



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년05월30일
(11) 등록번호 10-1740957
(24) 등록일자 2017년05월23일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) B60R 16/02 (2006.01)
B60R 25/10 (2006.01) H04L 12/40 (2006.01)
H04L 9/06 (2006.01) H04L 9/08 (2006.01)
H04L 9/14 (2006.01)

(52) CPC특허분류
H04L 9/3242 (2013.01)
B60R 16/02 (2013.01)

(21) 출원번호 10-2016-0005555

(22) 출원일자 2016년01월15일

심사청구일자 2016년01월15일

(56) 선행기술조사문헌

KR1020130021157 A*

A. Menezes 외 2명, Handbook of Applied Cryptography, Chapter .9,10,12, CRC Press (1996)*

조아람 외 4명, CAN 버스 공격에 안전한 메시지 인증 및 키 분배 메커니즘, 정보보호학회논문지 22(5), pp.1057-1068 (2012.10.)

김태수 외 3명, ECU간 기기인증을 위한 HB-Family 경량인증기법의 적용 방법, 정보보호학회논문지 Vol.23, No. 4 (2013.8.)

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

우사무엘

서울특별시 송파구 오금로53길 7 403호 (거여동, 명산주택)

이동훈

서울특별시 종로구 사직로8길 34, 1404호(내수동, 경희궁의아침3단지아파트)

조효진

서울특별시 성북구 안암로 145 자연계캠퍼스 로봇융합관 403호 (안암동5가,고려대학교안암캠퍼스)

(74) 대리인

김등용, 김홍석

전체 청구항 수 : 총 9 항

심사관 : 양종필

(54) 발명의 명칭 차량용 데이터의 인증 및 획득 방법

(57) 요약

적어도 하나 이상의 일반 전자제어장치와 게이트웨이 전자제어장치(GECU) 및 이를 연결하는 통신 버스를 포함하는 차량용 통신 시스템에서 상기 게이트웨이 전자제어장치(GECU) 및 일반 전자제어장치(ECU_i)가 차량용 데이터를 인증하고 획득하는 방법이 개시된다. 상기 차량용 데이터의 인증 및 획득 방법은 상기 게이트웨이 전자제어장

(뒷면에 계속)

대표도 - 도3



100

치(GECU) 및 상기 일반 전자제어장치(ECU_i)가 차량 제조 단계에서 미리 저장되어 있는 대칭키를 기반으로 세션 암호키 및 세션 인증키를 포함하는 세션키를 분배하는 단계 및 상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 어느 하나의 장치가 메시지 인증 코드, 데이터 프레임 카운터, 및 암호문(C)을 포함하는 차량용 데이터를 전송하고, 상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 다른 하나의 장치가 상기 메시지 인증 코드를 검증하고 상기 암호문을 복호화함으로써, 상기 차량용 데이터를 인증하고 획득하는 단계를 포함한다.

(52) CPC특허분류

B60R 25/10 (2013.01)
H04L 9/0625 (2013.01)
H04L 9/0819 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/0891 (2013.01)
H04L 9/14 (2013.01)
H04L 9/3228 (2013.01)
H04L 2012/40215 (2013.01)
H04L 2012/40273 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	B01011505530003003
부처명	미래창조과학부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보통신방송연구개발사업
연구과제명	자동차 전장 ECU간 보안전송기술 개발
기 여 율	1/1
주관기관	인포뱅크
연구기간	2015.03.01 ~ 2016.02.29

명세서

청구범위

청구항 1

CAN FD(Controller Area Network with Flexible Data rate) 통신 시스템을 이용하여 차량용 데이터를 전송하는 제1 전자제어장치 및 상기 차량용 데이터를 수신하는 제2 전자제어장치가 차량용 데이터를 인증하고 획득하는 방법에 있어서,

상기 제1 전자제어장치 및 상기 제2 전자제어장치가 차량 제조 단계에서 미리 저장되어 있는 대칭키를 기반으로 게이트웨이 전자제어장치(GECU)와 세션 암호키 및 세션 인증키를 포함하는 세션키를 분배하는 세션키 분배 단계;

상기 제1 전자제어장치가 상기 제1 전자제어장치의 데이터 프레임 카운터 및 암호화 함수를 이용하여 전송하고자 하는 데이터(M)를 암호화하여 암호문(C)을 생성하는 단계;

상기 제1 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 암호학적 해쉬 함수를 이용하여 메시지 인증 코드를 생성하는 단계;

상기 제1 전자제어장치가 상기 메시지 인증 코드, 상기 데이터 프레임 카운터, 및 상기 암호문(C)을 상기 제2 전자제어장치에 전송하는 단계;

상기 제2 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 상기 암호학적 해쉬 함수를 이용하여 상기 메시지 인증 코드를 검증하는 단계; 및

상기 메시지 인증 코드 검증에 통과하면, 상기 제2 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 상기 암호학적 해쉬 함수를 이용하여 상기 암호문(C)을 복호화하여 상기 데이터(M)를 획득하는 단계;를 포함하는

상기 세션키 분배 단계는,

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 제1 난수를 선택하는 단계;

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 상기 제1 난수를 상기 게이트웨이 전자제어장치(GECU)에 전송하는 단계;

상기 게이트웨이 전자제어장치(GECU)가 제2 난수를 선택하고, 아래의 수학적식1에 의해 제1 인증값을 생성하는 단계;

(수학적식1) $MAC_{ik-1} = H_{SK_i}(R_{i-k} || Seed_k)$

(여기서, i는 ECU의 ID, MAC_{ik-1} 는 ECU_i에 대한 k번째 세션에서의 제1 인증값, H_{SK_i} 는 ECU_i의 인증용 대칭키인 SK_i를 키로 사용하는 일 방향 해쉬 함수, R_{i-k} 는 ECU_i에 대한 k번째 세션에서의 제1 난수, Seed_k는 ECU_i에 대한 k번째 세션에서의 제2 난수)

상기 게이트웨이 전자제어장치(GECU)가 상기 제2 난수 및 상기 제1 인증값을 상기 제1 전자제어장치 또는 상기 제2 전자제어장치에 전송하는 단계;

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 상기 제1 인증값을 상기 수학적식1을 이용하여 검증하는 단계;

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 아래의 수학적식2에 의해 세션 암호키(EK_k) 및 세션 인증키(AK_k)를 포함하는 k번째 세션에서의 세션키를 생성하는 단계;

(수학적식2) $KDF_{SK_G}(Seed_k) = EK_k || AK_k$

(여기서 KDF_{SK_G} 는 키 생성용 대칭키인 SK_G를 키로 사용하는 키생성함수)

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 아래의 수학적식3에 의해 제2 인증값을 생성하는 단계;

(수학적식3) $MAC_{ik_2} = H_{SK_i}(Seed_k)$

(여기서, MAC_{ik_2} 는 ECU_i에 대한 k번째 세션에서의 제2 인증값)

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 상기 제2 인증값을 상기 게이트웨이 전자제어장치(GECU)에 전송하는 단계;

상기 게이트웨이 전자제어장치(GECU)가 상기 제2 인증값을 상기 수학적식3을 이용하여 검증하는 단계; 및

상기 게이트웨이 전자제어장치(GECU)가 상기 수학적식2에 의해 상기 세션 암호키(EK_k) 및 상기 세션 인증키(AK_k)를 포함하는 k번째 세션에서의 상기 세션키를 생성하는 단계;를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 2

제1항에 있어서,

상기 세션키 분배 단계 수행하기 전,

상기 제1 전자제어장치 및 상기 제2 전자제어장치가 상기 암호화 함수 및 상기 암호학적 해쉬 함수를 저장하는 단계를 더 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 3

제1항에 있어서,

상기 제1 전자제어장치가 상기 메시지 인증 코드, 상기 데이터 프레임 카운터, 및 상기 암호문(C)을 CAN FD 데이터 프레임의 데이터페이로드 영역에 적재하여 상기 제2 전자제어장치에 전송하며,

상기 데이터페이로드 영역은 상기 메시지 인증 코드를 적재하는 제1 영역, 상기 데이터 프레임 카운터를 적재하는 제2 영역, 및 상기 암호문(C)을 적재하는 제3 영역을 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 4

제1항에 있어서,

상기 제1 전자제어장치 또는 상기 제2 전자제어장치가 상기 세션키의 업데이트를 수행할지 여부를 결정하는 단계; 및

상기 세션키 업데이트를 수행하기로 결정한 경우, 상기 제1 전자제어장치 및 상기 제2 전자제어장치가 상기 대칭키를 기반으로 업데이트 세션 암호키 및 업데이트 세션 인증키를 포함하는 업데이트 세션키를 분배하는 단계;를 더 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 5

제4항에 있어서,

상기 암호화 함수는 상기 제1 전자제어장치가 차량용 데이터를 송신하는 세션에 대응하는 세션 암호키 또는 업데이트 세션 암호키로 암호화를 수행하고,

상기 암호학적 해쉬 함수는 상기 제1 전자제어장치가 차량용 데이터를 송신하는 세션에 대응하는 세션 인증키 또는 업데이트 세션 인증키로 상기 메시지 인증 코드를 생성하는 차량용 데이터의 인증 및 획득 방법.

청구항 6

적어도 하나 이상의 일반 전자제어장치와 게이트웨이 전자제어장치(GECU) 및 이를 연결하는 통신 버스를 포함하는 차량용 통신 시스템에서 상기 게이트웨이 전자제어장치(GECU) 및 일반 전자제어장치(ECU_i)가 차량용 데이터를 인증하고 획득하는 방법에 있어서,

상기 게이트웨이 전자제어장치(GECU) 및 상기 일반 전자제어장치(ECU_i)가 차량 제조 단계에서 미리 저장되어

있는 대칭키를 기반으로 세션 암호키 및 세션 인증키를 포함하는 세션키를 분배하는 세션키 분배 단계; 및

상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 어느 하나의 장치가 메시지 인증 코드, 데이터 프레임 카운터, 및 암호문(C)을 포함하는 차량용 데이터를 전송하고, 상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 다른 하나의 장치가 상기 메시지 인증 코드를 검증하고 상기 암호문을 복호화함으로써, 상기 차량용 데이터를 인증하고 획득하는 단계;를 포함하고,

상기 세션키 분배 단계는,

상기 일반 전자제어장치(ECU_i)가 제1 난수를 선택하는 단계;

상기 일반 전자제어장치(ECU_i)가 상기 제1 난수를 상기 게이트웨이 전자제어장치(GECU)에 전송하는 단계;

상기 게이트웨이 전자제어장치(GECU)가 제2 난수를 선택하고, 아래의 수학식1에 의해 제1 인증값을 생성하는 단계;

$$(수학식1) MAC_{ik_1} = H_{SK_i}(R_{i_k} || Seed_k)$$

(여기서, MAC_{ik_1} 는 ECU_i에 대한 k번째 세션에서의 제1 인증값, H_{SK_i} 는 ECU_i의 인증용 대칭키인 SK_i 를 키로 사용하는 일 방향 해쉬 함수, R_{i_k} 는 ECU_i에 대한 k번째 세션에서의 제1 난수, $Seed_k$ 는 ECU_i에 대한 k번째 세션에서의 제2 난수)

상기 게이트웨이 전자제어장치(GECU)가 상기 제2 난수 및 상기 제1 인증값을 상기 일반 전자제어장치(ECU_i)에 전송하는 단계;

상기 일반 전자제어장치(ECU_i)가 상기 제1 인증값을 상기 수학식1을 이용하여 검증하는 단계;

상기 일반 전자제어장치(ECU_i)가 아래의 수학식2에 의해 세션 암호키(EK_k) 및 세션 인증키(AK_k)를 포함하는 k번째 세션에서의 세션키를 생성하는 단계;

$$(수학식2) KDF_{SK_G}(Seed_k) = EK_k || AK_k$$

(여기서 KDF_{SK_G} 는 키 생성용 대칭키인 SK_G 를 키로 사용하는 키생성함수)

상기 일반 전자제어장치(ECU_i)가 아래의 수학식3에 의해 제2 인증값을 생성하는 단계;

$$(수학식3) MAC_{ik_2} = H_{SK_i}(Seed_k)$$

(여기서, MAC_{ik_2} 는 ECU_i에 대한 k번째 세션에서의 제2 인증값)

상기 일반 전자제어장치(ECU_i)가 상기 제2 인증값을 상기 게이트웨이 전자제어장치(GECU)에 전송하는 단계;

상기 게이트웨이 전자제어장치(GECU)가 상기 제2 인증값을 상기 수학식3을 이용하여 검증하는 단계; 및

상기 게이트웨이 전자제어장치(GECU)가 상기 수학식2에 의해 상기 세션 암호키(EK_k) 및 상기 세션 인증키(AK_k)를 포함하는 k번째 세션에서의 상기 세션키를 생성하는 단계;를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 7

제6항에 있어서,

상기 게이트웨이 전자제어장치(GECU) 및 상기 일반 전자제어장치(ECU_i)는 CAN FD(Controller Area Network with Flexible Data rate) 통신 시스템을 이용하여 통신하며,

상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i)가 메시지 인증 코드, 데이터 프레임 카운터, 및 암호문(C)을 CAN FD 데이터 프레임의 데이터페이로드 영역에 적재하여 상기 일반 전자제어장치(ECU_i) 또는 상기 게이트웨이 전자제어장치(GECU)에 전송하고,

상기 데이터페이로드 영역은 상기 메시지 인증 코드를 적재하는 제1 영역, 상기 데이터 프레임 카운터를 적재하는 제2 영역, 및 상기 암호문(C)을 적재하는 제3 영역을 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 8

제6항에 있어서,

상기 일반 전자제어장치(ECU_i)에 저장된 대칭키는 상기 일반 전자제어장치(ECU_i) 고유의 인증용 대칭키(SK_i) 및 키 생성용 대칭키(SK_G)를 포함하고,

상기 게이트웨이 전자제어장치(GECU)에 저장된 대칭키는 상기 게이트웨이 전자제어장치(GECU)와 통신을 수행하는 일반 전자제어장치(ECU_i)들의 인증용 대칭키(SK_i)들 및 상기 키 생성용 대칭키(SK_G)를 포함하는 차량용 데이터의 인증 및 획득 방법.

청구항 9

제6항에 있어서,

상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i)가 상기 세션키의 업데이트를 수행할지 여부를 결정하는 단계를 포함하고,

상기 세션키의 업데이트를 수행하기로 결정한 경우, 상기 게이트웨이 전자제어장치(GECU) 및 상기 일반 전자제어장치(ECU_i)가 상기 세션키를 분배하는 단계를 반복하여 수행하는 차량용 데이터의 인증 및 획득 방법.

발명의 설명

기술 분야

[0001] 본 발명의 개념에 따른 실시 예는 차량용 데이터의 인증 및 획득 방법에 관한 것으로, 특히, 게이트웨이 전자제어장치(GECU) 및 게이트웨이 전자제어장치와 데이터 통신을 수행하는 전자제어장치(ECU_i)가 대칭키 기반의 세션키를 분배하고, 상기 세션키를 이용하여 차량용 데이터의 인증 및 암호화/복호화를 수행함으로써, 데이터의 기밀성과 인증을 보장할 수 있는 차량용 데이터의 인증 및 획득 방법에 관한 것이다.

배경 기술

[0002] 최근에 출시되는 자동차들은 주행 안전과 연비 향상을 위해 전자제어 환경으로 변하고 있다. 자동차 내부에 탑재된 전자제어시스템들은 하나 이상의 전자제어장치 (ECU, Electronic Control Unit)로 구성된다. 각 전자제어시스템에 소속된 전자제어장치들은 상호 간의 데이터 전송을 위해 통신 환경을 구성하고 있다. 자동차 내부 전자제어장치 간 통신환경 구축을 위해 CAN (Controller Area Network), CAN FD(Controller Area Network with Flexible Data rate), FlexRay 등의 표준 통신 프로토콜을 사용하고 있다.

[0003] CAN은 BUS Network 구조를 사용하여 자동차 내부에 통신 회선을 획기적으로 감소시켰다. 또한 1Mbps(Mega bit per second)의 통신 속도를 제공하면서도 외부 전자기파나 노이즈에 강한 장점을 갖고 있다. 그러나 자동차-IT 기술 융합이 급증하고 자동차와 가전기기(예를 들어, 태블릿 PC, 스마트폰)를 연결하는 서비스가 상용화되면서 자동차 내부 네트워크 트래픽 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] 이러한 제약사항을 극복하기 위해 2012년 데이터 전송 속도와 데이터 페이로드를 확장한 CAN FD(CAN with Flexible Data rate)가 개발되었다. CAN FD는 기존 CAN과 동일한 통신방식을 사용하면서 전송 속도와 데이터 페이로드를 증가시켰다. CAN FD는 최대 10Mbps(Mega bit per second)의 전송 속도와 64바이트(byte)의 데이터 페이로드를 지원함으로써 자동차-IT 융합기술로 인해 급증한 자동차 내부 ECU간의 데이터 전송 수요를 충족시킬 수 있다.

[0005] 하지만, 보안적인 측면에서 CAN 및 CAN FD는 몇 가지 취약점을 갖고 있다. CAN 및 CAN FD는 브로드캐스트 통신 방식을 사용하기 때문에 통신상의 모든 데이터가 외부로 노출되는 문제점이 있다. 또한, 데이터 기밀성을 제공하지 않기 때문에 통신상의 모든 데이터의 의미를 분석할 수 있으며, 데이터 인증을 제공하지 않기 때문에 통신상에 전송되는 데이터의 위조-변조를 방지할 수 없으며, 재전송 공격으로부터 안전하지 않다. 또한, 접근제어 기능이 없기 때문에 통신 회선에 접속한 모든 노드는 통신상의 모든 데이터를 모니터링 할 수 있고, 자신이 원

하는 데이터를 송신할 수 있다. 즉, CAN FD에는 데이터의 도청이나 위/변조 및 재전송을 방지할 수 있는 보안 메커니즘이 적용되어 있지 않으며, 따라서 악의적인 공격자는 이를 이용하여 차량을 임의로 제어하거나 내부의 중요 데이터를 획득할 수 있다.

[0006] 이러한 문제점을 해결하기 위하여, 향상된 통신 속도와 데이터 페이로드를 지원하는 CAN FD를 이용하고 ECU의 연산 능력을 고려한 차량용 제어 데이터의 기밀성과 인증을 보장하는 보안 기술이 요구된다.

[0007] 한편, 이하에서 인용되는 선행기술 문헌에서는 인증서 기반으로 세션키를 생성하고 이를 이용하여 차량용 데이터의 인증을 수행하는 방법을 개시하고 있다.

[0008] 본 명세서에서는 ECU 고유의 대칭키를 기반으로 세션키를 생성하고, 데이터 프레임에 메시지 카운터를 추가함으로써 보다 효율적으로 차량용 데이터를 인증할 수 있는 방법을 제안한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) KR 10-1481403 B1

발명의 내용

해결하려는 과제

[0010] 본 발명이 이루고자 하는 기술적인 과제는 차량 내부 통신 시스템에 포함된 ECU들 간의 네트워크 통신 시, 송수신 되는 차량용 데이터의 인증을 용이하게 수행하는 차량용 데이터의 인증 방법을 제공하는 것이다.

[0011] 데이터 기밀성 및 인증을 제공하는 CAN FD 데이터 프레임 구조를 제공하는 것이다.

과제의 해결 수단

[0012] 본 발명의 실시 예에 따른 차량용 통신 시스템에서 차량용 데이터를 전송하는 제1 전자제어장치 및 상기 차량용 데이터를 수신하는 제2 전자제어장치가 차량용 데이터를 인증하고 획득하는 방법은 상기 제1 전자제어장치 및 상기 제2 전자제어장치가 차량 제조 단계에서 미리 저장되어 있는 대칭키를 기반으로 세션 암호키 및 세션 인증키를 포함하는 세션키를 분배하는 단계, 상기 제1 전자제어장치가 상기 제1 전자제어장치의 데이터 프레임 카운터 및 암호화 함수를 이용하여 전송하고자 하는 데이터(M)를 암호화하여 암호문(C)을 생성하는 단계, 상기 제1 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 암호학적 해쉬 함수를 이용하여 메시지 인증코드를 생성하는 단계, 상기 제1 전자제어장치가 상기 메시지 인증 코드, 상기 데이터 프레임 카운터, 및 상기 암호문(C)을 상기 제2 전자제어장치에 전송하는 단계, 상기 제2 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 상기 암호학적 해쉬 함수를 이용하여 상기 메시지 인증 코드를 검증하는 단계, 및 상기 메시지 인증 코드 검증에 통과하면, 상기 제2 전자제어장치가 상기 데이터 프레임 카운터, 상기 암호문(C), 및 상기 암호학적 해쉬 함수를 이용하여 상기 암호문(C)을 복호화하여 상기 데이터(M)를 획득하는 단계를 포함한다.

[0013] 또한, 본 발명의 실시 예에 따른 적어도 하나 이상의 일반 전자제어장치와 게이트웨이 전자제어장치(GECU) 및 이를 연결하는 통신 버스를 포함하는 차량용 통신 시스템에서 상기 게이트웨이 전자제어장치(GECU) 및 일반 전자제어장치(ECU_i)가 차량용 데이터를 인증하고 획득하는 방법은 상기 게이트웨이 전자제어장치(GECU) 및 상기 일반 전자제어장치(ECU_i)가 차량 제조 단계에서 미리 저장되어 있는 대칭키를 기반으로 세션 암호키 및 세션 인증키를 포함하는 세션키를 분배하는 단계, 및

[0014] 상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 어느 하나의 장치가 메시지 인증 코드, 데이터 프레임 카운터, 및 암호문(C)을 포함하는 차량용 데이터를 전송하고, 상기 게이트웨이 전자제어장치(GECU) 또는 상기 일반 전자제어장치(ECU_i) 중 다른 하나의 장치가 상기 메시지 인증 코드를 검증하고 상기 암호문을 복호화함으로써, 상기 차량용 데이터를 인증하고 획득하는 단계를 포함한다.

발명의 효과

[0015] 본 발명의 실시 예에 따른 차량용 데이터의 인증 방법에 의하면, 자동차 제조 단계에 모든 ECU에 저장되는 대칭

키를 기반으로 ECU를 인증함으로써, 정당한 ECU만 통신에 참여할 수 있어 기밀성이 보장되는 효과가 있다.

[0016] 또한, CAN FD 데이터 프레임 필드 중 데이터페이로드필드를 메시지인증코드를 위한 공간으로 사용함으로써, 데이터 기밀성 및 인증을 제공할 수 있으며, 또한, CAN FD 데이터 프레임 필드 중 데이터페이로드필드를 데이터 프레임 카운터를 위한 공간으로 사용함으로써, 동기화를 생략할 수 있다.

[0017] 메시지 인증코드 생성 시 카운터 값을 이용하여 데이터 재전송 공격을 통한 비정상적인 자동차 제어를 방지하는 효과가 있다.

[0018] 또한, 메시지 인증코드와 메시지 카운터 그리고 암호문을 효율적으로 적재할 수 있는 CAN FD 데이터 프레임에 이용하여 데이터 기밀성 및 인증을 제공하면서 ECU간 통신 데이터의 실시간 처리를 보장할 수 있다.

[0019] 또한, 업데이트키를 이용하여 세션키를 주기적으로 업데이트함으로써, 데이터 재전송 공격을 통한 비정상적인 자동차 제어를 방지하는 효과가 있다.

도면의 간단한 설명

[0020] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 차량용 통신 시스템을 도시한다.

도 2는 CAN FD 데이터 프레임 포맷을 도시한다.

도 3은 도 1에 도시된 차량용 데이터 인증 및 획득 장치의 기능 블록도이다.

도 4는 도 1에 도시된 차량용 데이터 인증 및 획득 장치들의 차량용 데이터 인증 및 획득 방법을 설명하기 위한 흐름도이다.

도 5는 도 4의 S200 단계를 보다 세부적으로 도시한 흐름도이고, 도 6은 도 4의 S300 단계를 보다 세부적으로 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0022] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0023] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0024] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0025] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

- [0026] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.
- [0027] 도 1은 본 발명의 일 실시 예에 의한 차량용 통신 시스템을 도시한다. 차량용 통신 시스템(10)은 차량용 통신 시스템을 의미할 수 있으며, 구체적으로는 CAN FD(Controller Area Network with Flexible Data rate) 통신 시스템일 수 있다. 그러나 본 발명이 차량용 통신 시스템(10)의 종류에 제한되는 것은 아니며, 실시 예에 따라 상기 통신 시스템은 CAN(Controller Area Network), Flexray, LIN(Local Interconnect Network), 또는 MOST(Multimedia Oriented Systems Transport) 통신 시스템일 수도 있다.
- [0028] 도 1을 참조하면, 통신 시스템(10)은 복수의 전자제어장치(Electronic Control Unit, ECU, 100)들과 게이트웨이 ECU(GECU, 100G), 및 버스(bus; 12)를 포함한다. 상기 GECU는 일반 ECU보다 성능이 높으며, 게이트웨이 역할을 하는 ECU를 의미한다.
- [0029] 상기 복수의 ECU들은 제1 ECU(ECU_1), 제2 ECU(ECU_2), 제3 ECU(ECU_3), 및 제4 ECU(ECU_4)를 포함한다. 도 1에는 총 4개의 전자제어장치(ECU_i, i는 ECU의 ID)가 도시되어 있으나, 통신 시스템(10)에 포함된 전자제어장치(ECU_i)의 개수는 n(n은 2 이상의 자연수)일 수 있다.
- [0030] 상기 복수의 전자제어장치(ECU_i)들 각각은 대응되는 전자 장치의 동작을 제어할 수 있으며, 버스(12)를 통하여 다른 ECU와 통신할 수 있다. 전자제어장치(ECU_i)들은 버스(12, 예를들어, CAN FD 통신 버스)에 연결되어 있고 브로드캐스트(broadcast) 방식으로 통신한다.
- [0031] GECU를 포함한 모든 ECU들은 안전한 환경에서 대칭키를 공유한다. 상기 ECU 및 상기 GECU를 제작할 때, 대칭키가 상기 ECU 및 상기 GECU에 탑재될 수 있다. 대칭키는 인증용 대칭키(SK_i)와 키 생성용 대칭키(SK_G)를 포함한다. 구체적으로, GECU를 포함하는 모든 ECU는 키 생성용 대칭키(SK_G)를 공유하고 있다. 제1 ECU에는 제1 인증용 대칭키(SK_1)가 탑재되어 있고, 제2 ECU에는 제2 인증용 대칭키(SK_2)가 탑재되어 있다. 제3 ECU 및 제4 ECU에는 각각 제3 인증용 대칭키(SK_3) 및 제4 인증용 대칭키(SK_4)가 탑재되어 있다. 게이트웨이 ECU(GECU)는 GECU와 연결된 복수의 ECU들에 대응하는 인증용 대칭키들(SK_1, SK_2, SK_3, SK_4)이 탑재되어 있다. 즉, 인증용 대칭키(SK_i)는 ID가 i인 ECU(ECU_i)와 GECU가 사전에 공유하고 있는 인증키를 의미하고, 키 생성용 대칭키(SK_G)는 GECU를 포함하는 모든 ECU가 사전에 공유하고 있는 키 생성키를 의미한다.
- [0032] 도 2는 본 발명에 일 실시예에 따른 CAN FD 프로토콜의 데이터 프레임의 구성을 도시한 것으로서, 크게 데이터 프레임의 송신자를 식별할 수 있는 ID 정보를 포함하는 중재 필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터페이로드(Data Payload)로 구성된다. CAN FD 데이터 프레임은 최대 64바이트(byte)의 데이터페이로드를 지원하며, 64byte의 데이터를 한 번에 전송할 수 있다.
- [0033] 본 발명의 일 실시예에 따른 CAN FD 데이터 프레임의 데이터페이로드는 총 3가지 영역을 포함한다. 제1 영역은 메시지인증코드(MAC) 적재 영역이다. 제1 영역에는 암호문과 데이터 프레임 카운터를 이용하여 생성된 메시지인증코드(MAC)를 적재한다. 제1 영역의 사이즈는 16바이트(byte)이다.
- [0034] 제2 영역은 데이터 프레임 카운터 적재 영역이다. 데이터 프레임 카운터(CTR_ECU_i)는 특정 ECU가 송신한 데이터 프레임의 전송 횟수를 나타낸다. 예를 들어, ECU_i가 총 4개의 데이터 프레임을 전송한 후 5번째 데이터 프레임을 전송하려 할 때 ECU_i의 데이터 프레임 카운터(CTR_ECU_i)는 5로 설정된다. 제2 영역의 사이즈는 4바이트(byte)이다. 제 1 영역 및 제 2영역의 사이즈는 고정이다. 제 1 영역과 제 2 영역을 제외한 44바이트(byte)를 데이터 전송에 사용할 수 있다.
- [0035] 제 3 영역은 암호문 적재 영역이다. 암호문(C)은 해당 세션에 대한 암호화 키(EK_k)를 이용하여 평문(M)을 암호화하여 생성한다.
- [0036] 도 3는 본 발명의 일 실시예에 따른 차량용 데이터의 인증 및 획득을 수행하는 장치(100)의 기능 블록도이다. 본 발명의 일 실시예에 따른 차량용 데이터 인증 및 획득 장치는 차량용 전자제어장치(ECU, 100)일 수 있다.
- [0037] 도 3을 참조하면, 차량용 데이터의 인증 및 획득을 수행하는 차량용 데이터의 인증 및 획득 장치(100)는 세션키 관리부(110), 인증부(130), 암호화부(150), 복호화부(160), 통신부(170), 저장부(180) 및 제어부(190)을 포함한다.
- [0038] 세션키 관리부(110)는 세션키 생성부 및 업데이트 관리부를 포함하며, 제어부(190)의 제어 하에,
- [0039] 인증부(130)는 메시지 인증 코드 생성부 및 메시지 인증 코드 검증부를 포함하며, 제어부(190)의 제어 하에 메시지 인증 코드를 생성하고 이를 검증하여 차량용 데이터의 인증을 수행한다.

- [0040] 암호화부(150)는 제어부(190)의 제어하에, 다른 차량용 데이터의 인증 및 획득 장치로 전송하고자 하는 데이터(CAN FD 데이터)를 데이터 프레임 카운터 및 세션키 중 암호키(EK_k)를 이용하여 암호화한다.
- [0041] 복호화부(160)는 다른 차량용 데이터의 인증 및 획득 장치로부터 수신한 암호문에 대하여, 데이터 프레임 카운터 및 세션키 중 암호키(EK_k)를 이용하여 복호화를 수행하고 평문을 획득한다.
- [0042] 통신부(170)는 제어부(190)의 제어 하에, 통신 버스(CAN FD 버스, 12)를 이용하여 복수 개의 차량용 데이터의 인증 및 획득 장치(ECU 또는 GECU, 100)와 통신을 수행할 수 있다. 즉, 각각의 ECU(ECU_i) 및 GECU로부터 CAN FD 데이터를 수신할 수 있으며, 각각의 ECU(ECU_i) 및 GECU에 메시지 인증 코드, 데이터 프레임 카운터, 및 암호문 등을 포함하는 CAN FD 데이터를 전송할 수 있다. 본 실시예와는 달리, 상기 통신부는 대응되는 전자제어장치와 별도로 구현될 수도 있다.
- [0043] 저장부(180)는 제어부(190)의 제어하에, 차량용 데이터 인증 및 획득에 필요한 함수, 키, 인증값, 또는 차량용 데이터 등을 저장한다.
- [0044] 제어부(190)는 차량용 데이터의 인증 및 획득을 수행하는 전자제어장치(ECU, 100)의 전반적인 동작을 제어한다. 즉, 세션키 관리부(110), 인증부(130), 암호화부(150), 복호화부(160), 통신부(170), 및 저장부(180)의 동작을 제어할 수 있다.
- [0045] 도 4는 본 발명의 일 실시예에 따른 차량용 데이터의 인증 및 획득을 수행하는 전자제어장치의 차량용 데이터의 인증 및 획득 방법을 설명하기 위한 흐름도이다.
- [0046] 도 4를 참조하면, 차량용 데이터의 인증 및 획득 방법은 대칭키 공유 단계(S100), 세션키 분배 단계(S200), 차량용 데이터 인증 및 획득 단계(S300), 및 세션키 업데이트(재분배) 여부를 결정하는 단계(S400)를 포함한다. 해당 세션에 대응하는 세션키를 이용하여, 해당 세션동안 데이터 인증 및 획득 단계를 반복하여 수행한다. 또한, 일정 기준에 따라 세션키를 주기적으로 업데이트하여 업데이트된 세션키를 이용하여 데이터 인증 및 획득 단계를 반복 수행한다.
- [0047] 먼저, 차량용 통신 시스템(10)에서 차량용 데이터의 인증 및 획득을 수행하기에 앞서, GECU를 포함한 모든 ECU들은 안전한 환경에서 대칭키를 공유한다(S100). ECU의 제조사는 상기 ECU 및 상기 GECU를 제작할 때, 대칭키를 상기 ECU 및 상기 GECU에 탑재할 수 있다. 구체적으로 대칭키는 인증용 대칭키(SK_i)와 키 생성용 대칭키(SK_G)를 포함한다. GECU를 포함한 모든 ECU들은 키 생성용 대칭키(SK_G)를 안전하게 공유하며, 각각의 ECU_i는 각각의 ECU_i에 대응하는 인증용 대칭키(SK_i)를 안전하게 저장하고, GECU는 GECU와 연결된 모든 ECU_i의 인증용 대칭키(SK_i)들을 안전하게 저장한다.
- [0048] 다음, 차량용 데이터 인증 및 획득 장치는 차량용 데이터를 송수신하기 전, 세션키를 분배한다(S200). 세션키 분배 단계는 초기 세션키 분배 단계 및 세션키 재분배(업데이트) 단계를 포함한다. 자동차에 시동이 걸리면 가장 먼저 초기 세션 키(제1 세션키, Initial Session Key)를 분배한다.
- [0049] 도 5는 초기 세션키 분배 과정을 보다 세부적으로 도시한 도면이다.
- [0050] 도 5를 참조하면 세션 키는 제k 세션 암호 키(EK_k)와 제k 세션 인증 키(AK_k) 두 가지가 있다. 이때, k는 현재 통신하려고 하는 세션의 순서를 의미한다. 세션 키 분배 과정은 ECU의 ID 순서대로 진행된다. 특정 ECU_i가 GECU와 세션 키 분배과정을 수행할 때 다른 ECU들은 통신에 참여하지 않고 자신의 순서를 기다린다. 초기 세션 키 분배과정을 통해 생성되는 세션 키는 제1 세션 암호 키(EK₁)와 제1 세션 인증 키(AK₁)이며 이때 사용되는 Seed는 Seed₁이다. 이후 k번째 세션에서 사용될 세션 키는 제k 세션 암호 키(EK_k)와 제k 세션 인증 키(AK_k)이며 이때 사용되는 Seed는 Seed_k이다. ECU_i와 GECU 사이에 수행되는 세션 키 분배 과정은 다음과 같다.
- [0051] 먼저, 초기 세션 키 분배 과정 시작을 위해 ECU_i는 제1 난수(R_i)를 생성(S210)하여 GECU에게 전송한다(S220).
- [0052] 다음, 제1 난수(R_i)를 수신한 GECU는 제2 난수(Seed₁)를 생성한다(S231).
- [0053] 다음, GECU는 제1 난수 및 제2 난수를 이용하여 제1 인증 값(MAC₁)을 생성한다(S233). 제1 인증 값(MAC₁)을 생성하는 식은 아래와 같다.

수학식 1

[0054] $MAC_1 = H_{SK_i}(R_i || Seed_1)$

[0055] 이때, $H_{SK_i}()$ 는 'SK_i'를 키로 사용하는 일 방향 해쉬 함수를 의미한다.

[0056] 다음, GECU는 제2 난수(Seed_1)와 제1 인증값(MAC_1)을 ECU_i에게 전송한다(S240).

[0057] 다음, ECU_i는 전송받은 제1 인증값(MAC_1)을 검증한다(S251). 제1 인증값(MAC_1)검증 방법은 상기 수학식 1과 동일하다. 모든 ECU들과 GECU는 인증용 대칭키(SK_i) 및 상기 해쉬 함수를 공유하고 있기 때문에 제1 인증값(MAC_1)의 생성과 검증을 수행할 수 있다.

[0058] 제1 인증값(MAC_1) 검증이 정상적으로 종료되면 ECU_i는 제2 난수(Seed_1)를 이용하여 세션 키를 생성한다(S253). 제k 세션에 대응하는 세션 키는 데이터 프레임 암호화에 사용하는 제k 세션 암호 키(EK_k)와 데이터 프레임 인증에 사용하는 제k 세션 인증키(AK_k)를 포함하며, 초기 세션 키 분배 과정에서, ECU_i는 제1 인증값(MAC_1)을 검증한 후, 제1 세션 암호 키(EK_1) 및 제1 세션 인증 키(AK_1)를 포함하는 제1 세션키를 생성한다. 첫 번째 세션의 세션 키 생성 방법은 수학식 2와 같다.

수학식 2

[0059] $KDF_{SK_G}(Seed_1) = EK_1 || AK_1$

[0060] 이때, $KDF_{SK_G}()$ 는 'SK_G'를 키로 사용하는 키 생성 함수(또는 키 유도 함수, public key derivation function)를 의미한다.

[0061] 다음, 세션 키 생성을 완료한 ECU_i는 제 2 인증값(MAC_2)을 생성한다(S255). 제 2 인증값(MAC_2) 생성 방법은 수학식 3과 같다.

수학식 3

[0062] $MAC_2 = H_{SK_i}(Seed_1)$

[0063] 다음, ECU_i는 GECU에게 제2 인증값(MAC_2)을 전송한다(S260).

[0064] GECU는 제2 인증값(MAC_2) 수신 후, 상기 수학식 3을 이용하여, 제2 인증값(MAC_2) 검증을 수행한다(S271).

[0065] 제2 인증값(MAC_2) 검증이 정상적으로 종료되면 GECU는 제2 난수(Seed_1)를 이용하여 제1 세션 키(EK_1, AK_1)를 생성한다(S273). 세션 키 생성 방법은 상기 수학식 3과 동일하다.

[0066] 상기 과정을 모두 수행하면 GECU와 ECU_i 사이의 초기 세션 키 분배과정이 종료된다. 모든 ECU들은 ECU_i와 동일한 초기 세션 키 분배 과정을 수행한다. 모든 ECU들이 상기 과정을 정상적으로 수행하면 초기 세션 키 분배과정이 종료된다.

[0067] 초기 세션 키 분배과정을 정상적으로 종료한 후 자동차는 데이터 암호화 및 인증(S300)을 수행하여 안전한 통신 환경을 구축한다. 다음, 일정 기준에 따라 세션키 업데이트 여부를 결정(S400)하고 새로운 세션키를 분배한다(S200). 예를 들어, 초기 세션 키를 사용하는 동안 특정 시간(T)이 지난 시점, 또는 송신 ECU의 데이터 프레임 카운터(CTR_ECU_i)가 '0'으로 초기화되기 전 시점을 세션키 업데이트 여부를 결정하는 기준 시점으로 설정하고, 이를 기준으로 세션키 업데이트 여부를 결정한 후, 세션키 업데이트 단계를 수행한다. 세션 키 업데이트 단계는 초기 세션 키 분배 단계와 동일한 과정을 수행한다. k번째 세션에서 수행되는 세션 키 업데이트 방법은 아래와 같다.

[0068] ECU_i는 k번째 세션의 임의의 제1 난수(R_i_k)를 생성하여 GECU에게 전송하고, k번째 세션의 제1 난수(R_i_k)를

수신한 GECU는 k번째 세션의 제2 난수(Seed_k)를 생성한다. GECU는 ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1})을 생성하고, k번째 세션의 제2 난수(Seed_k)와 ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1})을 ECU_i에게 전송한다. ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1}) 생성 방법은 아래와 같다.

수학식 4

$$MAC_{ik-1} = H_{SK_i}(R_{i_k} || Seed_k)$$

ECU_i는 전송받은 상기 수학식 4를 이용하여 ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1})을 검증한다. 모든 ECU들과 GECU는 SK_i 및 해쉬 함수를 공유하고 있기 때문에 ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1})의 생성과 검증을 수행할 수 있다.

ECU_i에 대한 k번째 세션에서의 제1 인증 값(MAC_{ik-1}) 검증이 정상적으로 종료되면 ECU_i는 k번째 세션의 제2 난수(Seed_k)를 이용하여 제k 세션 암호 키(EK_k)과 제k 세션 인증 키(AK_k)를 포함하는 제k 세션 키를 생성한다. 제k 세션 키 생성 방법은 수학식 5와 같다.

수학식 5

$$KDF_{SK_G}(Seed_k) = EK_k || AK_k$$

제k 세션 키 생성을 완료한 ECU_i는 k번째 세션에서의 제2 인증 값(MAC_{ik-2})를 생성하여 GECU에게 전송한다. ECU_i에 대한 k번째 세션에서의 제2 인증 값(MAC_{ik-2}) 생성 방법은 수학식 6과 같다.

수학식 6

$$MAC_{ik-2} = H_{SK_i}(Seed_k)$$

다음, GECU는 상기 수학식 6을 이용하여 전송받은 ECU_i에 대한 k번째 세션에서의 제2 인증 값(MAC_{ik-2})을 검증하고, 검증이 정상적으로 종료되면 GECU는 k번째 세션의 제2 난수 및 상기 수학식 5를 이용하여 제k 세션 키(EK_k, AK_k)를 생성한다.

상기 과정을 모두 수행하면 GECU와 ECU_i 사이의 세션 키 업데이트 과정이 종료된다. 모든 ECU들에 대하여 동일한 과정을 수행한다. 모든 ECU들이 상기 과정을 정상적으로 수행하면 세션 키 업데이트 과정이 종료된다.

초기 세션 키 분배 과정 또는 키 업데이트 과정을 정상적으로 수행한 GECU와 모든 ECU들은 두 개의 세션 키를 저장하고 있다. 즉, k번째 세션에 GECU와 모든 ECU들은 제k 세션 암호키(EK_k) 및 제k 세션 인증키(AK_k)를 포함하는 제k 세션키를 저장하고 있다.

다음, 상기 제k 세션키를 이용하여, 차량용 데이터를 인증하고 획득한다(S300). 송신 ECU는 데이터 프레임을 송신할 때 데이터 프레임 암호화와 인증을 수행하고, 수신 ECU는 수신한 데이터 프레임의 메시지인증코드(MAC) 검증 작업을 수행한 후 암호문 복호화를 수행한다.

도 6은 차량용 보안 데이터 송신/수신 과정 및 인증/획득 과정을 보다 상세하게 도시한 도면이다. 도 6을 참조하면, 송신 ECU(ECU_s)는 자신의 데이터 프레임 카운터(CTR_{ECU_s})와 전송하고자 하는 평문(M)을 이용하여 암호문(C)을 생성한다(S311). 암호문 생성 방법은 아래의 수학식 7과 같다.

수학식 7

[0080]

$$C = E_{EK_k}(CTR_ECU_s) \oplus M$$

[0081]

이때, $E_{EK_k}()$ 는 'EK_k'를 키로 사용하는 암호화 함수를 의미한다.

[0082]

다음, 송신 ECU(ECU_s)는 데이터 프레임 카운터(CTR_ECU_s)와 암호문(C)를 이용하여 메시지 인증 코드(MAC_s)를 생성한다(S313). 메시지 인증 코드(MAC_s) 생성 방법은 수학식 8과 같다.

수학식 8

[0083]

$$MAC_s = H_{AK_k}(C || CTR_ECU_s)$$

[0084]

다음, 송신 ECU(ECU_s)는 메시지 인증 코드(MAC_s), 데이터 프레임 카운터(CTR_ECU_s), 및 암호문(C)을 포함하는 데이터 프레임을 수신 ECU(ECU_r)에게 송신하고(S330), 송신 ECU(ECU_s)는 데이터 프레임 카운터(CTR_ECU_s)를 1만큼 증가시킨다.

[0085]

수신 ECU(ECU_r)는 송신 ECU(ECU_s)가 송신한 데이터 프레임을 수신하고, 상기 데이터 프레임으로부터 메시지 인증 코드(MAC_s), 데이터 프레임 카운터(CTR_ECU_s), 및 암호문(C)을 획득한다.

[0086]

수신 ECU(ECU_r)는 상기 수학식 8을 이용하여 메시지 인증 코드(MAC_s)를 검증한다(S351).

[0087]

메시지 인증 코드(MAC_s) 검증이 정상적으로 종료되면, 상기 수학식 7을 이용하여 평문(M)을 획득한다(S353).

[0088]

상술한 차량용 데이터 인증 및 획득 방법은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0089]

예를 들어, 기록매체에 저장되며 대칭키 기반으로 세션키를 생성하고, 이를 이용하여 차량용 데이터의 암호화, 인증, 및 복호화를 수행하는 차량용 데이터 인증 및 획득 프로그램으로서, 상기 프로그램은 컴퓨팅 시스템에서 실행되는 세션키 분배하는 명령어 세트, 세션키를 업데이트하는 명령어 세트, 데이터의 암호화를 수행하는 명령어 세트, 메시지 인증 코드를 이용하여 데이터 인증을 수행하는 명령어 세트, 및 암호화된 데이터의 복호화를 수행하는 명령어 세트를 포함할 수 있다.

[0090]

상기 차량용 데이터 인증 및 분석 프로그램은 상기 기록매체에 저장되며, 상기 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)와 같은 저장매체를 포함한다. 또한, 상기 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 명령어 세트가 저장되고 실행될 수 있다.

[0091]

본 발명에서 개시된 블록도들은 본 발명의 원리들을 구현하기 위한 회로를 개념적으로 표현한 형태라고 당업자에게 해석될 수 있을 것이다. 유사하게, 임의의 흐름 차트, 흐름도, 상태 전이도, 의사코드 등은 컴퓨터 판독가능 매체에서 실질적으로 표현되어, 컴퓨터 또는 프로세서가 명시적으로 도시되든지 아니든지 간에 이러한 컴퓨터 또는 프로세서에 의해 실행될 수 있는 다양한 프로세스를 나타낸다는 것이 당업자에게 인식될 것이다.

[0092]

본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0093]

10 : 차량용 통신 시스템

12 : 버스

100 : 차량용 데이터 인증 및 획득 장치, ECU

- 110 : 세션키 관리부

130 : 인증부

150 : 암호화부

160 : 복호화부

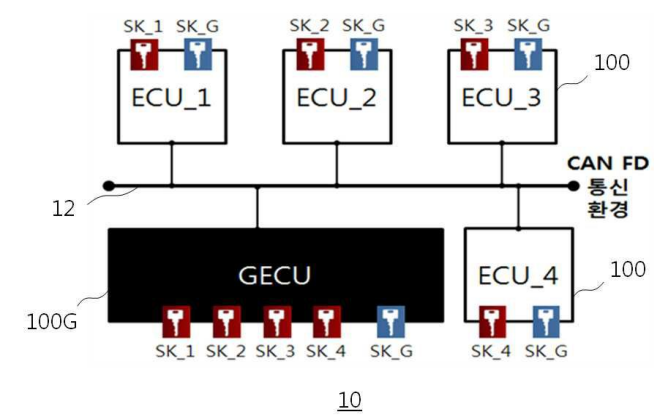
170 : 통신부

180 : 저장부

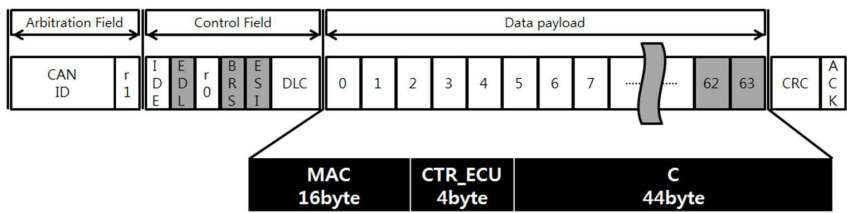
190 : 제어부

도면

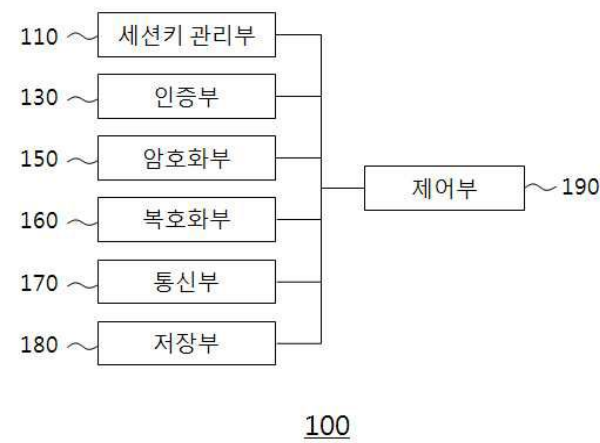
도면1



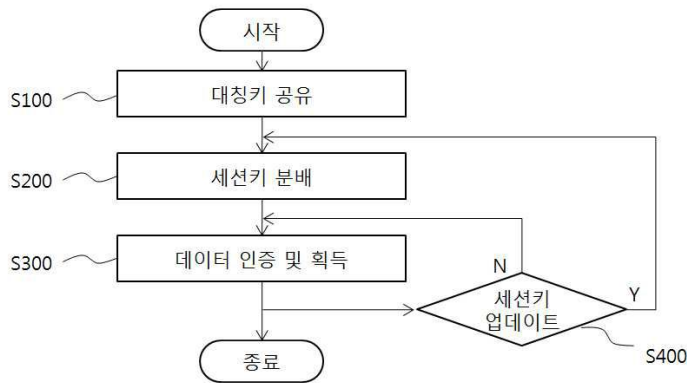
도면2



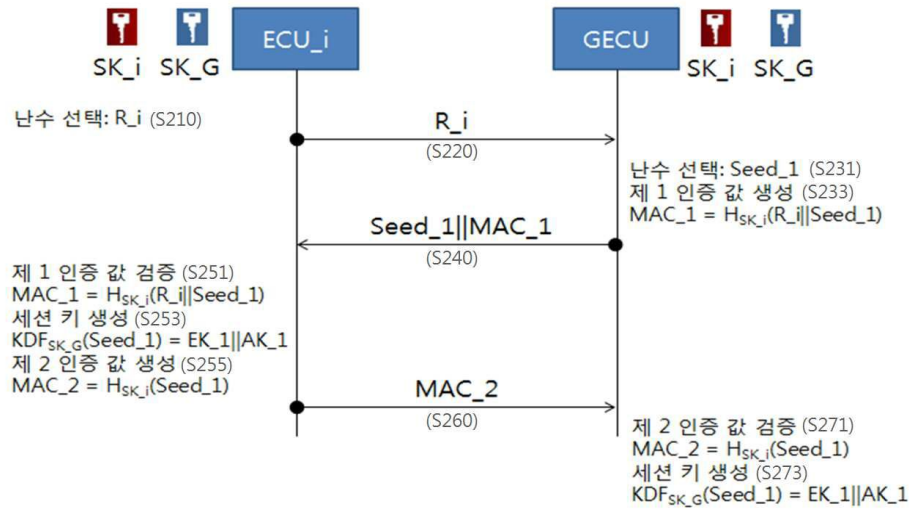
도면3



도면4



도면5



도면6

