐스트(boradcast) 통신함으로써, 상기 제어부가 상기 메시지를 네트워크로 송신할 경우, 상기 네트워크에 연결된 게이트웨이제어부를 포함하는 모든 제어부로 상기 메시지가 송신되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 5

제 1 항에 있어서,

상기 메시지인증코드는 상기 패킷 내의 CRC필드 및 확장필드에 포함되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 6

제 1 항에 있어서,

상기 그룹세션키를 저장하는 단계는,

상기 게이트웨이제어부가 상기 해쉬체인값 및 상기 그룹세션키를 생성하여 상기 그룹키로 암호화하는 단계;

상기 게이트웨이제어부가 상기 암호화된 해쉬체인값 및 상기 암호화된 그룹세션키를 자신의 개인키로 서명하고, 상기 서명된 해쉬체인값 및 상기 서명된 그룹세션키를 상기 제어부로 송신하는 단계; 및

상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 서명된 해쉬체인값 및 상기 서명된 그룹세션키를 공개키를 통해 검증하며, 상기 검증된 해쉬체인값 및 상기 검증된 그룹세션키를 상기 그룹키를 통해 복호화함으로써, 상기 복호화된 해쉬체인값 및 상기 복호화된 그룹세션키를 획득하여 저장하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 7

제 6 항에 있어서,

상기 게이트웨이제어부는 상기 그룹세션키 및 상기 해쉬체인값을 소정의 키 업데이트 주기에 따라 갱신하며, 갱신된 상기 그룹세션키 및 상기 해쉬체인값을 상기 그룹키를 통해 암호화하여 네트워크로 송신하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 8

제 1 항에 있어서,

상기 네트워크로 송신하는 단계는,

메시지를 송신하고자 하는 상기 제어부가 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성하는 단계;

메시지를 송신하고자 하는 상기 제어부가 상기 인증키를 이용하여 송신하고자 하는 메시지의 메시지인증코드를 생성하는 단계;

메시지를 송신하고자 하는 상기 제어부가 상기 메시지 및 상기 메시지인증코드를 상기 그룹세션키로 암호화하는 단계; 및

메시지를 송신하고자 하는 상기 제어부가 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 송신하고자 하는 패킷 내에 포함하여 네트워크로 송신하는 단계를 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 9

제 8 항에 있어서,

상기 카운터값은,

게이트웨이제어부가 상기 인증키를 사용하여 메시지 인증에 성공할 때마다 1이 증가하고, 제어부가 상기 인증키를 생성할 때마다 1이 증가하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 10

제 1 항에 있어서,

상기 메시지를 획득하는 단계는,

상기 제어부가 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값이 수신되도록 대기하는 단계;

상기 게이트웨이제어부는 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성하며, 상기 인증키를 통해 상기 메시지인증코드를 인증하는 단계; 및

상기 제어부는 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값의 수신이 없을 경우 상기 메시지를 인증함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 11

제 10 항에 있어서,

상기 게이트웨이제어부가 상기 인증키를 통해 상기 메시지인증코드의 인증에 실패할 경우 상기 해쉬체인값을 상기 그룹세션키로 암호화하여 네트워크로 송신하는 단계;

상기 제어부가 상기 게이트웨이제어부로부터 수신한 암호화된 해쉬체인값을 그룹세션키로 복호화하는 단계;

상기 제어부가 상기 메시지를 획득하는 단계 이전에 저장된 해쉬체인값과 상기 메시지를 획득하는 단계에서 수신된 해쉬체인값을 상호비교하여 동일 여부를 확인하는 단계; 및

상기 제어부가 상기 동일 여부 확인결과 동일하다고 판단된 경우 상기 메시지를 처리하지 않는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 차량용 데이터의 인증 및 획득 방법에 관한 것으로, 특히 차량 내 구비되는 적어도 하나의 제어부(ECU: Electronic Control Unit)간 상호 송수신 되는 차량용 데이터를 용이하게 인증하고, 획득할 수 있는 차량용 데이터의 인증 및 획득 방법에 관한 것이다.

배 경 기 술

[0002] 최근의 차량 기술은 차량 본연의 기능 외에도 안전성, 사용자의 편의성, 타 분야의 기기와의 통신을 통한 다양한 서비스의 제공 등에 초점을 맞추어 개발되고 있다. 따라서, 차량 내부에 탑재되는 ECU의 개수가 급격히 증가되고 있다. 상기 ECU 간의 통신은 CAN(Controller Area Networks)을 통해 이루어진다. 최근 차량에서 다양한 서비스를 제공하기 위한 시도가 이뤄짐에 따라, 차량 제어를 위한 데이터는 물론 운전자의 개인정보와 같은 중요한 데이터가 CAN을 통해 송수신 될 수 있다. 또한, 차량 내부에 사용되는 네트워크는 CAN 이외에도 LIN(Local Interconnect Network), FlexRay, MOST(Media Oriented Systems Transport)가 있고, 타 네트워크 간의 통신 프로토콜의 연동을 위해 게이트웨이(gateway)ECU가 사용된다. 이 중에서도 CAN은 그 물리적인 특징 때문에, 외부 전자파나 노이즈에 강한 장점을 갖고 있으며, 이런 특성 때문에 차량 내부 통신 네트워크 중에 가장 큰 비중을 갖고 있다. 하지만 보안적인 측면에서 CAN은 몇 가지 취약점을 갖고 있다. 특히, 최근 많은 서드파티(Third-Party) 업체에서 OBD-2(On Board Diagnostics)단자를 통해 CAN과 통신하여 차량을 자가 진단하거나 CAN의 데이터를 가공하여 사용자 편의를 제공하는 상품을 제공하고 있다. 해당 서비스 모델에서는 CAN의 특성을 악용한 공격자가 차량을 제어할 수 있는 취약점이 존재한다.

[0003] 한편, 이하에서 인용되는 선행기술 문헌에는 ECU와 CAN을 소개하고, CAN 프로토콜이 보안에 매우 취약하다는 점을 지적하며, CAN에서의 보안에 대한 중요성을 강조하고 있다. CAN은 브로드캐스트(Broadcast) 통신 방식을 사용하기 때문에 데이터의 도청에 취약하다. 특히, 최근 차량 기술의 동향은 외부 환경과의 통신을 지향하고 있기 때문에 현재의 CAN구조에서는 외부에서의 도청을 방지할 수 없다. 또한 CAN에는 도청으로 수집된 데이터에 대한 메시지 재전송공격을 방지할 수 있는 보안 메커니즘이 적용되어 있지 않다.

[0004] 이와 같은 관점에서, CAN에서의 도청을 방지하고, 공격자의 데이터 재전송 공격을 통한 비정상적인 차량의 제어를 방지하고, 차량의 실시간적인 데이터 처리를 보장하며, 외부로부터 접근 가능한 텔레매틱스(Telematics) ECU가 공격자에 의해 해킹 되더라도 모든 ECU를 제어하지 못하게 하는 기술적 수단이 필요하다는 사실을 알 수 있다.

선행기술문헌

비특허문헌

[0005] (비특허문헌 0001) CAN 통신 도청 및 조작을 통한 차량 ECU의 외부위협 가능성 분석, 김강석, 고려대학교, 학위논문, 2011.

발명의 내용

해결하려는 과제

[0006] 따라서, 본 발명이 해결하고자 하는 과제는 차량 내 구비되는 다수의 제어부간의 네트워크 통신 시, 송수신 되는 차량용 데이터의 인증 및 획득을 용이하게 수행하는 차량용 데이터의 인증 및 획득 방법을 제공하는 것이다.

과제의 해결 수단

[0007] 본 발명의 과제를 달성하기 위하여, 차량 내 구비되는 적어도 하나의 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 송수신하는 차량용 데이터의 인증 및 획득 방법에 있어서, 게이트웨이제어부가 메시지의 인증에 사용되는 비밀키 및 키 암호화에 사용되는 그룹키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 비밀키 및 상기 그룹키를 저장하는 단계; 상기 게이트웨이제어부가 그룹세션키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 그룹세션키를 저장하는 단계; 상기 제어부가 송신하고자 하는 메시지의 인증에 필요한 메시지인증코드(Message Authentication Code)를 생성하고, 송신하고자 하는 메시지 및 상기 메시지인증코드를 상기 그룹세션키로 암호화하며, 송신하고자 하는 패킷 내 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 포함시켜 네트워크로 송신하는 단계; 및 상기 패킷을 수신한 제어부는 상기 패킷 내 포함된 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 복호화하고, 상기 메시지에 대한 처리를 결정하는 해쉬체인(hash chain)값의 수신 여부에 따라 상기 복호화된 메시지인증코드를 인증함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법을 제공한다.

[0008] 본 발명의 일 실시예에 의하면, 상기 비밀키 및 상기 그룹키를 저장하는 단계 수행 전, 상기 게이트웨이제어부가 인증서를 상기 제어부에 전송하고, 상기 제어부는 수신된 인증서를 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0009] 또한, 상기 비밀키 및 상기 그룹키를 저장하는 단계는, 상기 게이트웨이제어부 및 상기 제어부가 상기 메시지에 대한 인증을 나타내는 카운터의 초기값을 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0010] 본 발명의 다른 실시예에 의하면, 상기 네트워크는, CAN(Controller Area Network) 프로토콜을 사용하며, 브로드캐스트(boradcast) 통신함으로써, 상기 제어부가 상기 메시지를 네트워크로 송신할 경우, 상기 네트워크에 연결된 게이트웨이제어부를 포함하는 모든 제어부로 상기 메시지가 송신되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0011] 본 발명의 또 다른 실시예에 의하면, 상기 메시지인증코드는 상기 패킷 내의 CRC필드 및 확장필드에 포함되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0012] 본 발명의 또 다른 실시예에 의하면, 상기 그룹세션키를 저장하는 단계는, 상기 게이트웨이제어부가 상기 해쉬체인값 및 상기 그룹세션키를 생성하여 상기 그룹키로 암호화하는 단계; 상기 게이트웨이제어부가 상기 암호화된 해쉬체인값 및 상기 암호화된 그룹세션키를 자신의 개인키로 서명하고, 상기 서명된 해쉬체인값 및 상기 서명된 그룹세션키를 상기 제어부로 송신하는 단계; 및 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 서명된 해쉬체인값 및 상기 서명된 그룹세션키를 공개키로 검증하며, 상기 검증된 해쉬체인값 및 상기 검증된 그룹세션키를 상기 그룹키를 통해 복호화함으로써, 상기 복호화된 해쉬체인값 및 상기 복호화된 그룹세션키를 획득하여 저장하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0013] 본 발명의 또 다른 실시예에 의하면, 상기 게이트웨이제어부는 상기 그룹세션키 및 상기 해쉬체인값을 소정의 키 업데이트 주기에 따라 갱신하며, 갱신된 상기 그룹세션키 및 상기 해쉬체인값을 상기 그룹키를 통해 암호화하여 네트워크로 송신하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0014] 본 발명의 또 다른 실시예에 의하면, 상기 네트워크로 송신하는 단계는, 메시지를 송신하고자 하는 상기 제어부가 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성하는 단계; 메시지를 송신하고자 하는 상기 제어부가 상기 인증키를 이용하여 송신하고자 하는 메시지의 메시지인증코드를 생성하는 단계; 메시지를 송신하고자 하는 상기 제어부가 상기 메시지 및 상기 메시지인증코드를 상기 그룹세션키로 암호화하는 단계; 및 메시지를 송신하고자 하는 상기 제어부가 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 송신하고자 하는 패킷 내에 포함하여 네트워크로 송신하는 단계를 포함하는 것을 특징으로 하는

차량용 데이터의 인증 및 획득 방법일 수 있다.

[0015] 본 발명의 또 다른 실시예에 의하면, 상기 카운터값은, 게이트웨이제어부가 상기 인증키를 사용하여 메시지 인증에 성공할 때마다 1이 증가하고, 제어부가 상기 인증키를 생성할 때마다 1이 증가하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0016] 본 발명의 또 다른 실시예에 의하면, 상기 메시지를 획득하는 단계는, 상기 제어부가 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값이 수신되도록 대기하는 단계; 상기 게이트웨이제어부는 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성하며, 상기 인증키를 통해 상기 메시지인증코드를 인증하는 단계; 및 상기 제어부는 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값의 수신이 없을 경우 상기 메시지를 인증함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0017] 본 발명의 또 다른 실시예에 의하면, 상기 게이트웨이제어부가 상기 인증키를 통해 상기 메시지인증코드의 인증에 실패할 경우 상기 해쉬체인값을 상기 그룹세션키로 암호화하여 네트워크로 송신하는 단계; 상기 제어부가 상기 게이트웨이제어부로부터 수신한 암호화된 해쉬체인값을 그룹세션키로 복호화하는 단계; 상기 제어부가 상기 메시지를 획득하는 단계 이전에 저장된 해쉬체인값과 상기 메시지를 획득하는 단계에서 수신된 해쉬체인값을 상호비교하여 동일 여부를 확인하는 단계; 및 상기 제어부가 상기 동일 여부 확인결과 동일하다고 판단된 경우 상기 메시지를 처리하지 않는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

발명의 효과

[0018] 본 발명에 따르면, 제어부가 각기 다른 인증키들을 사용하고, 해쉬체인값을 사용함으로써, 게이트웨이제어부 외에 제어부가 공격을 받을 경우 또 다른 제어부를 제어할 수 없다.

[0019] 또한, 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.

[0020] 또한, 차량용 데이터의 인증 및 획득 방법 및 시스템은 제어부가 네트워크를 통한 차량용 데이터의 송수신 시, 메시지 인증값을 이용하여 상기 차량용 데이터를 인증함에 따라, 상기 차량용 데이터의 위변조를 방지할 수 있는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 차량용 데이터의 인증 및 획득 방법을 도시한 흐름도이다.

도 2는 도 1의 제어부가 수신한 비밀키 및 그룹키를 저장하는 단계를 세부적으로 도시한 도면이다.

도 3은 도 1의 제어부가 수신된 그룹세션키를 저장하는 단계를 세부적으로 도시한 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 게이트웨이제어부가 해쉬체인값 및 그룹세션키를 암호화하여 제어부로 송신하는 과정을 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 게이트웨이제어부가 해쉬체인값 및 그룹세션키를 갱신하여 제어부로 송신하는 과정을 도시한 도면이다.

도 6은 도 1의 패킷 내에 암호화된 메시지 및 암호화된 메시지인증코드를 포함시켜 네트워크로 전송하는 단계를 세부적으로 도시한 흐름도이다.

도 7은 본 발명의 일 실시예에 따른 CAN에서 사용하는 패킷포맷을 세부적으로 도시한 도면이다.

도 8은 본 발명의 일 실시예에 따른 게이트웨이제어부가 메시지 검증에 성공할 경우 메시지의 전송 과정을 도시한 도면이다.

도 9는 본 발명의 일 실시예에 따른 게이트웨이제어부가 메시지 검증에 실패할 경우 메시지의 전송 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0022] 본 발명의 실시예들을 설명하기에 앞서, 기존의 차량용 데이터의 송수신 과정에서 발생하는 문제점들을 검토한 후, 이들 문제점을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 기술적 수단을 개괄적으로 소개하도록 한다.

[0023] 전자제어장치인 ECU(Electonic Control Unit)는 차량의 내부에서 사용되는 포로토콜을 이용하여 상호간 통신을 수행한다. 이때, 사용되는 프로토콜은 CAN(Controller Area Network), LIN(Local Interconnect Network), FlexRay, MOST(Media Oriented Systems Transport)가 있으며, 상기의 CAN, LIN, FlexRay, MOST 중 CAN 프로토콜이 차량에서 주로 사용되고 있다. 상기의 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. 하지만, 상기 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 있다.

[0024] 따라서, 본 발명은 차량 내부의 CAN에서 송수신 되는 제어 데이터의 도청, 위변조 및 재전송을 방지하며, 외부로부터 접근 가능한 ECU가 해킹될 경우, 인접한 ECU를 제어하는 것을 불가능하도록 하는 기술적 수단을 제안하고자 한다.

[0025] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0026] 도 1은 본 발명의 일 실시예에 따른 차량용 데이터의 인증 및 획득 방법을 도시한 흐름도로서, 차량 내 구비되는 적어도 하나의 제어부가 상기 차량의 내부 네트워크를 통해 적어도 하나의 차량용 데이터를 송수신하는 차량용 데이터의 인증 및 획득 방법이다.

[0027] S110 단계에서, 게이트웨이제어부가 메시지의 인증에 사용되는 비밀키 및 키 암호화에 사용되는 그룹키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 비밀키 및 상기 그룹키를 저장한다.

[0028] S110 단계는 이하에서 도 2를 통해 상세하게 설명하도록 한다.

[0029] 도 2는 도 1의 제어부가 수신한 비밀키 및 그룹키를 저장하는 단계를 세부적으로 도시한 도면이다.

[0030] 보다 구체적으로, 게이트웨이제어부(gateway ECU)(21)는 암호화된 해쉬체인값 및 암호화된 그룹세션키를 서명 또는 검증에 사용되는 비밀키(SK)를 생성하고, 상기 해쉬체인값 및 상기 그룹세션키를 암호화 또는 복호화에 사용되는 그룹키(GK)를 생성하여 제어부(ECU)에 전달하기 위하여 네트워크로 송신한다. 여기서, 상기 네트워크는 CAN 프로토콜을 사용하며, 브로드캐스트(boradcast) 통신함으로써, 상기 게이트웨이제어부(21)가가 키분배 및 공유를 위하여 상기 그룹키(GK) 및 비밀키(SK)를 네트워크로 송신할 경우, 상기 네트워크에 연결된 모든 제어부로 상기 비밀키(SK) 및 상기 그룹키(GK)가 송신될 수 있다. 이후, 게이트웨이제어부(21)로부터 상기 비밀키(SK) 및 상기 그룹키(GK)를 수신한 모든 제어부는 상기 비밀키(SK) 및 상기 그룹키(GK)를 저장하며, 메시지에 대한 인증을 나타내는 카운터의 초기값을 각각 생성하여 추가로 저장한다. 여기서, 게이트웨이제어부(21)는 자신의 그룹키(GK)와 네트워크로 연결된 모든 제어부들의 비밀키(SK), 카운터를 저장한다. 또한, 상기 비밀키(SK)는 차량 제조 시에 안전한 채널을 통해 상기 비밀키를 제어부로 전송 가능할 수 있으며, 제어부가 M2M통신을 위해 기기인증서를 사용할 경우 상기 기기인증서를 이용하여 게이트웨이제어부(21)가 상기 비밀키(SK)를 제어부로 전송할 수 있다. 여기서, 게이트웨이제어부(21)가 상기 비밀키(SK)를 제어부로 전송하는 과정은 간헐적으로 발생함으로써, 연산속도 및 통신속도를 고려하지 않고 상기 비밀키(SK)를 전송할 수 있다.

[0031] 또한, 110 단계 수행 전, 상기 게이트웨이제어부가 인증서를 상기 제어부에 전송하고, 상기 제어부는 수신된 인증서를 저장하는 단계를 더 포함할 수 있다. 상기 인증서는 서명을 위한 개인키 및 검증을 위한 공개키를 포함할 수 있다.

[0032] 이제 다시 도 1로 돌아가 S110 단계 이후를 설명하도록 한다.

[0033] S120 단계에서 상기 게이트웨이제어부가 그룹세션키를 생성하여 상기 제어부로 송신하고, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 그룹세션키를 저장한다.

[0034] S120 단계는 이하에서 도 3을 통해 상세하게 설명하도록 한다.

[0035] 도 3은 도 1의 제어부가 수신된 그룹세션키를 저장하는 단계를 세부적으로 도시한 흐름도이다.

[0036] S210 단계에서, 상기 게이트웨이제어부가 상기 해쉬체인값 및 상기 그룹세션키를 생성하여 상기 그룹키로 암호화한다.

[0037] 보다 구체적으로, 상기 게이트웨이제어부가 메시지의 처리를 결정하는 해쉬체인값을 순차적으로 생성하고, 전송하고자 하는 메시지 및 메시지인증코드를 암호화 또는 복호화에 사용되는 그룹세션키(GSK)를 생성하며, 상기 생성한 해쉬체인값 및 상기 생성한 그룹세션키(GSK)를 도 1의 S110 단계에서 생성한 그룹키(GK)로 암호화한다. 여기서, 상기 해쉬체인값은 메시지 인증에 사용될 수 있으며, 상기 해쉬체인값으로부터 메시지를 인증하는 과정은 추후 아래에서 설명하도록 한다.

[0038] S220 단계에서, 상기 게이트웨이제어부가 상기 암호화된 해쉬체인값 및 상기 암호화된 그룹세션키를 개인키로 서명하고, 상기 서명된 해쉬체인값 및 상기 서명된 그룹세션키를 상기 제어부로 송신한다.

[0039] 보다 구체적으로, 상기 게이트웨이제어부가 그룹키(GK)를 통해 상기 암호화된 해쉬체인값 및 상기 암호화된 그룹세션키(GSK)를 상기 개인키로 서명(Sig)하고, 상기 서명(Sig)된 해쉬체인값 및 상기 서명(Sig)된 그룹세션키(GSK)를 상기 제어부로 송신하다. 여기서, 상기 게이트웨이제어부가 상기 제어부로 상기 서명(Sig)된 해쉬체인값 및 상기 서명(Sig)된 그룹세션키(GSK)를 상기 제어부로 송신할 경우 브로드캐스트 통신함으로써, 네트워크에 연결된 모든 제어부에 상기 서명(Sig)된 해쉬체인값 및 상기 서명(Sig)된 그룹세션키(GSK)를 송신할 수 있다.

[0040] S230 단계에서, 상기 제어부가 상기 게이트웨이제어부로부터 수신된 상기 서명(Sig)된 해쉬체인값 및 상기 서명(Sig)된 그룹세션키(GSK)를 상기 공개키를 통해 검증하며, 상기 검증된 해쉬체인값 및 상기 검증된 그룹세션키(GSK)를 상기 그룹키(GK)를 통해 복호화함으로써, 상기 복호화된 해쉬체인값 및 상기 복호화된 그룹세션키(GSK)를 획득하여 저장한다. 이하에서는 도 3의 게이트웨이제어부가 제어부에게 해쉬체인값 및 그룹세션키를 전송하는 단계를 도면으로 설명하도록 한다.

[0041] 도 4는 본 발명의 실시예에 따른 게이트웨이제어부가 해쉬체인값 및 그룹세션키를 암호화하여 제어부로 송신하는 과정을 도시한 도면이다.

[0042] 보다 구체적으로, 게이트웨이제어부(21)는 그룹세션키(GSK) 및 해쉬체인(K_0)을 생성하고, 상기 그룹세션키(GSK) 및 상기 해쉬체인(K_0)을 그룹키로 암호화(E_{GK})하며, 상기 암호화(E_{GK})된 그룹세션키(GSK) 및 상기 암호화(E_{GK})된 해쉬체인(K0)을 개인키로 서명(Sig)할 수 있다. 이후, 게이트웨이제어부(21)가 상기 서명(Sig)된 해쉬체인(K_0) 및 서명(Sig)된 그룹세션키(GSK)를 네트워크로 송신하며, 상기 네트워크는 브로드캐스트 통신함으로써, 네트워크에 연결된 모든 제어부(22)는 상기 서명(Sig)된 해쉬체인(K_0) 및 상기 서명(Sig)된 그룹세션키(GSK)를 수신할 수 있다. 또한, 상기 게이트웨이제어부(21)는 그룹세션키(GSK) 및 해쉬체인(K_0)을 업데이트 주기에 따라 갱신하여 제어부(22)로 송신하며, 상기 그룹세션키(GSK) 및 해쉬체인(K_0)을 업데이트 주기에 따라 갱신하여 제어부로 송신하는 것은 이하에서 도 5를 통해 상세하게 설명하도록 한다.

[0043] 도 5는 본 발명의 다른 실시예에 따른 게이트웨이제어부가 해쉬체인값 및 그룹세션키를 갱신하여 제어부로 송신하는 과정을 도시한 도면이다.

[0044] 보다 구체적으로, 게이트웨이제어부(21)는 정해진 키 업데이트 주기에 따라 상기 해쉬체인값 및 그룹세션키(GSK)를 갱신할 수 있다. 여기서 키 업데이트 주기는 상황에 따라 변경가능 할 수 있다. 또한, 키 업데이트 주기에 맞춰 새로 생성된 그룹세션키(GSK)와 사용되어야할 순서의 해쉬체인값은 그룹키(GK)로 암호화하여 네트워크로 송신한다. 상기 네트워크는 브로드캐스트 통신함으로써, 상기 네트워크에 연결된 모든 제어부는 키 업데이트 주기에 맞춰 새로 생성된 암호화된 그룹세션키(GSK)와 사용되어야할 순서의 암호화된 해쉬체인값을 수신하여 상기 그룹키(GK)로 복호화하여 저장하고, 기존의 해쉬체인값과 기존의 그룹세션키는 삭제할 수 있다. 여기서 상기 해쉬체인값은 도 2의 S210 단계에서 순차적으로 생성되고, 생성된 순서의 역순에 따라 키 업데이트에 사용할 수 있다. 즉, 상기 해쉬체인의 생성과정은 아래와 같이 표현할 수 있다.

수학식 1

[0045] $$S \rightarrow K_n = H(S) \rightarrow K_{n-1} = H^2(S) \rightarrow \cdots K_2 = H^n(S) \rightarrow K_1 = H^n(S) \rightarrow K_0 = H^{n+1}(S)$$

[0046] 여기서, K는 해쉬체인값이고, H()는 일반적인 SHA-1과 같은 해쉬함수이며, H(S)는 해쉬함수의 입력값으로 S가 입력된 것일 때, 수학식 1의 해쉬체인값은 아래와 같이 풀어서 표현할 수 있다.

수학식 2

[0047] $$K_1 = H(S)$$

[0048] $$K_2 = H^2(S) = H(K_1) = H(H(S)),$$

[0049] $$K_3 = H^3(S) = H(K_2) = H(H(H(S))),$$

[0050] K_n은 $H^n(S)=H(K_n-1)=H$를 S에 n만큼 반복하여 곱함으로써 표현될 수 있다.

[0051] 이제 다시 도 1로 돌아가 S120 단계 이후를 설명하도록 한다.

[0052] S130 단계에서, 상기 제어부가 송신하고자 하는 메시지의 인증에 필요한 메시지인증코드(Message Authentication Code)를 생성하고, 송신하고자 하는 메시지 및 상기 메시지인증코드를 상기 그룹세션키로 암호화하며, 송신하고자 하는 패킷 내 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 포함시켜 네트워크로 송신한다.

[0053] 보다 구체적으로, S130 단계는 이하에서 도 6을 통해 설명하도록 한다.

[0054] 도 6은 도 1의 패킷 내에 암호화된 메시지 및 암호화된 메시지인증코드를 포함시켜 네트워크로 전송하는 단계를 세부적으로 도시한 흐름도이다.

[0055] S610 단계에서, 메시지를 송신하고자 하는 상기 제어부가 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성한다.

[0056] 보다 구체적으로, 메시지를 송신하고자 하는 상기 제어부가 보내고자 하는 메시지를 인증하기 위한 인증키(AK)를 생성하되, 상기 인증키는 메시지의 인증을 나타내는 카운터값과 상기 비밀키(SK) 간의 배타적연산(xor)을 수행함으로써, 상기인증키를 생성하고, 상기 제어부는 상기 인증키를 생성 후 상기 카운터를 1 증가 시킬 수 있다. 상기 인증키(AK)는 아래와 같이 표현할 수 있다.

수학식 3

[0057] $$AK_1' = SK_1 \veebar Counter_1$$

[0058] S620 단계에서, 메시지를 송신하고자 하는 상기 제어부가 상기 인증키를 이용하여 송신하고자 하는 메시지의 메시지인증코드를 생성한다.

[0059] 보다 구체적으로, 메시지를 송신하고자 하는 상기 제어부가 S610 단계에서 생성한 인증키를 사용하여 송신하고자 하는 메시지의 인증에 필요한 메시지인증코드(MAC)를 생성할 수 있다.

[0060] S630 단계에서, 메시지를 송신하고자 하는 상기 제어부가 상기 메시지 및 상기 메시지인증코드(MAC)를 상기 그

룹세션키(GSK)로 암호화한다.

[0061] 보다 구체적으로, 메시지를 송신하고자 하는 상기 제어부는 송신하고자 하는 메시지와 상기 메시지에 대한 인증값인 메시지인증코드를 상기 게이트웨이제어부로부터 수신받은 그룹세션키(GSK)로 암호화할 수 있다.

[0062] S640 단계에서, 메시지를 송신하고자 하는 상기 제어부가 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 송신하고자 하는 패킷 내에 포함하여 네트워크로 송신한다.

[0063] 보다 구체적으로, 메시지를 송신하고자 하는 상기 제어부는 S630 단계에서 암호화된 송신하고자 하는 메시지와 암호화된 메시지인증코드를 송신하고자 하는 패킷 내의 확장필드 및 CRC필드에 포함하여 네트워크로 송신할 수 있다. 여기서, 상기 패킷은 이하에서 도 7을 통해 설명하도록 한다.

[0064] 도 7은 본 발명의 일 실시예에 따른 CAN에서 사용하는 패킷포맷을 세부적으로 도시한 도면이다.

[0065] CAN 패킷포맷(70)에는 데이터 필드(72) 외에 확장필드(71) 및 CRC필드(73)가 존재한다. CAN 통신에서는 확장필드(71)가 사용되지 않고, CRC필드(73)의 경우 CRC를 통한 에러체크역할을 상기 메시지인증코드가 대신 수행가능함으로써, 확장필드(71)의 18비트와 CRC필드(73)의 15비트를 상기 메시지인증코드를 삽입할 수 있는 공간으로 활용할 수 있다. 따라서, CAN 통신에서 확장필드(71)와 CRC필드(73)를 활용하여 메시지인증코드를 삽입할 경우 데이터 지연 없는 실시간 데이터의 처리가 가능할 수 있다. 또한, 메시지인증코드의 안정성을 확보하기 위하여 데이터필드(72)의 1~2바이트를 사용할 수 있다.

[0066] 이제 다시 도 1로 돌아와 S130 단계 이후를 설명하도록 한다.

[0067] S140 단계에서, 상기 패킷을 수신한 제어부는 상기 패킷 내 포함된 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 복호화하고, 상기 메시지에 대한 처리를 결정하는 해쉬체인값의 수신 여부에 따라 상기 메시지를 인증함으로써, 상기 메시지를 획득한다.

[0068] 보다 구체적으로, 상기 제어부가 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값이 수신되도록 대기할 수 있다. 이제, 상기 게이트웨이제어부는 수신한 패킷 내에 존재하는 상기 암호화된 메시지 및 상기 암호화된 메시지인증코드를 상기 그룹세션키를 이용하여 복호화하고, 메시지의 인증을 나타내는 카운터값과 상기 비밀키 간에 배타적연산을 수행하여 인증키를 생성하며, 상기 인증키를 통해 상기 메시지인증코드를 인증할 수 있다. 이후, 상기 제어부는 상기 게이트웨이제어부로부터 소정의 시간만큼 상기 해쉬체인값의 수신이 없을 경우 상기 메시지를 인증함으로써, 상기 메시지를 획득할 수 있다. 여기서, 게이트웨이제어부가 메시지인증코드의 인증에 성공하여 상기 제어부가 수신된 메시지를 획득하는 일련의 과정은 이하에서 도 8을 통해 보다 세부적으로 설명하도록 한다.

[0069] 도 8은 본 발명의 다른 실시예에 따른 게이트웨이제어부가 메시지 검증에 성공할 경우 메시지의 전송 과정을 도시한 도면이다.

[0070] S810 단계에서, 제어부(22)는 보내고자 하는 메시지(M_1)의 인증을 나타내는 카운터값($Counter_1$)과 비밀키(SK_1) 간의 배타적연산(xor)을 수행함으로써 인증키(AK_1')를 생성하고, 상기 인증키(AK_1')를 통해 상기 메시지(M_1)를 인증하기 위한 메시지인증코드(MAC)을 생성하며, 상기 메시지(M_1)와 상기 메시지인증코드(MAC)를 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})할 수 있다. 또한, 제어부(22)는 상기 메시지인증코드를 생성 후 상기 카운터를 1 증가시킬 수 있다.

[0071] S820 단계에서, 제어부(22)는 상기 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 네트워크로 전송한다. 상기 네트워크는 브로드캐스트 통신함으로써, 상기 네트워크에 연결된 게이트웨이제어부(21) 및 제어부(23) 상기 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신할 수 있다.

[0072] S830 단계에서, 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신한 제어부(23)는 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 복호화하며, 임의의 시간(T) 동안 게이트웨이제어부(21)로부터 응답을 기다릴 수 있다.

[0073] S840 단계에서, 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신한 게이트웨이제어

부(21)는 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 복호화하고, 제어부(22)와 공유한 카운터값($Counter_1$)과 비밀키(SK_1)를 이용하여 인증키(AK_1')를 생성하며, 상기 인증키(AK_1')를 이용하여 상기 복호화된 메시지인증코드(MAC)를 검증할 수 있다. 또한, 상기 복호화된 메시지인증코드(MAC)를 검증이 성공할 경우 게이트웨이제어부(21)는 카운터값($Counter_1$)을 1 증가시키고, 리포트를 생성하지 않는다.

[0074] S850 단계에서, 제어부(23)는 임의의 시간(T) 동안 게이트웨이제어부(21) 부터 응답이 없을 경우 상기 복호화된 메시지를 인증함으로써, 상기 메시지를 획득할 수 있다. 여기서, 상기 게이트웨이 제어부로부터 리포트에 대한 수신이 없으므로, 상기 제어부는 메시지를 처리할 수 있다. 상기 게이트웨이제어부와 상기 제어부 간에는 상기 비밀키가 공유되어 있으나, 상기 제어부 간에는 상기 비밀키가 공유되어 있지 않으므로 상기 메시지 인증키를 직접 생성할 수 없다. 또한, 임의의 시간(T)는 고정된 값이 아니며, 설정으로 인해 변경 가능할 수 있다.

[0075] 이하에서는 상기 게이트웨이제어부가 상기 제어부로부터 수신된 메시지인증코드의 인증에 실패할 경우에 대하여 설명하도록 한다.

[0076] 상기 게이트웨이제어부가 상기 인증키를 통해 상기 메시지인증코드의 인증에 실패할 경우 상기 해쉬체인값을 상기 그룹세션키로 암호화하여 네트워크로 송신할 수 있다. 이제, 상기 제어부가 상기 게이트웨이제어부로부터 수신한 암호화된 해쉬체인값을 그룹세션키로 복호화하고, 상기 제어부가 상기 메시지를 획득하는 단계 이전에 저장된 해쉬체인값과 상기 메시지를 획득하는 단계에서 수신된 해쉬체인값을 상호비교하여 동일 여부를 확인할 수 있다. 이후, 상기 제어부가 상기 동일 여부 확인결과 동일하다고 판단된 경우 상기 메시지를 처리하지 않을 수 있다. 여기서, 상기 게이트웨이제어부가 상기 제어부로부터 수신된 메시지인증코드의 인증에 실패할 경우 상기 제어부가 수신된 메시지를 처리하는 일련의 과정은 이하에서 도 9을 통해 보다 세부적으로 설명하도록 한다.

[0077] 도 9는 본 발명의 다른 실시예에 따른 게이트웨이제어부가 메시지 검증에 실패할 경우 메시지의 전송 과정을 도시한 도면이다.

[0078] S910 단계에서, 제어부(22)는 보내고자 하는 메시지(M_1)의 인증을 나타내는 카운터값($Counter_1$)과 비밀키(SK_1) 간의 배타적연산(xor)을 수행함으로써 인증키(AK_1')를 생성하고, 상기 인증키(AK_1')를 통해 상기 메시지(M_1)를 인증하기 위한 메시지인증코드(MAC)을 생성하며, 상기 메시지(M_1)와 상기 메시지인증코드(MAC)를 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})할 수 있다. 또한, 제어부(22)는 상기 메시지인증코드를 생성 후 상기 카운터를 1 증가시킬 수 있다.

[0079] S920 단계에서, 제어부(22)는 상기 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 네트워크로 전송한다. 상기 네트워크는 브로드캐스트 통신함으로써, 상기 네트워크에 연결된 게이트웨이제어부(21) 및 제어부(23) 상기 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신할 수 있다.

[0080] S930 단계에서, 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신한 제어부(23)는 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 복호화하며, 임의의 시간(T) 동안 대기한다.

[0081] S940 단계에서, S840 단계에서, 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 수신한 게이트웨이제어부(21)는 그룹세션키(GSK)를 사용하여 암호화(E_{GSk})된 상기 메시지(M_1)와 암호화(E_{GSk})된 메시지인증코드(MAC)를 복호화하고, 제어부(22)와 공유한 카운터값($Counter_1$)과 비밀키(SK_1)를 이용하여 인증키(AK_1')를 생성하며, 상기 인증키(AK_1')를 이용하여 상기 복호화된 메시지인증코드(MAC)를 검증할 수 있다. 여기서, 상기 복호화된 메시지인증코드(MAC)를 검증에 실패할 경우 게이트웨이제어부(21)는 카운터값($Counter_1$)을 증가시키지 않고, 리포트를 생성하여 네트워크로 송신한다. 상기 리포트는 그룹세션키(GSK)로 암호화 된 해쉬체인(K_1)을 포함할 수 있다.

[0082] S950 단계에서, 게이트웨이제어부(21)는 그룹세션키(GSK)로 암호화 된 해쉬체인(K_1)을 포함하는 리포트를 네트워크로 전송하며, 상기 네트워크는 브로드캐스트 통신 함으로써, 제어부(22) 및 제어부(23)에서 송신될 수

있다.

[0083] S960 단계에서, 제어부(23)는 임의의 시간(T) 안에 게이트웨이제어부로부터 그룹세션키(GSK)로 암호화된 해쉬체인(K_1)을 포함하는 리포트가 수신될 경우, 상기 리포트에 포함된 암호화된 해쉬체인(K_1)을 그룹세션키(GSK)로 복호화하고, 상기 복호화된 해쉬체인(K_1)과 도 3의 S230 단계에서 획득한 해쉬체인값을 상호비교하여 동일 여부를 확인하며, 동일 여부 확인결과 동일하다고 판단될 경우, 제어부(23)는 게이트웨이제어부(21)로부터 상기 리포트가 수신되었다고 판단하여 수신된 메시지를 처리하지 않을 수 있다. 여기서 임의의 시간(T)는 고정된 값이 아니며, 설정으로 인해 변경 가능할 수 있다.

[0084] 상기의 본 발명의 실시예들에 따르면, 제어부가 각기 다른 인증키들을 사용하고, 해쉬체인값을 사용함으로써, 게이트웨이제어부 외에 제어부가 공격을 받을 경우 또 다른 제어부의 제어를 방지한다. 또한, 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. 또한, 차량용 데이터의 인증 및 획득 방법 및 시스템은 제어부가 네트워크를 통한 차량용 데이터의 송수신 시, 메시지 인증값을 이용하여 상기 차량용 데이터를 인증함에 따라, 상기 차량용 데이터의 위변조를 방지한다.

[0085] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0086] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0087] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0088] 21 : 게이트웨이제어부(Gagteway ECU)

22 : 제어부(ECU)

70 : CAN 패킷포맷

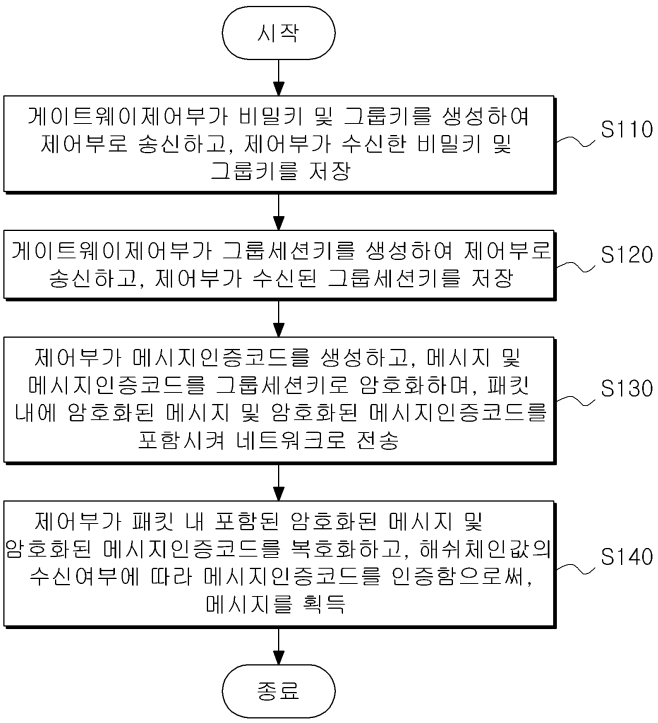
71 : 확장필드

72 : 데이터필드

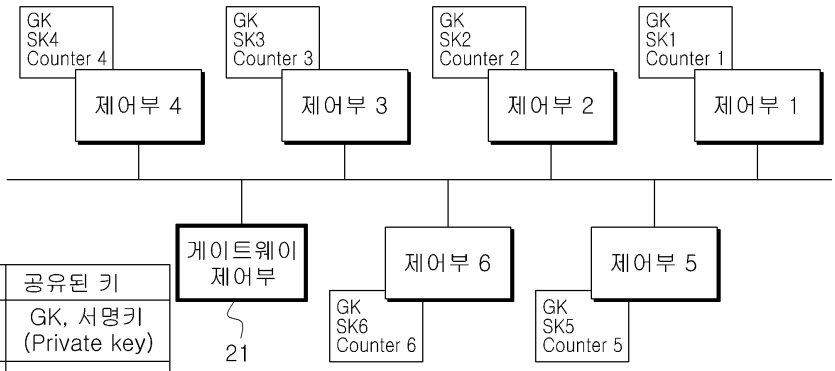
73 : CRC필드

도면

도면1



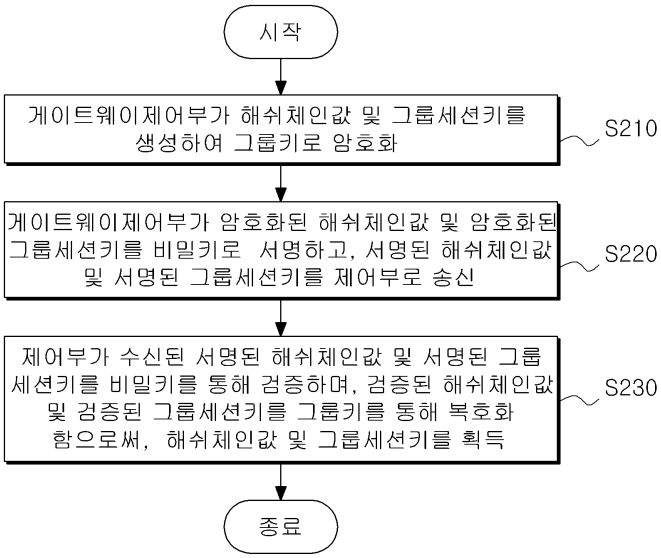
도면2



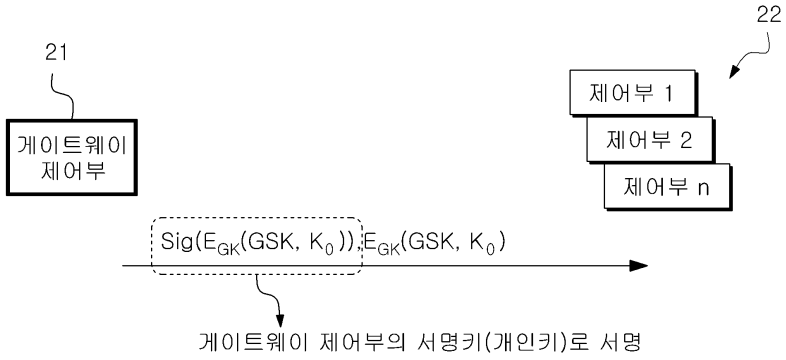
ECU 종류	공유된 키
G_제어부	GK, 서명키 (Private key)
제어부 1	SK1, counter1 G_제어부의 인증서
제어부 2	SK2, counter2 G_제어부의 인증서
제어부 3	SK3, counter3 G_제어부의 인증서
제어부 4	SK4, counter4 G_제어부의 인증서
제어부 5	SK5, counter5 G_제어부의 인증서
제어부 6	SK6, counter6 G_제어부의 인증서

게이트웨이 제어부가 저장하는 정보

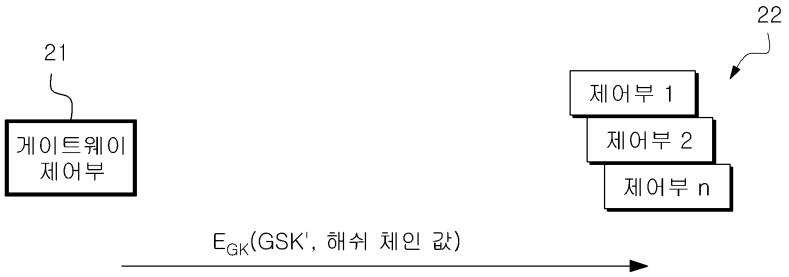
도면3


시작
게이트웨이제어부가 해쉬체인값 및 그룹세션키를 생성하여 그룹키로 암호화
S210
게이트웨이제어부가 암호화된 해쉬체인값 및 암호화된 그룹세션키를 비밀키로 서명하고, 서명된 해쉬체인값 및 서명된 그룹세션키를 제어부로 송신
S220
제어부가 수신된 서명된 해쉬체인값 및 서명된 그룹세션키를 비밀키를 통해 검증하며, 검증된 해쉬체인값 및 검증된 그룹세션키를 그룹키를 통해 복호화 함으로써, 해쉬체인값 및 그룹세션키를 획득
S230
종료

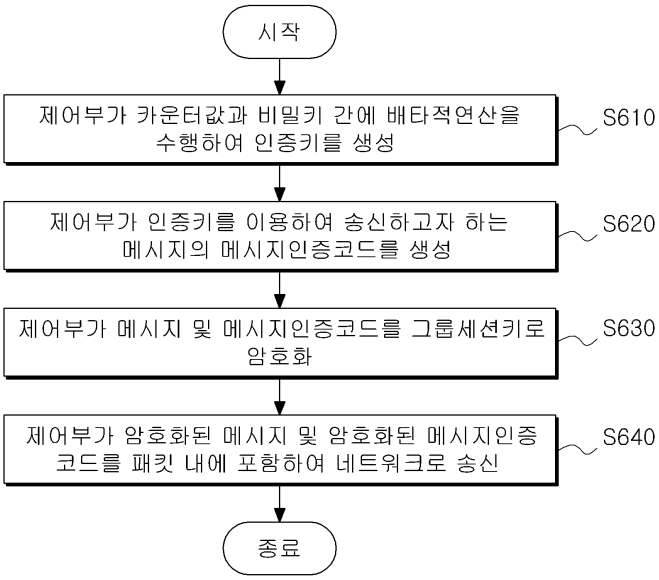
도면4


21
게이트웨이 제어부
22
제어부 1
제어부 2
제어부 n
Sig(E_GK(GSK, K_0)), E_GK(GSK, K_0)
게이트웨이 제어부의 서명키(개인키)로 서명

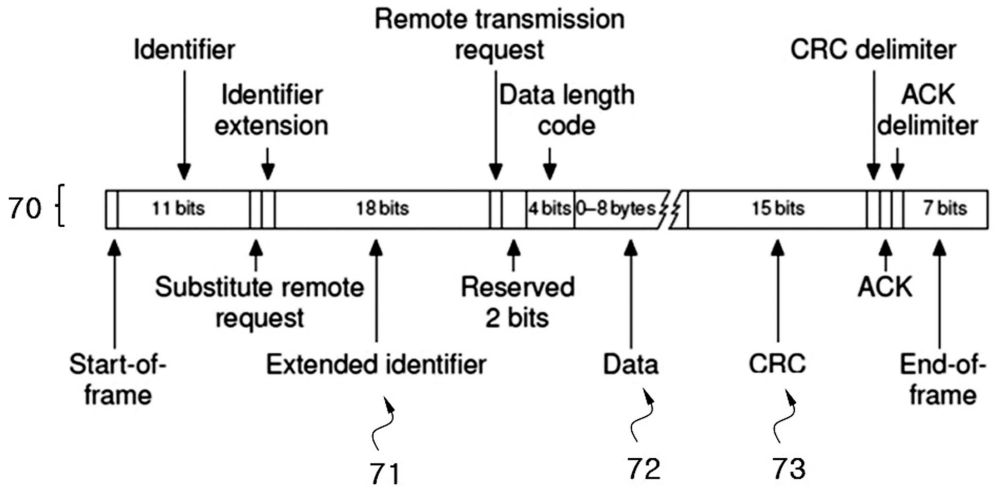
도면5


21
게이트웨이 제어부
22
제어부 1
제어부 2
제어부 n
E_GK(GSK', 해쉬 체인 값)

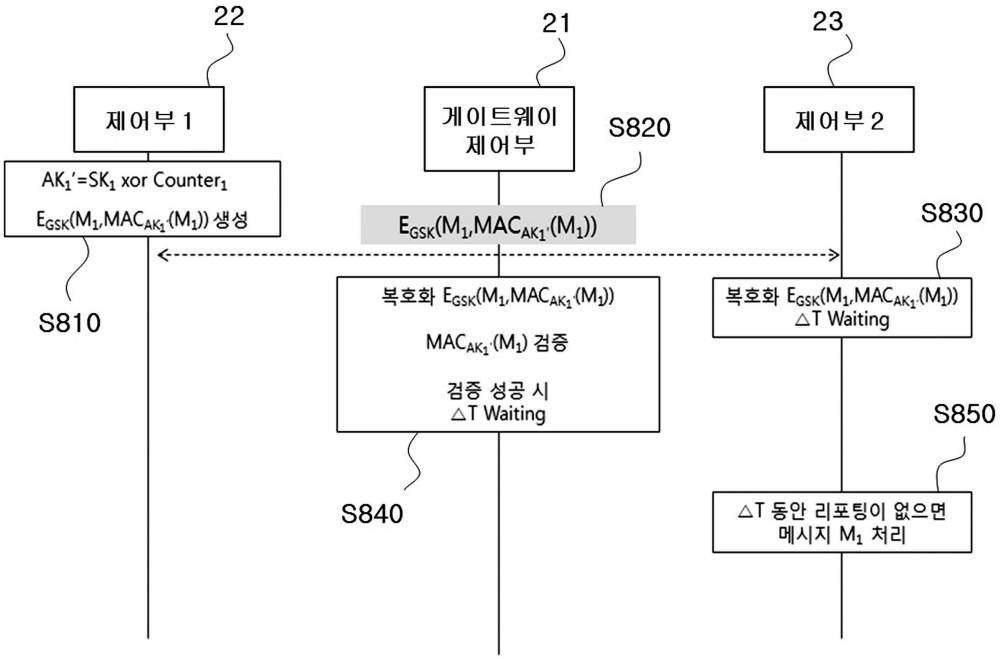
도면6


시작
제어부가 카운터값과 비밀키 간에 배타적연산을 수행하여 인증키를 생성
S610
제어부가 인증키를 이용하여 송신하고자 하는 메시지의 메시지인증코드를 생성
S620
제어부가 메시지 및 메시지인증코드를 그룹세션키로 암호화
S630
제어부가 암호화된 메시지 및 암호화된 메시지인증코드를 패킷 내에 포함하여 네트워크로 송신
S640
종료

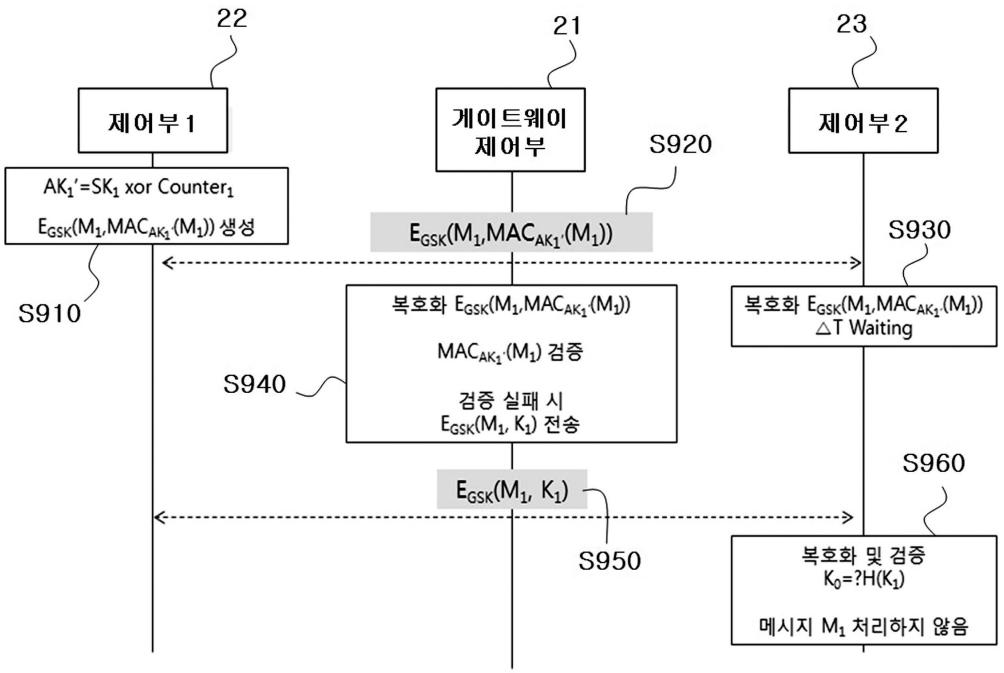
도면7


Identifier
Identifier extension
Remote transmission request
Data length code
CRC delimiter
ACK delimiter
70
11 bits
18 bits
4 bits
0–8 bytes
15 bits
7 bits
Start-of-frame
Substitute remote request
Extended identifier
Reserved 2 bits
Data
CRC
ACK
End-of-frame
71
72
73

도면8


22
21
23
제어부 1
게이트웨이 제어부
제어부 2
S820
AK1'=SK1 xor Counter1
EGSK(M1,MACAK1'(M1)) 생성
EGSK(M1,MACAK1'(M1))
S830
S810
복호화 EGSK(M1,MACAK1'(M1))
MACAK1'(M1) 검증
검증 성공 시
△T Waiting
복호화 EGSK(M1,MACAK1'(M1))
△T Waiting
S850
S840
△T 동안 리포팅이 없으면
메시지 M1 처리

도면9


22
21
23
제어부 1
게이트웨이 제어부
제어부 2
S920
AK1'=SK1 xor Counter1
EGSK(M1,MACAK1'(M1)) 생성
EGSK(M1,MACAK1'(M1))
S930
S910
복호화 EGSK(M1,MACAK1'(M1))
MACAK1'(M1) 검증
검증 실패 시
EGSK(M1, K1) 전송
복호화 EGSK(M1,MACAK1'(M1))
△T Waiting
S940
S960
EGSK(M1, K1)
S950
복호화 및 검증
K0=?H(K1)
메시지 M1 처리하지 않음