



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년01월21일

(11) 등록번호 10-1481403

(24) 등록일자 2015년01월06일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01) H04L 9/30 (2006.01)

(21) 출원번호 10-2013-0101169

(22) 출원일자 2013년08월26일

심사청구일자 2013년08월26일

(56) 선행기술조사문헌

KR1020130021157 A

KR1020100091089 A

T. Dierks, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246 (2008.08.)

Sung Hoon Kim 외 3명, Auditable and Privacy-Preserving Authentication in Vehicular Networks, UBICOMM 2008, IEEE Computer Society (2008.)

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

이동훈

서울 종로구 사직로8길 34, 1404호 (내수동, 경희궁의아침3단지)

우사무엘

서울 송파구 오금로53길 7, 403호 (거여동)

조효진

서울 동대문구 안암로22길 25, (제기동)

(74) 대리인

특허법인충현

전체 청구항 수 : 총 10 항

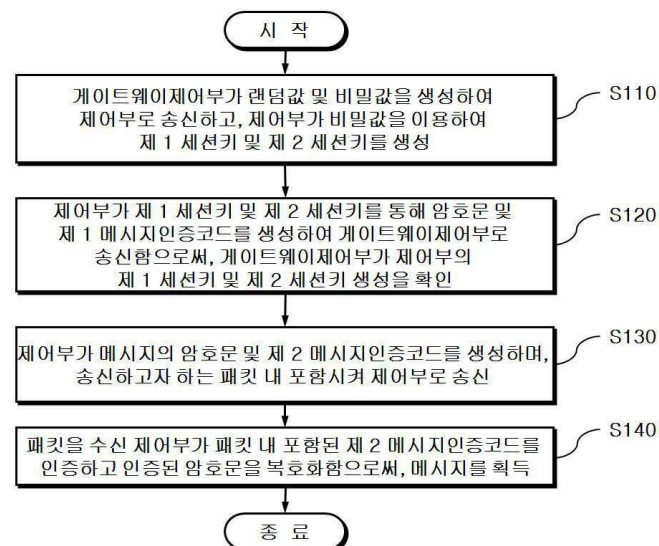
심사관 : 양종필

(54) 발명의 명칭 차량용 데이터의 인증 및 획득 방법

(57) 요약

차량용 데이터의 인증 및 획득 방법에 관한 것으로서, 게이트웨이제어부가 랜덤값 및 비밀값을 생성하여 제어부로 송신하고, 제어부는 랜덤값 및 비밀값을 이용하여 제 1 세션키 및 제 2 세션키를 생성하고, 제어부가 제 1 세션키 및 제 2 세션키를 통해 암호문 및 제 1 메시지인증코드를 생성하여 게이트웨이제어부로 송신함으로써, 게이트웨이제어부는 수신된 암호문 및 수신된 제 1 메시지인증코드로부터 제어부의 제 1 세션키 및 제 2 세션키 생성을 확인하고, 제어부가 송신하고자 하는 메시지의 암호문 및 제 2 메시지인증코드를 생성하며, 송신하고자 하는 패킷 내 암호문 및 제 2 메시지인증코드를 포함시켜 제어부로 송신하며, 패킷을 수신한 제어부가 패킷 내 포함된 제 2 메시지인증코드를 인증하고, 인증된 암호문을 복호화함으로써, 메시지를 획득한다.

대표도 - 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 랜덤값 및 비밀값을 생성하여 메시지를 송신하고자 하는 송신 제어부로 송신하고, 상기 송신 제어부는 상기 비밀값을 이용하여 제 1 세션키 및 제 2 세션키를 생성하는 단계;

상기 송신 제어부가 상기 제 1 세션키를 이용하여 상기 랜덤 값 및 자신의 식별자필드값에 대한 제 1 암호문을 생성하고, 상기 제 2 세션키와 자신의 카운터 값을 이용하여 제 1 메시지인증코드(Message Authentication Code)를 생성하여 상기 제 1 암호문과 상기 제 1 메시지인증코드를 상기 게이트웨이제어부로 송신하면, 상기 게이트웨이제어부는 상기 수신된 제 1 암호문 및 상기 수신된 제 1 메시지인증코드로부터 상기 송신 제어부의 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인하는 단계;

상기 송신 제어부가 송신하고자 하는 메시지에 대한 제 2 암호문을 생성하고, 상기 생성된 제 2 암호문과 자신의 카운터 값을 이용하여 제 2 메시지인증코드를 생성하며, 송신하고자 하는 패킷 내 상기 제 2 암호문 및 상기 제 2 메시지인증코드를 포함시켜 내부 네트워크를 통해 다른 제어부로 송신하는 단계; 및

상기 패킷을 수신한 수신 제어부가 상기 패킷 내 포함된 제 2 메시지인증코드를 인증하고, 상기 제 2 암호문을 복호화함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 2

제 1 항에 있어서,

상기 제 1 세션키 및 제 2 세션키를 생성하는 단계 수행 전,

상기 게이트웨이제어부 및 상기 송신 제어부는 각각 서명용인증서 및 암호화용인증서를 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 세션키 및 제 2 세션키를 생성하는 단계는,

상기 게이트웨이제어부가 생성한 상기 랜덤값 및 상기 비밀값을 송신 제어부의 암호화용공개키로 암호화하고, 상기 암호화된 랜덤값 및 상기 암호화된 비밀값을 자신의 서명용개인키로 서명하여 상기 송신 제어부로 송신하는 단계;

상기 송신 제어부가 게이트웨이제어부의 서명용공개키로 상기 서명된 랜덤값 및 상기 서명된 비밀값을 검증하고, 상기 검증된 랜덤값 및 상기 검증된 비밀값을 자신의 암호화용개인키로 복호화함으로써, 상기 비밀값 및 상기 랜덤값을 획득하여 저장하는 단계; 및

상기 송신 제어부가 상기 비밀값에 기초하여 키유도함수(KDF: Key Derivation Function)를 통해 상기 제 1 세션키, 상기 제 2 세션키 및 상기 제 1 내지 2 세션키 갱신을 위한 업데이트키를 생성하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 4

제 3 항에 있어서,

상기 게이트웨이제어부는 상기 업데이트키를 소정의 키 업데이트 주기에 따라 갱신하고, 상기 업데이트키가 갱신되었을 때, 새로운 랜덤값 및 새로운 비밀값을 생성하고 갱신 이전의 업데이트키를 통해 암호화하여 상기 송신 제어부로 송신하고,

상기 송신 제어부는 상기 새로운 랜덤값 및 상기 새로운 비밀값을 이용하여 제 1 세션키와 제 2 세션키를 갱신

하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 5

제 1 항에 있어서,

상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인하는 단계는,

상기 게이트웨이제어부가 상기 수신된 제 1 메시지인증코드를 검증하여 상기 제 2 세션키 생성을 확인하고, 상기 제 1 암호문을 상기 제 1 세션키를 통해 복호화하여 상기 제 1 세션키 생성을 확인하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 6

제 1 항에 있어서,

상기 카운터값은,

상기 송신 제어부 및 상기 수신 제어부가 해당 패킷 전송을 순차적으로 모두 완료할 때마다 1이 증가하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 7

제 1 항에 있어서,

상기 다른 제어부로 송신하는 단계는,

상기 송신 제어부가 상기 자신의 카운터값을 상기 제 1 세션키로 암호화하고, 상기 암호화된 카운터값과 상기 송신하고자 하는 메시지 간에 배타적연산을 수행하여 상기 제 2 암호문을 생성하는 단계; 및

상기 송신 제어부가 상기 제 2 암호문 및 상기 식별자필드를 입력값으로 설정하고, 상기 자신의 카운터값과 상기 제 2 세션키를 배타적연산한 결과를 키 값으로 이용하여 상기 제 2 메시지인증코드를 생성하는 단계;를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 8

제 1 항에 있어서,

상기 메시지를 획득하는 단계는,

상기 수신 제어부가 상기 패킷 내 포함된 상기 제 2 메시지인증코드를 상기 송신 제어부의 카운터값 및 제 2 세션키를 통해 인증하는 단계; 및

상기 수신 제어부가 상기 제 2 암호문을 상기 송신 제어부의 제 1 세션키를 통해 복호화함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 9

제 1 항에 있어서,

상기 제 1 내지 2 암호문 및 상기 제 1 내지 2 메시지인증코드는 상기 패킷 내의 데이터페이로드필드(Data payload field)에 포함되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

청구항 10

제 1 항에 있어서,

상기 게이트웨이제어부 및 상기 모든 제어부는 CAN FD(Controller Area Network with Flexible Data rate) 프로토콜을 통해 메시지를 송수신하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법.

명세서

기술분야

[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.

배경 기술

[0002] 최근에 출시되는 자동차들은 운전 편의성 및 주행 안전성을 높이기 위해 다양한 IT 기술과 융합되고 있다. 자동차에 IT 기술을 접목시키기 위해서 ECU(Electronic Control Unit)의 사용은 필수적이다. 최근 출시되는 자동차의 경우 첨단 IT 기술을 자동차에 적용하기 위해 최대 100여개의 ECU를 자동차 제조에 사용하고 있다. 이러한 ECU 간의 효율적인 통신을 위해 다양한 네트워크 기술들이 자동차 내부에 구축되어 있다. 대표적인 자동차 내부 네트워크 기술로는 CAN(Controller Area Network), LIN(Local Interconnect Network), MOST(Media Oriented Systems Transport), Flexray 등이 있다. 또한, 자동차 내부에 구축된 이기종 네트워크 간의 통신 프로토콜 연동을 위해서는 게이트웨이(Gateway) ECU가 사용된다.

[0003] 여기서, 상기 CAN은 버스 네트워크(BUS Network) 구조를 사용하여 자동차 내부에 통신 회선을 획기적으로 감소시켰다. 또한, 1메가(Mega bit per second)의 통신 속도를 제공하면서도 외부 전자파나 노이즈에 강한 장점을 갖고 있다. 그러나, 자동차-IT 기술 융합이 급증하고 자동차와 가전기기들(예; 태블릿 PC, 스마트폰) 연결하는 서비스가 상용화되면서 자동차 내부 네트워크의 트래픽에 대한 부하가 급증하였다. 특히, CAN은 8바이트(byte)의 제한적인 데이터페이로드(data payload)를 사용하기 때문에 최신 자동차에 탑재되는 모든 IT 기술 및 기기들의 데이터 전송 수요를 충족시킬 수 없게 되었다.

[0004] 또한, 상기 CAN의 제약사항을 극복하기 위해 2012년 데이터 전송 속도와 데이터페이로드를 확장한 CAN FD(CAN with Flexible Data rate)가 개발되었다. 상기 CAN FD는 기존 CAN과 동일한 통신방식을 사용하면서 전송 속도와 데이터페이로드를 증가시켰다. 상기 CAN FD는 최대 15 메가(Mega bit per second)의 전송 속도와 64바이트(byte)의 데이터페이로드를 지원함으로써 자동차-IT 융합기술로 인해 급증한 자동차 내부 ECU간의 데이터 전송 수요를 충족시킬 수 있다.

[0005] 한편, 이하에서 인용되는 선행기술 문헌에는 ECU와 CAN을 소개하고, CAN 프로토콜이 보안에 매우 취약하다는 점을 지적하며, CAN에서의 보안에 대한 중요성을 강조하고 있다. 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. 상기 CAN FD 역시 데이터 암호화나 인증을 전혀 고려하지 않고 설계되어 상기 CAN의 취약점을 동일하게 내포하고 있다는 치명적인 단점이 존재한다.

[0006] 이와 같은 관점에서, CAN FD에서의 데이터의 도청 및 위변조를 방지하고, 공격자의 데이터 재전송 공격을 통한 비정상적인 차량의 제어를 방지하며, 데이터의 기밀성과 인증을 제공하면서 ECU간 통신 데이터의 실시간 처리를 보장하는 기술적 수단이 필요하다는 사실을 알 수 있다.

선행기술문헌

비특허문헌

[0007] (비특허문헌 0001) CAN 통신 도청 및 조작을 통한 차량 ECU의 외부위협 가능성 분석, 김강석, 고려대학교, 학위논문, 2011.

발명의 내용

해결하려는 과제

[0008] 따라서, 본 발명이 해결하고자 하는 과제는 차량 내 구비되는 다수의 제어부 간의 네트워크 통신 시, 송수신 되는 차량용 데이터의 인증 및 획득을 용이하게 수행하는 차량용 데이터의 인증 및 획득 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 본 발명의 과제를 달성하기 위하여, 차량 내 구비되는 적어도 하나의 제어부가 상기 차량의 내부 네트워크를 통

해 적어도 하나의 차량용 데이터를 송수신하는 차량용 데이터의 인증 및 획득 방법에 있어서, 게이트웨이제어부가 랜덤값 및 비밀값을 생성하여 상기 제어부로 송신하고, 상기 제어부는 상기 비밀값을 이용하여 제 1 세션키 및 제 2 세션키를 생성하는 단계; 상기 제어부가 상기 제 1 세션키 및 상기 제 2 세션키를 통해 암호문 및 제 1 메시지인증코드(Message Authentication Code)를 생성하여 상기 게이트웨이제어부로 송신함으로써, 상기 게이트웨이제어부는 상기 수신된 암호문 및 상기 수신된 제 1 메시지인증코드로부터 상기 제어부의 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인하는 단계; 상기 제어부가 송신하고자 하는 메시지의 암호문 및 제 2 메시지인증코드를 생성하며, 송신하고자 하는 패킷 내 상기 암호문 및 상기 제 2 메시지인증코드를 포함시켜 상기 제어부로 송신하는 단계; 및 상기 패킷을 수신한 제어부가 상기 패킷 내 포함된 제 2 메시지인증코드를 인증하고, 상기 인증된 암호문을 복호화함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0010] 본 발명의 일 실시예에 의하면, 상기 제 1 세션키 및 제 2 세션키를 생성하는 단계 수행 전, 상기 게이트웨이제어부 및 상기 제어부는 각각 서명용인증서 및 암호화용인증서를 저장하는 단계를 더 포함하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0011] 또한, 상기 제 1 세션키 및 제 2 세션키를 생성하는 단계는, 상기 게이트웨이제어부가 상기 랜덤값 및 상기 비밀값을 생성하여 상기 제어부의 암호화용공개키로 암호화하고, 상기 암호화된 랜덤값 및 상기 암호화된 비밀값을 자신의 서명용개인키로 서명하여 상기 제어부로 송신하는 단계; 상기 제어부가 상기 게이트웨이제어부의 서명용공개키로 상기 서명된 랜덤값 및 상기 서명된 비밀값을 검증하고, 상기 검증된 랜덤값 및 상기 검증된 비밀값을 자신의 암호화용개인키로 복호화함으로써, 상기 복호화된 비밀값 및 상기 복호화된 랜덤값을 획득하여 저장하는 단계; 및 상기 제어부가 상기 복호화된 비밀값에 기초하여 키유도함수(KDF: Key Derivation Function)를 통해 상기 제 1 세션키와 상기 제 2 세션키 및 상기 세션키 갱신을 위한 업데이트키를 생성하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0012] 본 발명의 다른 실시예에 의하면, 상기 게이트웨이제어부는 상기 제 1 세션키와 상기 제 2 세션키 및 상기 업데이트키를 소정의 키 업데이트 주기에 따라 갱신하고, 상기 갱신된 제 1 세션키 및 상기 갱신된 제 2 세션키를 상기 갱신 이전의 업데이트키를 통해 암호화하여 상기 제어부로 송신하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0013] 본 발명의 또 다른 실시예에 의하면, 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인하는 단계는, 상기 제어부가 상기 랜덤값 및 상기 메시지의 수신여부를 결정하는 식별자필드를 상기 제 1 세션키를 이용하여 암호화하여 상기 암호문을 생성하는 단계; 상기 제어부가 상기 제 2 세션키 및 메시지 전송완료를 나타내는 카운터값을 이용하여 상기 제 1 메시지인증코드를 생성하고, 상기 암호문 및 상기 제 1 메시지인증코드를 상기 게이트웨이제어부로 송신하는 단계; 및 상기 게이트웨이제어부가 상기 수신된 제 1 메시지인증코드를 검증함으로써, 상기 검증된 암호문을 상기 제 1 세션키를 통해 복호화하여 상기 제어부의 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법.

[0014] 본 발명의 또 다른 실시예에 의하면, 상기 카운터값은, 상기 게이트웨이제어부 및 상기 제어부가 패킷 전송을 순차적으로 모두 완료할 때마다 1이 증가하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0015] 본 발명의 또 다른 실시예에 의하면, 상기 제어부로 송신하는 단계는, 메시지를 송신하고자 하는 상기 제어부가 메시지 전송 완료를 나타내는 카운터값을 상기 제 1 세션키로 암호화하고, 상기 암호화된 카운터값과 송신하고자 하는 메시지 간에 배타적연산을 수행하여 상기 암호문을 생성하는 단계; 메시지를 송신하고자 하는 상기 제어부가 상기 암호문 및 상기 메시지의 수신여부를 결정하는 식별자필드를 입력값으로 설정하고, 상기 메시지 전송 완료를 나타내는 카운터값과 상기 제 2 세션키를 이용하여 상기 제 2 메시지인증코드를 생성하는 단계; 및 메시지를 송신하고자 하는 상기 제어부가 송신하고자 하는 패킷 내 상기 암호문 및 상기 제 2 메시지인증코드를 포함시켜 상기 제어부로 송신하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0016] 본 발명의 또 다른 실시예에 의하면, 상기 메시지를 획득하는 단계는, 상기 패킷을 수신한 제어부가 상기 패킷 내 포함된 상기 제 2 메시지인증코드를 상기 카운터값 및 상기 제 2 세션키를 통해 인증하는 단계; 및 상기 패킷을 수신한 제어부가 상기 인증된 암호문을 상기 제 1 세션키를 통해 복호화함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0017] 본 발명의 또 다른 실시예에 의하면, 상기 암호문 및 상기 메시지인증코드는 상기 패킷 내의 데이터페이로드필드

드(Data payload field)에 포함되는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

[0018] 본 발명의 또 다른 실시예에 의하면, 상기 게이트웨이제어부 및 제어부는 CAN FD(Controller Area Network with Flexible Data rate) 프로토콜을 통해 메시지를 송수신하는 것을 특징으로 하는 차량용 데이터의 인증 및 획득 방법일 수 있다.

발명의 효과

[0019] 본 발명에 따르면, 인증서를 통해 제어부를 인증함으로써, 인증된 제어부만 통신에 참여할 수 있어 기밀성이 보장되는 효과가 있다.

[0020] 또한, CAN FD 데이터 프레임 필드 중 데이터페이로드필드를 메시지인증코드를 위한 공간으로 사용함으로써, 데이터프레임의 무결성 및 인증기능을 수행할 수 있는 효과가 있다.

[0021] 또한, 업데이트키를 이용하여 키를 주기적으로 업데이트 하고, 업데이트 되기전 키와 업데이트 되는 키를 함께 사용하는 유예기간이 존재함으로써, 업데이트 시 실시간적인 데이터의 처리를 보장하는 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 따른 차량용 데이터의 인증 및 획득 방법을 도시한 흐름도이다.

도 2는 본 발명의 다른 실시예에 따른 게이트웨이제어부 및 제어부에 인증서가 전송되는 과정을 도시한 도면이다.

도 3은 도 1의 S110 단계를 보다 세부적으로 도시한 도면이다.

도 4는 도 1의 S120 단계를 보다 세부적으로 도시한 흐름도이다.

도 5는 본 발명의 다른 실시예에 따른 키를 업데이트하는 과정을 도시한 흐름도이다.

도 6은 도 1의 S130 단계를 보다 세부적으로 도시한 흐름도이다.

도 7은 도 1의 S140 단계를 보다 세부적으로 도시한 흐름도이다.

도 8은 도 1 내지 도 7에서 사용되는 네트워크 패킷 구조를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 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.

[0024] 전자제어장치인 ECU(Electronic Control Unit)는 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, 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.

[0025] 상기 CAN의 통신 제약성을 극복하기 위해 2012년 CAN FD(Controller Area Network with Flexible Data rate)가 개발되었고, 상기 CAN FD는 CAN을 대체하는 차세대 차량 내부 네트워크 기술로 주목받고 있으며, 향후 출시되는 차량은 상기 CAN FD를 이용하여 상기 ECU 간의 데이터 전송을 수행하고 특정 기능을 수행하는 상기 ECU를 제어하여 차량을 구동한다. 하지만, 이러한 CAN FD 역시 제어 데이터의 도청이나 위변조 및 재전송을 방지할 수 있는 보안 메커니즘이 적용되어 있지 않으므로 악의적인 공격자는 차량을 임의로 제어하거나 내부의 중요 데이터를 획득할 수 있는 치명적인 결함이 존재한다.

[0026] 따라서, 본 발명은 CAN FD에서의 데이터 도청 및 위변조를 방지하고, 공격자의 데이터 재전송 공격을 통한 비정

상적인 차량의 제어를 방지하며, 데이터의 기밀성과 인증을 제공하면서 ECU 간 통신 데이터의 실시간 처리를 보장하는 기술적 수단이 필요하다는 사실을 알 수 있다.

[0027] 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. 또한, 본 발명의 실시예들에서는 상기 ECU를 제어부로 표현하고, 게이트웨이ECU를 게이트웨이제어부로 표현한다.

[0028] 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 방법에 있어서, 게이트웨이제어부가 랜덤값 및 비밀값을 생성하여 상기 제어부로 송신하고, 상기 제어부는 상기 비밀값을 이용하여 제 1 세션키 및 제 2 세션키를 생성한다. 이후, 상기 제어부가 상기 제 1 세션키 및 상기 제 2 세션키를 통해 암호문 및 제 1 메시지인증코드(Message Authentication Code)를 생성하여 상기 게이트웨이제어부로 송신함으로써, 상기 게이트웨이제어부는 상기 수신된 암호문 및 상기 수신된 제 1 메시지인증코드로부터 상기 제어부의 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인한다. 이후, 상기 제어부가 송신하고자 하는 메시지의 암호문 및 제 2 메시지인증코드를 생성하며, 송신하고자 하는 패킷 내 상기 암호문 및 상기 제 2 메시지인증코드를 포함시켜 상기 제어부로 송신한다. 이후, 상기 패킷을 수신한 제어부가 상기 패킷 내 포함된 제 2 메시지인증코드를 인증하고, 상기 인증된 암호문을 복호화함으로써, 상기 메시지를 획득하는 단계를 포함하는 차량용 데이터의 인증 및 획득 방법이다.

[0029] 보다 구체적으로, S110 단계에서, 게이트웨이제어부가 랜덤값 및 비밀값을 생성하여 상기 제어부로 송신하고, 상기 제어부는 상기 랜덤값 및 상기 비밀값을 이용하여 제 1 세션키 및 제 2 세션키를 생성한다. 여기서, S110 단계 수행 전 상기 게이트웨이제어부 및 상기 제어부에 인증서가 전송되는 과정을 포함할 수 있다. 상기 인증서가 전송되는 과정은 이하에서 도 2를 통해 설명하도록 한다.

[0030] 도 2는 본 발명의 다른 실시예에 따른 게이트웨이제어부 및 제어부에 인증서가 전송되는 과정을 도시한 도면으로서, 도 1의 S110 단계 이전에, 상기 게이트웨이제어부 및 상기 제어부는 각각 서명용인증서 및 암호화용인증서를 저장하는 단계를 더 포함할 수 있다.

[0031] 보다 구체적으로, 인증기관(Certification Authority)의 인증을 받은 상기 제어부 제조사는 상기 제어부(22) 및 상기 게이트웨이제어부(21)를 제작할 때, 상기 암호화용인증서 및 상기 서명용인증서를 상기 제어부(22) 및 상기 게이트웨이제어부(21)에 탑재할 수 있다. 또한, 차량 제작업체에서 차량이 출고되는 경우, 상기 제어부(22) 및 상기 게이트웨이제어부(21)가 고장 및 수리로 인해 상기 차량에 탑재한 상기 제어부(22) 및 상기 게이트웨이제어부(21)를 교체하는 경우에 상기 암호화용인증서 및 상기 서명용인증서를 상기 제어부(22) 및 상기 게이트웨이제어부(21)로 전송할 수 있다. 상기, 암호화용인증서 및 상기 서명용인증서를 전송하는 과정에서 상기 암호화용인증서 및 상기 서명용인증서에 대한 유효성을 검증할 수 있으며, 상기 유효성 검증이 완료된 후에 저장할 수 있다. 또한, 상기 암호화용인증서 및 상기 서명용인증서를 전송하는 경우 SSL(Secure Socket Layer), TLS(Transport Layer Security)와 같은 안전한 채널을 통해 이루어질 수 있다.

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

[0033] 도 3은 도 1의 S110 단계를 보다 세부적으로 도시한 도면으로서, 상기 게이트웨이제어부가 상기 랜덤값 및 상기 비밀값을 생성하여 상기 제어부의 암호화용공개키로 암호화하고, 상기 암호화된 랜덤값 및 상기 암호화된 비밀값을 자신의 서명용공개키로 서명하여 상기 제어부로 송신할 수 있다. 이후, 상기 제어부가 상기 게이트웨이제어부의 서명용공개키로 상기 서명된 랜덤값 및 상기 서명된 비밀값을 검증하고, 상기 검증된 랜덤값 및 상기 검증된 비밀값을 자신의 암호화용공개키로 복호화함으로써, 상기 복호화된 비밀값 및 상기 복호화된 랜덤값을 획득하여 저장한다. 이후, 상기 제어부가 상기 복호화된 비밀값 및 상기 복호화된 랜덤값에 기초하여 키유도함수(KDF: Key Derivation Function)를 통해 상기 제 1 세션키와 상기 제 2 세션키 및 상기 세션키 갱신을 위한 업데이트키를 생성한다.

[0034] 보다 구체적으로, 현재 통신하려고 하는 세션이 i 번째 세션이라고 할 때, 상기 게이트웨이제어부(21)가 상기 랜덤값(N_i) 및 상기 비밀값(S_i)을 생성한 후, 상기 제어부(22)의 암호화용공개키(PK_{Ai}^E) 이용하여 암호화하

고, 상기 암호화된 랜덤값(N_i) 및 상기 암호화된 비밀값(S_i)을 자신의 서명용공개키(SK_G^S)를 이용하여 서명함으로써, 상기 제어부(21)로 전송할 수 있다.

[0035]

이후, 상기 서명된 랜덤값(N_i) 및 상기 서명된 비밀값(S_i)을 수신한 제어부(22)는 상기 게이트웨이제어부(21)의 서명용공개키(SK_G^S)를 이용하여 상기 서명된 랜덤값(N_i) 및 상기 서명된 비밀값(S_i)에 대한 서명을 검증하고, 자신의 암호화용공개키(SK_{Ai}^E)로 상기 검증된 랜덤값(N_i) 및 상기 검증된 비밀값(S_i)을 복호화함으로써, 상기 복호화된 랜덤값(N_i) 및 복호화된 비밀값(S_i)를 획득할 수 있다.

[0036]

이후, 제어부(22)가 상기 복호화된 비밀값(S_i) 이용하여 키유도함수(KDF: Key Derivation Function)를 통해 상기 제 1 세션키(EK_{Si})와 상기 제 2 세션키(AK_{Si}) 및 상기 세션키 갱신을 위한 업데이트키(KEK_{Si})를 생성할 수 있으며, 상기 제 1 세션키(EK_{Si})와 제 2 세션키(AK_{Si}) 및 상기 업데이트키(KEK_{Si})를 생성하는 것은 다음과 같이 표현할 수 있다.

수학식 1

$$KDF(S_i) = EK_i || AK_i || KEK_i$$

[0037]

또한, 게이트웨이제어부(21)가 n번째 제어부(22)에게 상기 제 1 세션키(EK_{Si})와 제 2 세션키(AK_{Si}) 및 상기 업데이트키(KEK_{Si})를 생성함에 있어서 필요한 파라미터인 비밀값(S_i) 및 랜덤값(N_i)을 암호화 및 서명하여 전달하는 것은 다음과 같이 표현할 수 있다.

수학식 2

$$Enc_{PK_{An}}(S_i, N_i) || Sign_{SK_G^S}(Enc_{PK_{An}}(S_i, N_i))$$

[0039]

여기서, 상기 암호화용 공개키 및 비밀키, 서명용 공개키 및 비밀키는 도 2의 인증서 등록과정에서 인증서에 포함되어 배포되거나, 도 1의 S110 단계 이전에 게이트웨이제어부가 안전한 채널을 통해 배포되거나, 제어부 제조과정에서 안전한 채널을 통해 등록될 수 있다.

[0040]

이제 다시 도 1로 돌아가 S110 단계 이후를 설명하도록 한다.

[0041]

도 4는 도 1의 S120 단계를 보다 세부적으로 도시한 흐름도이다.

[0042]

S410 단계에서, 상기 제어부가 상기 랜덤값 및 상기 메시지의 수신여부를 결정하는 식별자필드를 상기 제 1 세션키를 이용하여 암호화하여 상기 암호문을 생성한다.

[0043]

보다 구체적으로, 상기 제어부는 상기 제 1 세션키와 제 2 세션키 및 상기 업데이트키를 생성한 후, 키 생성 확인을 위해 상기 랜덤값과 상기 메시지의 수신여부를 결정하는 자신의 식별자필드(identifier field)를 상기 제 1 세션키를 이용하여 암호화함으로써 암호문을 생성할 수 있다.

[0044]

S420 단계에서, 상기 제어부가 상기 제 2 세션키 및 메시지 전송완료를 나타내는 카운터값을 이용하여 상기 제 1 메시지인증코드를 생성하고, 상기 암호문 및 상기 제 1 메시지인증코드를 상기 게이트웨이제어부로 송신할 수 있다.

[0045]

S430 단계에서, 상기 게이트웨이제어부가 상기 수신된 제 1 메시지인증코드를 검증함으로써, 상기 검증된 암호문을 상기 제 1 세션키를 통해 복호화하여 상기 제어부의 상기 제 1 세션키 및 상기 제 2 세션키 생성을 확인할

[0046]

수 있다.

- [0047] 보다 구체적으로, 상기 게이트웨이제어부는 수신된 제 1 메시지인증코드를 검증하여 암호문을 복호화함으로써, 상기 암호문에 포함된 상기 제어부의 식별자필드를 확인하여 연결된 제어부 중 어느 제어부가 세션키 생성을 완료하였는지를 확인할 수 있다.
- [0048] 여기서, 상기 카운터값은 게이트웨이제어부 및 상기 제어부가 패킷 전송을 순차적으로 모두 완료할 때마다 1이 증가할 수 있다.
- [0049] 또한, 상기 게이트웨이제어부는 상기 제 1 세션키와 상기 제 2 세션키 및 상기 업데이트키를 소정의 키 업데이트 주기에 따라 갱신하고, 상기 갱신된 제 1 세션키 및 상기 갱신된 제 2 세션키를 상기 갱신 이전의 업데이트키를 통해 암호화하여 상기 제어부로 송신할 수 있다. 여기서, 상기 제 1 세션키와 상기 제 2 세션키 및 상기 업데이트키를 갱신하는 것은 이하에서 도 5를 통해 설명하도록 한다.
- [0050] 도 5는 본 발명의 다른 실시예에 따른 키를 업데이트하는 과정을 도시한 흐름도로서, 제어부 간의 통신이 i 번째 세션이라고 할 때, $i+1$ 번째 세션을 위해 상기 제 1 세션키와 상기 제 2 세션키 및 상기 업데이트키가 갱신되는 과정이다.
- [0051] S510 단계에서, 게이트웨이제어부가 $i+1$ 번째 세션을 위해 키 생성에 필요한 랜덤값(N_{i+1}) 및 비밀값(S_{i+1})을 생성할 수 있다.
- [0052] S520 단계에서, S510 단계에서 생성한 랜덤값(N_{i+1}) 및 비밀값(S_{i+1})을 상기 i 번째 세션의 업데이트키(KEK_i)로 암호화하여 제어부로 전송할 수 있다.
- [0053] S530 단계에서, 상기 암호화된 랜덤값(N_{i+1}) 및 상기 암호화된 비밀값(S_{i+1})을 수신한 제어부는 상기 i 번째 세션의 업데이트키(KEK_i)로 복호화하여 상기 복호화된 랜덤값(N_{i+1}) 및 상기 복호화된 비밀값(S_{i+1})을 획득하며, 상기 복호화된 비밀값(S_{i+1})을 이용하여 키유도함수를 통해 제 1 세션키(EK_{i+1}')와 제 2 세션키(AK_{i+1}') 및 업데이트키(KEK_{i+1})를 생성할 수 있다.
- [0054] S540 단계에서, S530 단계에서 제 1 세션키(EK_{i+1}')와 제 2 세션키(AK_{i+1}') 및 업데이트키(KEK_{i+1})를 생성한 제어부가 상기 랜덤값(N_{i+1})과 자신의 식별자필드를 상기 제 1 세션키(EK_{i+1}')를 이용하여 암호화하여 암호문을 생성하고, 상기 제 2 세션키(AK_{i+1}') 및 카운터값을 이용하여 상기 제 1 메시지인증코드를 생성하며, 상기 암호문 및 상기 제 1 메시지인증코드를 상기 게이트웨이제어부로 송신할 수 있다. 또한, 상기 암호문 및 상기 제 1 메시지인증코드를 수신한 상기 게이트웨이제어부는 수신된 제 1 메시지인증코드를 검증하여 암호문을 복호화함으로써, 상기 암호문에 포함된 상기 제어부의 식별자필드를 확인하여 연결된 제어부 중 어느 제어부가 세션키 생성을 완료하였는지를 확인할 수 있다.
- [0055] S550 단계에서, 상기 게이트웨이제어부 및 제어부는 임의의 시간(T) 경과 후 i 번째 세션의 제 1 세션키(EK_i)와 상기 제 2 세션키(AK_i) 및 상기 업데이트키(KEK_i)를 삭제하고, $i+1$ 번째 세션의 제 1 세션키(EK_{i+1}')와 제 2 세션키(AK_{i+1}') 및 업데이트키(KEK_{i+1})를 사용하며, S510 단계로 돌아가 상기 게이트웨이제어부는 $i+2$ 번째 세션의 제 1 세션키(EK_{i+2}')와 제 2 세션키(AK_{i+2}') 및 상기 업데이트키(KEK_{i+2})를 생성하기 위한 랜덤값(N_{i+2}) 및 비밀값(S_{i+2}) 생성을 준비할 수 있다.
- [0056] 이제 다시 도 1로 돌아가 S120 단계 이후를 설명하도록 한다.
- [0057] 도 6은 도 1의 S130 단계를 보다 세부적으로 도시한 흐름도이다.
- [0058] S610 단계에서, 메시지를 송신하고자 하는 상기 제어부가 메시지 전송 완료를 나타내는 카운터값을 상기 제 1 세션키로 암호화하고, 상기 암호화된 카운터값과 송신하고자 하는 메시지 간에 배타적연산을 수행하여 상기 암호문을 생성한다.
- [0059] 보다 구체적으로, 현재 하나 이상의 제어부 간에 통신하는 세션을 i 세션이라고 할 때, 메시지를 송신하고자 하는 상기 제어부가 메시지 전송 완료를 나타내는 카운터값(CTR_i)을 상기 제 1 세션키(EK_i)로 암호화하고, 상기 암호화된 카운터값(CTR_i)과 송신하고자 하는 메시지(M) 간에 배타적연산(XOR)을 수행하여 상기 암호문(C)을 생성

하며, 상기 암호문(C)는 다음과 같이 표현할 수 있다.

수학식 3

$$C = E_{EK_{S_i}}(CTR_i) \oplus M$$

[0060]

[0061]

S620 단계에서, 메시지를 송신하고자 하는 상기 제어부가 상기 암호문 및 상기 메시지의 수신여부를 결정하는 식별자필드를 입력값으로 설정하고, 상기 메시지 전송 완료를 나타내는 카운터값과 상기 제 2 세션키를 이용하여 상기 제 2 메시지인증코드를 생성할 수 있다.

[0062]

보다 구체적으로, 메시지를 송신하고자 하는 상기 제어부가 상기 암호문(C) 및 상기 메시지의 수신여부를 결정

하는 식별자필드를 입력 값으로, $AK_i \oplus CTR_i$ 을 키값으로 하는 제 2 메시지인증코드를 생성할 수 있으며, 상기 제 2 메시지인증코드는 AES(Advanced Encryption Standard)알고리즘을 이용하는 K bits HMAC(Hash-based message authentication code)을 사용할 수 있으며, 상기 K 는 시스템 파라미터로서 사용되는 환경에 따라 64비트부터 512비트까지 암호학적 강도를 높여가며 적용가능할 수 있다.

[0063]

S630 단계에서, 메시지를 송신하고자 하는 상기 제어부가 송신하고자 하는 패킷 내 상기 암호문 및 상기 제 2 메시지인증코드를 포함시켜 상기 제어부로 송신한다. 이후, 상기 암호문 및 상기 제 2 메시지인증코드가 포함된 패킷을 전송완료한 상기 제어부는 자신의 카운터를 1만큼 증가시킬 수 있다.

[0064]

이제 다시 도 1로 돌아가 S130 단계 이후를 설명하도록 한다.

[0065]

도 7은 도 1의 S140 단계를 보다 세부적으로 도시한 흐름도이다.

[0066]

S710 단계에서, 상기 패킷을 수신한 제어부가 상기 패킷 내 포함된 상기 제 2 메시지인증코드를 상기 카운터값 및 상기 제 2 세션키를 통해 인증한다.

[0067]

보다 구체적으로, 도 6의 S630 단계에서 송신한 패킷을 수신한 제어부는 패킷 내 포함된 상기 제 2 메시지인증코드를 상기 카운터값 및 상기 제 2 세션키를 이용하여 상기 제 2 메시지인증코드를 인증함으로써, 인증된 암호문을 획득할 수 있다.

[0068]

S720 단계에서, 상기 패킷을 수신한 제어부가 상기 인증된 암호문을 상기 제 1 세션키를 통해 복호화함으로써, 상기 메시지를 획득한다.

[0069]

보다 구체적으로, S710 단계에서 획득한 인증된 암호문을 상기 제 1 세션키를 이용하여 복호화함으로써, 상기 복호화된 메시지를 획득할 수 있다. 이후 상기 패킷을 수신한 제어부는 상기 복호화된 메시지를 처리할 수 있다.

[0070]

도 8은 도 1 내지 도 7에서 사용되는 네트워크 패킷 구조를 도시한 도면이다.

[0071]

보다 구체적으로, 도 1 내지 도 7에서 사용되는 암호문(82) 및 메시지인증코드(83)는 상기 패킷 내의 데이터페이로드필드(Data payload field)(81)에 포함될 수 있다. 상기 네트워크 패킷 필드는 CAN FD 프로토콜에서 사용될 수 있으며, 상기 데이터페이로드필드는 최대 64바이트를 지원할 수 있다. 또한, 상기 게이트웨이제어부 및 제어부는 상기 CAN FD 프로토콜을 통해 메시지를 송수신할 수 있다.

[0072]

상기의 본 발명의 실시예들에 따르면, 인증서를 통해 제어부를 인증함으로써, 인증된 제어부만 통신에 참여할 수 있어 기밀성이 보장되는 효과가 있다. 또한, CAN FD 데이터 프레임 필드 중 데이터페이로드필드를 메시지인증코드를 위한 공간으로 사용함으로써, 데이터의 실시간 처리를 보장하며, 데이터의 무결성 및 인증기능을 수행할 수 있는 효과가 있다. 또한, 업데이트키를 이용하여 키를 주기적으로 업데이트 하고, 업데이트 되기전 키와 업데이트 되는 키를 함께 사용하는 유예기간이 존재함으로써, 업데이트 시 실시간적인 데이터의 처리를 보장하는 효과가 있다.

[0073]

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.

[0074] 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.

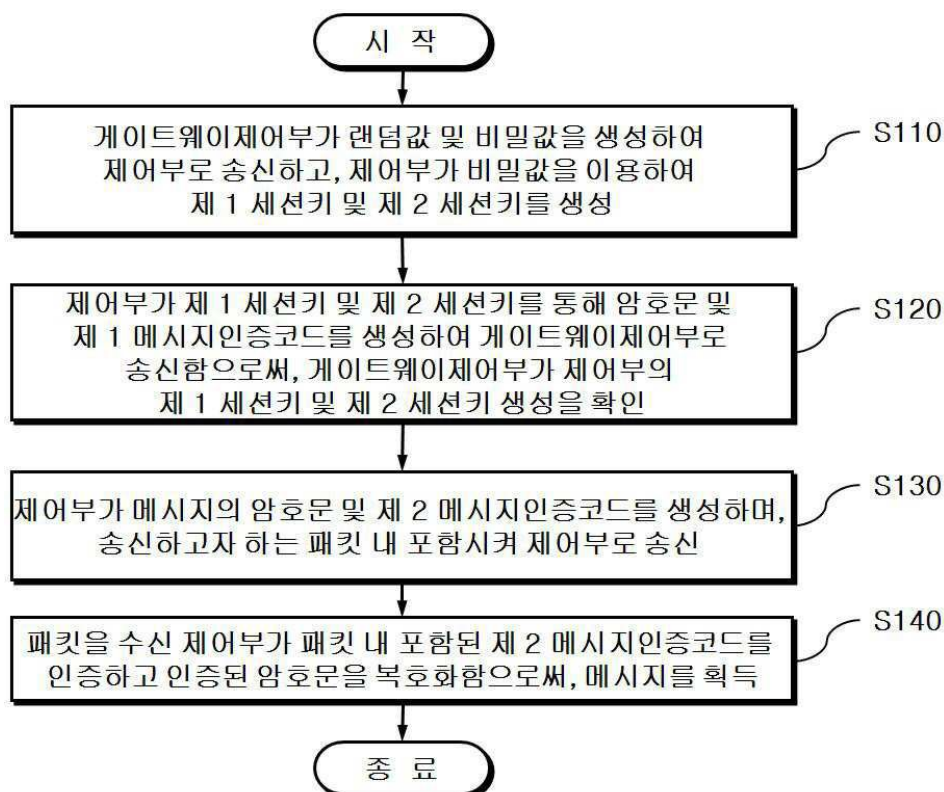
[0075] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

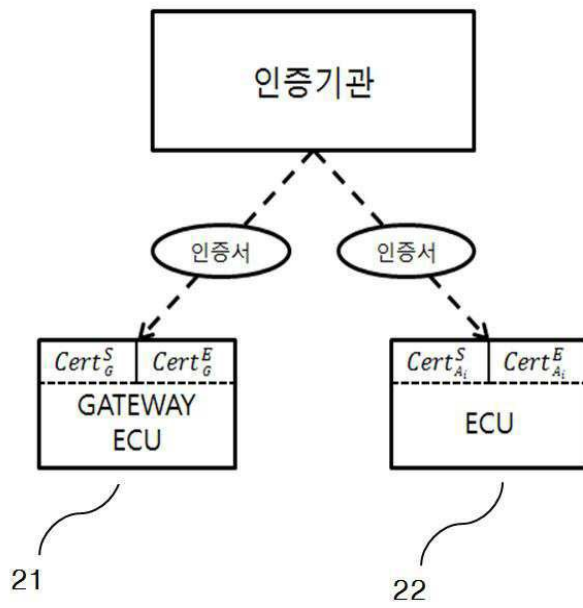
[0076] 21 : 게이트웨이제어부(gateway ECU)
22 : 제어부(ECU)
81 : 데이터페이로드필드
82 : 암호문
83 : 메시지인증코드

도면

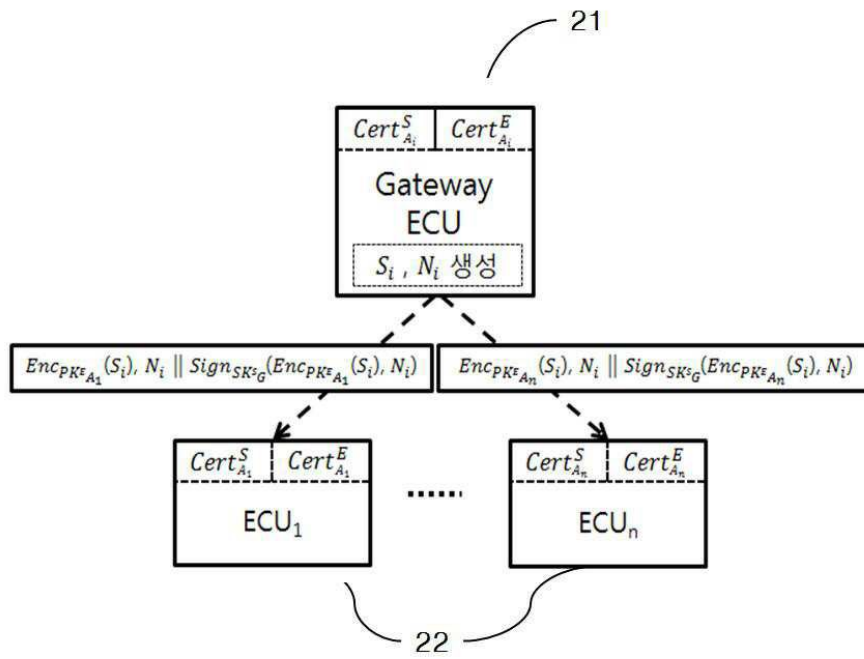
도면1



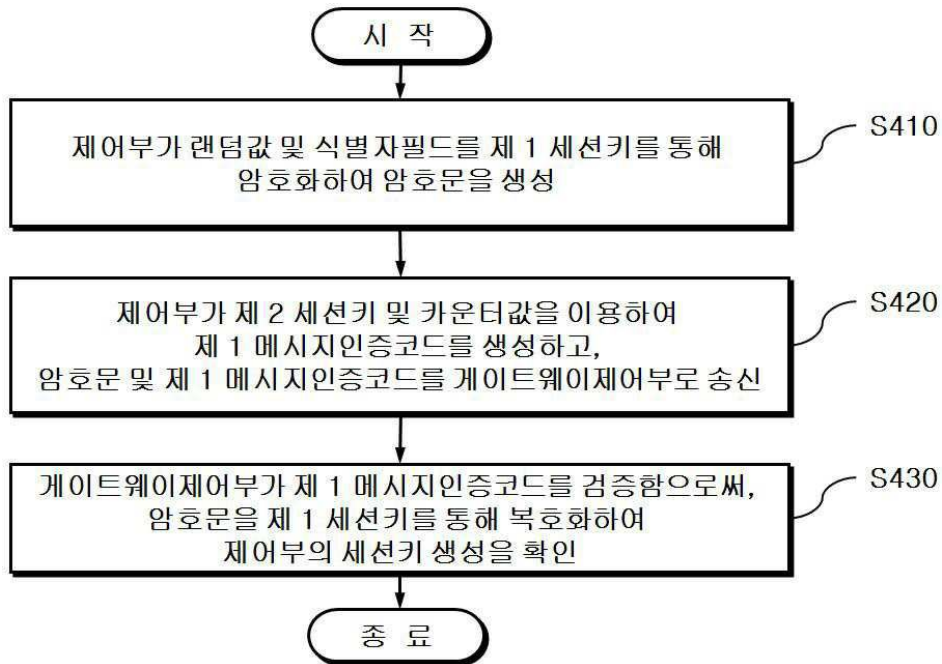
도면2



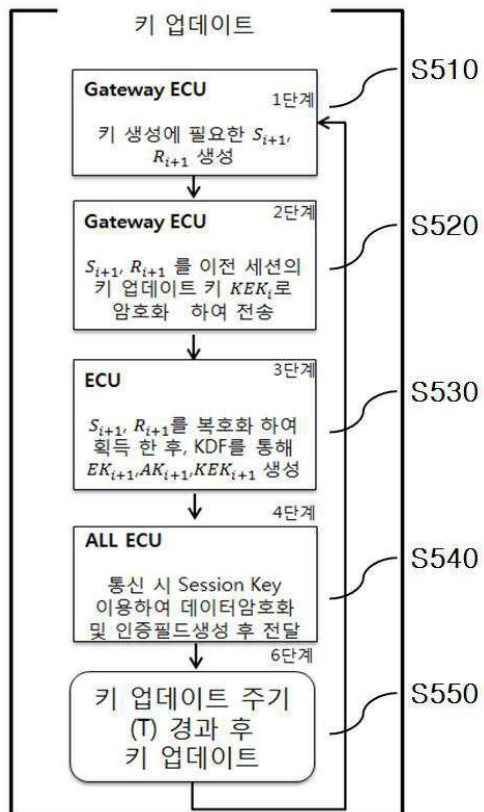
도면3



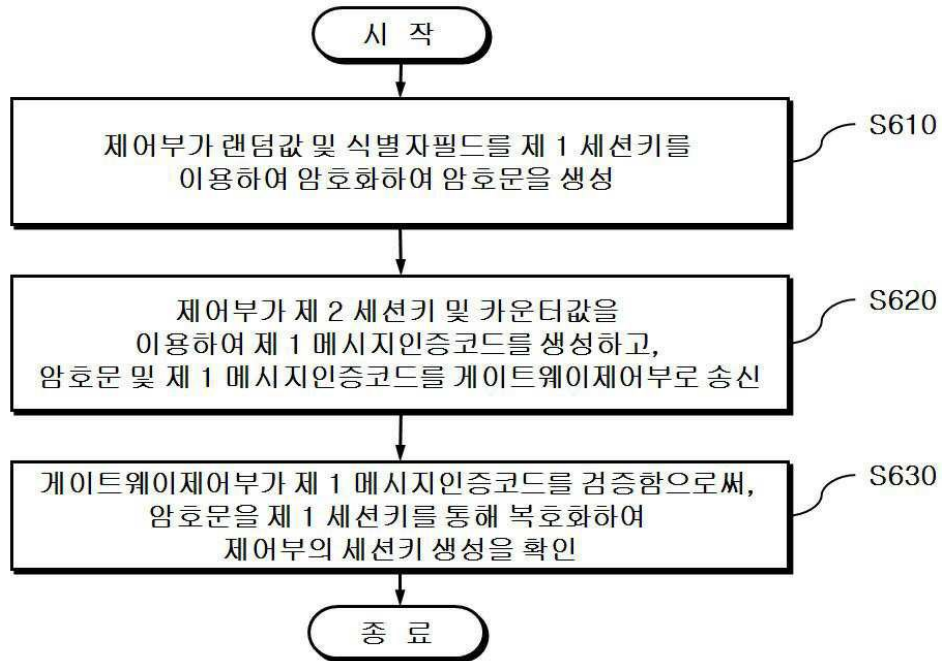
도면4



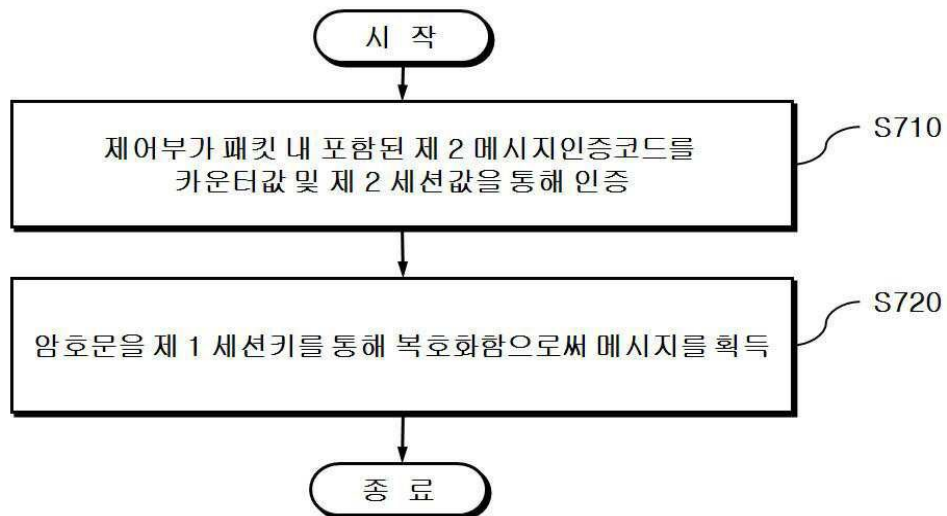
도면5



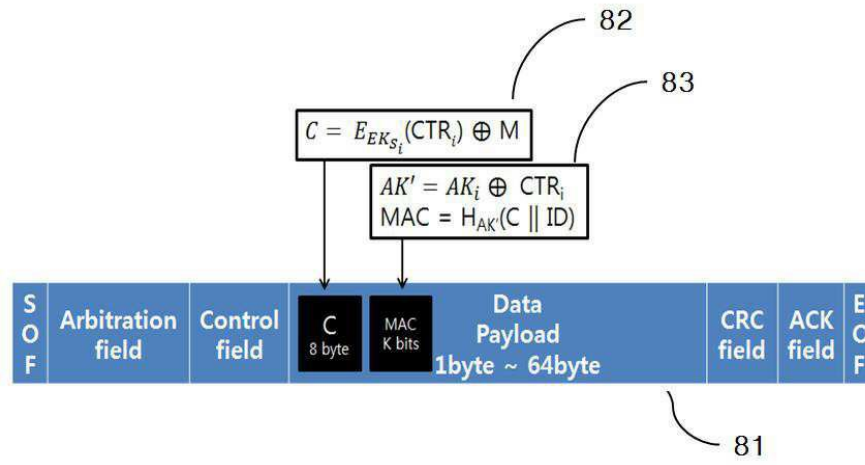
도면6



도면7



도면8



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제7항

【변경전】

"상기 암호문"

【변경후】

"상기 제 2 암호문"