(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0014796
(43) 공개일자 2022년02월07일

(51) 국제특허분류(Int. Cl.)
H04L 12/40 (2006.01) *H04L 43/00* (2022.01)
(52) CPC특허분류
H04L 12/40104 (2013.01)
H04L 12/40058 (2013.01)
(21) 출원번호 10-2021-0000237
(22) 출원일자 2021년01월04일
심사청구일자 없음
(30) 우선권주장
1020200094193 2020년07월29일 대한민국(KR)

(71) 출원인
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
기아 주식회사
서울특별시 서초구 헌릉로 12 (양재동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울 성북구 고려대로22길 6-7 고려대학교 자연계 캠퍼스 미래융합기술관 607호
최원석
서울 성북구 고려대로22길 6-7 고려대학교 자연계 캠퍼스 로봇융합관 403호
(뒷면에 계속)
(74) 대리인
이철희

전체 청구항 수 : 총 20 항

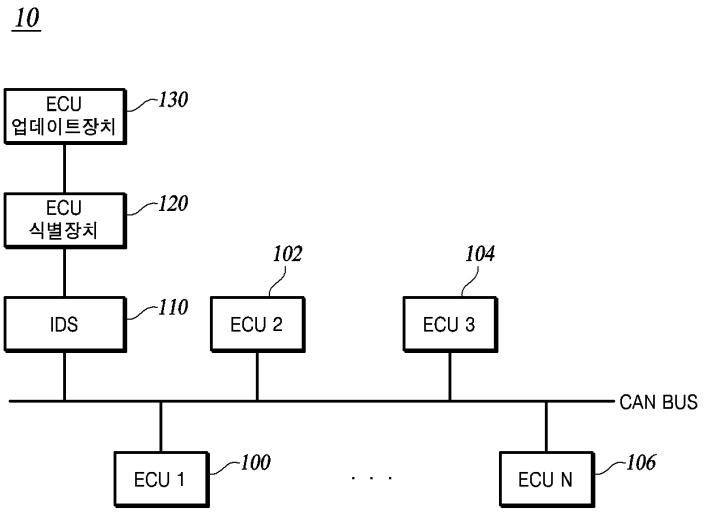
(54) 발명의 명칭 **의도적 에러를 이용한 위변조 제어기 식별 시스템 및 방법**

(57) 요 약

의도적 에러를 이용한 위변조 제어기 식별 시스템 및 방법을 개시한다.

본 개시의 일 측면에 의하면, CAN 버스(Controller Area Network bus) 상에 주기적으로 공격 메시지를 전송하는 위변조 ECU(Electronic Control Unit)를 식별하는 방법으로서, 공격 메시지가 탐지됨에 따라, 상기 CAN 버스에 연결된 복수의 ECU들 중 제1 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 과정; 및 상기 제1 ECU와 관련된 복구 파라미터들(recovery parameters)로부터 예측되는 상기 제1 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 과정을 포함하는, 식별 방법을 제공한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 43/0823 (2013.01)
H04L 2012/40215 (2013.01)
H04L 2012/40273 (2013.01)
(72) 발명자
주경호
서울 성북구 고려대로22길 6-7 고려대학교 자연계 캠퍼스 로봇융합관 403호
이세영
서울특별시 성북구 안암로 145 고려대학교 자연계 캠퍼스 로봇융합관 403호
조아람
인천광역시 연수구 송도과학로27번길 55, 106동 3102호

명 세 서

청구범위

청구항 1

CAN 버스(Controller Area Network bus) 상에 주기적으로 공격 메시지를 전송하는 위변조 ECU(Electronic Control Unit)를 식별하는 방법으로서,

공격 메시지가 탐지됨에 따라, 상기 CAN 버스에 연결된 복수의 ECU들 중 제1 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 과정; 및

상기 제1 ECU와 관련된 복구 파라미터들(recovery parameters)로부터 예측되는 상기 제1 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 과정

을 포함하는, 식별 방법.

청구항 2

제1항에 있어서,

상기 버스오프 상태로 천이시키는 과정은,

상기 제1 ECU에 대응하는 진단요청 메시지를 전송하는 과정;

상기 제1 ECU에 의한 진단응답 메시지 전송 개시를 검출하기 위해 상기 CAN 버스를 모니터링하는 과정; 및

상기 제1 ECU가 버스오프 상태로 천이될 때까지, 상기 진단응답 메시지 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들(dominant bits)을 상기 CAN 버스에 전송하여 상기 진단응답 메시지에 전송에러를 발생시키는 과정

을 포함하는 것을 특징으로 하는, 식별 방법.

청구항 3

제1항에 있어서,

상기 판단하는 과정은,

상기 제1 ECU와 관련된 복구 파라미터들을 이용하여 상기 CAN 메시지의 전송이 재개될 시점을 예측하는 과정; 및

예측된 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점 간의 차이가 기 설정된 임계치보다 작거나 같은 경우에, 상기 제1 ECU가 위변조 ECU이라고 결정하는 과정

을 포함하는 것을 특징으로 하는, 식별 방법.

청구항 4

제3항에 있어서,

상기 예측된 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점 간의 차이가 상기 기 설정된 임계치보다 큰 경우에,

상기 제1 ECU와는 상이한 제2 ECU를 의도적으로 버스오프 상태로 천이시키는 과정; 및

상기 제2 ECU와 관련된 복구 파라미터들로부터 예측되는 상기 제2 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제2 ECU가 위변조 ECU 인지 여부를 판단하는 과정

을 더 포함하는 것을 특징으로 하는, 식별 방법.

청구항 5

제1항에 있어서,

상기 판단하는 과정은,

상기 제1 ECU와 관련된 복구 파라미터들을 이용하여 상기 제1 ECU가 버스오프 상태로부터 복구(recovery)되는 복구시점을 산출하는 과정; 및

산출된 복구시점 이전에 상기 CAN 버스 상에서 상기 공격 메시지가 재차 검출되는지 여부에 따라, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 과정

을 포함하는 것을 특징으로 하는, 식별 방법.

청구항 6

제1항에 있어서,

상기 버스오프 상태로 천이시키는 과정은,

상기 공격 메시지의 전송 주기보다 긴 기간 동안 상기 제1 ECU에 의한 CAN 메시지 전송이 허용되지 않도록, 상기 제1 ECU를 반복적으로 버스오프 상태로 천이시키는 과정을 포함하고,

상기 판단하는 과정은,

상기 제1 ECU가 버스오프 상태에 있는 동안에 상기 CAN 버스 상에서 상기 공격 메시지가 재차 검출되는지 여부에 따라, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 과정을 포함하는 것을 특징으로 하는, 식별 방법.

청구항 7

CAN 버스(Controller Area Network bus) 상의 ECU(Electronic Control Unit)가 버스오프 상태에서 복구되는 고유의 특성과 관련된 복구 파라미터들(recovery parameters)을 분석하는 방법으로서,

주기적으로 CAN 메시지(Controller Area Network message)를 전송하는 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 과정;

상기 ECU가 상기 버스오프 상태로부터 복구(recovery)됨에 따라 전송이 재개되는 CAN 메시지를 수신하기 위해, 상기 CAN 버스를 모니터링하는 과정; 및

상기 CAN 메시지의 수신 시점에 부분적으로 기초하여 상기 ECU의 복구 파라미터들을 분석하는 과정

을 포함하는 것을 특징으로 하는, 분석 방법.

청구항 8

제7항에 있어서,

상기 버스오프 상태로 천이시키는 과정은,

상기 ECU에 대응하는 진단요청 메시지를 전송하는 과정;

상기 ECU에 의한 진단응답 메시지 전송 개시를 검출하기 위해 상기 CAN 버스를 모니터링하는 과정; 및

상기 ECU가 버스오프 상태로 천이될 때까지, 상기 진단응답 메시지 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들(dominant bits)을 상기 CAN 버스에 전송하여 상기 진단응답 메시지에 전송에러를 발생시키는 과정

을 포함하는 것을 특징으로 하는, 분석 방법.

청구항 9

제7항에 있어서,

상기 분석하는 과정은,

상기 ECU가 상기 버스오프 상태로 천이되기 이전에 마지막으로 CAN 메시지를 전송한 시점, 상기 ECU가 상기 버

스오프 상태로 천이된 시점, 및 상기 ECU가 상기 버스오프 상태로부터 복구된 이후 첫 번째 CAN 메시지를 전송한 시점 중 적어도 하나에 기초하여, 상기 ECU의 Wait Time, Controller Recovery Type, 및 Timer Behavior를 포함하는 상기 복구 파라미터들을 분석하는 것을 특징으로 하는, 분석 방법.

청구항 10

제7항에 있어서,

상기 복구 파라미터들을 비일시적으로 저장하는 과정을 추가로 포함하는 것을 특징으로 하는, 분석 방법.

청구항 11

CAN 버스(Controller Area Network bus) 상에 주기적으로 공격 메시지를 전송하는 위변조 ECU(Electronic Control Unit)를 식별하는 장치로서,

공격 메시지가 탐지됨에 따라, 상기 CAN 버스에 연결된 복수의 ECU들 중 제1 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 에러발생부;

상기 제1 ECU와 관련된 복구 파라미터들(recovery parameters)로부터 예측되는 상기 제1 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 위변조 ECU 식별부

를 포함하는 것을 특징으로 하는, 식별 장치.

청구항 12

제11항에 있어서,

상기 에러발생부는,

상기 제1 ECU에 대응하는 진단요청 메시지를 전송하고,

상기 제1 ECU에 의한 진단응답 메시지 전송 개시를 검출하기 위해 상기 CAN 버스를 모니터링하고,

상기 제1 ECU가 버스오프 상태로 천이될 때까지, 상기 진단응답 메시지 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들(dominant bits)을 상기 CAN 버스에 전송하여 상기 진단응답 메시지에 전송에러를 유발하도록 구성된 것을 특징으로 하는, 식별 장치.

청구항 13

제11항에 있어서,

상기 위변조 ECU 식별부는,

상기 제1 ECU와 관련된 복구 파라미터들을 이용하여 상기 CAN 메시지의 전송이 재개될 시점을 예측하고, 예측된 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점 간의 차이가 기 설정된 임계치보다 작거나 같은 경우에, 상기 제1 ECU가 위변조 ECU이라고 결정하도록 구성된 것을 특징으로 하는, 식별 장치.

청구항 14

제13항에 있어서,

상기 에러발생부는, 상기 예측된 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점 간의 차이가 기 설정된 임계치보다 큰 경우에, 상기 제1 ECU와는 상이한 제2 ECU를 의도적으로 버스오프 상태로 천이시키도록 구성되고,

상기 위변조 ECU 식별부는, 상기 제2 ECU와 관련된 복구 파라미터들로부터 예측되는 상기 제2 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제2 ECU가 위변조 ECU 인지 여부를 판단하도록 구성된 것을 특징으로 하는, 식별 장치.

청구항 15

제11항에 있어서,

상기 위변조 ECU 식별부는,

상기 제1 ECU와 관련된 복구 파라미터들을 이용하여 상기 제1 ECU가 버스오프 상태로부터 복구(recovery)되는 복구시점을 산출하고,

산출된 복구시점 이전에 상기 CAN 버스 상에서 상기 공격 메시지가 재차 검출되는지 여부에 따라, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하도록 구성된 것을 특징으로 하는, 식별 장치.

청구항 16

제11항에 있어서,

상기 에러발생부는,

상기 공격 메시지의 전송 주기보다 긴 기간 동안 상기 제1 ECU의 CAN 메시지 전송이 허용되지 않도록, 상기 제1 ECU를 반복적으로 버스오프 상태로 천이시키도록 구성되고,

상기 위변조 ECU 식별부는,

상기 제1 ECU가 버스오프 상태에 있는 동안에 상기 CAN 버스 상에서 상기 공격 메시지가 재차 검출되는지 여부에 따라, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하도록 구성된 것을 특징으로 하는, 식별 장치.

청구항 17

CAN 버스(Controller Area Network bus) 상의 ECU(Electronic Control Unit)가 버스오프 상태에서 복구되는 고유의 특성과 관련된 복구 파라미터들(recovery parameters)을 분석하는 장치로서,

주기적으로 CAN 메시지(Controller Area Network message)를 전송하는 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 에러발생부; 및

상기 ECU가 상기 버스오프 상태로부터 복구(recovery)됨에 따라 전송이 재개되는 CAN 메시지를 수신하기 위해, 상기 CAN 버스를 모니터링하고, 상기 CAN 메시지의 수신 시점에 부분적으로 기초하여 상기 ECU의 복구 파라미터들을 분석하는 파라미터 분석부

를 포함하는 것을 특징으로 하는, 분석 장치.

청구항 18

제17항에 있어서,

상기 에러발생부는,

상기 ECU에 대응하는 진단요청 메시지를 전송하고,

상기 ECU에 의한 진단응답 메시지 전송 개시를 검출하기 위해 상기 CAN 버스를 모니터링하고,

상기 ECU가 버스오프 상태로 천이될 때까지, 상기 진단응답 메시지 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들(dominant bits)을 상기 CAN 버스에 전송하여 상기 진단응답 메시지에 전송에러를 유발하도록 구성된 것을 특징으로 하는, 분석 장치.

청구항 19

제17항에 있어서,

상기 파라미터 분석부는,

상기 ECU가 상기 버스오프 상태로 천이되기 이전에 마지막으로 CAN 메시지를 전송한 시점, 상기 ECU가 상기 버스오프 상태로 천이된 시점, 및 상기 ECU가 상기 버스오프 상태로부터 복구된 이후 첫 번째 CAN 메시지를 전송한 시점 중 적어도 하나에 기초하여, 상기 ECU의 Wait Time, Controller Recovery Type, 및 Timer Behavior를 포함하는 상기 복구 파라미터들을 분석하도록 구성된 것을 특징으로 하는, 분석 장치.

청구항 20

제17항에 있어서,

상기 파라미터 분석부는,

상기 복구 파라미터들을 상기 ECU에 연관시켜 비일시적으로 저장하도록 구성된 것을 특징으로 하는, 분석 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 차량 내부 네트워크에서 위변조된 제어기를 식별하는 것에 관한 것이다.

배 경 기 술

[0002] 이 부분에 기술된 내용은 단순히 본 발명에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0003] 차량에 더 많은 소프트웨어 모듈과 외부 인터페이스가 추가됨에 따라 차량 내부 네트워크에 대한 새로운 공격과 취약점이 등장하고 있다.

[0004] 차량 사이버 공격을 탐지 또는 방지하기 위해 차량 내부 네트워크를 위한 다양한 유형의 보안 솔루션이 제안되고 있으며, 특히, 차량 내부 네트워크의 사실상 표준으로 사용되는 CAN(Controller Area Network) 상에서 발생한 공격을 탐지하는 침입 탐지 시스템(Intrusion Detection System: IDS)에 대한 기술 연구가 활발히 이루어져 오고 있다.

[0005] 스푸핑 공격의 한 유형에서 공격자는 ECU(Electronic Control Unit) 중 하나에 대한 제어권을 획득하고, 이러한 위변조된 ECU를 사용하여 다른 ECU에서 발생한 것처럼 보이는 메시지를 네트워크를 통해 브로드캐스트하여 ECU들 중 하나를 가장할 수 있다. IDS가 CAN 상에 발생한 공격을 탐지한 이후, 예컨대, 스푸핑 공격에 이용되는 위변조 ECU의 정상 패치 또는 업데이트를 위해서는 그러한 위변조된 ECU를 식별하는 것이 전제되어야 한다.

[0006] 특허문헌 1 및 특허문헌 2에는 ECU가 메시지를 전송할 때 CAN 버스(CAN bus)에 흐르는 전력신호의 특성을 이용하여 ECU를 식별하는 기술이 개시되어 있다. 이러한 기술은 전력신호 측정을 위해 추가적인 고성능의 하드웨어가 필요하며, 전력신호가 온도, 전자기장, 연식 등과 같은 외부 환경의 변화에 민감하다는 문제가 있다.

[0007] 특허문헌 3에는 CAN 버스 상에 전송되는 CAN 메시지의 클럭 스큐(clock skew)와 같은 ECU의 물리적 속성을 이용하여 ECU를 식별하는 기술이 개시되어 있다. 이러한 기술은 위변조 ECU가 다른 ECU의 클럭 스큐를 모방(emulation)하는 경우, 위변조 ECU를 정확히 식별하기 어렵다는 문제가 있다.

[0008] 2016년에 CAN 버스에 대한 새로운 DoS(denial of service) 공격으로 버스-오프(bus-off) 공격이 보고되었다. 버스-오프 공격에서, 공격자는 CAN 프로토콜의 장애 제한 메커니즘(Fault confinement mechanisms)을 이용하여 타겟 ECU를 버스-오프 상태로 전환시켜 메시지를 송수신할 수 없게 한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 등록특허공보 제10-1669946호 (2016.10.28.)

(특허문헌 0002) 미국 특허출원공개공보 US2018/0337934 (2018.11.22.)

(특허문헌 0003) 미국 특허출원공개공보 US2017/0286675 (2017.10.05.)

발명의 내용

해결하려는 과제

[0010] 본 개시는, 이러한 CAN 프로토콜의 장애 제한 메커니즘을 이용하여, CAN 네트워크 상에서 공격에 이용되고 있는 위변조된 제어기를 식별하는 방법 및 시스템을 개시한다.

과제의 해결 수단

[0011] 본 개시의 일 측면에 의하면, CAN 버스(Controller Area Network bus) 상에 주기적으로 공격 메시지를 전송하는 위변조 ECU(Electronic Control Unit)를 식별하는 방법으로서, 공격 메시지가 탐지됨에 따라, 상기 CAN 버스에 연결된 복수의 ECU들 중 제1 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 과정; 및 상기 제1 ECU와 관련된 복구 파라미터들(recovery parameters)로부터 예측되는 상기 제1 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 과정을 포함하는, 식별 방법을 제공한다.

[0012] 본 개시의 다른 측면에 의하면, CAN 버스(Controller Area Network bus) 상의 ECU(Electronic Control Unit)가 버스오프 상태에서 복구되는 고유의 특성과 관련된 복구 파라미터들(recovery parameters)을 분석하는 방법으로서, 주기적으로 CAN 메시지(Controller Area Network message)를 전송하는 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 과정; 상기 ECU가 상기 버스오프 상태로부터 복구(recovery)됨에 따라 전송이 재개되는 CAN 메시지를 수신하기 위해, 상기 CAN 버스를 모니터링하는 과정; 및 상기 CAN 메시지의 수신 시점에 부분적으로 기초하여 상기 ECU의 복구 파라미터들을 분석하는 과정을 포함하는 것을 특징으로 하는, 분석 방법을 제공한다.

[0013] 본 개시의 다른 측면에 의하면, CAN 버스(Controller Area Network bus) 상에 주기적으로 공격 메시지를 전송하는 위변조 ECU(Electronic Control Unit)를 식별하는 장치로서, 공격 메시지가 탐지됨에 따라, 상기 CAN 버스에 연결된 복수의 ECU들 중 제1 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 에러발생부; 상기 제1 ECU와 관련된 복구 파라미터들(recovery parameters)로부터 예측되는 상기 제1 ECU에 의한 CAN 메시지의 전송이 재개될 시점과 상기 공격 메시지가 상기 CAN 버스 상에서 재차 검출되는 시점에 적어도 부분적으로 기초하여, 상기 제1 ECU가 위변조 ECU 인지 여부를 판단하는 위변조 ECU 식별부를 포함하는 것을 특징으로 하는, 식별 장치를 제공한다.

[0014] 본 개시의 다른 측면에 의하면, CAN 버스(Controller Area Network bus) 상의 ECU(Electronic Control Unit)가 버스오프 상태에서 복구되는 고유의 특성과 관련된 복구 파라미터들(recovery parameters)을 분석하는 장치로서, 주기적으로 CAN 메시지(Controller Area Network message)를 전송하는 ECU를 의도적으로 버스오프(bus-off) 상태로 천이시키는 에러발생부; 및 상기 ECU가 상기 버스오프 상태로부터 복구(recovery)됨에 따라 전송이 재개되는 CAN 메시지를 수신하기 위해, 상기 CAN 버스를 모니터링하고, 상기 CAN 메시지의 수신 시점에 부분적으로 기초하여 상기 ECU의 복구 파라미터들을 분석하는 파라미터 분석부를 포함하는 것을 특징으로 하는, 분석 장치를 제공한다.

발명의 효과

[0015] 이상에서 설명한 바와 같이 본 개시의 방법들 및 장치들에 의하면, CAN 프로토콜의 장애 제한 메커니즘을 이용하여 CAN 내부네트워크에 공격을 수행하는 ECU를 식별할 수 있다. 따라서, 기존 CAN 프로토콜의 변경 없이, 현재 상용화된 자동차에 적용 가능하다.

[0016] 또한, 본 개시의 실시예에 의하면, 동일한 CAN 네트워크 구성과 ECU를 보유하는 차량이라면 동일한 복구정책(recovery policy)을 따르므로, 높은 확장성을 가질 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 개시의 일 실시예에 따른 CAN 시스템을 개략적으로 나타낸 블록구성도이다.

도 2는 본 개시의 일 실시예에 따른 ECU 식별장치를 개략적으로 나타낸 블록구성도이다.

도 3은 본 개시의 일 실시예에 따른 ECU를 버스오프 상태로 천이시키는 방법을 설명하기 위한 예시도이다.

도 4는 본 개시의 일 실시예에 따른 복구 파라미터를 설명하기 위한 예시도이다.

도 5는 본 개시의 일 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 예시도이다.

도 6은 본 개시의 다른 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 예시도이다.

도 7은 본 개시의 일 실시예에 따른 ECU를 버스오프 상태로 천이시키는 방법을 설명하기 위한 순서도이다.

도 8은 본 개시의 일 실시예에 따른 복구 파라미터 분석방법을 설명하기 위한 순서도이다.

도 9는 본 개시의 일 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 순서도이다.

도 10은 본 개시의 다른 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 본 개시의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 개시를 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 개시의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0019] 또한, 본 개시의 구성 요소를 설명하는 데 있어서, 제 1, 제 2, A, B, (a), (b) 등의 용어를 사용할 수 있다. 이러한 용어는 그 구성 요소를 다른 구성 요소와 구별하기 위한 것일 뿐, 그 용어에 의해 해당 구성 요소의 본질이나 차례 또는 순서 등이 한정되지 않는다. 명세서 전체에서, 어떤 부분이 어떤 구성요소를 '포함', '구비'한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 '…부', '모듈' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0020] 본 개시의 다양한 실시예들을 서술하기에 앞서, CAN 프로토콜(Controller Area Network Protocol)의 장애 제한 메커니즘(Fault confinement mechanisms)을 설명한다.

[0021] CAN 버스 상에 연결된 각 ECU(Electronic Control Unit)는, 메시지 송수신 성공 또는 에러 발생에 따라 특정 가중치를 가지고 증가하거나 감소하는 TEC(Transmit Error Count) 및 REC(Receive Error Count)를 가진다. ECU의 상태는 TEC 및 REC를 바탕으로 정의된다. 특히, TEC가 256 이상이 되면 ECU는 CAN 버스 상으로 어떠한 메시지도 송수신할 수 없는 상태로 천이되는데, 이러한 상태를 버스오프(Bus-Off) 상태라 한다.

[0022] 한편, ECU가 버스오프 상태로부터 다시 CAN 통신에 참여할 수 있는 액티브(active) 상태로 돌아가는 것을 복구(recovery)라고 한다. ECU는 128번의 연속된 11 열성 비트(recessive bit)를 모니터링 함으로써 복구될 수 있는데, 실제 동작 환경에서는 ECU별로 수십 내지 수백 밀리 초(milliseconds)의 추가적인 시간이 더 소요된다.

[0023] 이러한 장애 제한 메커니즘을 바탕으로, 본 개시의 다양한 실시예에서는 ECU를 강제로 버스오프시키고, 복구과정에서 나타나는 특성을 이용하여 ECU를 식별하는 방법 및 시스템을 제안한다.

[0024] 도 1은 본 개시의 일 실시예에 따른 CAN 시스템을 개략적으로 나타낸 블록구성도이다.

[0025] 도 1을 참조하면, 본 개시의 일 실시예에 따른 CAN 시스템(10)은 적어도 하나의 ECU(100 내지 106), IDS(Intrusion Detection System, 110), ECU 식별장치(120), 및 ECU 업데이트장치(130)를 전부 또는 일부 포함한다. 도 1에 도시된 모든 블록이 필수 구성요소는 아니며, 다른 실시예에서 CAN 시스템(10)에 포함된 일부 블록이 추가, 변경 또는 삭제될 수 있다. 즉, 도 1의 경우는 본 개시의 일 실시예에 따른 CAN 시스템(10)이 위변조 ECU를 식별하기 위한 구성요소를 예시적으로 도시한 것으로서, CAN 시스템(10)은 다른 기능의 구현을 위해 도시한 것보다 많거나 적은 구성요소 또는 상이한 구성요소의 구성을 가질 수 있음을 인식하여야 한다.

[0026] ECU(100 내지 106)는 CAN 통신 기능을 가진 전자장치로서, CAN 버스 상으로 일반 CAN 메시지 및/또는 공격 CAN 메시지를 주기적으로 전송한다.

[0027] IDS(110)는 CAN 버스 상에 발생한 공격을 탐지하는 장치이다. IDS(110)는 CAN 버스 상의 공격을 탐지하면, ECU 식별장치(120)에게 식별 개시정보를 전송한다. 이때, 식별 개시정보는 공격 CAN 메시지의 ID 및/또는 공격 CAN 메시지의 전송주기를 포함할 수 있다.

[0028] ECU 식별장치(120)는 각 ECU(100 내지 106)에 대응하는 복구 파라미터들(recovery parameters)을 분석 및 저장하고, 이를 이용하여 ECU를 식별한다. 본 개시의 일 실시예에 따르면, ECU 식별장치(120)는 IDS(110)가 공격을 탐지하기에 앞서 각 ECU(100 내지 106)에 대응하는 복구 파라미터들을 분석 및 저장한다. IDS(110)가 공격을 탐지함에 따라 ECU 식별장치(120)에게 식별 개시정보를 전송하면, ECU 식별장치(120)는 복구 파라미터들을 이용하여 공격을 수행하는 위변조 ECU를 식별한다. 한편, 본 개시의 다른 실시예에 따르면, ECU 식별장치(120)는 외부에 연결된 ECU 분석장치(미도시)로부터 각 ECU(100 내지 106)에 대응하는 복구 파라미터들을 수신하여 저장할 수 있다. ECU 식별장치(120)에 대한 구체적인 설명은 도 2를 참조하여 설명하기로 한다.

[0029] ECU 업데이트장치(130)는, ECU 식별장치(120)가 식별한 위변조 ECU의 업데이트를 수행하여 위변조 ECU를 정상 ECU로 복구시킨다.

[0030] 한편, 본 개시에서의 IDS 또는 ECU 업데이트장치는, 이 분야의 통상의 기술자가 용이하게 채용할 수 있는 모든 IDS 또는 ECU 업데이트장치를 포괄하며, 특정한 구성 및/또는 기능을 가지는 IDS 또는 ECU 업데이트장치로 한정되지 않는다.

[0031] 도 2는 본 개시의 일 실시예에 따른 ECU 식별장치를 개략적으로 나타낸 블록구성도이다.

[0032] 도 2를 참조하면, 본 개시의 일 실시예에 따른 ECU 식별장치(120)는 에러발생부(200), 파라미터 분석부(210), 파라미터 저장부(220), 산출부(230), 및 위변조 ECU 식별부(240)를 전부 또는 일부 포함한다. 도 2에 도시된 모든 블록이 필수 구성요소는 아니며, 다른 실시예에서 ECU 식별장치(120)에 포함된 일부 블록이 추가, 변경 또는 삭제될 수 있다. 예컨대, ECU 식별장치(120)와 연동되는 별개의 자립형 장치인 ECU 분석장치로부터 복구 파라미터를 수신하는 경우, ECU 식별장치는 파라미터 분석부(210)를 포함하지 않을 수 있다. 이 경우, ECU 분석장치는 에러발생부(200) 및 파라미터 분석부(210)를 전부 또는 일부 포함할 수 있다.

[0033] 에러발생부(200)는 CAN 버스 상으로 에러를 발생시켜 ECU를 버스오프 상태로 천이시킨다.

[0034] 본 개시의 일 실시예에 따르면, 에러발생부(200)는 ECU 진단 프로토콜(ECU diagnosis protocol)을 이용하여 대상 ECU를 버스오프 상태로 천이시킨다. 여기서 대상 ECU란, 복구 파라미터를 분석할 분석대상 ECU 또는 해당 ECU가 위변조 ECU 인지 여부를 확인할 식별대상 ECU를 의미한다.

[0035] 도 3은 본 개시의 일 실시예에 따른 ECU를 버스오프 상태로 천이시키는 방법을 설명하기 위한 예시도이다.

[0036] CAN 시스템에는 각 ECU에 대응하는 진단요청 ID 및 진단응답 ID를 정의되어 있다. 예를 들어, 0x700 이상의 범위에서 진단요청 ID 및 진단응답 ID가 정의될 수 있다. 도 3을 참조하면, 에러발생부(200)가 CAN 버스 상으로 대상 ECU에 대응하는 진단요청 ID(DQ_ID_N)를 포함하는 진단요청 메시지를 전송하면, 대상 ECU가 진단응답 ID(DR_ID_N)를 포함하는 진단응답 메시지를 CAN 버스 상으로 전송한다.

[0037] 본 개시의 일 실시예에 따른 에러발생부(200)는 대상 ECU에 대응하는 진단요청 메시지를 전송하고, 대상 ECU에 의한 진단응답 메시지의 전송 개시(the initiation of transmission)를 검출하기 위해 CAN 버스를 모니터링하고, 대상 ECU에 의한 진단응답 메시지의 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들(dominant bits)을 CAN 버스 상으로 전송하여 대상 ECU의 진단응답 메시지에 전송에러를 유발한다.

[0038] 예를 들어, 에러발생부(200)는 대상 ECU에 대응하는 진단응답 ID가 검출됨에 따라, 연속된 6개의 도미넌트 비트를 CAN 버스 상으로 전송한다. 이에 따라, 대상 ECU는 bit 에러를 감지하게 되고, 대상 ECU는 진단응답 메시지 전송에 실패한다. 대상 ECU는 에러프레임 메시지를 CAN 버스 상으로 전송하면서 TEC를 증가시키고, 진단응답 메시지를 재전송한다.

[0039] 본 개시의 일 실시예에 따른 에러발생부(200)는 재전송된 진단응답 ID를 검출함에 따라 다시 복수의 도미넌트 비트들을 CAN 버스 상으로 전송한다. 에러발생부(200)는 CAN 버스를 모니터링하여 대상 ECU의 에러프레임 메시지 전송 및 진단응답 메시지 전송 개시를 검출한다. 에러발생부(200)는 대상 ECU의 진단응답 메시지 전송 개시를 검출할 때마다 복수의 도미넌트 비트를 CAN 버스 상으로 전송함으로써, 대상 ECU의 TEC를 증가시켜, 대상 ECU를 버스오프 상태로 천이시킨다.

[0040] 에러발생부(200)는 마지막 에러프레임 메시지가 CAN 버스 상으로 전송된 시점($t[e_n]$)을 대상 ECU가 버스오프 상태로 천이된 시점으로 판단한다.

[0041] 한편, 전술한 ECU 진단 프로토콜을 이용한 에러발생부(200)는 대상 ECU를 버스오프 상태로 천이시키기 위한 수단의 하나의 실시예에 불과한 것이고, 이 분야 통상의 기술자가 용이하게 채용할 수 있는 수단이라면 본 개시의 다른 실시예에서 대상 ECU를 버스오프 상태로 천이시키기 위한 수단으로서 채용할 수 있다.

[0042] 파라미터 분석부(210)는 분석대상 ECU가 버스오프 상태에서 복구되는 고유의 특성과 관련된 복구 파라미터(recovery parameter)들을 분석한다. 구체적으로, 파라미터 분석부(210)는 분석대상 ECU가 버스오프 상태로 천이된 이후 일반 CAN 메시지의 전송을 재개하는 시점을 바탕으로 분석대상 ECU의 복구 파라미터들을 분석한다.

[0043] 이하, 파라미터 분석부(210)가 복구 파라미터를 분석하는 방법을 설명하기에 앞서, 본 개시에서 정의하는 복구 파라미터를 설명한다.

[0044] 도 4는 본 개시의 일 실시예에 따른 복구 파라미터를 설명하기 위한 예시도이다.

[0045] 본 개시에서는 분석대상 ECU가 버스오프 상태에서 복구되어 메시지 전송을 재개하는 과정에서 나타나는 고유의

특성을 분석하기 위해 3가지의 복구 파라미터 Wait Time, Controller Recovery Type, 및 Timer Behavior를 정의한다.

[0046] 도 4의 (a)를 참조하면, Wait Time(d)은 ECU가 자신이 버스오프 상태로 천이되었음을 탐지한 이후 복구를 수행하기까지 대기하는 시간이다. Wait Time은 특정 시간 또는 특정 인터럽션(interruption) 수로 설정될 수 있다. 예를 들어, ECU는 버스오프 상태 탐지 이후 60 내지 70 ms를 대기한 이후 복구를 수행할 수 있다. 또는, ECU는 버스오프 상태로 천이되기 이전에 마지막으로 CAN 메시지를 전송한 시점으로부터 7번의 인터럽션을 대기한 이후 복구를 수행할 수 있다.

[0047] Controller Recovery Type은 ECU 내부의 CAN 컨트롤러가 복구를 수행하기 위해 128번의 연속된 11 열성 비트(recessive bit)를 모니터링하는 시점을 정의하는 파라미터로서, Immediate recovery 또는 Wait-then-recovery로 분류된다. 도 4의 (a)를 참조하면, Controller Recovery Type이 Immediate recovery인 경우 r의 값은 0(zero)이고, Controller Recovery Type가 Wait-then-recovery인 경우 r은 0보다 큰 값을 가진다.

[0048] Controller Recovery Type이 Immediate recovery인 경우, CAN 컨트롤러는 버스오프 상태 탐지 즉시 128번의 연속된 11 열성 비트를 모니터링한다. 즉, CAN 컨트롤러는 Wait Time 동안 모니터링을 수행하고, Wait Time 이후 바로 복구를 수행한다. 반면, Controller Recovery Type이 Wait-then-recovery인 경우에는, CAN 컨트롤러는 Wait Time을 대기한 이후, 128번의 연속된 11 열성 비트를 모니터링하고 복구를 수행한다.

[0049] Timer Behavior는 주기적으로 CAN 메시지를 전송하기 위해 구비되는 ECU 내부 타이머(timer)가 버스오프 상태 및 복구 시에 동작하는 방식을 정의하는 파라미터로서, Initialized Timer, Suspended Timer, 및 Alive Timer로 분류된다.

[0050] 도 4의 (b)를 참조하면, Timer Behavior가 Initialized Timer인 경우, ECU는 버스오프 상태로부터 복구됨에 따라 타이머를 초기화한다. 이에 따라 메시지 전송 인터럽트(interrupt)가 발생하여 ECU는 복구 이후 즉시 CAN 메시지 전송을 재개한다.

[0051] 도 4의 (c)를 참조하면, Timer Behavior가 Suspended Timer인 경우, ECU는 버스오프 상태를 탐지함에 따라 타이머를 중지하고, 복구 이후 타이머를 다시 카운팅(counting)한다. ECU가 복구되기 전에는 타이머가 중지되어 있으므로 메시지 전송 인터럽트가 발생하지 않는다.

[0052] 도 4의 (d)를 참조하면, Timer Behavior가 Alive Timer인 경우, 타이머는 ECU의 버스오프 및 복구에 상관없이 동작하며, 정상 상태와 동일하게 메시지 전송 인터럽트를 발생시킨다. ECU는 버스오프 상태일 때 발생한 메시지 전송 인터럽트를 무시한다.

[0053] 본 개시의 일 실시예에 따른 파라미터 분석부(210)는 분석대상 ECU가 일반 CAN 메시지의 전송을 재개하는 시점($t[m_{i+1}]$) 및 분석대상 ECU가 버스오프 상태로 천이된 시점($t[e_n]$)을 기초로 분석대상 ECU의 Wait Time(d) 및 Controller Recovery Type(r)을 분석한다.

[0054] 구체적으로, 파라미터 분석부(210)는 분석대상 ECU가 일반 CAN 메시지의 전송을 재개하는 시점과 분석대상 ECU가 버스오프 상태로 천이된 시점의 차이인 제1시간($t[m_{i+1}]-t[e_n]$)과 제1시간으로부터 128번의 연속된 11비트를 모니터링하는 시간(t_{AR})을 뺀 제2시간($t[m_{i+1}]-t[e_n]-t_{AR}$)을 이용하여 분석대상 ECU의 Wait Time(d) 및 Controller Recovery Type(r)을 분석한다.

[0055] 파라미터 분석부(210)는 분석대상 ECU의 버스오프, 복구, 및 메시지 재전송을 하나의 분석단위로 하여 복수의 분석단위를 모니터링한다. 파라미터 분석부(210)는 매 분석단위마다 측정된 $t[e_n]$, $t[m_{i+1}]$, 및 t_{AR}를 바탕으로 제1시간 및 제2시간을 산출한다. 파라미터 분석부(210)는 제1시간의 분포 및 제2시간의 분포를 비교하여 분석대상 ECU의 Wait Time(d) 및 Controller Recovery Type(r)을 결정한다. 예를 들어, 파라미터 분석부(210)는 제1시간의 분산(또는 표준 편차, 이하 동일)이 제2시간의 분산보다 작은 경우, Controller Recovery Type이 Immediate recovery인 것으로 결정하고, 제1시간의 분산이 제2시간의 분산보다 큰 경우, Controller Recovery Type이 Wait-then-recovery인 것으로 결정할 수 있다. 또한, 파라미터 분석부(210)는 제1시간 및 제2시간 중 분산이 더 작은 값의 평균을 Wait Time으로 결정할 수 있다.

[0056] 본 개시의 일 실시예에 따른 파라미터 분석부(210)는 CAN 메시지 전송주기(T) 및 버스오프 전·후 CAN 메시지 전송간격(B)을 이용하여 분석대상 ECU의 Timer Behavior를 알아낼 수 있다. 표 1은 CAN 메시지 전송주기(T) 및 버스오프 전·후 CAN 메시지 전송간격(B)에 따른 Timer Behavior를 나타낸다.

표 1

[0057]

버스오프 전·후 CAN 메시지 전송간격(B)	Timer Behavior
d + r ≤ B ≤ T + d + r	Initialized
B = T + d + r	Suspended
B = n·T, (n=자연수)	Alive

[0058] 파라미터 분석부(210)는 분석한 복구 파라미터를 분석대상 ECU의 진단요청 ID 및 진단응답 ID와 매핑(mapping)하여 파라미터 저장부(220)에 저장한다.

[0059] 산출부(230)는 파라미터 저장부(220)에 저장된 복구 파라미터를 이용하여 위변조 ECU 식별과 관련된 시점을 산출한다.

[0060] 본 개시의 일 실시예에 따르면, 산출부(230)는 공격 CAN 메시지의 전송이 재개될 재전송시점을 산출한다. 즉, 식별대상 ECU가 공격 CAN 메시지를 전송하는 위변조 ECU라고 가정하고, 식별대상 ECU가 버스오프 상태로부터 복구되어 공격 CAN 메시지 전송을 재개할 시점을 산출한다. 산출부(230)는 식별대상 ECU가 버스오프 상태로 천이된 시점($t[e_n]$), 식별대상 ECU가 버스오프 상태로 천이되기 이전 마지막으로 공격 CAN 메시지를 전송한 시점($t[m_i]$), 및 복구 파라미터 중 적어도 하나를 이용하여 재전송시점($t[m_{new}]$)을 산출한다.

[0061] 표 2는 식별대상 ECU의 Timer Behavior에 따라, 산출되는 재전송시점($t[m_{new}]$)을 나타낸다.

표 2

[0062]

Timer Behavior	공격 CAN 메시지의 재전송시점($t[m_{new}]$)
Initialized	$t[m_{new}] = t[e_n] + d + r$
Suspended	$t[m_{new}] = t[m_i] + T + d + r$
Alive	$t[m_{new}] = t[m_i] + n \cdot T$, $(t[m_i] + n \cdot T > t[r])$

[0063] 본 개시의 다른 실시예에 따르면, 산출부(230)는 식별대상 ECU가 버스오프 상태로부터 복구되는 복구시점을 산출한다. 예컨대, 도 4의 (a)를 참조하면, 산출부(230)는 식별대상 ECU가 버스오프 상태로 천이된 시점($t[e_n]$), Wait Time(d) 및 Controller Recovery Type(r)을 이용하여 복구시점을 산출할 수 있다.

[0064] 위변조 ECU 식별부(240)는 산출부(230)가 산출한 시점 및 식별대상 ECU가 버스오프 상태로 천이된 후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$)을 이용하여, 식별대상 ECU가 위변조 ECU 인지 여부를 판단한다.

[0065] 도 5는 본 개시의 일 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 예시도이다.

[0066] 도 5의 (a)를 참조하면, 식별대상 ECU가 위변조 ECU인 경우, 즉 에러발생부(200)가 위변조 ECU를 버스오프 상태로 천이시킨 경우에는, 식별대상 ECU가 버스오프 상태로부터 복구됨에 따라 산출부(230)가 산출한 재전송시점($t[m_{new}]$)에 공격 CAN 메시지 전송을 재개한다. 반면, 도 5의 (b)를 참조하면, 식별대상 ECU가 위변조 ECU가 아닌 경우, 즉 에러발생부(200)가 위변조 ECU가 아닌 다른 ECU를 버스오프 상태로 천이시킨 경우에는 산출부(230)가 산출한 재전송시점($t[m_{new}]$)과 무관하게 CAN 버스 상으로 공격 CAN 메시지가 전송된다.

[0067] 이 점에 기인하여, 본 개시의 일 실시예에 따른 위변조 ECU 식별부(240)는 산출부(230)가 산출한 재전송시점($t[m_{new}]$)에 공격 CAN 메시지가 전송되는지에 따라, 식별대상 ECU가 위변조 ECU 인지 여부를 판단한다. 구체적으로, 위변조 ECU 식별부(240)는 식별대상 ECU가 버스오프 상태로 천이된 이후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$) 및 산출부(230)가 산출한 재전송시점($t[m_{new}]$)을 비교하여 위변조 ECU를 식별한다

[0068] 도 5의 (a)에 나타나듯이, 식별대상 ECU가 버스오프 상태로 천이된 이후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$) 및 산출부(230)가 산출한 재전송시점($t[m_{new}]$)의 차가 기 설정된 임계치보다 작거나 같은 경우에, 위변조 ECU 식별부(240)는 식별대상 ECU가 위변조 ECU라고 판단한다. 반면, 도 5의 (b)에 나타나듯이, 식별대상 ECU

가 버스오프 상태로 천이된 후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$) 및 산출부(230)가 산출한 재전송시점($t[m_{new}]$)의 차가 기 설정된 임계치보다 큰 경우에, 위변조 ECU 식별부(240)는 식별대상 ECU는 위변조 ECU가 아닌 것으로 판단한다.

[0069] 도 6은 본 개시의 다른 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 예시도이다.

[0070] 식별대상 ECU가 위변조 ECU인 경우, 즉 에러발생부(200)가 위변조 ECU를 버스오프 상태로 천이시킨 경우에는, 식별대상 ECU가 복구되기 전까지는 CAN 버스 상으로 공격 CAN 메시지가 전송되지 않는다. 반면, 도 6의 (a)를 참조하면, 식별대상 ECU가 위변조 ECU가 아닌 경우, 즉 에러발생부(200)가 위변조 ECU가 아닌 다른 ECU를 버스오프 상태로 천이시킨 경우에는 식별대상 ECU의 복구와 무관하게 CAN 버스 상으로 공격 CAN 메시지가 전송된다. 특히, 빠른 주기로 CAN 버스 상으로 주입되는 공격 CAN 메시지의 경우에는, 식별대상 ECU가 복구되기 이전에 공격 CAN 메시지가 한번 이상 CAN 버스 상으로 전송될 수 있다.

[0071] 이 점에 기인하여, 본 개시의 다른 실시예에 따른 위변조 ECU 식별부(240)는 산출부(230)가 산출한 복구시점($t[r']$) 이전에 공격 CAN 메시지가 CAN 버스 상으로 전송되는지에 따라, 식별대상 ECU가 위변조 ECU 인지 여부를 판단한다. 구체적으로, 위변조 ECU 식별부(240)는 식별대상 ECU가 버스오프 상태로 천이된 후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$) 및 산출부(230)가 산출한 복구시점($t[r']$)을 비교하여, 식별대상 ECU가 버스오프 상태로 천이된 후 첫 번째 공격 CAN 메시지 전송시점($t[m_{i+1}]$)이 산출부(230)가 산출한 복구시점($t[r']$)보다 앞선 경우, 식별대상 ECU를 위변조 ECU로 식별한다.

[0072] 도 6의 (b)를 참조하면, 본 개시의 다른 실시예에 따르면, 식별대상 ECU의 Wait Time(d)보다 긴 주기로 공격 CAN 메시지를 전송하는 위변조 ECU를 식별하거나 위변조 ECU 식별의 신뢰도를 높이기 위해, 에러발생부(200)는 공격 CAN 메시지의 전송 주기보다 긴 기간 동안 식별대상 ECU에 의한 CAN 메시지 전송이 허용되지 않도록, 식별대상 ECU를 일정 시간 및/또는 일정 횟수 이상 반복적으로 버스오프 상태로 천이시키고, 위변조 ECU 식별부(240)는 식별대상 ECU가 버스오프 상태에 있는 동안에 CAN 버스 상에서 공격 CAN 메시지가 검출되는지 여부에 따라, 식별대상 ECU가 위변조 ECU 인지 여부를 식별할 수 있다.

[0073] 본 개시의 일 실시예에 따르면, 식별 대상 ECU가 위변조 ECU가 아닌 경우, 위변조 ECU 식별부(240)는 에러발생부(200) 및 산출부(230)가 다른 ECU를 대상으로 위변조 ECU 식별과정을 수행하도록 하는 제어정보를 전송할 수 있다.

[0074] 도 7은 본 개시의 일 실시예에 따른 ECU를 버스오프 상태로 천이시키는 방법을 설명하기 위한 순서도이다.

[0075] ECU 식별장치(120)는 대상 ECU에 대응하는 진단요청 메시지를 CAN 버스 상으로 전송한다(S700). 여기서, 대상 ECU란 파라미터 분석을 위해 버스오프 상태로 천이시킬 분석대상 ECU 또는 해당 ECU가 위변조 ECU 인지 여부를 확인하기 위해 버스오프 상태로 천이시킬 식별대상 ECU를 의미한다.

[0076] ECU 식별장치(120)는 CAN 버스를 모니터링하여(S710), 대상 ECU에 의한 진단응답 메시지의 전송 개시를 검출한다(S720). ECU 식별장치(120)는 CAN 버스 상에서 대상 ECU에 대응하는 진단응답 ID를 검출함으로써, 대상 ECU에 의한 진단응답 메시지의 전송 개시를 검출할 수 있다.

[0077] ECU 식별장치(120)는 진단응답 메시지 전송 개시의 검출에 응답하여, 복수의 도미넌트 비트들을 CAN 버스에 전송한다(S730). 예컨대, ECU 식별장치(120)는 연속된 6개의 도미넌트 비트를 CAN 버스 상으로 전송한다. 이에 따라, 대상 ECU는 bit 에러를 감지하게 된다.

[0078] ECU 식별장치(120)는 CAN 버스를 모니터링하여(S710), 대상 ECU에 의한 진단응답 메시지의 전송 개시를 재검출한다(S720).

[0079] ECU 식별장치(120)는 진단응답 메시지 전송 개시의 재검출에 응답하여, 복수의 도미넌트 비트들을 CAN 버스에 전송한다(S730). ECU 식별장치(120)는 대상 ECU가 버스오프 상태로 천이되어 더이상 진단응답 메시지를 전송하지 못할 때까지 과정 S710 내지 S730을 반복한다.

[0080] 대상 ECU에 의한 진단응답 메시지의 전송 개시가 더이상 검출되지 않으면, ECU 식별장치(120)는 대상 ECU가 버스오프 상태로 천이된 것으로 판단한다(S740).

[0081] 도 8은 본 개시의 일 실시예에 따른 복구 파라미터 분석방법을 설명하기 위한 순서도이다.

[0082] ECU 식별장치(120)는 CAN 버스를 모니터링하여, 분석대상 ECU가 전송하는 일반 CAN 메시지의 ID 및 일반 CAN 메

시지의 주기를 획득한다(S810).

[0083] ECU 식별장치(120)는 분석대상 ECU를 버스오프 상태로 천이시킨다(S820).

[0084] 분석대상 ECU가 버스오프 상태로부터 복구됨에 따라, ECU 식별장치(120)는 다시 일반 CAN 메시지를 수신한다(S820).

[0085] ECU 식별장치(120)는 분석대상 ECU의 복구 파라미터들을 분석한다(S830). 예를 들어, ECU 식별장치(120)는 분석대상 ECU가 버스오프 상태로 천이되기 이전 마지막으로 CAN 메시지를 전송한 시점, 분석대상 ECU가 버스오프 상태로부터 복구된 이후 첫 번째 CAN 메시지를 전송한 시점, 및 분석대상 ECU가 버스오프 상태로 천이된 시점 중 적어도 하나에 기초하여, 분석대상 ECU의 Wait Time, Controller Recovery Type, 및 Timer Behavior를 포함하는 복구 파라미터들을 분석한다.

[0086] ECU 식별장치(120)는 분석한 복구 파라미터들을 저장한다(S840). ECU 식별장치(120)는 복구 파라미터들을 분석대상 ECU에 연관시켜 비일시적으로 저장할 수 있다.

[0087] 도 9는 본 개시의 일 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 순서도이다.

[0088] ECU 식별장치(120)는 공격 CAN 메시지의 ID 및 공격 CAN 메시지의 전송주기를 획득한다(S900). 본 개시의 일 실시예에 따르면, ECU 식별장치(120)는 IDS(110)가 공격을 탐지함에 따라 IDS(110)로부터 공격 CAN 메시지의 ID 및 공격 CAN 메시지의 전송주기를 포함하는 식별 개시정보를 전달받을 수 있다. 본 개시의 다른 실시예에 따르면, ECU 식별장치(120)는 IDS(110)가 공격을 탐지함에 따라 IDS(110)로부터 식별 개시정보를 전달받은 이후, 직접 CAN 버스를 모니터링하여 공격 CAN 메시지의 ID 및 공격 CAN 메시지의 전송주기를 획득할 수 있다.

[0089] ECU 식별장치(120)는 위변조 ECU 인지 여부를 확인할 식별대상 ECU를 선택한다(S910). ECU 식별장치(120)는 기저장된 진단요청 ID 중에서 하나를 선택함으로써, 식별대상 ECU를 선택할 수 있다.

[0090] ECU 식별장치(120)는 식별대상 ECU를 버스오프 상태로 천이시킨다(S920).

[0091] ECU 식별장치(120)는 공격 CAN 메시지의 재전송시점을 산출한다(S930). 즉, ECU 식별장치(120)는 식별대상 ECU가 공격 CAN 메시지를 전송하는 위변조 ECU라고 가정하고, 식별대상 ECU가 버스오프 상태로부터 복구되어 공격 CAN 메시지 전송을 재개할 시점을 산출한다. ECU 식별장치(120)는 진단요청 ID와 매핑되어 있는 복구 파라미터를 이용하여 공격 CAN 메시지의 재전송시점을 산출할 수 있다.

[0092] ECU 식별장치(120)는 산출된 재전송시점에 공격 CAN 메시지가 전송되는지 확인한다(S940). 산출된 재전송시점으로부터 기설정된 임계치 이전 및/또는 이후의 시점에 공격 CAN 메시지가 전송되는 경우, ECU 식별장치(120)는 식별대상 ECU가 위변조 ECU가 아닌 것으로 판단하고, 다른 ECU를 식별대상 ECU로 선택한다.

[0093] 산출된 재전송시점으로부터 기설정된 임계치 이내의 시점에 공격 CAN 메시지가 전송되는 경우, ECU 식별장치(120)는 식별대상 ECU가 위변조 ECU인 것으로 판단한다(S950).

[0094] 도 10은 본 개시의 다른 실시예에 따른 위변조 ECU 식별방법을 설명하기 위한 순서도이다.

[0095] 여기서, 단계 S1000 내지 S1020은 앞서 설명된 도 9의 과정 S900 내지 S920에 대응되므로 상세한 설명은 생략한다.

[0096] ECU 식별장치(120)는 공격 CAN 메시지의 ID 및 공격 CAN 메시지의 전송주기를 획득한다(S1000).

[0097] ECU 식별장치(120)는 위변조 ECU 인지 여부를 확인할 식별대상 ECU를 선택한다(S1010). ECU 식별장치(120)는 기저장된 진단요청 ID 중에서 하나를 선택함으로써, 식별대상 ECU를 선택할 수 있다.

[0098] ECU 식별장치(120)는 식별대상 ECU를 버스오프 상태로 천이시킨다(S1020).

[0099] ECU 식별장치(120)는 식별대상 ECU가 버스오프 상태로부터 복구될 시점을 산출한다(S1030). ECU 식별장치(120)는 진단요청 ID와 매핑되어 있는 복구 파라미터를 이용하여 공격 CAN 메시지의 재전송시점을 산출할 수 있다.

[0100] ECU 식별장치(120)는 산출된 복구시점 전에 공격 CAN 메시지가 전송되는지 확인한다(S1040). 산출된 복구시점 전에 공격 CAN 메시지가 전송되지 않는 경우, ECU 식별장치(120)는 식별대상 ECU가 위변조 ECU가 아닌 것으로 판단하고, 다른 ECU를 식별대상 ECU로 선택한다.

[0101] 산출된 복구시점 전에 공격 CAN 메시지가 전송되는 경우, ECU 식별장치(120)는 식별대상 ECU가 위변조 ECU인 것으로 판단한다(S1050).

[0102] 도 7 내지 도 10에서는 각 과정들을 순차적으로 실행하는 것으로 기재하고 있으나, 이는 본 개시의 일 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것이다. 다시 말해, 본 개시의 일 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 개시의 일 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 도 7 내지 도 10에 기재된 순서를 변경하여 실행하거나 하나 이상의 과정을 병렬적으로 실행하는 것으로 다양하게 수정 및 변형하여 적용 가능할 것이므로, 도 7 내지 도 10은 시계열적인 순서로 한정되는 것은 아니다.

[0103] 본 명세서에 설명되는 시스템들 및 기법들의 다양한 구현예들은, 디지털 전자 회로, 집적 회로, FPGA(field programmable gate array), ASIC(application specific integrated circuit), 컴퓨터 하드웨어, 펌웨어, 소프트웨어, 및/또는 이들의 조합으로 실현될 수 있다. 이러한 다양한 구현예들은 프로그래밍가능 시스템 상에서 실행가능한 하나 이상의 컴퓨터 프로그램들로 구현되는 것을 포함할 수 있다. 프로그래밍가능 시스템은, 저장 시스템, 적어도 하나의 입력 디바이스, 그리고 적어도 하나의 출력 디바이스로부터 데이터 및 명령들을 수신하고 이들에게 데이터 및 명령들을 전송하도록 결합되는 적어도 하나의 프로그래밍가능 프로세서(이것은 특수 목적 프로세서일 수 있거나 혹은 범용 프로세서일 수 있음)를 포함한다. 컴퓨터 프로그램들(이것은 또한 프로그램들, 소프트웨어, 소프트웨어 애플리케이션들 혹은 코드로서 알려져 있음)은 프로그래밍가능 프로세서에 대한 명령어들을 포함하며 "컴퓨터가 읽을 수 있는 기록매체"에 저장된다.

[0104] 컴퓨터가 읽을 수 있는 기록매체는, 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 이러한 컴퓨터가 읽을 수 있는 기록매체는 ROM, CD-ROM, 자기 테이프, 플로피디스크, 메모리 카드, 하드 디스크, 광자기 디스크, 스토리지 디바이스 등의 비휘발성(non-volatile) 또는 비일시적인(non-transitory) 매체일 수 있으며, 또한 데이터 전송 매체(data transmission medium)와 같은 일시적인(transitory) 매체를 더 포함할 수도 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수도 있다.

[0105] 본 명세서에 설명되는 시스템들 및 기법들의 다양한 구현예들은, 프로그램가능 컴퓨터에 의하여 구현될 수 있다. 여기서, 컴퓨터는 프로그램가능 프로세서, 데이터 저장 시스템(휘발성 메모리, 비휘발성 메모리, 또는 다른 종류의 저장 시스템이거나 이들의 조합을 포함함) 및 적어도 한 개의 커뮤니케이션 인터페이스를 포함한다. 예컨대, 프로그램가능 컴퓨터는 서버, 네트워크 기기, 셋탑 박스, 내장형 장치, 컴퓨터 확장 모듈, 개인용 컴퓨터, 랩탑, PDA(Personal Data Assistant), 클라우드 컴퓨팅 시스템 또는 모바일 장치 중 하나일 수 있다.

[0106] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0107] 10: CAN 시스템 100 ~ 106: ECU

110: IDS 120: ECU 식별장치

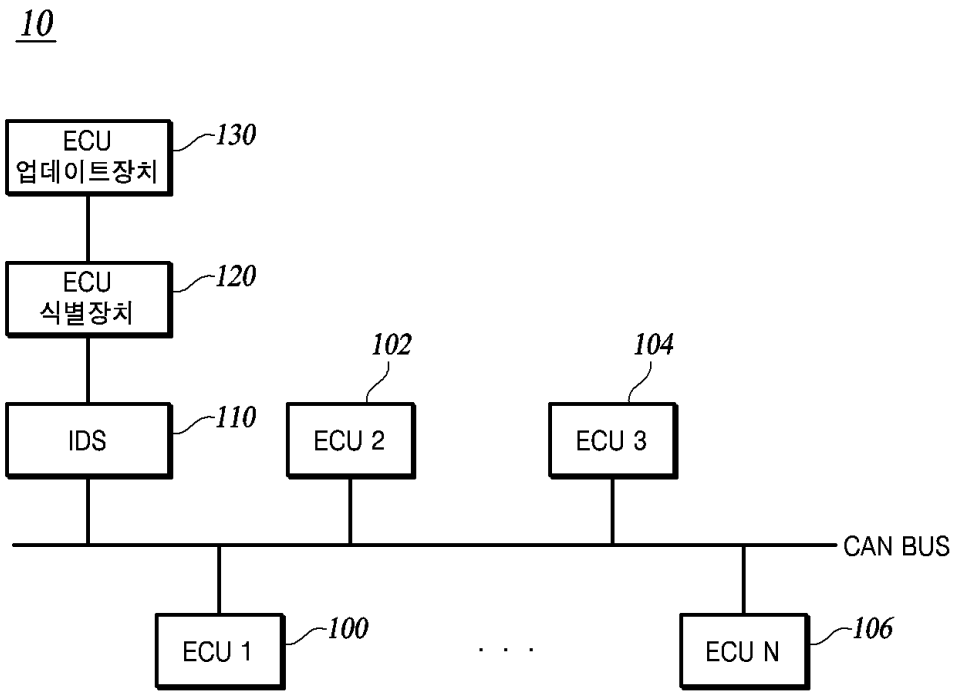
130: ECU 업데이트장치 200: 에러발생부

210: 파라미터 분석부 220: 파라미터 저장부

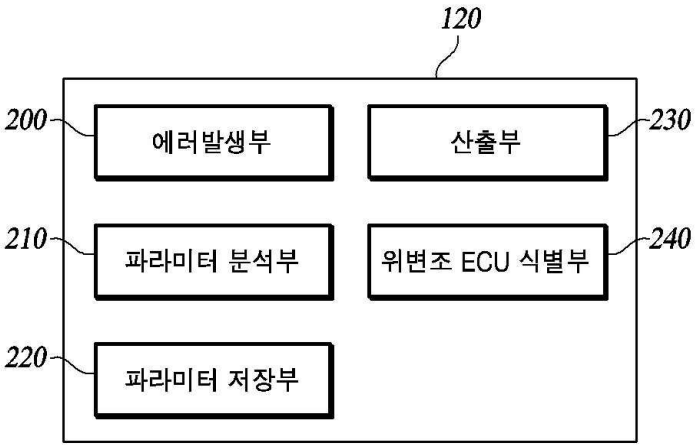
230: 산출부 240: 위변조 ECU 식별부

도면

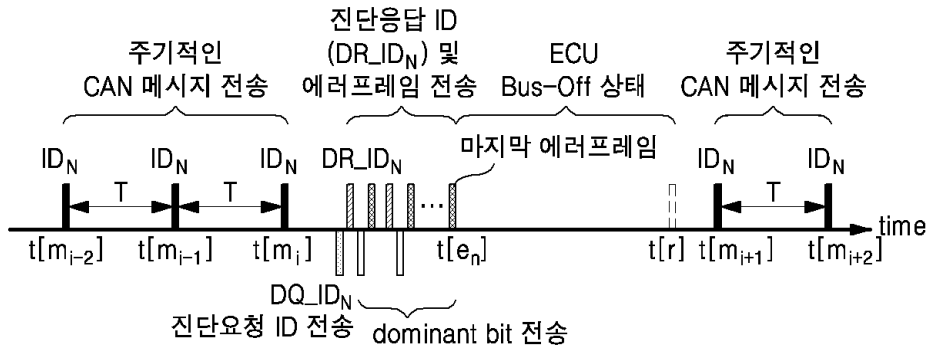
도면1


10
ECU
업데이트장치
130
ECU
식별장치
120
IDS
110
102
ECU 2
104
ECU 3
CAN BUS
ECU 1
100
ECU N
106

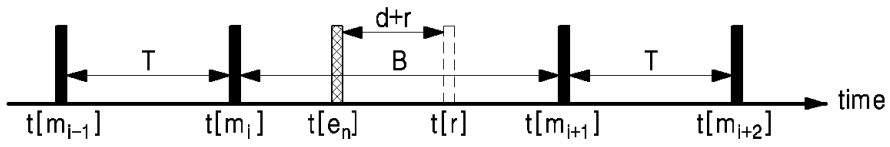
도면2


120
200
에러발생부
산출부
230
210
파라미터 분석부
위변조 ECU 식별부
240
220
파라미터 저장부

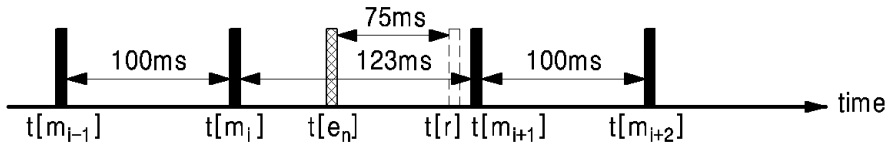
도면3


주기적인
CAN 메시지 전송
진단응답 ID
(DR_ID$_N$) 및
에러프레임 전송
ECU
Bus-Off 상태
주기적인
CAN 메시지 전송
마지막 에러프레임
ID$_N$
DR_ID$_N$
T
time
t[m$_{i-2}$]
t[m$_{i-1}$]
t[m$_i$]
t[e$_n$]
t[r]
t[m$_{i+1}$]
t[m$_{i+2}$]
DQ_ID$_N$
진단요청 ID 전송
dominant bit 전송

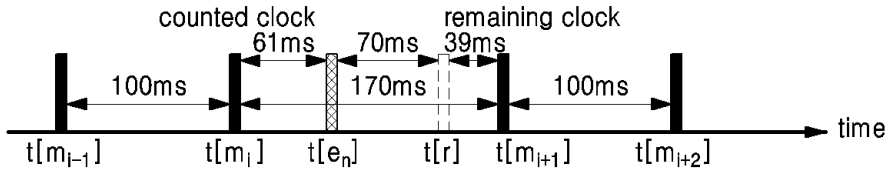
도면4


d+r
T
B
time
t[m$_{i-1}$]
t[m$_i$]
t[e$_n$]
t[r]
t[m$_{i+1}$]
t[m$_{i+2}$]

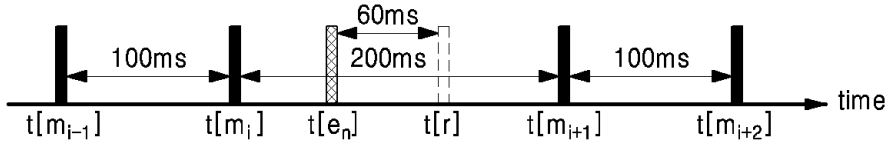
(a)


75ms
100ms
123ms
100ms
time
t[m$_{i-1}$]
t[m$_i$]
t[e$_n$]
t[r]
t[m$_{i+1}$]
t[m$_{i+2}$]

(b)

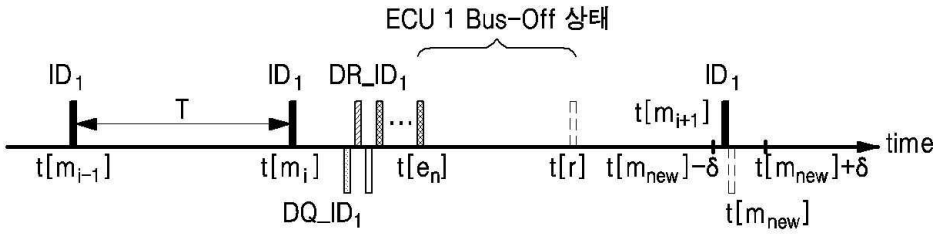

counted clock
remaining clock
61ms
70ms
39ms
100ms
170ms
100ms
time
t[m$_{i-1}$]
t[m$_i$]
t[e$_n$]
t[r]
t[m$_{i+1}$]
t[m$_{i+2}$]

(c)

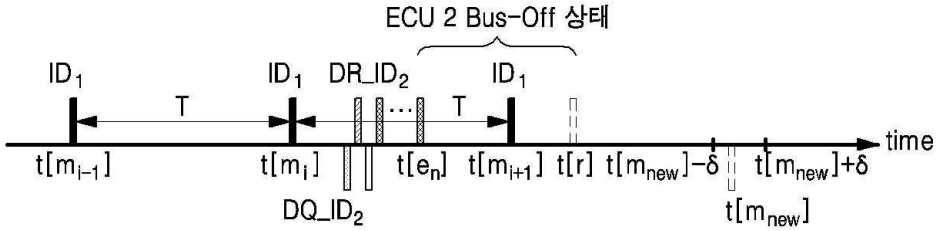

60ms
100ms
200ms
100ms
time
t[m$_{i-1}$]
t[m$_i$]
t[e$_n$]
t[r]
t[m$_{i+1}$]
t[m$_{i+2}$]

(d)

도면5

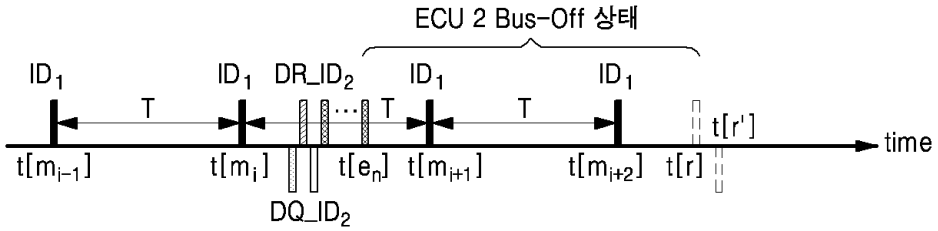

ECU 1 Bus-Off 상태
ID1
ID1
DR_ID1
ID1
T
t[mi+1]
time
t[mi-1]
t[mi]
t[en]
t[r]
t[mnew]-δ
t[mnew]+δ
DQ_ID1
t[mnew]

(a)

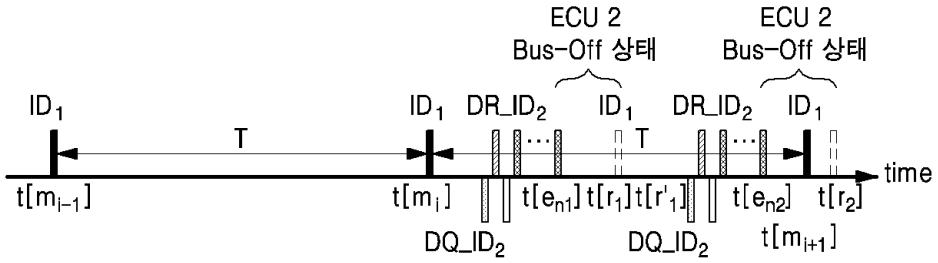

ECU 2 Bus-Off 상태
ID1
ID1
DR_ID2
ID1
T
T
time
t[mi-1]
t[mi]
t[en]
t[mi+1]
t[r]
t[mnew]-δ
t[mnew]+δ
DQ_ID2
t[mnew]

(b)

도면6

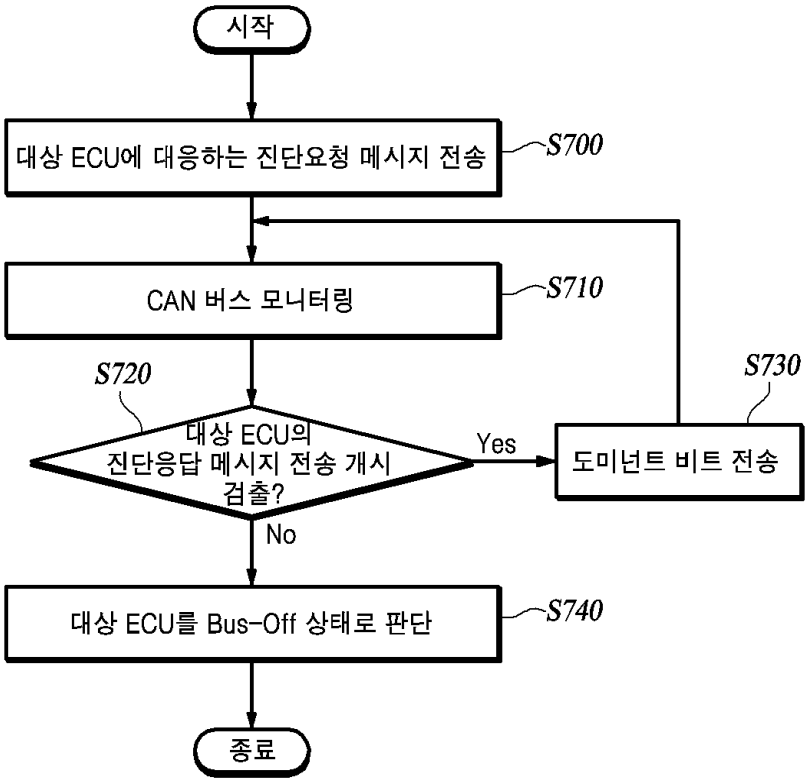

ECU 2 Bus-Off 상태
ID1
ID1
DR_ID2
ID1
ID1
T
T
T
t[r']
time
t[mi-1]
t[mi]
t[en]
t[mi+1]
t[mi+2]
t[r]
DQ_ID2

(a)

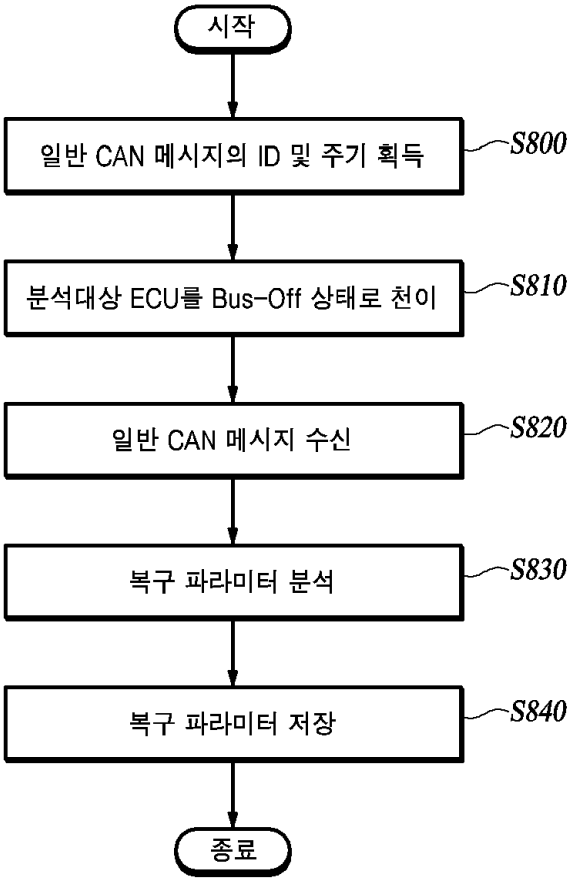

ECU 2
Bus-Off 상태
ECU 2
Bus-Off 상태
ID1
ID1
DR_ID2
ID1
DR_ID2
ID1
T
T
time
t[mi-1]
t[mi]
t[en1]
t[r1]
t[r'1]
t[en2]
t[r2]
DQ_ID2
DQ_ID2
t[mi+1]

(b)

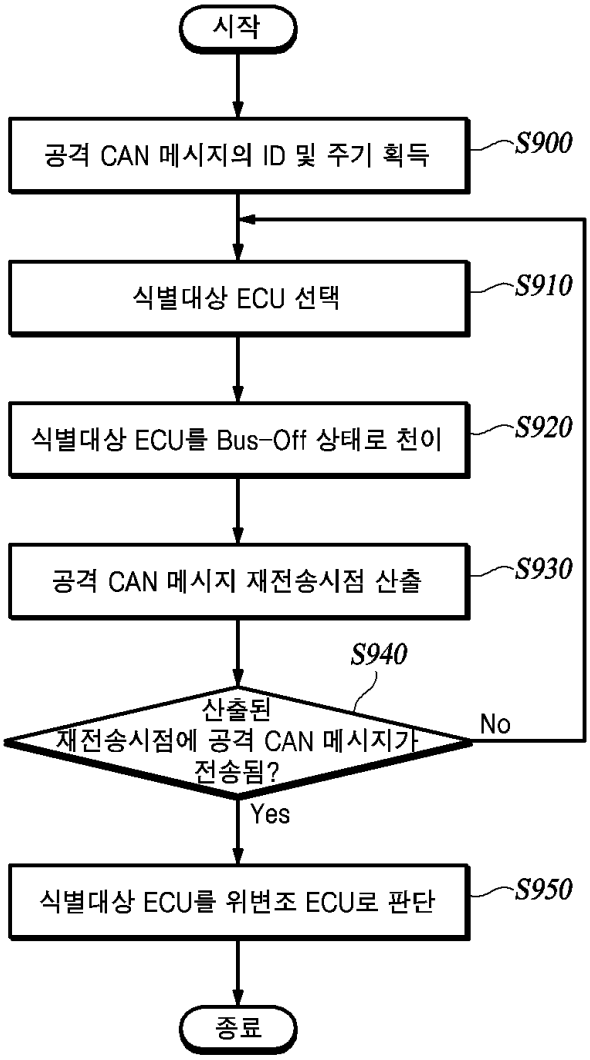
도면7


시작
대상 ECU에 대응하는 진단요청 메시지 전송
S700
CAN 버스 모니터링
S710
S720
대상 ECU의
진단응답 메시지 전송 개시
검출?
Yes
S730
도미넌트 비트 전송
No
대상 ECU를 Bus-Off 상태로 판단
S740
종료

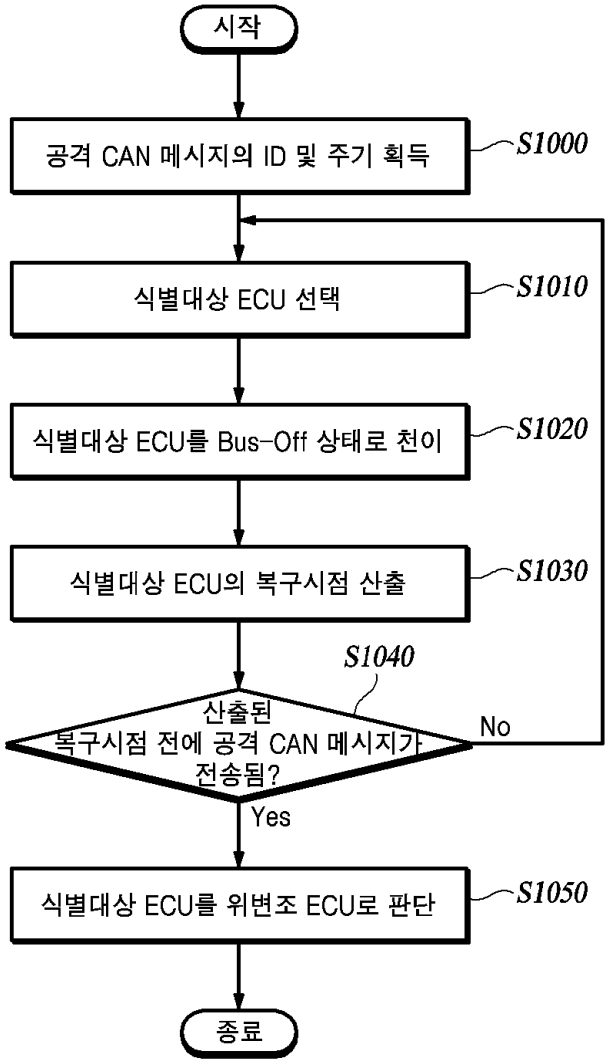
도면8


시작
일반 CAN 메시지의 ID 및 주기 획득
S800
분석대상 ECU를 Bus-Off 상태로 천이
S810
일반 CAN 메시지 수신
S820
복구 파라미터 분석
S830
복구 파라미터 저장
S840
종료

도면9


시작
공격 CAN 메시지의 ID 및 주기 획득
S900
식별대상 ECU 선택
S910
식별대상 ECU를 Bus-Off 상태로 천이
S920
공격 CAN 메시지 재전송시점 산출
S930
S940
산출된 재전송시점에 공격 CAN 메시지가 전송됨?
No
Yes
식별대상 ECU를 위변조 ECU로 판단
S950
종료

도면10


시작
공격 CAN 메시지의 ID 및 주기 획득
S1000
식별대상 ECU 선택
S1010
식별대상 ECU를 Bus-Off 상태로 천이
S1020
식별대상 ECU의 복구시점 산출
S1030
S1040
산출된 복구시점 전에 공격 CAN 메시지가 전송됨?
No
Yes
식별대상 ECU를 위변조 ECU로 판단
S1050
종료