



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0075458
(43) 공개일자 2021년06월23일

- (51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) H04L 1/00 (2006.01)
H04L 12/26 (2006.01) H04L 12/40 (2006.01)
H04L 9/32 (2006.01)
- (52) CPC특허분류
H04L 63/1408 (2013.01)
H04L 1/0061 (2013.01)
- (21) 출원번호 10-2019-0166546
(22) 출원일자 2019년12월13일
심사청구일자 2019년12월13일
- (71) 출원인
한림대학교 산학협력단
강원도 춘천시 한림대학길 1, 한림대학교(옥천동)
- (72) 발명자
조효진
강원도 춘천시 한림대학길 1, 한림대학교 공학관 1305호
김형훈
서울특별시 강북구 덕릉로 191-10, 2층
정연선
강원도 춘천시 영서로 2169, 111동 2104호 (퇴계동, 퇴계이안아파트)
- (74) 대리인
김남혁

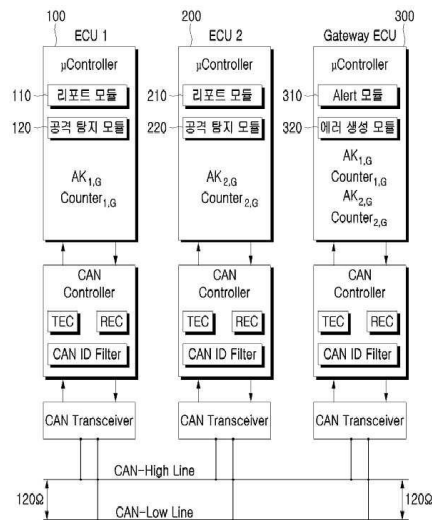
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법, 장치 및 프로그램

(57) 요약

CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법이 제공된다. 상기 제어 방법은, 제1 ECU가, 상기 제1 ECU가 사용하는 제1 CAN ID를 CAN ID 필터에 저장하는 단계; 상기 제1 ECU가, 외부 공격을 감지하는 단계; 상기 외부 공격이 감지된 경우, 상기 제1 ECU가, 게이트웨이 ECU로 리포트 메시지를 전송하는 단계; 상기 게이트웨이 ECU가, 상기 리포트 메시지를 인증하는 단계; 및 상기 게이트웨이 ECU가, 상기 리포트 메시지가 인증되지 않은 경우, 상기 상기 리포트 메시지에 비트 에러를 추가하는 단계; 를 포함한다.

대표도 - 도4



(52) CPC특허분류

H04L 12/40104 (2013.01)
H04L 12/40143 (2013.01)
H04L 43/06 (2013.01)
H04L 63/0236 (2013.01)
H04L 9/3242 (2013.01)
H04L 2012/40215 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	NRF-2018R1C1B5086261
부처명	한국연구재단
과제관리(전문)기관명	한국연구재단
연구사업명	생애 첫 연구사업
연구과제명	차량 해킹 공격에 강건한 스마트 자동차 시스템을 위한 인증, 도스 미터게이터 그리
고 로깅 기술의 연구	
기 여 율	1/1
과제수행기관명	한림대학교 산학협력단
연구기간	2019.03.01 ~ 2020.02.29

명세서

청구범위

청구항 1

제1 ECU, 제2 ECU 및 게이트웨이 ECU를 포함하는 CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법에 있어서,

상기 제1 ECU가, 상기 제1 ECU가 사용하는 제1 CAN ID를 CAN ID 필터에 저장하는 단계;

상기 제1 ECU가, 외부 공격을 감지하는 단계;

상기 외부 공격이 감지된 경우, 상기 제1 ECU가, 상기 게이트웨이 ECU로 리포트 메시지를 전송하는 단계;

상기 게이트웨이 ECU가, 상기 리포트 메시지를 인증하는 단계; 및

상기 게이트웨이 ECU가, 상기 리포트 메시지가 인증되지 않은 경우, 상기 상기 리포트 메시지에 비트 에러를 부가하는 단계; 를 포함하는 제어 방법.

청구항 2

제1항에 있어서,

상기 외부 공격을 감지하는 단계는,

상기 제2 ECU가 상기 제1 CAN ID를 수신한 경우, 상기 제1 ECU 상기 제1 ECU의 공격 탐지 모듈이, 상기 제1 CAN ID가 상기 제1 ECU에서 전송된 것인지 판단하는 단계; 및

상기 공격 탐지 모듈이, 상기 제1 CAN ID가 제1 ECU에서 전송되지 않은 것으로 판단되면, 상기 제2 ECU로 전송된 제1 CAN ID를 외부 공격으로 감지하는 단계; 를 포함하는 제어 방법.

청구항 3

제1항에 있어서,

상기 리포트 메시지를 전송하는 단계는,

상기 제1 ECU와 상기 게이트웨이 ECU가 MAC 인증키를 공유하는 단계;

상기 제1 ECU의 리포트 모듈이, 상기 제1 CAN ID와 상기 리포트 메시지의 우선순위를 판단하는 단계; 및

상기 판단된 우선순위를 바탕으로 상기 상기 리포트 메시지를 전송하는 단계; 를 포함하는 제어 방법.

청구항 4

제3항에 있어서,

상기 리포트 메시지는, 리포트 CAN ID 및 m바이트의 CAN 데이터를 포함하고,

상기 CAN 데이터는, 상기 MAC 인증키에 대응되는 n 바이트의 MAC (Message authentication code) 데이터 및 m-n 바이트의 0 값을 포함하는 것을 특징으로 하는 제어 방법.

청구항 5

제3항에 있어서,

상기 리포트 메시지를 인증하는 단계는,

상기 게이트웨이 ECU의 Alert 모듈이, 상기 제1 ECU와 공유된 상기 MAC 인증키를 바탕으로, 상기 수신한 리포트 메시지를 인증하는 단계;

상기 리포트 메시지가 인증되면, 상기 제1 ECU의 카운터 값을 1 증가시키는 단계; 및

상기 리포트 메시지에 대응되는 결과를 상기 시스템으로 제공하는 단계; 를 포함하는 제어 방법.

청구항 6

제1항에 있어서,

상기 리포트 메시지에 비트 에러를 부가하는 단계는,

상기 게이트웨이 ECU의 에러 생성 모듈이, 상기 리포트 메시지에 비트 에러를 부가하는 단계;

상기 부가된 비트 에러를 바탕으로, 공격 ECU의 TEC(Transmission Error Counter)를 증가시키는 단계; 및

상기 TEC를 바탕으로, 상기 공격 ECU의 상태를 변경하는 단계; 를 포함하고,

상기 공격 ECU의 상태는, Error Active 상태, Error passive 상태 및 Bus-Off 상태 중 적어도 하나의 상태인 것을 특징으로 하는 제어 방법.

청구항 7

공격 탐지 모듈 및 리포트 모듈을 포함하는 제1 ECU의 제어 방법에 있어서,

상기 제1 ECU가, 상기 제1 ECU가 사용하는 제1 CAN ID를 CAN ID 필터에 저장하는 단계;

상기 공격 탐지 모듈이, 외부 공격을 감지하는 단계; 및

상기 외부 공격이 감지된 경우, 상기 리포트 모듈이, 상기 게이트웨이 ECU로 리포트 메시지를 전송하는 단계;를 포함하는 제어 방법.

청구항 8

Alert 모듈 및 에러 생성 모듈을 포함하는 게이트웨이 ECU의 제어 방법에 있어서,

상기 Alert 모듈이, 제1 ECU로부터 리포트 메시지를 수신하는 단계;

상기 Alert 모듈이, 상기 리포트 메시지를 인증하는 단계;

상기 에러 생성 모듈이, 상기 리포트 메시지가 인증되지 않은 경우, 상기 상기 리포트 메시지에 비트 에러를 부가하는 단계; 를 포함하는 제어 방법.

청구항 9

하나 이상의 인스트럭션을 저장하는 메모리; 및

상기 메모리에 저장된 상기 하나 이상의 인스트럭션을 실행하는 프로세서를 포함하고,

상기 프로세서는 상기 하나 이상의 인스트럭션을 실행함으로써,

제1 항의 방법을 수행하는, 장치.

청구항 10

하드웨어인 컴퓨터와 결합되어, 제1 항의 방법을 수행할 수 있도록 컴퓨터에서 독출가능한 기록매체에 저장된 컴퓨터프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법, 장치 및 프로그램에 관한 것이다.

배경 기술

[0002] 최근에는 자동차의 전자식 제어를 넘어 오토파일럿 등의 기초적인 자율주행 지원 모듈들이 활발하게 개발되고

있다. 특히, 완전한 자율주행 기술 (Full Self-Driving Automation)을 위해 LiDAR (거리 측정/사물인지 센서) 등의 센서 기술들과 외부 통신기술 (V2X: Vehicle to Everything)을 지원하는 자동차 IT 융합 기술들이 개발되고 있는 실정이다.

[0003] 다양한 기술에 따른 다양한 정보를 효과적으로 전송하기 위하여, 자동차 내부의 제어유닛 (Electronic Control Unit, ECU)들은 자동차 내부 네트워크를 (Controller Area Network (CAN), 차량용 Ethernet) 통해 정보 공유 및 자동차를 제어할 수 있다.

[0004] 이때, 자동차 내부 네트워크의 CAN 메시지는 주기적으로 전송되는 Periodic 메시지와, 이벤트가 발생했을때만 전송되는 Event 메시지 그리고 주기적으로 전송됨과 동시에 이벤트가 발생했을 때 주기가 변동되는 Periodic and Event 메시지로 구분될 수 있다.

[0005] 자동차의 전자 장치화에 따라, 자동차 내외부에서 전달되는 메시지를 보호하기 위한 보안의 필요성 또한 급증하고 있다. 일례로, 자동차 내부 네트워크에 대한 공격을 탐지하기 위해 침입 탐지 시스템들이 제안되고 있으나, 비주기적인 CAN 메시지 (i.e., Event 메시지와 Periodic and Event 메시지)를 이용하는 공격을 탐지하는 방법에 대한 구체적인 대안 제시가 필요한 상황이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 등록특허공보 제10-1198724호, 2012.11.01

발명의 내용

해결하려는 과제

[0007] 본 발명이 해결하고자 하는 과제는 본 발명은 CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법, 장치 및 프로그램을 제공하는 것이다.

[0008] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 상술한 과제를 해결하기 위한 본 발명의 일 면에 따른 제1 ECU, 제2 ECU 및 게이트웨이 ECU를 포함하는 CAN ID 필터링 기반의 침입 탐지 시스템의 제어 방법은, 상기 제1 ECU가, 상기 제1 ECU가 사용하는 제1 CAN ID를 CAN ID 필터에 저장하는 단계; 상기 제1 ECU가, 외부 공격을 감지하는 단계; 상기 외부 공격이 감지된 경우, 상기 제1 ECU가, 상기 게이트웨이 ECU로 리포트 메시지를 전송하는 단계; 상기 게이트웨이 ECU가, 상기 리포트 메시지를 인증하는 단계; 및 상기 게이트웨이 ECU가, 상기 리포트 메시지가 인증되지 않은 경우, 상기 상기 리포트 메시지에 비트 에러를 추가하는 단계; 를 포함한다.

[0010] 이때, 상기 외부 공격을 감지하는 단계는, 상기 제2 ECU가 상기 제1 CAN ID를 수신한 경우, 상기 제1 ECU의 공격 탐지 모듈이, 상기 제1 CAN ID가 상기 제1 ECU에서 전송된 것인지 판단하는 단계; 및 상기 공격 탐지 모듈이, 상기 제1 CAN ID가 제1 ECU에서 전송되지 않은 것으로 판단되면, 상기 제2 ECU로 전송된 제1 CAN ID를 외부 공격으로 감지하는 단계; 를 포함할 수 있다.

[0011] 이때, 상기 리포트 메시지를 전송하는 단계는, 상기 제1 ECU와 상기 게이트웨이 ECU가 MAC 인증키를 공유하는 단계; 상기 제1 ECU의 리포트 모듈이, 상기 제1 CAN ID와 상기 리포트 메시지의 우선순위를 판단하는 단계; 및 상기 판단된 우선순위를 바탕으로 상기 상기 리포트 메시지를 전송하는 단계; 를 포함할 수 있다.

[0012] 이때, 상기 리포트 메시지는, 리포트 CAN ID 및 m바이트의 CAN 데이터를 포함하고, 상기 CAN 데이터는, 상기 MAC 인증키에 대응되는 n 바이트의 MAC (Message authentication code) 데이터 및 m-n 바이트의 0 값을 포함할 수 있다.

[0013] 이때, 상기 리포트 메시지를 인증하는 단계는, 상기 게이트웨이 ECU의 Alert 모듈이, 상기 제1 ECU와 공유된 상기 MAC 인증키를 바탕으로, 상기 수신한 리포트 메시지를 인증하는 단계; 상기 리포트 메시지가 인증되면, 상기

제1 ECU의 카운터 값을 1 증가시키는 단계; 및 상기 리포트 메시지에 대응되는 결과를 상기 시스템으로 제공하는 단계;를 포함할 수 있다.

[0014] 이때, 상기 리포트 메시지에 비트 에러를 추가하는 단계는, 상기 게이트웨이 ECU의 에러 생성 모듈이, 상기 리포트 메시지에 비트 에러를 추가하는 단계; 상기 추가된 비트 에러를 바탕으로, 공격 ECU의 TEC(Transmission Error Counter)를 증가시키는 단계; 및 상기 TEC를 바탕으로, 상기 공격 ECU의 상태를 변경하는 단계;를 포함하고, 상기 공격 ECU의 상태는, Error Active 상태, Error passive 상태 및 Bus-Off 상태 중 적어도 하나의 상태일 수 있다.

[0015] 한편, 본 발명의 또 다른 실시예에 따른 공격 탐지 모듈 및 리포트 모듈을 포함하는 제1 ECU의 제어 방법은, 상기 제1 ECU가, 상기 제1 ECU가 사용하는 제1 CAN ID를 CAN ID 필터에 저장하는 단계; 상기 공격 탐지 모듈이, 외부 공격을 감지하는 단계; 및 상기 외부 공격이 감지된 경우, 상기 리포트 모듈이, 상기 게이트웨이 ECU로 리포트 메시지를 전송하는 단계;를 포함할 수 있다.

[0016] 한편, 본 발명의 또 다른 실시예에 따른 Alert 모듈 및 에러 생성 모듈을 포함하는 게이트웨이 ECU의 제어 방법은, 상기 Alert 모듈이, 제1 ECU로부터 리포트 메시지를 수신하는 단계; 상기 Alert 모듈이, 상기 리포트 메시지를 인증하는 단계; 상기 에러 생성 모듈이, 상기 리포트 메시지가 인증되지 않은 경우, 상기 상기 리포트 메시지에 비트 에러를 추가하는 단계;를 포함할 수 있다.

[0017] 본 발명의 기타 구체적인 사항들은 상세한 설명 및 도면들에 포함되어 있다.

발명의 효과

[0018] 상술한 본 발명의 다양한 실시예에 따라, CAN 메시지 전송에서의 보안성을 향상시킬 수 있는 효과가 존재한다.

[0019] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 일 실시예에 따른 CAN 네트워크를 설명하기 위한 예시도이다.

도 2는 본 발명의 일 실시예에 따른 ECU의 CAN 에러 관리 방법을 설명하기 위한 예시도이다.

도 3은 본 발명의 일 실시예에 따른 CAN 2.0 A 메시지 포맷을 설명하기 위한 예시도이다.

도 4는 본 발명의 일 실시예에 따른, CAN ID 필터링 기반의 침입 탐지 시스템을 설명하기 위한 예시도이다.

도 5는 본 발명의 일 실시예에 따른 CAN ID 필터링 기반의 침입 탐지 방법을 설명하기 위한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 공격 탐지 모듈을 설명하기 위한 흐름도이다.

도 7은 본 발명의 일 실시예에 따른 리포트 모듈을 설명하기 위한 흐름도이다.

도 8은 본 발명의 일 실시예에 따른 Alert 모듈을 설명하기 위한 흐름도이다.

도 9는 본 발명의 일 실시예에 따른 에러 생성 모듈을 설명하기 위한 흐름도이다.

도 10은 본 발명의 일 실시예에 따른 공격 탐지 모듈을 설명하기 위한 예시도이다.

도 11은 본 발명의 일 실시예에 따른 리포트 모듈을 설명하기 위한 예시도이다.

도 12는 본 발명의 일 실시예에 따른 리포트 메시지의 구성을 설명하기 위한 예시도이다.

도 13은 본 발명의 일 실시예에 따른 장치의 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

- [0022] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.
- [0023] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야의 통상의 기술자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또한, 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0024] 명세서에서 사용되는 "부" 또는 "모듈"이라는 용어는 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, "부" 또는 "모듈"은 어떤 역할들을 수행한다. 그렇지만 "부" 또는 "모듈"은 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부" 또는 "모듈"은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부" 또는 "모듈"은 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다. 구성요소들과 "부" 또는 "모듈"들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 "부" 또는 "모듈"들로 결합되거나 추가적인 구성요소들과 "부" 또는 "모듈"들로 더 분리될 수 있다.
- [0025] 공간적으로 상대적인 용어인 "아래(below)", "아래(beneath)", "하부(lower)", "위(above)", "상부(upper)" 등은 도면에 도시되어 있는 바와 같이 하나의 구성요소와 다른 구성요소들과의 상관관계를 용이하게 기술하기 위해 사용될 수 있다. 공간적으로 상대적인 용어는 도면에 도시되어 있는 방향에 더하여 사용시 또는 동작시 구성요소들의 서로 다른 방향을 포함하는 용어로 이해되어야 한다. 예를 들어, 도면에 도시되어 있는 구성요소를 뒤집을 경우, 다른 구성요소의 "아래(below)"또는 "아래(beneath)"로 기술된 구성요소는 다른 구성요소의 "위(above)"에 놓여질 수 있다. 따라서, 예시적인 용어인 "아래"는 아래와 위의 방향을 모두 포함할 수 있다. 구성요소는 다른 방향으로도 배향될 수 있으며, 이에 따라 공간적으로 상대적인 용어들은 배향에 따라 해석될 수 있다.
- [0026] 본 명세서에서, 컴퓨터는 적어도 하나의 프로세서를 포함하는 모든 종류의 하드웨어 장치를 의미하는 것이고, 실시 예에 따라 해당 하드웨어 장치에서 동작하는 소프트웨어적 구성도 포괄하는 의미로서 이해될 수 있다. 예를 들어, 컴퓨터는 스마트폰, 태블릿 PC, 데스크톱, 노트북 및 각 장치에서 구동되는 사용자 클라이언트 및 애플리케이션을 모두 포함하는 의미로서 이해될 수 있으며, 또한 이에 제한되는 것은 아니다.
- [0027] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [0028] 본 명세서에서 설명되는 각 단계들은 컴퓨터에 의하여 수행되는 것으로 설명되나, 각 단계의 주체는 이에 제한되는 것은 아니며, 실시 예에 따라 각 단계들의 적어도 일부가 서로 다른 장치에서 수행될 수도 있다.
- [0029] 도 1은 본 발명의 일 실시예에 따른 CAN 네트워크를 설명하기 위한 예시도이다.
- [0030] 도 1에 도시된 바와 같이, 각각의 ECU는, 마이크로 컨트롤러, CAN 컨트롤러를 포함할 수 있다. 각각의 ECU는 CAN controller와 CAN Transceiver를 통해 CAN 통신을 수행할 수 있다. 이때, CAN controller는 CAN ID 필터를 포함하고, 해당 필터를 통해 CAN 네트워크에 전송되는 CAN 메시지들을 필터링 할 수 있다.
- [0031] 일 실시예로, 각각의 ECU는, 자신이 수신해야 될 CAN ID를 자신의 CAN ID 필터에 설정하고, 설정된 CAN ID를 갖는 CAN 메시지를 수신할 수 있다.
- [0032] 도 2는 본 발명의 일 실시예에 따른 ECU의 CAN 에러 관리 방법을 설명하기 위한 예시도이다.
- [0033] CAN의 에러 관리를 위해, ECU는 TEC(Transmission Error Counter)와 REC (Receive Error Counter)를 포함할 수 있다. TEC 및 REC는, 데이터의 전송 및 수신단계에서 다양한 에러(Bit Error, Stuff Error, CRC Error, Form Error, ACK Error 등)가 발생한 경우, 에러 카운터를 증가시키기 위한 구성이다. 이 경우, 정상적인 데이터가

송수신되면, TEC 및 REC는 에러 카운터를 감소시킬 수 있다.

- [0034] ECU는 Error Active, Error Passive, 및 Bus-Off의 세가지 에러 상태가 존재하며, 도 2에 도시된 조건을 만족하는 경우, 에러 상태가 변경될 수 있다, 예를 들어, Error Active 상태에서 REC 또는 TEC의 카운터 값이 127 이상이 되면, 에러 상태는 Error Passive 상태로 변경될 수 있다. 한편, ECU가 Bus-Off 상태가 되면, 해당 ECU는 기 설정된 시간 동안 CAN 통신에 참여할 수 없다. 일반적으로 Bus-Off 상태는 문제가 있는 ECU로부터 데이터가 반복 전송 되는 경우 발생할 수 있다.
- [0035] 도 3은 본 발명의 일 실시예에 따른 CAN 2.0 A 메시지 포맷을 설명하기 위한 예시도이다.
- [0036] 도 3에 도시된 바와 같이 CAN 메시지 포맷은, 1비트의 SOF, 11비트의 CAN ID 및 1비트의 RTR을 포함하는 Arbitration Field, 1비트의 IDE, 1비트의 r0, 4비트의 DLC, 64비트의 CAN data, 16비트의 CRC, 2비트의 ACK 및 7비트의 EOF를 포함할 수 있다. 상술한 CAN 메시지 포맷은 CAN 2.0 A Frame의 표준을 따르며, 본 발명의 다양한 실시예에서는 필요에 따라 메시지 포맷이 변경될 수 있음은 물론이다.
- [0037] 이하에서는 도 4 내지 도 13을 참조하여, 본 발명의 다양한 실시예에 대하여 구체적으로 서술한다.
- [0038] 도 4는 본 발명의 일 실시예에 따른, CAN ID 필터링 기반의 침입 탐지 시스템을 설명하기 위한 예시도이다.
- [0039] 도 4에 도시된 바와 같이, 본 발명에 따른 시스템은, 일반 ECU 및 게이트웨이 ECU를 포함할 수 있다. 설명의 편의를 위해 일반 ECU는 제1 ECU(100) 및 제2 ECU(200)로 구현되고, 게이트웨이 ECU(300)는 단일 ECU로 구현되나, 필요에 따라 일반 ECU 및 게이트웨이 ECU의 개수는 변경될 수 있음은 물론이다.
- [0040] 제1 ECU(100)는 리포트 모듈(110) 및 공격 탐지 모듈(120)을 포함할 수 있다. 구체적으로, 리포트 모듈(110) 및 공격 탐지 모듈(120)은 제1 ECU(100)의 메모리에 저장되어 제1 ECU(100)의 마이크로 프로세서(또는 프로세서)에 의해 제어 될 수 있다.
- [0041] 제2 ECU(200)또한, 제1 ECU(100)와 같이, 리포트 모듈(210) 및 공격 탐지 모듈(220)을 포함할 수 있다. 리포트 모듈(210) 및 공격 탐지 모듈(220)은 제2 ECU(200)의 메모리에 저장되어 제2 ECU(200)의 마이크로 프로세서(또는 프로세서)에 의해 제어 될 수 있음은 물론이다.
- [0042] 일 실시예로, 공격 탐지 모듈(120, 220)은 공격 ECU의 공격을 탐지하기 위한 모듈이며, 리포트 모듈(110, 210)은 공격 ECU의 공격에 대한 리포트 메시지를 생성하기 위한 모듈일 수 있다.
- [0043] 구체적으로, 공격 탐지 모듈(120)은 제1 ECU(100)는 자신이 사용하는 CAN ID를 CAN ID 필터에 추가할 수 있다. 이때, 공격 ECU에서 자신의 CAN ID를 이용하여 공격을 한 경우, CAN ID 필터를 통해 자신의 CAN ID가 공격 ECU에 의해 사용되었음을 탐지할 수 있다. 구체적으로, 도 10을 참조하면, 제1 ECU(100)의 CAN ID 필터는 주기적으로 전송되는 0x01 및 비주기적으로 전송되는 0x10을 CAN ID로 저장할 수 있다. 이 경우, 공격 ECU가 0x01 또는 0x10의 CAN ID를 전송하는 경우, 공격 탐지 모듈(120)은 해당 CAN ID가 공격 ECU에 의해 생성된 것으로 판단할 수 있다.
- [0044] 리포트 모듈(110)은 공격 탐지 모듈(120)에 의해 탐지된 공격을 게이트웨이 ECU(300)에게 알리기 위한 리포트 메시지를 생성할 수 있다. 리포트 모듈(110)에서 이용하는 리포트용 CAN ID는 각각의 ECU마다 설정될 수 있다.
- [0045] 일 실시예로, 리포트용 CAN ID는 CAN 네트워크의 CAN ID 우선순위를 고려하여 동적으로 설정될 수 있다. 리포트 모듈(120)은 도 11에 도시된 바와 같이, 리포트용 CAN ID를 이용하여 CAN 메시지를 게이트웨이 ECU(300)로 전송할 수 있다. 이때, CAN 메시지의 페이로드의 첫 n바이트는 MAC (Message authentication code)을 보내고, 나머지 m-n바이트는 0으로 셋팅해서 전송할 수 있으며 n은 보안 파라미터일 수 있다. 일 실시예에 따라, m은 8 ($1 \leq m \leq 8$), n($1 \leq n \leq m$)은 4일 수 있으나, 이에 한정되는 것은 아니다.
- [0046] 한편, MAC (Message authentication code) 생성에는 Gateway ECU와 공유한 인증키와 카운터가 도 12와 같이 사용될 수 있다. 이때, AK_{i,G}는 제i ECU와 게이트웨이 ECU(300)가 공유하는 메시지 인증키를 의미하며, counter_{i,G}는 제i ECU와 게이트웨이 ECU(300)가 공유하는 카운터 값일 수 있다. 리포트 메시지가 성공적으로 전송되면, 제1 ECU(100) 및 게이트웨이 ECU(300)는 카운터값을 1증가시킬 수 있다.
- [0047] 한편, 도 12에 도시된 바와 같이, 리포트 메시지는 리포트용 CAN ID, DLC(data Length) 및 m바이트의 데이터를 포함할 수 있다.
- [0048] 한편, 게이트웨이 ECU(300)는 Alert 모듈(310) 및 에러 생성 모듈(320)을 포함할 수 있다. 구체적으로, Alert

모듈(310) 및 에러 생성 모듈(320)은 게이트웨이 ECU(300)의 메모리에 저장되어 게이트웨이 ECU(300)의 마이크로 프로세서(또는 프로세서)에 의해 제어 될 수 있다.

- [0049] 일 실시예로, Alert 모듈(310)은 리포트 모듈(110,210)으로부터 리포트 메시지를 수신한 경우, 공격 ECU의 공격에 대한 알람을 시스템에 제공하기 위한 모듈이고, 에러 생성 모듈(320)은 리포트 메시지가 공격 ECU에 의해 생성된 경우, 공격 ECU의 CAN 통신을 정지시키기 위한 구성일 수 있다.
- [0050] 구체적으로, Alert 모듈(310)은, 리포트 모듈(120)로부터 수신한 리포트 메시지를 인증하고, 리포트 메시지가 인증되면, 제1 ECU(100)의 카운터 값을 1 증가시킬 수 있다. 또한, 에러 생성 모듈은 공격 ECU를 Error Passive 또는 Bus-Off 상태로 변경시킬 수 있다.
- [0051] 도 5는 본 발명의 일 실시예에 따른 CAN ID 필터링 기반의 침입 탐지 방법을 설명하기 위한 흐름도이다.
- [0052] S110에서, 제1 ECU(100)가, 제1 ECU(100)가 사용하는 제1 CAN ID를 CAN ID 필터에 저장할 수 있다.
- [0053] 상술한 바와 같이, 제1 ECU(100) CAN ID 필터에 저장된 ID만을 다른 ECU로 전송할 수 있다.
- [0054] S120에서, 제1 ECU(100)가, 외부 공격을 감지할 수 있다.
- [0055] 일 실시예로, 제1 ECU(100)의 CAN ID 필터에 저장된 것과 동일한 CAN ID인 0x01이 제2 ECU(200)로 전송된 경우, 제1 ECU(100)는 0x01이 자신이 전송한 CAN ID인지 여부를 판단할 수 있다. 제2 ECU(200)가 수신한 0x01이 제1 ECU(100)가 전송한 것이 아닌 경우, 제1 ECU(100)는 해당 CAN ID가 공격 ECU가 전송한 CAN ID로 판단할 수 있다.
- [0056] S130에서, 외부 공격이 감지된 경우, 제1 ECU(100)가, 게이트웨이 ECU(300)로 리포트 메시지를 전송할 수 있다.
- [0057] S140에서, 게이트웨이 ECU(300)가, 리포트 메시지를 인증할 수 있다.
- [0058] 상술한 바와 같이, 제1 ECU(100) 및 게이트웨이 ECU(300)는 리포트 메시지 인증을 위한 공유 인증키를 각각 저장할 수 있으며, 게이트웨이 ECU(300)는 저장된 인증키를 바탕으로 리포트 메시지를 인증할 수 있다. 만일 공격 ECU가 악의적인 목적으로 리포트 메시지를 전송하였다고 하더라도, 제1 ECU(100)와 게이트웨이 ECU(300)가 공유하는 인증키를 알 수 없으므로, 게이트웨이 ECU(300)는 공격 ECU에 의해 전송된 리포트 메시지의 인증을 수행할 수 없을 것이다.
- [0059] S150에서, 게이트웨이 ECU(300)가, 리포트 메시지가 인증되지 않은 경우, 리포트 메시지에 비트 에러를 추가할 수 있다. S150에 대한 상세한 설명은 도 9에서 후술한다.
- [0060] 도 6은 본 발명의 일 실시예에 따른 공격 탐지 모듈을 설명하기 위한 흐름도이다.
- [0061] S210에서, 제2 ECU(200)가 제1 CAN ID를 수신한 경우, 제1 ECU(100) 제1 ECU(100)의 공격 탐지 모듈(120)이, 제1 CAN ID가 제1 ECU(100)에서 전송된 것인지 판단할 수 있다.
- [0062] S220에서, 공격 탐지 모듈(120)이, 제1 CAN ID가 제1 ECU(100)에서 전송되지 않은 것으로 판단되면, 제2 ECU(200)로 전송된 제1 CAN ID를 외부 공격으로 감지할 수 있다.
- [0063] 상술한 바와 같이, 제1 ECU(100)의 CAN ID 필터에 저장된 것과 동일한 CAN ID인 0x01이 제2 ECU(200)로 전송된 경우, 제1 ECU(100)는 0x01이 자신이 전송한 CAN ID인지 여부를 판단할 수 있다. 제2 ECU(200)가 수신한 0x01이 제1 ECU(100)가 전송한 것이 아닌 경우, 제1 ECU(100)는 해당 CAN ID가 공격 ECU가 전송한 CAN ID로 판단할 수 있다.
- [0064] 도 7은 본 발명의 일 실시예에 따른 리포트 모듈을 설명하기 위한 흐름도이다.
- [0065] S310에서, 제1 ECU(100)와 게이트웨이 ECU(300)가 MAC 인증키를 공유할 수 있다.
- [0066] S320에서, 제1 ECU(100)의 리포트 모듈(110)이, 제1 CAN ID와 리포트 메시지의 우선순위를 판단할 수 있다.
- [0067] S330에서, 판단된 우선순위를 바탕으로 리포트 메시지를 전송할 수 있다.
- [0068] 이때, 리포트 메시지는, 리포트 CAN ID 및 m바이트의 CAN 데이터를 포함하고, CAN 데이터는, MAC 인증키에 대응되는 n 바이트의 MAC (Message authentication code) 데이터 및 m-n 바이트의 0 값을 포함할 수 있다.
- [0069] 일 실시예로, 도 12에 도시된 바와 같이, 리포트 메시지는 리포트용 CAN ID, DLC(data Length) 및 m바이트의 데이터를 포함할 수 있으며, m은 8, n은 4의 값을 가질 수 있다.

- [0070] 도 8은 본 발명의 일 실시예에 따른 Alert 모듈을 설명하기 위한 흐름도이다.
- [0071] S410에서, 게이트웨이 ECU의 Alert 모듈(310)이, 제1 ECU(100)와 공유된 MAC 인증키를 바탕으로, 수신한 리포트 메시지를 인증할 수 있다.
- [0072] 구체적으로, 제1 ECU(100) 및 게이트웨이 ECU(300)는 인증을 위한 인증키(공유키)를 공유할 수 있다. 이후, 제1 ECU(100)의 리포트 모듈(110)은, 인증키 및 전송하고자 하는 데이터를 바탕으로 메시지 인증 코드를 생성할 수 있다. 이때, 전송하고자 하는 데이터는, 공격에 대응되는 CAN ID일 수 있으나, 이에 한정되는 것은 아니며, 제1 ECU(100)와 게이트웨이 ECU(300)사이에 공유되는 카운터 값을 데이터 메시지 인증 코드를 생성할 수 있음은 물론이다. 제1 ECU(100)는 전송하고자 하는 데이터 및 메시지 인증 코드를 게이트웨이 ECU(300)로 전송할 수 있다.
- [0073] 이후, 게이트웨이 ECU(300)는 수신한 리포트 메시지 중, 제1 ECU(100)가 전송한 데이터 및 메시지 인증 코드를 추출할 수 있다. 게이트웨이 ECU(300)는 제1 ECU(100)로부터 수신한 데이터 및 인증키를 바탕으로 메시지 인증 코드를 획득하고, 제1 ECU(100)로부터 수신한 메시지 인증코드를 비교하여 수신한 데이터가 적법한 데이터인지 여부를 판단할 수 있다.
- [0074] S420에서, 게이트웨이 ECU(300)는, 리포트 메시지가 인증되면, 제1 ECU(100)의 카운터 값을 1 증가시킬 수 있다.
- [0075] S430에서, 게이트웨이 ECU(300)는, 리포트 메시지에 대응되는 결과를 상기 시스템으로 제공할 수 있다.
- [0076] 도 9는 본 발명의 일 실시예에 따른 에러 생성 모듈을 설명하기 위한 흐름도이다.
- [0077] 상술한 단계 S410에서, 리포트 메시지가 인증되지 않은 경우, 게이트웨이 ECU(300)는, 에러 생성 모듈을 바탕으로 리포트 메시지를 가공할 수 있다.
- [0078] 구체적으로, S510에서, 게이트웨이 ECU(300)의 에러 생성 모듈(320)이, 리포트 메시지에 비트 에러를 추가할 수 있다.
- [0079] 즉, 게이트웨이 ECU(300)는, 임의로 비트 에러를 추가하여 수신한 리포트 메시지를 에러가 발생한 리포트 메시지로 변환할 수 있다. 일 실시예로, 게이트웨이 ECU(300)의 마이크로 프로세서가 CAN transceiver를 제어하여 비트 에러를 생성할 수 있다.
- [0080] S520에서, 게이트웨이 ECU(300)는, 부가된 비트 에러를 바탕으로, 공격 ECU의 TEC(Transmission Error Counter)를 증가시킬 수 있다.
- [0081] S530에서, 게이트웨이 ECU(300)는, TEC를 바탕으로, 공격 ECU의 상태를 변경할 수 있다.
- [0082] 이때, 공격 ECU의 상태는, Error Active 상태, Error passive 상태 및 Bus-Off 상태 중 적어도 하나의 상태일 수 있다. 즉, 게이트웨이 ECU(300)는, TEC 값을 바탕으로 에러 상태를 변경할 수 있다. 복수의 공격 리포트 메시지가 감지되면, 게이트웨이 ECU(300)는, 공격 ECU를 Bus-Off시킬 수 있다.
- [0083] 한편, 본 발명의 다양한 실시예에 따라, 게이트웨이 ECU(300)는, Bus-Off된 ECU의 리셋 시간을 기 설정된 조건을 바탕으로 결정할 수 있다.
- [0084] 일 실시예로, 게이트웨이 ECU(300)는, 리포트 메시지에 대응되는 제어 신호의 종류를 바탕으로 리셋 시간을 결정할 수 있다. 예를 들어, 제어 신호가 자동차의 주행과 같이 사용자의 안전과 연관된 경우, 게이트웨이 ECU(300)는, 리셋 시간을 제1 리셋 시간으로 설정하고, 제어 신호가 서비스 제공과 같이 사용자의 편의성과 연관된 경우, 게이트웨이 ECU(300)는, 리셋 시간을 제2 리셋 시간으로 설정하되, 제1 리셋 시간은 제2 리셋 시간보다 긴 시간이 되도록 리셋 시간을 설정할 수 있다.
- [0085] 도 13은 본 발명의 일 실시예에 따른 장치의 구성도이다.
- [0086] 프로세서(102)는 하나 이상의 코어(core, 미도시) 및 그래픽 처리부(미도시) 및/또는 다른 구성 요소와 신호를 송수신하는 연결 통로(예를 들어, 버스(bus) 등)를 포함할 수 있다.
- [0087] 일 실시예에 따른 프로세서(102)는 메모리(104)에 저장된 하나 이상의 인스트럭션을 실행함으로써, 도 5 내지 도 10과 관련하여 설명된 방법을 수행한다.
- [0088] 한편, 프로세서(102)는 프로세서(102) 내부에서 처리되는 신호(또는, 데이터)를 일시적 및/또는 영구적으로 저

장하는 램(RAM: Random Access Memory, 미도시) 및 롬(ROM: Read-Only Memory, 미도시)을 더 포함할 수 있다. 또한, 프로세서(102)는 그래픽 처리부, 램 및 롬 중 적어도 하나를 포함하는 시스템온칩(SoC: system on chip) 형태로 구현될 수 있다.

[0089] 메모리(104)에는 프로세서(102)의 처리 및 제어를 위한 프로그램들(하나 이상의 인스트럭션들)을 저장할 수 있다. 메모리(104)에 저장된 프로그램들은 기능에 따라 복수 개의 모듈들로 구분될 수 있다.

[0090] 본 발명의 실시예와 관련하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어로 직접 구현되거나, 하드웨어에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이들의 결합에 의해 구현될 수 있다. 소프트웨어 모듈은 RAM(Random Access Memory), ROM(Read Only Memory), EPROM(Erasable Programmable ROM), EEPROM(Electrically Erasable Programmable ROM), 플래시 메모리(Flash Memory), 하드 디스크, 착탈형 디스크, CD-ROM, 또는 본 발명이 속하는 기술 분야에서 잘 알려진 임의의 형태의 컴퓨터 판독가능 기록매체에 상주할 수도 있다.

[0091] 본 발명의 구성 요소들은 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램(또는 애플리케이션)으로 구현되어 매체에 저장될 수 있다. 본 발명의 구성 요소들은 소프트웨어 프로그래밍 또는 소프트웨어 요소들로 실행될 수 있으며, 이와 유사하게, 실시 예는 데이터 구조, 프로세스들, 루틴들 또는 다른 프로그래밍 구성들의 조합으로 구현되는 다양한 알고리즘을 포함하여, C, C++, 자바(Java), 어셈블리(assembler) 등과 같은 프로그래밍 또는 스크립팅 언어로 구현될 수 있다. 기능적인 측면들은 하나 이상의 프로세서들에서 실행되는 알고리즘으로 구현될 수 있다.

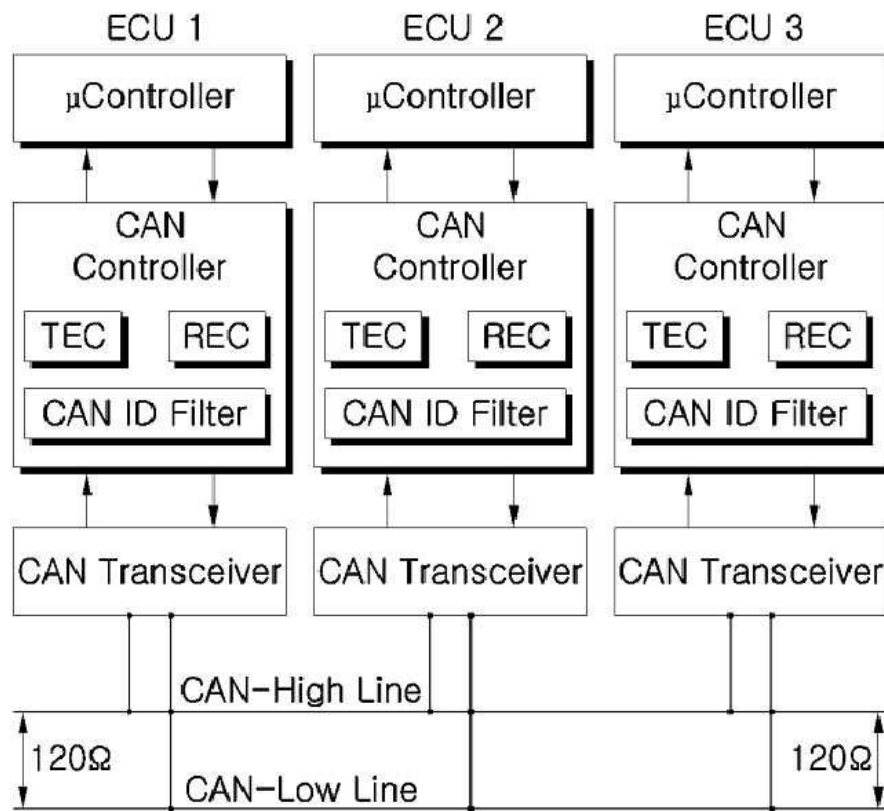
[0092] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이지 않은 것으로 이해해야만 한다.

부호의 설명

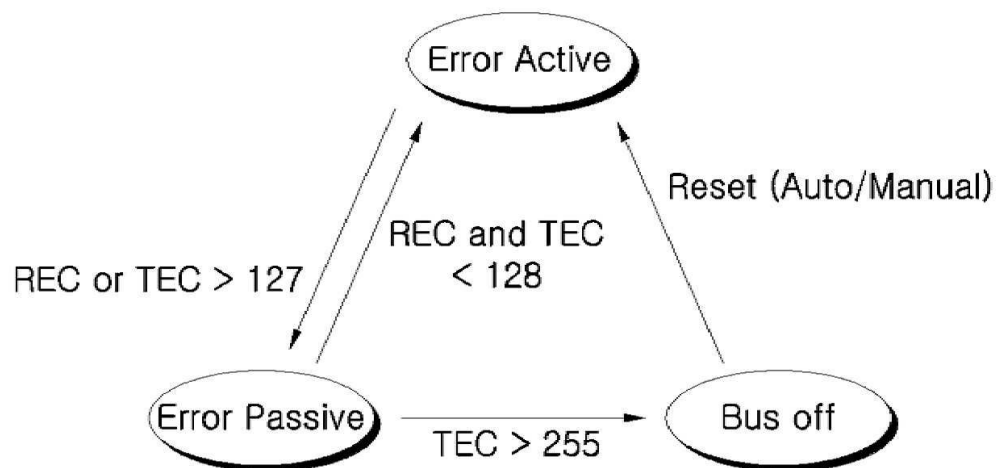
[0093] 100 : 제1 ECU
200 : 제2 ECU
300 : 게이트웨이 ECU

도면

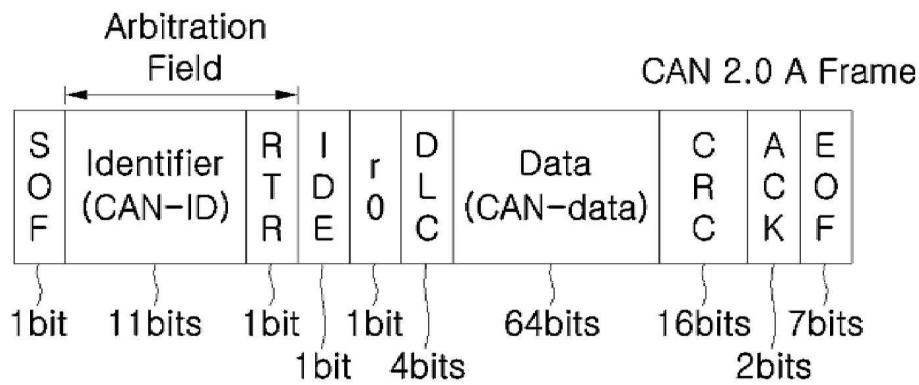
도면1



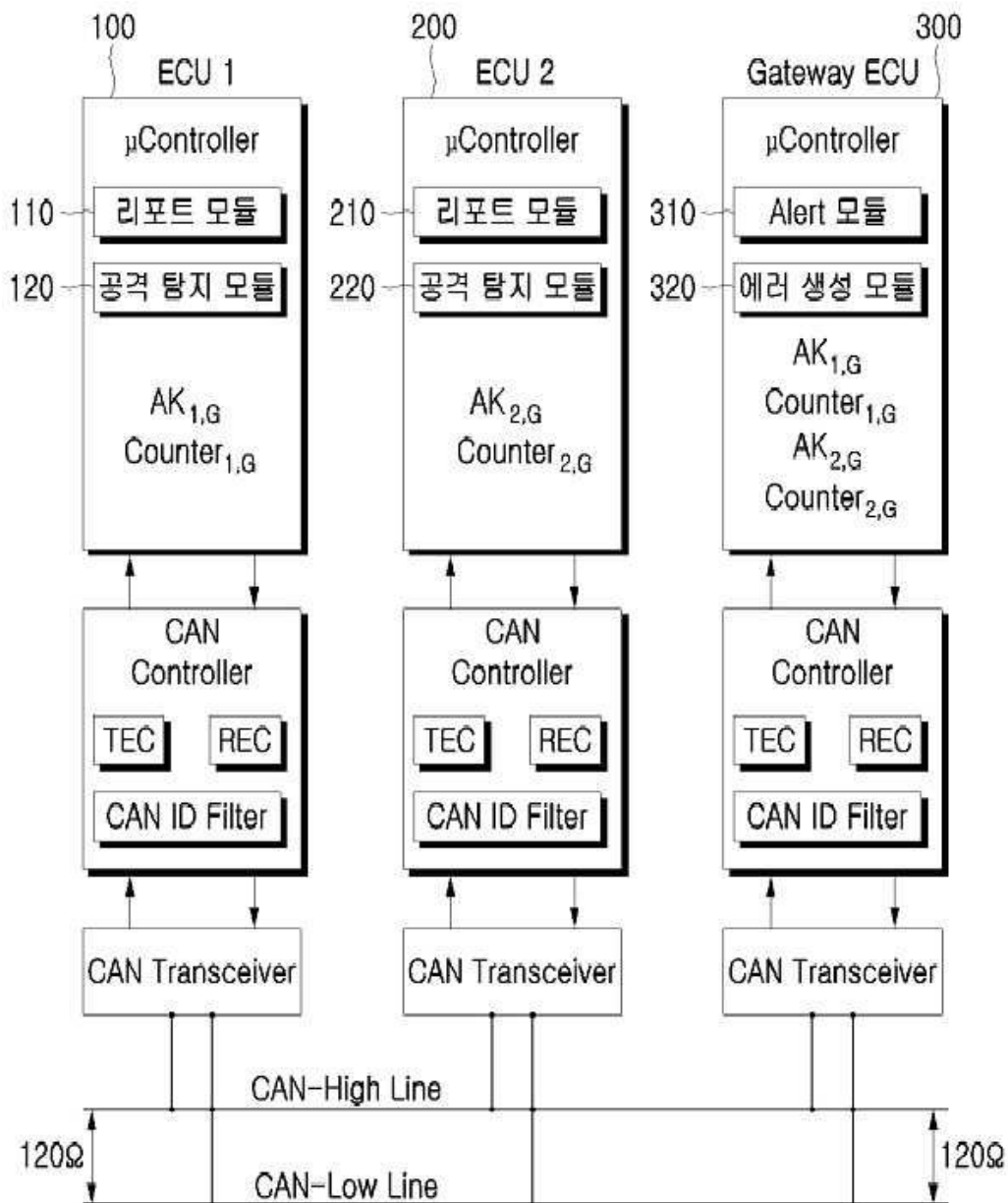
도면2



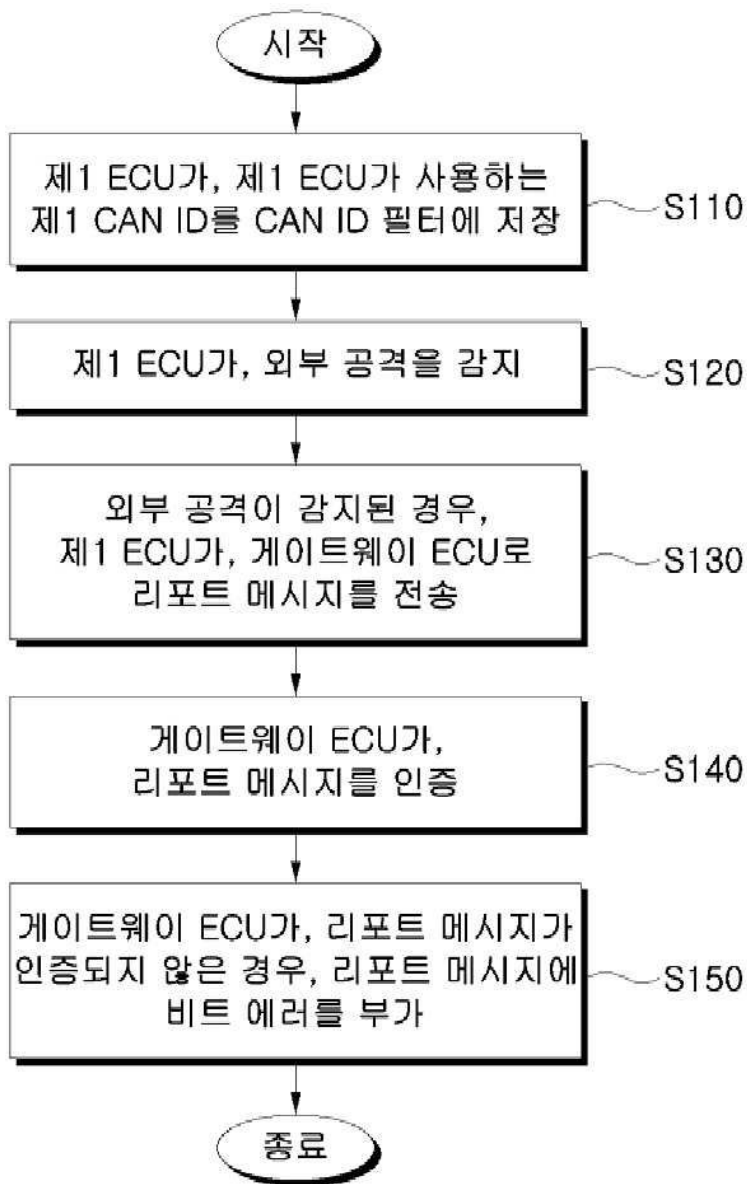
도면3



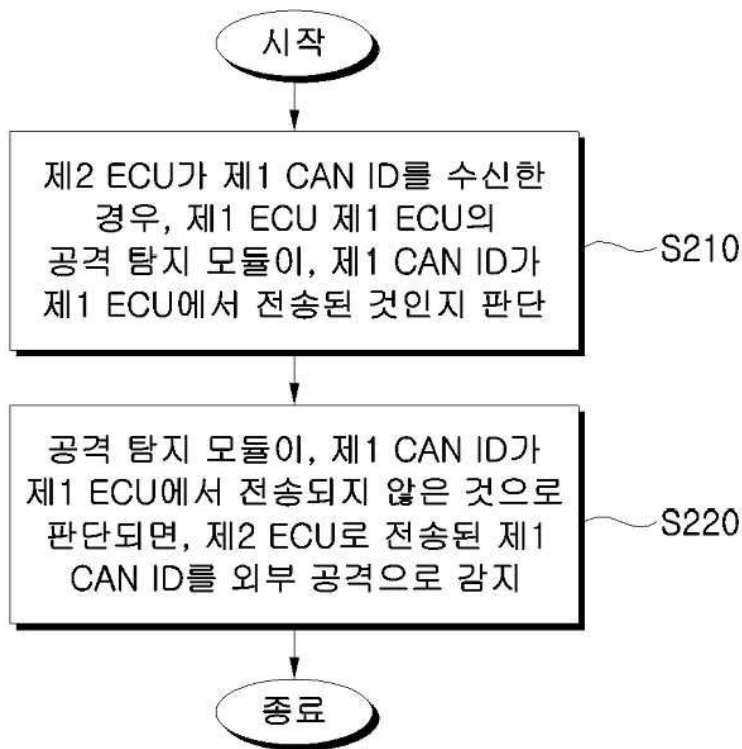
도면4



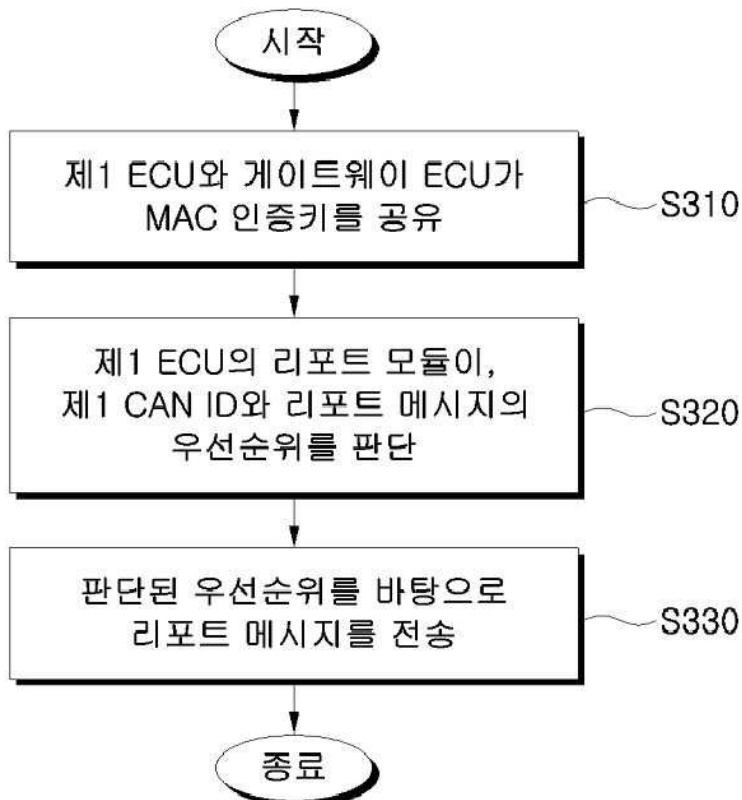
도면5



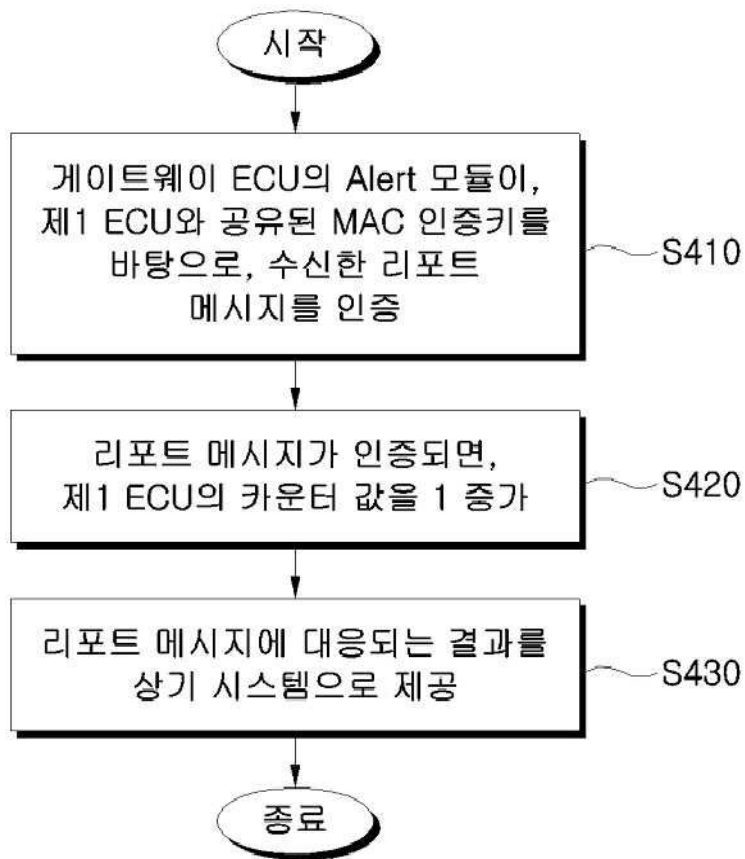
도면6



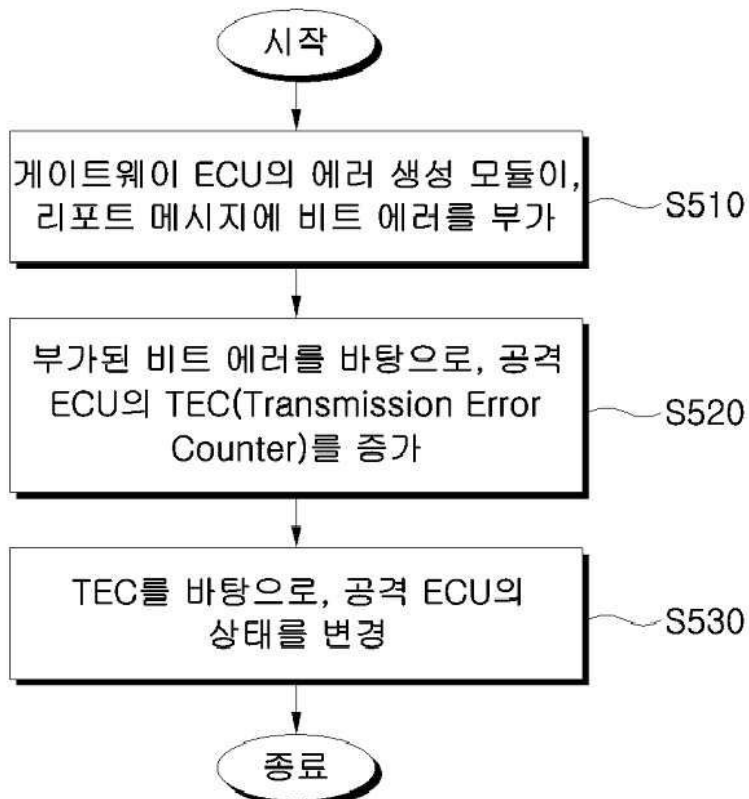
도면7



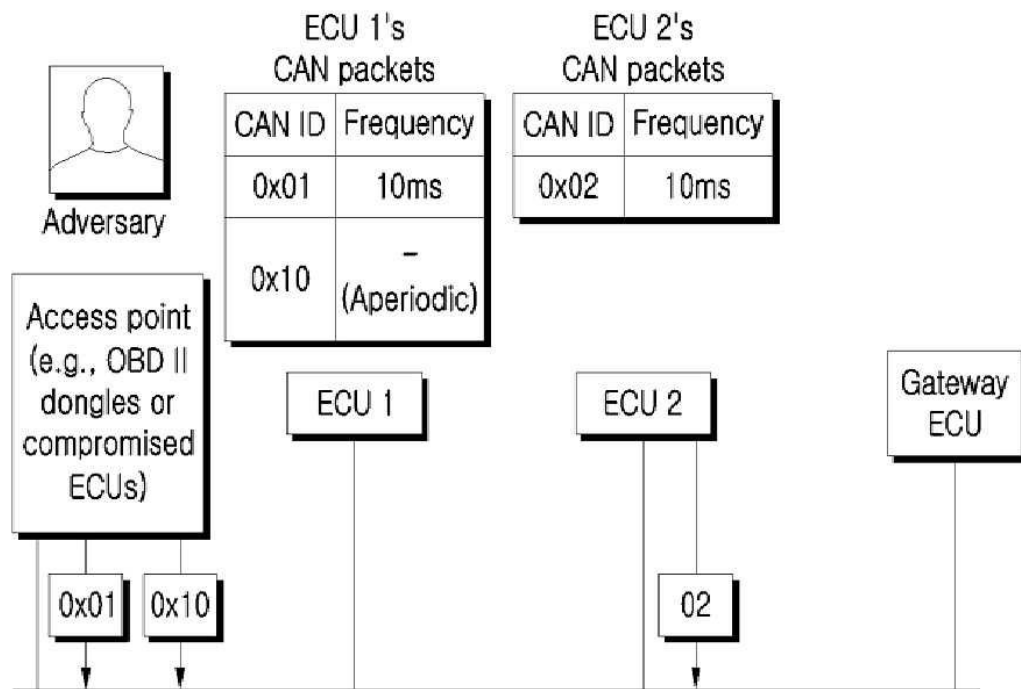
도면8



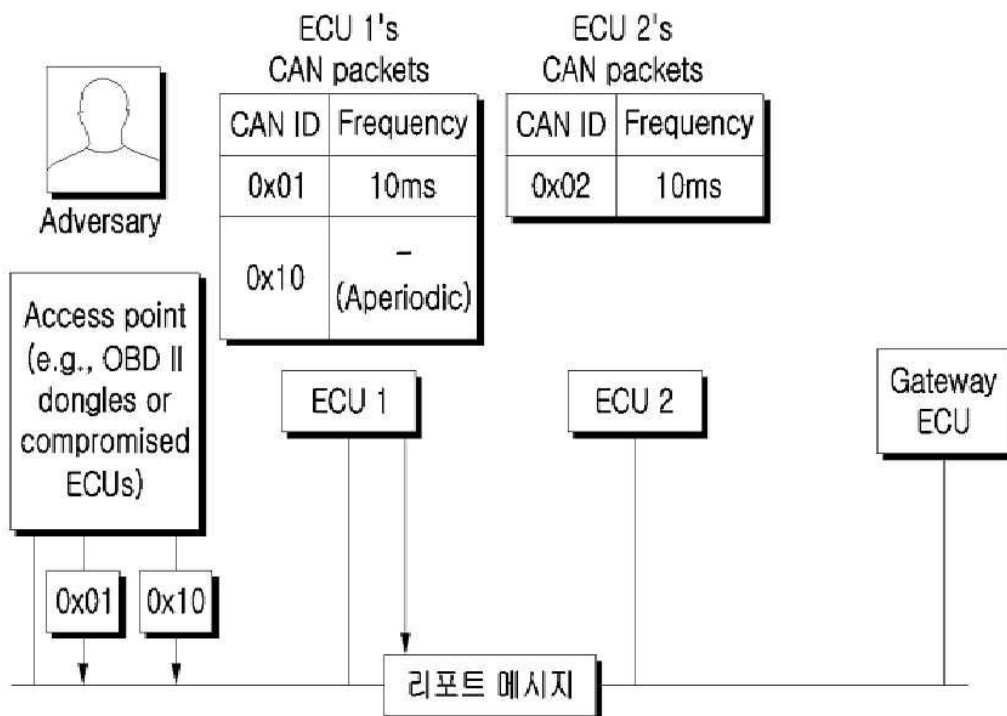
도면9



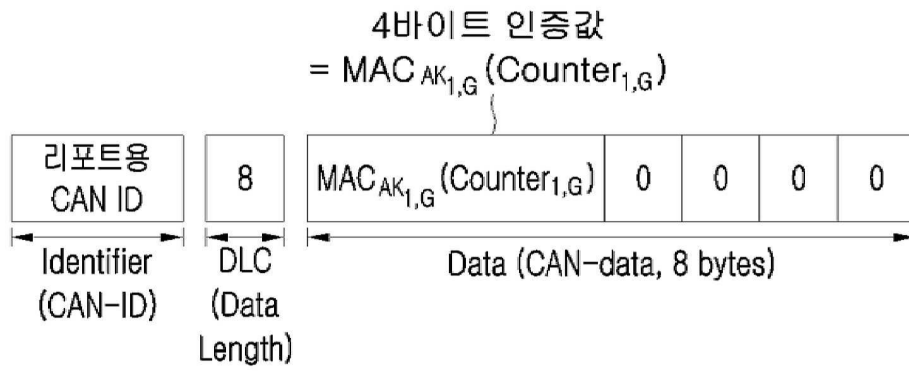
도면10



도면11



도면12



도면13

