



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0067605
(43) 공개일자 2025년05월15일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) H04L 12/40 (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3242 (2013.01)
H04L 9/0866 (2013.01)
(21) 출원번호 10-2023-0153920
(22) 출원일자 2023년11월08일
심사청구일자 2023년11월08일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
원종훈
경기도 광명시 소하로 38, 210동 104호(소하동, 휴먼시아2단지아파트)
안상훈
대전광역시 서구 만년로 25, 109동 102호(만년동, 강변아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 7 항

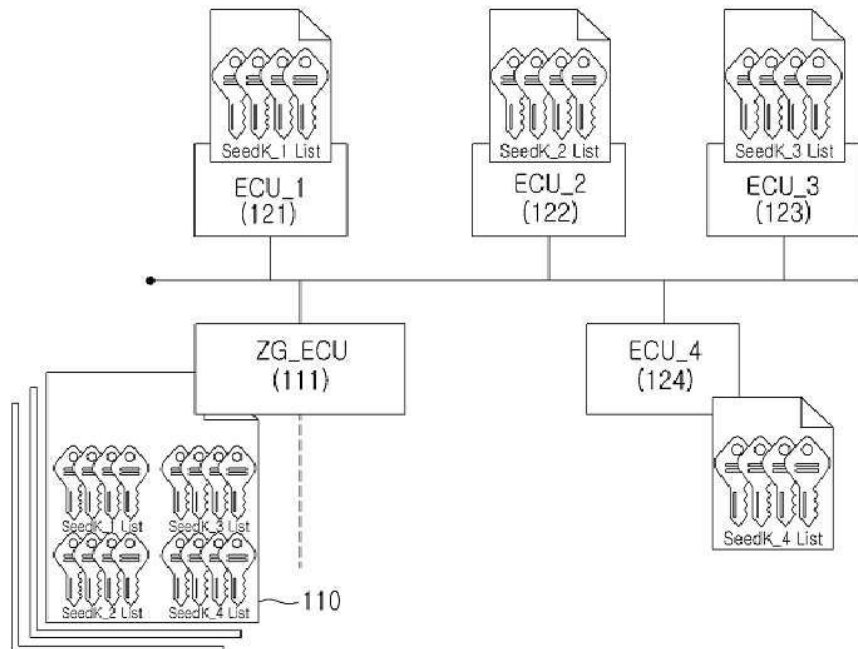
(54) 발명의 명칭 차량용 데이터의 인증 및 획득을 위한 방법 및 시스템

(57) 요약

게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 방법 및 시스템이 제시된다. 본 발명에서 제안하는 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 방법은 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기

(뒷면에 계속)

대표도 - 도1



초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 단계 -상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포됨-, 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 단계 및 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계를 포함한다.

(52) CPC특허분류

H04L 9/0869 (2013.01)

H04L 9/0891 (2013.01)

H04L 2012/40215 (2013.01)

H04L 2209/84 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711189818
과제번호	2020R1A2C2013091
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	중견연구
연구과제명	[Ezbaro] 미래 한국형 위성항법시스템을 이용하는 커넥티드 무인이동체 개발을 위한
민군겸용 가상환경 시뮬레이터 기술	
기 여 율	1/1
과제수행기관명	인하대학교
연구기간	2023.03.01 ~ 2024.02.29

명세서

청구범위

청구항 1

게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 방법에 있어서, 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 단계 -상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포됨-;

일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계;

상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 단계; 및

게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계

를 포함하는 차량용 데이터 인증 및 획득 방법.

청구항 2

제1항에 있어서,

상기 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC 태그 세션키를 생성하는 단계는,

복수의 일반 전자제어장치 각각에서 데이터 메시지에 대한 시드키 갱신 주기에 따라 일반 전자제어장치가 출력하는 CAN(Controller Area Network) 메시지는 시드키 목록을 공유하고, 상기 데이터 메시지 각각에 대한 ID 및 정보를 MAC 키 생성 함수에 입력하여 MAC 태그 세션키를 생성하는

차량용 데이터 인증 및 획득 방법.

청구항 3

제1항에 있어서,

상기 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계는,

데이터 프레임의 송신자 및 프레임 우선순위를 식별하는 ID 정보를 포함하는 중재 필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터 필드(Data Field)로 구성되는 CAN FD(CAN with Flexible Data rate) 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 제1 MAC를 생성하는

차량용 데이터 인증 및 획득 방법.

청구항 4

제1항에 있어서,

상기 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계는,

CAN FD 프로토콜의 데이터 프레임에 따른 데이터 메시지로 통신하는 일반 전자제어장치의 데이터 프레임 필드에서 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 MAC 태그 세션키를 생성하여 하나의 메시지 데이터 보안이 깨지더라도 해킹으로 획득한 데이터 인증절차를 다른 메시지 프레임에 적용할 수 없고,

게이트웨이 전자제어장치에서 일정 주기로 카운터 정보를 활용하여 MAC 태그 세션키를 주기적으로 업데이트 함

으로써 데이터 메시지 재전송을 통한 비정상적인 자동차 제어를 방지하는 차량용 데이터 인증 및 획득 방법.

청구항 5

게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 시스템에 있어서,

일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 MAC 태그 세션키 생성부 -상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포됨-;

일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하고, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 MAC 생성부; 및

게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 판별부

를 포함하는 차량용 데이터 인증 및 획득 시스템.

청구항 6

제5항에 있어서,

상기 MAC 태그 세션키 생성부는,

복수의 일반 전자제어장치 각각에서 데이터 메시지에 대한 시드키 갱신 주기에 따라 일반 전자제어장치가 출력하는 CAN(Controller Area Network) 메시지는 시드키 목록을 공유하고, 상기 데이터 메시지 각각에 대한 ID 및 정보를 MAC 키 생성 함수에 입력하여 MAC 태그 세션키를 생성하는

차량용 데이터 인증 및 획득 시스템.

청구항 7

제5항에 있어서,

상기 MAC 생성부는,

데이터 프레임의 송신자 및 프레임 우선순위를 식별하는ID 정보를 포함하는 중재 필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터 필드(Data Field)로 구성되는 CAN FD(CAN with Flexible Data rate) 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 MAC를 생성하는

차량용 데이터 인증 및 획득 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 차량용 데이터의 인증 및 획득을 위한 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 현대의 차량은 운전자의 편의성과 안정성, 효율성을 증대하기 위하여 첨단 운전자 보조 시스템(Advanced Driver Assistance Systems; ADAS)의 도입이 가속화되고 있다. 이로 인해 자동차 내부에 구비되는 전자 부품의 증대가 이뤄지고 있으며, 이를 제어하는 전자제어장치(Electronic Control Unit; ECU)의 개수가 증가하고 있다.

[0003] 전통적 차량의 E/E(Electiric and Electronic) 아키텍처로는 증가하는 ECU로 인한 통신 시스템 및 차량 배선의 복잡도를 감당할 수 없기에 현대적인 E/E 아키텍처인 영역 기반 아키텍처(Zonal architecture)방식으로 통신시스템을 적용하고 있다.

- [0004] Zonal 아키텍처는 Zonal 게이트웨이(ZG_ECU)로 다수의 ECU를 물리적 근접성에 따라 몇 개의 Zone으로 분할하며 상기 Zonal 게이트웨이는 Zone 내 연결된 전자 부품 및 ECU에 대한 인터페이스, 기기 간 배전 및 스위치 기능을 수행하여 통신 시스템을 최적화한다.
- [0005] 이러한 Zonal 통신 네트워크는 기존 차량의 파워트레인, 샤시, 바디에서 주로 사용되던 네트워크인 CAN(Controller Area Network), LIN(Local Interconnect Network), FlexRay중 제조비용의 최소화, 실시간 처리, 자동화, 분산처리 부분에서 장점이 있는 CAN 네트워크를 주로 적용하였으나, Zone 네트워크 내 전자 제어 장치(ECU)이 단순 전자부품의 제어 기능만을 수행하는 것이 아니라 센서 퓨전 및 ADAS 도메인 제어를 수행하기 위하여 고성능 AP(Application Processor)로 발전하고 있어, 이에 따른 Zone 백본(Backbone) 네트워크도 고속에 더 많은 데이터 전송 수요를 충족해야 한다.
- [0006] 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 Zone 네트워크에 연결된 고성능 AP가 탑재된 ECU간의 데이터 전송 수요를 충족시킬 수 있다.
- [0007] 하지만 보안적인 측면에서 CAN FD는 기존 CAN 네트워크의 브로드 캐스트 통신 방식을 사용하기 때문에 통신상의 모든 데이터가 외부로 노출되는 문제점이 여전히 존재한다. CAN 네트워크와의 호환성을 유지하기 위해 데이터 기밀성을 제공하지 않고, 통신상의 모든 데이터 의미 분석이 가능하며, 데이터 인증을 제공하지 않기에 통신상에 전송되는 데이터의 위/변조를 방지할 수 없어, 재 전송 공격으로부터 안전하지 않다.
- [0008] 즉, CAN FD는 CAN통신에서 비롯된 데이터의 도청, 위/변조 및 재전송을 방지하는 보안 매커니즘이 여전히 적용되어 있지 않아, 공격자는 ADAS기능이 탑재된 첨단 자동차의 ADAS 어플리케이션 기능을 임의로 제어하거나 내부 데이터를 획득할 수 있다. 이러한 문제점을 해결하기 위해 CAN FD를 이용하고 Zonal 게이트웨이 내 기동하는 ECU의 데이터 기밀성과 인증을 보장하는 보안기술이 요구된다.

선행기술문헌

특허문헌

- [0009] (특허문헌 0001) 한국등록특허 제10-1740957호(2017.05.23)

발명의 내용

해결하려는 과제

- [0010] 본 발명이 이루고자 하는 기술적 과제는 차량 내부 통신에 포함된 ECU간의 네트워크 통신 시 송/수신되는 차량용 데이터의 인증 및 보안을 ZG_ECU가 관장하여 차량용 데이터의 인증을 용이하게 수행하는 차량용 데이터의 인증 및 획득을 위한 방법 및 시스템을 제공하는데 있다. 본 발명의 실시예에 따르면, 데이터의 기밀성 및 인증을 제공하는 차량용 네트워크 및 CAN FD데이터 프레임 구조를 제공하고자 한다.

과제의 해결 수단

- [0011] 일 측면에 있어서, 본 발명에서 제안하는 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 방법은 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 단계 -상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포됨-, 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 단계 및 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계를 포함한다.
- [0012] 상기 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어

장치 MAC 태그 세션키를 생성하는 단계는 복수의 일반 전자제어장치 각각에서 데이터 메시지에 대한 시드키 갱신 주기에 따라 일반 전자제어장치가 출력하는 CAN(Controller Area Network) 메시지는 시드키 목록을 공유하고, 상기 데이터 메시지 각각에 대한 ID 및 정보를 MAC 키 생성 함수에 입력하여 MAC 태그 세션키를 생성한다.

[0013] 상기 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계는 데이터 프레임의 송신자 및 프레임 우선순위를 식별하는 ID 정보를 포함하는 중재 필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터 필드(Data Field)로 구성되는 CAN FD(CAN with Flexible Data rate) 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 제1 MAC를 생성한다.

[0014] 상기 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계는 CAN FD 프로토콜의 데이터 프레임에 따른 데이터 메시지로 통신하는 일반 전자제어장치의 데이터 프레임 필드에서 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 MAC 태그 세션키를 생성하여 하나의 메시지 데이터 보안이 깨지더라도 해킹으로 획득한 데이터 인증절차를 다른 메시지 프레임에 적용할 수 없고, 게이트웨이 전자제어장치에서 일정 주기로 카운터 정보를 활용하여 MAC 태그 세션키를 주기적으로 업데이트 함으로써 데이터 메시지 재전송을 통한 비정상적인 자동차 제어를 방지한다.

[0015] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 시스템은 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 MAC 태그 세션키 생성부 -상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포됨-, 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하고, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 MAC 생성부 및 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 판별부를 포함한다.

발명의 효과

[0016] 본 발명의 실시예들에 따르면 차량 제조 단계에 특정 ADAS 기능을 수행하는 ECU에 저장되는 대칭키를 기반으로 ECU를 인증함으로써, 정당한 ECU만 통신에 참여할 수 있어 기밀성이 보장되는 효과가 있다.

[0017] 또한, 차량 제조사는 분리된 Zone 게이트웨이 별로 대칭키를 관리하므로 차량 제조 단계에서 발생하는 차량 제조사-부품사 간의 보안자료가 유출되는 문제로 인해 차량 전체의 보안이 연쇄적으로 무너지는 문제를 방지할 수 있다.

[0018] CAN FD로 통신하는 ECU의 데이터 프레임 필드에서 메시지 우선순위 및 데이터 프레임 길이 정보를 기반으로 MAC 태그 세션키를 생성하여 하나의 메시지 데이터 보안이 깨지더라도 해킹으로 얻은 데이터 인증절차를 다른 메시지 프레임에 적용할 수 없어 전체 보안이 연쇄적으로 무너지지 않는다.

[0019] 또한, 메시지 인증코드와 메시지 카운터 그리고 암호문을 효율적으로 적재할 수 있는 CAN FD 데이터 프레임을 이용하여 데이터 기밀성 및 인증을 제공하면서 ECU 간 통신 데이터의 실시간 처리를 보장할 수 있다.

[0020] 또한, 게이트웨이 전자제어장치에서 일정 주기로 카운터 정보를 활용하여 세션키를 주기적으로 업데이트 함으로써 데이터 재전송을 통한 비정상적인 자동차 제어를 방지하는 효과가 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 일 실시예에 따른 데이터 전송 속도와 데이터 페이로드를 확장한 CAN FD 시스템을 설명하기 위한 도면이다.

도 2는 본 발명의 일 실시예에 따른 차량용 데이터 인증 및 획득 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 차량용 데이터 인증 및 획득 시스템의 구성을 나타내는 도면이다.

도 4는 본 발명의 일 실시예에 따른 CAN FD 프로토콜의 데이터 프레임 구성을 나타내는 도면이다.

도 5는 본 발명의 일 실시예에 따른 일반 전자제어장치에서 MAC 태그 세션키를 생성하는 과정을 설명하기 위한

도면이다.

도 6은 본 발명의 일 실시예에 따른 일반 전자제어장치 및 게이트웨이 전자제어장치 간 MAC인증 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0022] 본 발명에서는 차량내 통신 시스템인 제어기 영역 네트워크(Controller Area Network; CAN)의 통신 버스를 관리하는 게이트웨이 전자제어장치(G_ECU)와 통신 버스에 연결된 일반 전자제어장치(ECU_i)가 차량용 데이터를 인증하고 획득하는 차량용 데이터의 인증 및 획득을 위한 방법 및 시스템이 개시된다. 상기 차량용 데이터의 인증 및 획득 방법은 상기 게이트웨이 전자제어장치(G_ECU) 및 상기 일반 전자제어장치(ECU_i)가 차량 제조 단계에서 미리 규정한 대칭키 배열과 순서에 의하여 배포되며, 배포된 대칭키와 일반 전자제어장치(ECU_i)에서 정의된 데이터 패킷의 우선순위 및 패킷 정보를 기초해 MAC(Message Authentication Code) 태그(tag) 세션키를 생성한다. ECU_i는 생성한 MAC 태그 세션키를 기초하여 제1 MAC를 생성하고, 생성된 제1 MAC이 포함된 메시지를 수신한 Zonal 게이트웨이 전자제어장치(ZG_ECU)는 복수의 일반 전자제어장치(ECU_i)가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보에 기초하여 MAC 태그 세션키 및 제2 MAC를 생성하고 수신한 제1 MAC과 제2 MAC 동일성 여부를 판단하여 수신된 메시지를 인증한다. 대칭키 배열은 메시지 데이터 패킷에 정의된 갱신 주기에 따라 순번을 갱신한다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0024] 도 1은 본 발명의 일 실시예에 따른 데이터 전송 속도와 데이터 페이로드를 확장한 CAN FD 시스템을 설명하기 위한 도면이다.
- [0025] 도 1을 참고하면, 본 발명의 실시예에 따른 CAN FD 시스템은 Zonal 게이트웨이(110)을 관리하는 ZG_ECU(111)와 하나 이상의 일반 전자제어장치(Electronic Control Unit; ECU)(121~124)를 포함한다. 도 1에서 ECU는 총 4개가 도시되어 있으나 이는 일 실시예일뿐, CAN FD 시스템에 포함된 ECU의 개수는 n(n은 2이상의 자연수)일 수 있다.
- [0026] 본 발명의 실시예에 따른 ZG_ECU(111)는 Zonal 네트워크의 게이트웨이 역할을 하는 ECU를 의미한다.
- [0027] 본 발명의 실시예에 따른 각 ECU(1201~4)는 상호간의 메시지를 송수신하며 송수신 방식은 브로드캐스트(broadcast)방식으로 통신하며, CAN FD 프로토콜 데이터 프레임을 따른다. 각 ECU는 ZG_ECU가 저장하고 있는 세션키 배열(Seed K list)중 i번째 ECU에 맞는 Seed K_i List를 ZG_ECU와 공유한다.
- [0029] 도 2는 본 발명의 일 실시예에 따른 차량용 데이터 인증 및 획득 방법을 설명하기 위한 흐름도이다.
- [0030] 본 발명의 실시예에 따른 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치를 포함하는 차량용 데이터 인증 및 획득 방법은 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성하는 단계(210), 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하는 단계(220), 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성하는 단계(230) 및 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증하는 단계(240)를 포함한다. 본 발명의 실시예에 따른 상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포된다.
- [0031] 단계(210)에서, 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC(Message Authentication Code) 태그(tag) 세션키를 생성한다.
- [0032] 본 발명의 실시예에 따르면, 복수의 일반 전자제어장치 각각에서 데이터 메시지에 대한 시드키 갱신 주기에 따라 일반 전자제어장치가 출력하는 CAN(Controller Area Network) 메시지는 시드키 목록을 공유하고, 상기 데이터 메시지 각각에 대한 ID 및 정보를 MAC 키 생성 함수에 입력하여 MAC 태그 세션키를 생성한다.
- [0033] 단계(220)에서, 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성한다.
- [0034] 본 발명의 실시예에 따르면, 데이터 프레임의 송신자 및 프레임 우선순위를 식별하는ID 정보를 포함하는 중계

필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터 필드(Data Field)로 구성되는 CAN FD(CAN with Flexible Data rate) 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 제1 MAC를 생성한다.

[0035] 단계(230)에서, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자 제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성한다.

[0036] 상술된 바와 같이, 게이트웨이 전자제어장치에서도 CAN FD 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 제2 MAC를 생성한다.

[0037] 단계(240)에서, 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증한다.

[0038] 본 발명의 실시예에 따르면, CAN FD 프로토콜의 데이터 프레임에 따른 데이터 메시지로 통신하는 일반 전자제어 장치의 데이터 프레임 필드에서 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 MAC 태그 세션키를 생성하여 하나의 메시지 데이터 보안이 깨지더라도 해킹으로 획득한 데이터 인증절차를 다른 메시지 프레임에 적용할 수 없어 전체 보안이 연쇄적으로 무너지지 않는다.

[0039] 또한, 본 발명의 실시예에 따르면, 게이트웨이 전자제어장치에서 일정 주기로 카운터 정보를 활용하여 MAC 태그 세션키를 주기적으로 업데이트 함으로써 데이터 메시지 재전송을 통한 비정상적인 자동차 제어를 방지할 수 있다.

[0041] 도 3은 본 발명의 일 실시예에 따른 차량용 데이터 인증 및 획득 시스템의 구성을 나타내는 도면이다.

[0042] 본 실시예에 따른 차량용 데이터 인증 및 획득 시스템(300)은 프로세서(310), 버스(320), 네트워크 인터페이스(330), 메모리(340) 및 데이터베이스(350)를 포함할 수 있다. 메모리(340)는 운영체제(341) 및 차량용 데이터 인증 및 획득 루틴(342)을 포함할 수 있다. 프로세서(310)는 MAC 태그 세션키 생성부(311), MAC 생성부(312) 및 판별부(313)를 포함할 수 있다. 다른 실시예들에서 차량용 데이터 인증 및 획득 시스템(300)은 도 3의 구성 요소들보다 더 많은 구성요소들을 포함할 수도 있다. 그러나, 대부분의 종래기술적 구성요소들을 명확하게 도시할 필요성은 없다. 예를 들어, 차량용 데이터 인증 및 획득 시스템(300)은 디스플레이나 트랜시버(transceiver)와 같은 다른 구성요소들을 포함할 수도 있다.

[0043] 메모리(340)는 컴퓨터에서 판독 가능한 기록 매체로서, RAM(random access memory), ROM(read only memory) 및 디스크 드라이브와 같은 비소멸성 대용량 기록장치(permanent mass storage device)를 포함할 수 있다. 또한, 메모리(340)에는 운영체제(341)와 차량용 데이터 인증 및 획득 루틴(342)을 위한 프로그램 코드가 저장될 수 있다. 이러한 소프트웨어 구성요소들은 드라이브 메커니즘(drive mechanism, 미도시)을 이용하여 메모리(340)와는 별도의 컴퓨터에서 판독 가능한 기록 매체로부터 로딩될 수 있다. 이러한 별도의 컴퓨터에서 판독 가능한 기록 매체는 플로피 드라이브, 디스크, 테이프, DVD/CD-ROM 드라이브, 메모리 카드 등의 컴퓨터에서 판독 가능한 기록 매체(미도시)를 포함할 수 있다. 다른 실시예에서 소프트웨어 구성요소들은 컴퓨터에서 판독 가능한 기록 매체가 아닌 네트워크 인터페이스(330)를 통해 메모리(340)에 로딩될 수도 있다.

[0044] 버스(320)는 차량용 데이터 인증 및 획득 시스템(300)의 구성요소들간의 통신 및 데이터 전송을 가능하게 할 수 있다. 버스(320)는 고속 시리얼 버스(high-speed serial bus), 병렬 버스(parallel bus), SAN(Storage Area Network) 및/또는 다른 적절한 통신 기술을 이용하여 구성될 수 있다.

[0045] 네트워크 인터페이스(330)는 차량용 데이터 인증 및 획득 시스템(300)을 컴퓨터 네트워크에 연결하기 위한 컴퓨터 하드웨어 구성요소일 수 있다. 네트워크 인터페이스(330)는 차량용 데이터 인증 및 획득 시스템(300)을 무선 또는 유선 커넥션을 통해 컴퓨터 네트워크에 연결시킬 수 있다.

[0046] 데이터베이스(350)는 차량용 데이터 인증 및 획득을 위해 필요한 모든 정보를 저장 및 유지하는 역할을 할 수 있다. 도 3에서는 차량용 데이터 인증 및 획득 시스템(300)의 내부에 데이터베이스(350)를 구축하여 포함하는 것으로 도시하고 있으나, 이에 한정되는 것은 아니며 시스템 구현 방식이나 환경 등에 따라 생략될 수 있고 혹은 전체 또는 일부의 데이터베이스가 별개의 다른 시스템 상에 구축된 외부 데이터베이스로서 존재하는 것 또한 가능하다.

- [0047] 프로세서(310)는 기본적인 산술, 로직 및 차량용 데이터 인증 및 획득 시스템(300)의 입출력 연산을 수행함으로써, 컴퓨터 프로그램의 명령을 처리하도록 구성될 수 있다. 명령은 메모리(340) 또는 네트워크 인터페이스(330)에 의해, 그리고 버스(320)를 통해 프로세서(310)로 제공될 수 있다. 프로세서(310)는 MAC 태그 세션키 생성부(311), MAC 생성부(312) 및 판별부(313)를 위한 프로그램 코드를 실행하도록 구성될 수 있다. 이러한 프로그램 코드는 메모리(340)와 같은 기록 장치에 저장될 수 있다.
- [0048] MAC 태그 세션키 생성부(311), MAC 생성부(312) 및 판별부(313)는 도 2의 단계들(210~240)을 수행하기 위해 구성될 수 있다.
- [0049] 차량용 데이터 인증 및 획득 시스템(300)은 MAC 태그 세션키 생성부(311), MAC 생성부(312) 및 판별부(313)를 포함할 수 있다.
- [0050] 본 발명의 실시예에 따른 MAC 태그 세션키 생성부(311)는 일반 전자제어장치에서 정의된 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 일반 전자제어장치 MAC 태그 세션키를 생성한다. 본 발명의 실시예에 따른 상기 게이트웨이 전자제어장치 및 복수의 일반 전자제어장치는 미리 정해진 대칭키 배열과 순서에 의해 배포된다.
- [0051] 본 발명의 실시예에 따른 MAC 태그 세션키 생성부(311)는 복수의 일반 전자제어장치 각각에서 데이터 메시지에 대한 시드키 갱신 주기에 따라 일반 전자제어장치가 출력하는 CAN(Controller Area Network) 메시지는 시드키 목록을 공유하고, 상기 데이터 메시지 각각에 대한 ID 및 정보를 MAC 키 생성 함수에 입력하여 MAC 태그 세션키를 생성한다.
- [0052] 본 발명의 실시예에 따른 MAC 생성부(312)는 일반 전자제어장치에서 상기 생성된 MAC 태그 세션키에 기초하여 제1 MAC를 생성하고, 상기 생성된 제1 MAC이 포함된 메시지를 수신한 게이트웨이 전자제어장치에서 복수의 일반 전자제어장치가 송신한 메시지 데이터 패킷의 우선순위 및 패킷길이 정보 및 상기 MAC 태그 세션키에 기초하여 제2 MAC를 생성한다.
- [0053] 본 발명의 실시예에 따른 판별부(313)는 게이트웨이 전자제어장치에서 상기 제1 MAC와 상기 제2 MAC의 동일성 여부를 판단하여 수신된 메시지를 인증한다.
- [0054] 본 발명의 실시예에 따른 판별부(313)는 데이터 프레임의 송신자 및 프레임 우선순위를 식별하는 ID 정보를 포함하는 중재 필드(Arbitration Field), 컨트롤 필드(Control Field), 데이터 필드(Data Field)로 구성되는 CAN FD(CAN with Flexible Data rate) 프로토콜의 데이터 프레임에 따른 데이터 메시지 및 상기 생성된 MAC 태그 세션키를 MAC 인증 코드 생성 함수에 입력하여 MAC를 생성한다.
- [0055] 차량용 데이터 인증 및 획득 시스템(300)은 CAN FD 프로토콜의 데이터 프레임에 따른 데이터 메시지로 통신하는 일반 전자제어장치의 데이터 프레임 필드에서 데이터 패킷의 우선순위 및 패킷 정보와 대칭키에 기초하여 MAC 태그 세션키를 생성하여 하나의 메시지 데이터 보안이 깨지더라도 해킹으로 획득한 데이터 인증절차를 다른 메시지 프레임에 적용할 수 없어 전체 보안이 연쇄적으로 무너지지 않는다.
- [0056] 또한, 차량용 데이터 인증 및 획득 시스템(300)은 게이트웨이 전자제어장치에서 일정 주기로 카운터 정보를 활용하여 MAC 태그 세션키를 주기적으로 업데이트 함으로써 데이터 메시지 재전송을 통한 비정상적인 자동차 제어를 방지할 수 있다.
- [0058] 도 4는 본 발명의 일 실시예에 따른 CAN FD 프로토콜의 데이터 프레임 구성을 나타내는 도면이다.
- [0059] 본 발명 일 실시예에 따른 CAN FD 프로토콜의 데이터 프레임은 크게 데이터 프레임의 송신자 및 프레임 우선순위를 식별할 수 있는 ID 정보를 포함하는 중재 필드(Arbitration Field)(410), 컨트롤 필드(Control Field)(420), 데이터 필드(Data Field)(430)로 구성된다. CAN FD 데이터 프레임은 최대 64바이트(byte) 데이터 필드를 지원하며, 컨트롤 필드에 기재되는 정보 중 DLC(Data Length code)의 DLC Code에 따라 데이터 필드 길이가 결정되며, 데이터 필드 길이는 최소 20byte에서 최대 64byte까지 변경이 가능하다.
- [0060] 데이터 필드는 크게 3가지 메시지 정보가 기재되며, ECU_i가 MAC 인증 코드 생성함수(MGF)를 통해 생성한 MAC값, Seed K_i List의 갱신 주기를 알리는 CTR_{i,j}, 전자 장치 제어를 수행하는 Data Message이다.
- [0061] CTR_{i,k}는 ECU_i가 출력하는 Message ID_j의 메시지 카운터 정보이며, 사용자 정의에 따라 길이를 4bit에서 8bit까지 조절이 가능하며, 이는 Seed K_i List의 갱신 주기를 결정한다. 예를 들어, CTR_{i,j}의 size가 4bit이

면 CAN FD Frame이 16번 Frame마다 Seed_K_i List가 갱신된다.

- [0062] 본 발명의 일 실시예에 따른 CAN FD 데이터 프레임의 데이터 필드는 총 3가지 영역으로 구성된다. 제1 영역은 메시지 인증 코드(MAC) 적재 영역이며, 사이즈는 16바이트(byte)이다. 제2 영역은 데이터 프레임 카운트 적재 영역이며, 데이터 프레임 카운터(CTR_i_j)는 특정 ECU가 송신한 데이터 프레임의 전송 횟수를 나타낸다. 예를 들어, ECU_i가 j번째 메시지의 총 4개의 데이터 프레임을 전송 한 후 5번째 데이터 프레임을 전송할 때는 ECU_i의 데이터 프레임 카운터(CTR_i_j)는 5로 설정된다. 데이터 프레임 카운터는 영역 사이즈가 갖는 최대값에 도달한 후에는 0으로 회귀하며, 회귀하는 순간 MAC인증 코드를 생성하는데 필요한 Seed K_i 키가 갱신된다. 이 데이터 프레임 카운터(CTR_i_j)는 최소 4bit, 최대 8bit의 사이즈를 가지며, 사이즈가 작을수록 Seed K_i의 갱신 주기가 빨라진다.
- [0063] 본 발명의 일 실시예에 따른 제3 영역은 ECU_i가 j번째 메시지 데이터 패킷으로 제어하고자 하는 전자제어장치의 컨트롤 명령이 적재되는 Data Message이며, Data Message의 사이즈는 컨트롤 필드에 기재된 DLC Code에 따라 가변된 총 데이터 필드(최소 20byte, 최대 64byte)를 가지며, 데이터 필드 총 길이 중 제1 영역과 제2 영역 사이즈를 제외한 나머지 영역이 제3 영역 Data Message가 적재되는 공간이다.
- [0065] 도 5는 본 발명의 일 실시예에 따른 일반 전자제어장치에서 MAC 태그 세션키를 생성하는 과정을 설명하기 위한 도면이다.
- [0066] 본 발명의 일 실시예에 따른 ECU_i는 여러 개의 CAN Message ID를 출력할 수 있으며, 이는 Message ID_j(510)로 명시된다. 각 Message ID_j(510)의 Seed K_i 갱신 주기는 CTR_i_j로 서로 다르게 정의되므로, ECU_i가 출력하는 CAN 메시지는 Seed_K_i List(520)를 공유하나, 사용되는 Seed_K_i순번은 다르기에 이를 Seed K_i_j(530)로 표현한다.
- [0067] Seed K_i_j(530)는 갱신 규칙에 따라 로드된 뒤 CAN FD Message의 Message ID_j와 DLC code 정보를 MAC 키 생성 함수(KGF)(540)에 입력해 2nd MAC Tag 세션키(550)를 생성한다. Seed K_i_j(530)가 갱신되면 갱신된 키가 로드되어 KGF에 입력되고, 갱신된 2nd MAC Tag 세션키(550)가 생성된다.
- [0069] 도 6은 본 발명의 일 실시예에 따른 일반 전자제어장치 및 게이트웨이 전자제어장치 간 MAC인증 과정을 설명하기 위한 도면이다.
- [0070] 도 6은 본 발명의 실시예에 따른 ECU_i(610)와 ZG_ECU(620)간 2nd MAC Tag 세션키를 통한 MAC인증 과정을 도시한 것이다.
- [0071] ECU_i(610)와 ZG_ECU(620)는 사전에 공유된 Seed K_i List에서 Seed K_i_j를 선택한 후 이를 KGF 함수를 통해 2nd MAC Tag 세션키를 생성한다.
- [0072] ECU_i(610)가 전자제어장치를 제어하기 위한 Data Message(611)를 2nd MAC Tag키와 함께 MAC 인증 코드 생성 함수(MGF)(612)에 입력하여 MAC 1 인증값을 생성한다(613).
- [0073] ECU_i(610)는 Data Message(611)와 MAC 1 인증값(613)을 CAN FD 프로토콜의 데이터 프레임의 규격에 맞춰 전송(Broadcast)하면 ZG_ECU(620)는 Data Message(621)와 MAC 1 인증값(623)을 수신 받아 Data Message(621)를 ZG_ECU(620)에서 2nd MAC Tag 세션키와 함께 MGF(622)에 입력하여 MAC 2 인증값(624)을 생성한다.
- [0074] ZG_ECU(620)는 수신 받은 MAC 1 인증값(623)과 MAC 2 인증값(624)의 동일성 여부를 판별(625)하여 ECU_i(610)에서 수신 받은 메시지를 검증한다. 동일하지 않을 경우 인증실패(626)로 판단하고, 동일할 경우 인증성공(627)으로 판단한다.
- [0076] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴

퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0077] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

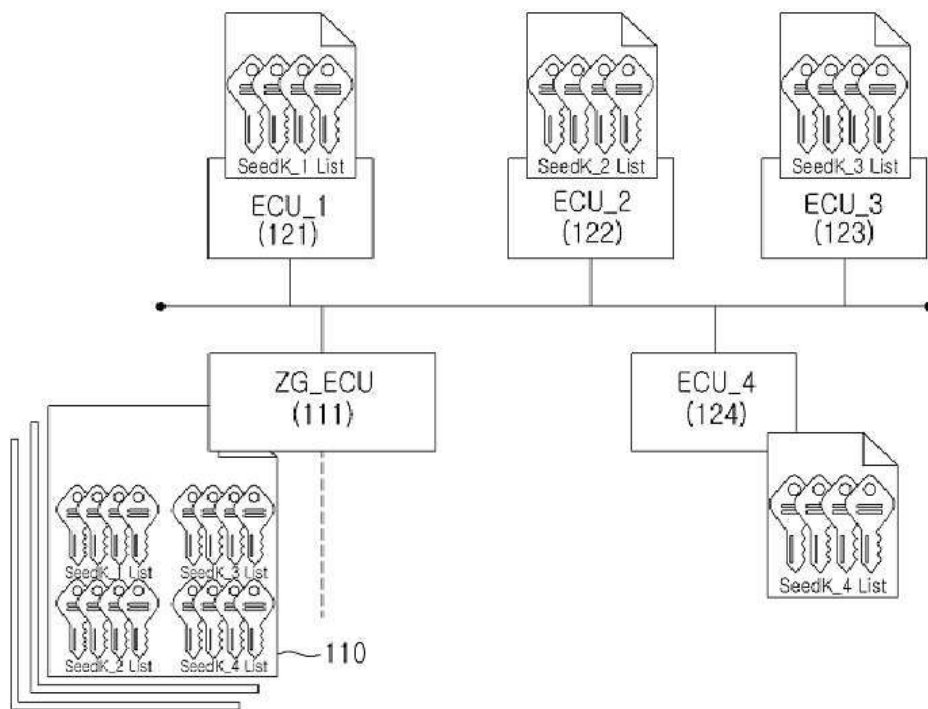
[0078] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0079] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

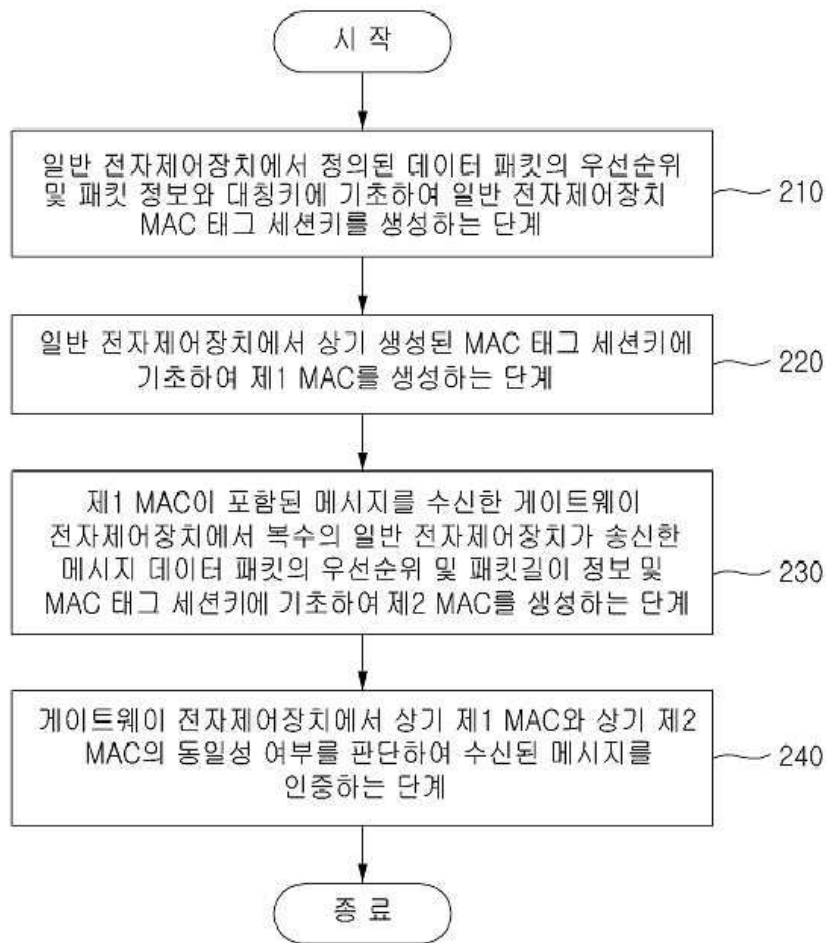
[0080] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

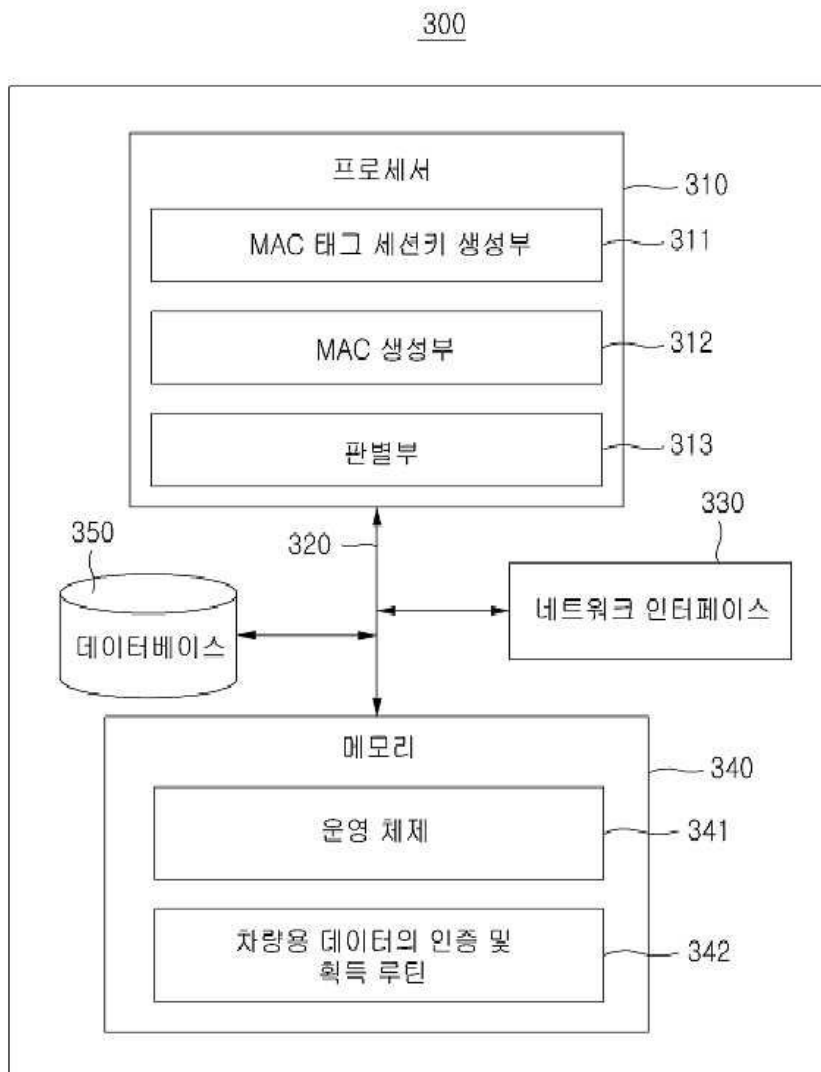
도면1



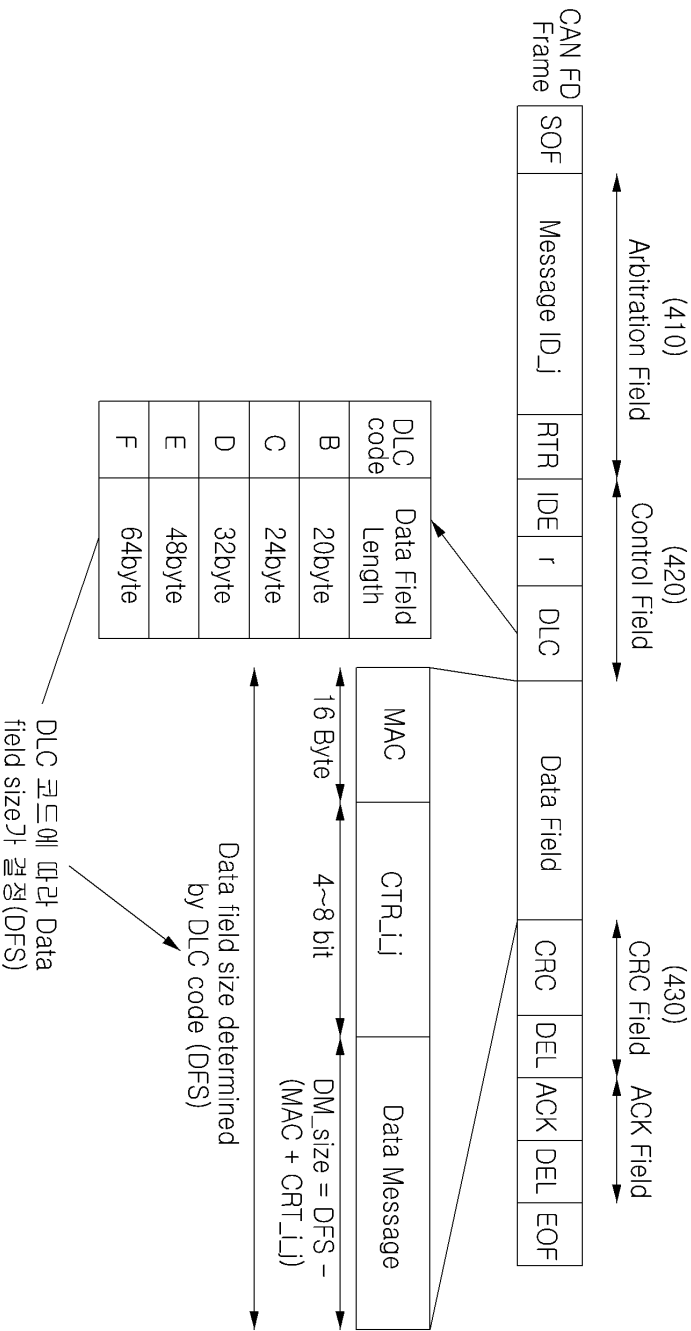
도면2



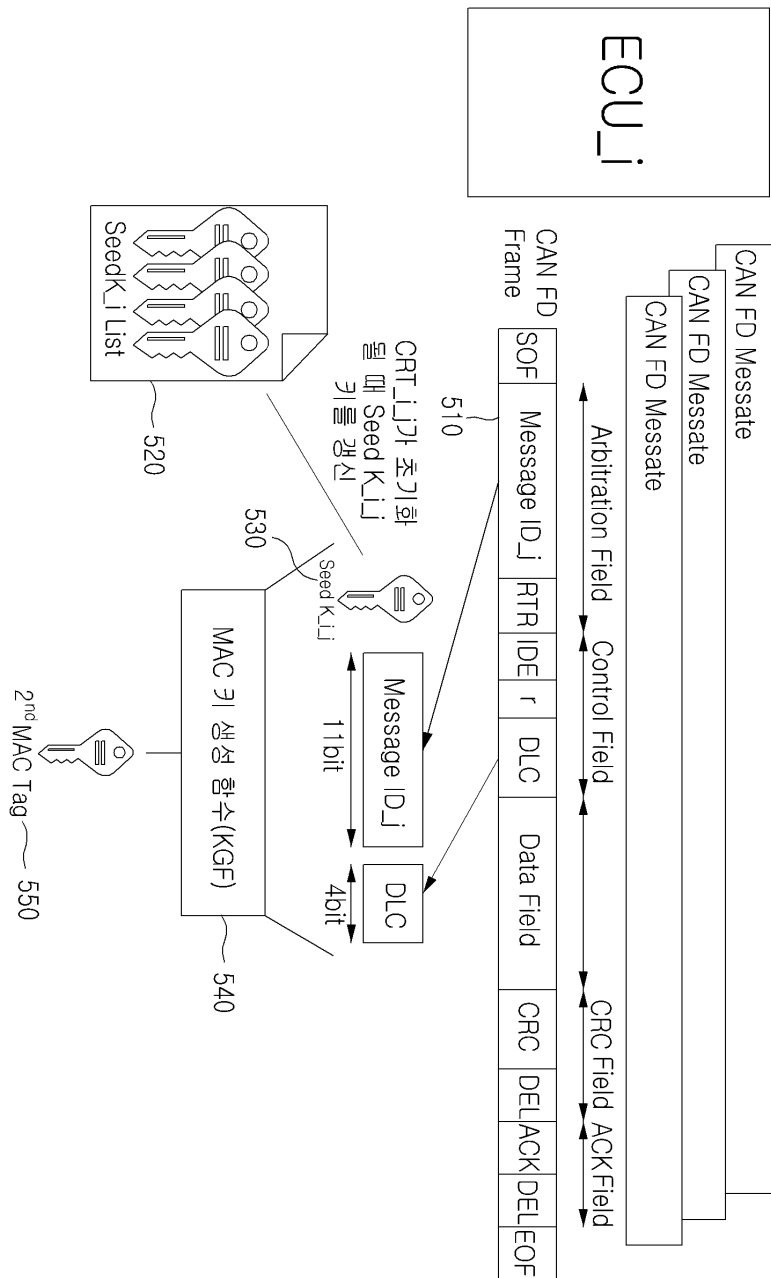
도면3



도면4



도면5



도면6

