



(19) 대한민국특허청(KR)

(12) 등록특허공보(B1)

(45) 공고일자 2015년12월11일

(11) 등록번호 10-1572935

(24) 등록일자 2015년11월24일

(51) 국제특허분류(Int. Cl.)

H04L 9/32 (2006.01) *H04L 12/58* (2006.01)

(21) 출원번호 10-2014-0133321

(22) 출원일자 2014년10월02일

심사청구일자 2014년10월02일

(56) 선행기술조사문헌

KR1020050064343 A

KR1020080093635 A

KR1020090085639 A

KR1020140023799 A

(73) 특허권자

현대자동차주식회사

서울특별시 서초구 현릉로 12 (양재동)

기아자동차주식회사

서울특별시 서초구 현릉로 12 (양재동)

(뒷면에 계속)

(72) 발명자

이병욱

서울특별시 양천구 오목로17길 7, 101동 303호(신월동, 동도 센트리움 아파트)

이정희

서울특별시 관악구 양지7길 38, 3층 (신림동)

(뒷면에 계속)

(74) 대리인

박영복

전체 청구항 수 : 총 32 항

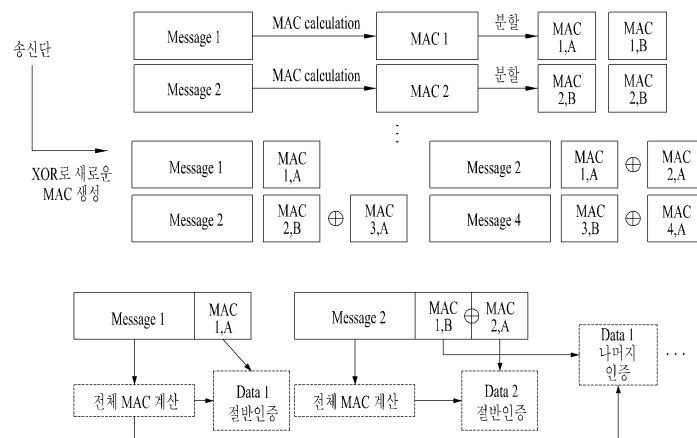
심사관 : 양종필

(54) 발명의 명칭 메시지 인증 코드 혼합을 통한 CAN 패킷 인증 방법 및 그 장치

(57) 요약

본 발명은 CAN 네트워크에서 패킷을 인증하는 방법에 관한 것으로, 보다 상세히는 분할 및 혼합된 메시지 인증 코드를 이용한 효율적인 인증 방법 및 이를 위한 장치에 관한 것이다. 본 발명의 일 실시예에 따른 CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 방법은 제 1 메시지를 이용하여 제 1 MAC을 생성하는 단계; 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하는 단계; 제 2 메시지를 이용하여 제 2 MAC을 생성하는 단계; 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하는 단계; 상기 제 2 부분 MAC 및 상기 제 3 부분 MAC을 선형연산하여 제 1 인증 MAC을 생성하는 단계; 상기 제 1 메시지를 상기 제 1 부분 MAC과 함께 전송하는 단계; 및 상기 제 2 메시지를 상기 제 1 인증 MAC과 함께 전송하는 단계를 포함할 수 있다.

대표도 - 도3



(73) 특허권자

조선대학교산학협력단

광주광역시 동구 필문대로 309 (서석동)

서울대학교산학협력단

서울특별시 관악구 관악로 1 (신림동)

(72) 발명자

류호

경기도 수원시 영통구 매영로310번길 27, 642동
1501호 (영통동, 신원아파트)

정호진

서울특별시 금천구 시흥대로 165, 210동 904호(시
흥동, 남서울힐스테이트아파트)

안현수

서울특별시 송파구 올림픽로35길 104, 27동 407호
(신천동, 장미아파트)

김호연

서울특별시 영등포구 국제금융로 109, A동 802호
(여의도동, 삼익아파트)

문영식

서울특별시 관악구 낙성대역길 58, 애당 403호 (봉
천동)

우준영

서울특별시 서초구 사평대로 240, 501동 101호 (반
포동, 반포미도2차아파트)

김영식

광주광역시 서구 풍암2로 36, 105동 903호 (
풍암동, 주은모아아파트)

이강석

경기도 고양시 일산서구 대화2로 68, 204동 1004호
(대화동, 대화마을2단지아파트)

노종선

서울특별시 강남구 광평로10길 15, 109동 406호 (
일원동, 상록수아파트)

명세서

청구범위

청구항 1

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 방법에 있어서,
제 1 메시지를 이용하여 제 1 MAC을 생성하는 단계;
상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하는 단계;
제 2 메시지를 이용하여 제 2 MAC을 생성하는 단계;
상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하는 단계;
상기 제 2 부분 MAC 및 상기 제 3 부분 MAC을 선형연산하여 제 1 인증 MAC을 생성하는 단계;
상기 제 1 메시지를 상기 제 1 부분 MAC과 함께 전송하는 단계; 및
상기 제 2 메시지를 상기 제 1 인증 MAC과 함께 전송하는 단계를 포함하는, 메시지 전송 방법.

청구항 2

제 1항에 있어서,
상기 각 분할하는 단계는, 상기 제 1 MAC 및 상기 제 2 MAC을 동일한 크기로 분할하도록 수행되는, 메시지 전송 방법.

청구항 3

제 2항에 있어서,
상기 제 1 부분 MAC은 상기 제 1 MAC의 앞쪽 절반에 해당하고,
상기 제 2 부분 MAC은 상기 제 1 MAC의 뒷쪽 절반에 해당하는, 메시지 전송 방법.

청구항 4

제 2항에 있어서,
상기 제 3 부분 MAC은 상기 제 2 MAC의 앞쪽 절반에 해당하고,
상기 제 4 부분 MAC은 상기 제 2 MAC의 뒷쪽 절반에 해당하는, 메시지 전송 방법.

청구항 5

제 1항에 있어서,
상기 선형 연산은,
익스클루시브 오어(XOR) 연산인, 메시지 전송 방법.

청구항 6

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 수신하는 방법에 있어서,
제 1 메시지 및 제 1 인증 MAC을 포함하는 제 1 프레임을 수신하는 단계;
상기 제 1 메시지를 이용하여 제 1 MAC을 계산하는 단계;
상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하는 단계;
상기 제 1 인증 MAC과 상기 제 1 부분 MAC을 비교하여 상기 제 1 메시지를 부분인증하는 단계;

제 2 메시지 및 제 2 인증 MAC을 포함하는 제 2 프레임을 수신하는 단계;

상기 제 2 메시지를 이용하여 제 2 MAC을 계산하는 단계;

상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하는 단계;

상기 제 2 부분 MAC과 상기 제 2 인증 MAC을 선형연산하여 상기 제 3 부분 MAC을 계산하는 단계; 및

상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교하여 상기 제 2 메시지를 부분인증하는 단계를 포함하는, 메시지 수신 방법.

청구항 7

제 6항에 있어서,

상기 제 2 인증 MAC과 상기 분할된 제 3부분 MAC을 선형연산하여 상기 제 2 부분 MAC을 계산하는 단계; 및

상기 계산된 제 2 부분 MAC과 상기 분할된 제 2 부분 MAC을 비교하여 상기 제 1 메시지를 최종 인증하는 단계를 더 포함하는, 메시지 수신 방법.

청구항 8

제 6항에 있어서,

상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교한 결과, 일치하는 경우 상기 제 1 메시지도 최종 인증된 것으로 판단하는 단계를 더 포함하는, 메시지 수신 방법.

청구항 9

제 6항에 있어서,

상기 각 분할하는 단계는, 상기 제 1 MAC 및 상기 제 2 MAC을 동일한 크기로 분할하도록 수행되는, 메시지 수신 방법.

청구항 10

제 7항에 있어서,

상기 제 1 부분 MAC은 상기 제 1 MAC의 앞쪽 절반에 해당하고,

상기 제 2 부분 MAC은 상기 제 1 MAC의 뒷쪽 절반에 해당하는, 메시지 수신 방법.

청구항 11

제 7항에 있어서,

상기 제 3 부분 MAC은 상기 제 2 MAC의 앞쪽 절반에 해당하고,

상기 제 4 부분 MAC은 상기 제 2 MAC의 뒷쪽 절반에 해당하는, 메시지 수신 방법.

청구항 12

제 6항에 있어서,

상기 선형 연산은,

익스클루시브 오어(XOR) 연산인, 메시지 수신 방법.

청구항 13

제 6항에 있어서,

상기 각 부분 인증하는 단계의 결과를 기 설정된 판정 규칙과 비교하여 오류가 발생한 프레임을 판단하는 단계를 더 포함하는, 메시지 수신 방법.

청구항 14

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 제어기에 있어서,

제 1 메시지 및 제 2 메시지를 생성하는 메시지 관리 모듈;

상기 제 1 메시지를 이용하여 제 1 MAC을 생성하고, 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하며, 제 2 메시지를 이용하여 제 2 MAC을 생성하고, 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하며, 상기 제 2 부분 MAC 및 상기 제 3 부분 MAC을 선형연산하여 제 1 인증 MAC을 생성하는 인증 모듈; 및

상기 제 1 메시지를 상기 제 1 부분 MAC과 함께 전송하고, 상기 제 2 메시지를 상기 제 1 인증 MAC과 함께 전송하는 송수신 모듈을 포함하는, 제어기.

청구항 15

제 14항에 있어서,

상기 인증 모듈은,

상기 각 부분 MAC이 동일한 크기를 갖도록 분할하는, 제어기.

청구항 16

제 15항에 있어서,

상기 제 1 부분 MAC은 상기 제 1 MAC의 앞쪽 절반에 해당하고,

상기 제 2 부분 MAC은 상기 제 1 MAC의 뒷쪽 절반에 해당하는, 제어기.

청구항 17

제 15항에 있어서,

상기 제 3 부분 MAC은 상기 제 2 MAC의 앞쪽 절반에 해당하고,

상기 제 4 부분 MAC은 상기 제 2 MAC의 뒷쪽 절반에 해당하는, 제어기.

청구항 18

제 14항에 있어서,

상기 선형 연산은,

익스클루시브 오어(XOR) 연산인, 제어기.

청구항 19

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 수신하는 제어기에 있어서,

제 1 메시지 및 제 1 인증 MAC을 포함하는 제 1 프레임과, 제 2 메시지 및 제 2 인증 MAC을 포함하는 제 2 프레임을 수신하는 송수신 모듈; 및

상기 제 1 메시지를 이용하여 제 1 MAC을 계산하고, 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하며, 상기 제 1 인증 MAC과 상기 제 1 부분 MAC을 비교하여 상기 제 1 메시지를 부분인증하고,

상기 제 2 메시지를 이용하여 제 2 MAC을 계산하고, 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하며, 상기 제 2 부분 MAC과 상기 제 2 인증 MAC을 선형연산하여 상기 제 3 부분 MAC을 계산하여 상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교하여 상기 제 2 메시지를 부분인증하는 인증 모듈을 포함하는, 제어기.

청구항 20

제 19항에 있어서,

상기 인증 모듈은,

상기 제 2 인증 MAC과 상기 분할된 제 3부분 MAC을 선형연산하여 상기 제 2 부분 MAC을 계산하고, 상기 계산된 제 2 부분 MAC과 상기 분할된 제 2 부분 MAC을 비교하여 상기 제 1 메시지를 최종 인증하는, 제어기.

청구항 21

제 19항에 있어서,

상기 인증 모듈은,

상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교한 결과, 일치하는 경우 상기 제 1 메시지도 최종 인증된 것으로 판단하는, 제어기.

청구항 22

제 19항에 있어서,

상기 인증 모듈은,

상기 각 부분 MAC이 동일한 크기를 갖도록 분할하는, 제어기.

청구항 23

제 20항에 있어서,

상기 제 1 부분 MAC은 상기 제 1 MAC의 앞쪽 절반에 해당하고,

상기 제 2 부분 MAC은 상기 제 1 MAC의 뒷쪽 절반에 해당하는, 제어기.

청구항 24

제 20항에 있어서,

상기 제 3 부분 MAC은 상기 제 2 MAC의 앞쪽 절반에 해당하고,

상기 제 4 부분 MAC은 상기 제 2 MAC의 뒷쪽 절반에 해당하는, 제어기.

청구항 25

제 19항에 있어서,

상기 선형 연산은,

익스클루시브 오어(XOR) 연산인, 제어기.

청구항 26

제 19항에 있어서,

상기 인증 모듈은,

상기 각 부분 인증의 결과를 기 설정된 판정 규칙과 비교하여 오류가 발생한 프레임을 판단하는, 제어기.

청구항 27

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 방법에 있어서,

메시지를 이용하여 MAC을 생성하는 단계;

상기 메시지의 이전 메시지를 이용하여 생성된 MAC의 뒷쪽 절반과, 상기 메시지를 이용하여 생성된 MAC의 앞쪽 절반을 선형 연산하는 단계;

상기 선형 연산의 결과를 상기 메시지와 함께 전송하는 단계를 포함하는, 메시지 전송 방법.

청구항 28

제 27항에 있어서,

상기 이전 메시지가 첫 메시지인 경우,

상기 이전 메시지는, 상기 이전 메시지를 이용하여 생성된 MAC의 앞쪽 절반과 함께 전송되는, 메시지 전송 방법.

청구항 29

제 27항에 있어서,

상기 선형 연산은,

익스클루시브 오어(XOR) 연산인, 메시지 전송 방법.

청구항 30

CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 수신하는 방법에 있어서,

메시지 및 인증 MAC을 포함하는 프레임을 수신하는 단계;

상기 메시지를 이용하여 MAC을 계산하는 단계;

이전 수신된 프레임에 포함된 메시지를 이용하여 계산된 MAC의 뒷쪽 절반과 상기 인증 MAC을 선형연산하는 단계;

상기 선형연산의 결과와 상기 메시지를 이용하여 계산된 MAC의 앞쪽 절반을 비교하여 상기 메시지를 부분 인증하는 단계;

다음 프레임을 수신하는 단계;

상기 다음 프레임에 포함된 메시지를 이용하여 다음 MAC을 계산하는 단계;

상기 메시지를 이용하여 계산된 MAC의 뒷쪽 절반과 상기 다음 프레임에 포함된 인증 MAC을 선형연산하는 단계; 및

상기 선형연산의 결과와 상기 다음 MAC의 앞쪽 절반을 비교하여 상기 메시지를 최종 인증하는 단계를 더 포함하는, 메시지 수신 방법.

청구항 31

제 30항에 있어서,

상기 이전 수신된 프레임에 포함된 메시지가 첫 메시지인 경우,

상기 이전 수신된 프레임에 포함된 인증 MAC과 상기 이전 수신된 프레임에 포함된 메시지를 이용하여 계산된 MAC의 앞쪽 절반을 비교하여 상기 이전 수신된 프레임에 포함된 메시지를 부분 인증하는 단계를 더 포함하는, 메시지 수신 방법.

청구항 32

제 30항에 있어서,

상기 선형 연산은,

익스클루시브 오어(XOR) 연산인, 메시지 수신 방법.

발명의 설명

기술 분야

[0001]

본 발명은 CAN 네트워크에서 패킷을 인증하는 방법에 관한 것으로, 보다 상세히는 분할 및 혼합된 메시지 인증 코드를 이용한 효율적인 인증 방법 및 이를 위한 장치에 관한 것이다.

배경 기술

[0002]

차량에서는 일반적으로 제어 영역 네트워크(CAN: Controller Area Network) 방식으로 각 제어기간 데이터 패킷

교환이 수행된다. 현재 출시되는 차량의 경우 최근까지도 차량의 내부는 외부 네트워크와 독립적으로 운영되기 때문에 차량의 내부의 네트워크 정보에 대한 보호 수단이 전혀 마련되어 있지 않다. 따라서 브로드 캐스팅 방식을 사용하는 차량용 CAN 네트워크의 특성상 차량 진단을 위한 연결 포트를 통해 차량 운행에 관한 정보를 탈취하거나 악의적인 CAN 패킷을 주입하여도 이를 인증 할 수 있는 보안 기술이 마련되어 있지 않은 상황이다.

[0003] CAN 패킷 내의 메시지의 보안을 위해 메시지 인증 코드(MAC: Message Authentication Code) 인증 방식이 고려될 수 있다. 여기서 MAC이란, 메시지의 인증에 쓰이는 비교적 작은 크기의 정보를 의미한다. 이를 도 1을 참조하여 설명한다.

[0004] 도 1은 MAC 인증 방식을 설명하기 위한 도면이다.

[0005] 도 1에서는 송신단(110)에서 수신단(120)으로 메시지(131)가 전송되는 경우를 가정한다. 이때, 송신단과 수신단에는 미리 비밀키(Key (K), 141)와 MAC 생성을 위한 알고리즘(즉, MAC 알고리즘, 151)이 공유된다. 송신단(110)에서는 비밀키(141)와 메시지(131)로 MAC 알고리즘(151)을 거쳐 MAC(161)을 생성하고, 이를 메시지(131)와 함께 수신단(120)으로 전송한다. 수신단(120)에서는 수신된 메시지와 미리 공유된 비밀키로 MAC 알고리즘(151')을 통해 MAC(161')을 계산하고, 계산된 MAC(161')이 수신된 MAC(161)과 동일한지 여부를 비교하여 메시지의 무결성을 검증할 수 있다.

[0006] CAN 망에서 보안을 위해 이러한 MAC 인증 방식을 도입할 때의 가장 큰 문제점으로, CAN 프레임에 인증을 위한 MAC 데이터가 삽입될 수 있는 공간이 부족함을 들 수 있다. 보다 상세히, CAN 프레임에서 사용 가능한 데이터는 최대 64비트이나, 일반적인 MAC 데이터가 프레임에 삽입될 경우, 해당 프레임에서 삽입될 수 있는 순수 CAN 데이터의 크기가 절반 이하로 감소하는 문제점이 발생한다. 뿐만 아니라, 차량의 브레이크나 에어백 등의 지연 시간에 민감한 전자 장비에는 MAC 인증 방식이 지연 시간의 문제로 적용되기 어렵다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 차량용 CAN 네트워크에서 보다 효율적인 MAC 인증 방법 및 그를 위한 장치를 제공하기 위한 것이다.

[0008] 특히, 본 발명은 비교적 적은 용량의 MAC 데이터로 인증이 가능한 방법 및 그를 위한 장치를 제공하기 위한 것이다.

[0009] 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 상기와 같은 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 방법은 제 1 메시지를 이용하여 제 1 MAC을 생성하는 단계; 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하는 단계; 제 2 메시지를 이용하여 제 2 MAC을 생성하는 단계; 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하는 단계; 상기 제 2 부분 MAC 및 상기 제 3 부분 MAC을 선형연산하여 제 1 인증 MAC을 생성하는 단계; 상기 제 1 메시지를 상기 제 1 부분 MAC과 함께 전송하는 단계; 및 상기 제 2 메시지를 상기 제 1 인증 MAC과 함께 전송하는 단계를 포함할 수 있다.

[0011] 또한, 본 발명의 일 실시예에 따른 CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 전송하는 제어기는 제 1 메시지 및 제 2 메시지를 생성하는 메시지 관리 모듈; 상기 제 1 메시지를 이용하여 제 1 MAC을 생성하고, 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하며, 제 2 메시지를 이용하여 제 2 MAC을 생성하고, 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하며, 상기 제 2 부분 MAC 및 상기 제 3 부분 MAC을 선형연산하여 제 1 인증 MAC을 생성하는 인증 모듈; 및 상기 제 1 메시지를 상기 제 1 부분 MAC과 함께 전송하고, 상기 제 2 메시지를 상기 제 1 인증 MAC과 함께 전송하는 송수신 모듈을 포함할 수 있다.

[0012] 또한, 본 발명의 일 실시예에 따른 CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 수신하는 방법은 제 1 메시지 및 제 1 인증 MAC을 포함하는 제 1 프레임을 수신하는 단계; 상기 제 1 메시지를 이용하여 제 1 MAC을 계산하는 단계; 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하는 단계; 상기 제 1 인증 MAC과 상기 제 1 부분 MAC을 비교하여 상기 제 1 메시지를 부분인증하는 단계; 제 2 메시지 및 제 2 인증

MAC을 포함하는 제 2 프레임을 수신하는 단계; 상기 제 2 메시지를 이용하여 제 2 MAC을 계산하는 단계; 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하는 단계; 상기 제 2 부분 MAC과 상기 제 2 인증 MAC을 선형연산하여 상기 제 3 부분 MAC을 계산하는 단계; 및 상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교하여 상기 제 2 메시지를 부분인증하는 단계를 포함할 수 있다.

[0013] 아울러, 본 발명의 일 실시예에 따른 CAN 네트워크에서 메시지를 혼합 메시지 인증 코드(MAC)를 이용하여 수신하는 제어기는 제 1 메시지 및 제 1 인증 MAC을 포함하는 제 1 프레임과, 제 2 메시지 및 제 2 인증 MAC을 포함하는 제 2 프레임을 수신하는 송수신 모듈; 및 상기 제 1 메시지를 이용하여 제 1 MAC을 계산하고, 상기 제 1 MAC을 제 1 부분 MAC 및 제 2 부분 MAC으로 분할하며, 상기 제 1 인증 MAC과 상기 제 1 부분 MAC을 비교하여 상기 제 1 메시지를 부분인증하고, 상기 제 2 메시지를 이용하여 제 2 MAC을 계산하고, 상기 제 2 MAC을 제 3 부분 MAC 및 제 4 부분 MAC으로 분할하며, 상기 제 2 부분 MAC과 상기 제 2 인증 MAC을 선형연산하여 상기 제 3 부분 MAC을 계산하여 상기 분할된 제 3 부분 MAC과 상기 계산된 제 3 부분 MAC을 비교하여 상기 제 2 메시지를 부분인증하는 인증 모듈을 포함할 수 있다.

발명의 효과

[0014] 상기와 같이 구성되는 본 발명의 적어도 하나의 실시예에 관련된 인증 방법을 통해 차량용 CAN 네트워크에서 효율적인 인증이 수행될 수 있다.

[0015] 특히, MAC이 분할 및 혼합되어 전송되기 때문에 비교적 적은 크기의 MAC 데이터로 인증이 가능하다.

[0016] 아울러, 분할된 MAC 간의 배타적 연산이 수행되어 전송되므로 수신단에서 연산을 통한 인증이 수행됨에 따라 전체 MAC을 전송하는 것과 유사한 효과를 얻을 수 있다.

[0017] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0018] 도 1은 MAC 인증 방식을 설명하기 위한 도면이다.

도 2는 일반적인 MAC 인증 방식이 적용될 때 지연 시간이 발생하는 형태의 일례를 나타낸다.

도 3은 본 발명의 일 실시예에 따른 분할 MAC 데이터의 혼합을 이용한 순차적 인증 방법의 일례를 나타낸다.

도 4는 수신단에서 수신된 두 개의 메시지의 인증 성공 여부의 일례를 나타낸다.

도 5는 본 발명의 일 실시예에 따른 혼합 MAC 인증을 수행할 수 있는 장치 구조의 일례를 나타내는 블록 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 본 발명과 관련된 CAN 메시지의 인증 방법에 대하여 도면을 참조하여 보다 상세하게 설명한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0020] 일반적으로, MAC 인증 방식이 차량의 CAN 망에 적용되는 경우, CAN 데이터를 먼저 전송하고, 해당 데이터에 대한 MAC 데이터를 나중에 전송하도록 할 수 있다. 이러한 경우, 수신단에서 먼저 수신된 CAN 데이터에 대한 MAC 데이터가 수신될 때까지 CAN 데이터에 대한 인증이 수행될 수 없기 때문에 지연시간이 발생하게 된다. 이를 도 2를 참조하여 보다 상세히 설명한다.

[0021] 도 2는 일반적인 MAC 인증 방식이 적용될 때 지연 시간이 발생하는 형태의 일례를 나타낸다.

[0022] 도 2를 참조하면 메시지들(즉, 페이로드, 231 및 232)이 송신단(210)에서 수신단(220)으로 전송될 때, 각 메시지들은 서로 다른 CAN 프레임을 통해 전송된다. 이후, 전송된 메시지들(231, 232)에 대한 MAC 데이터가 둘(241, 242)로 분할되어 서로 다른 프레임에 포함되어 전송된다. 수신단(220)에서는 먼저 수신된 2개의 CAN 프레임들을 통해 메시지들을 수신할 수는 있으나, 분할된 MAC들을 포함하는 나머지 CAN프레임들이 수신될 때까지는 메시지들을 검증할 수 없기 때문에 첫 번째 프레임을 통해 메시지가 수신될 때부터 3 프레임에 해당하는 레이턴시가

발생하게 된다.

[0023] 정리하면, 인증을 위한 MAC 데이터는 실제 전송을 희망하는 메시지와 함께 전송되는 것이 아니라 사후에 별도로 전송된다. 따라서, 즉시 인증 확인이 이루어지지 않으므로 레이턴시에 민감한 중요 데이터에 대한 인증 용도로 사용하기 어려운 문제점이 있다. 뿐만 아니라, 분할된 MAC 데이터 중 한 쪽이라도 손상/손실되었을 경우, 전체 MAC 데이터를 사용할 수 없는 문제점이 있다.

[0024] 상술한 문제점을 보완하기 위하여, 본 발명의 일 실시예에서는 송신단에서 MAC을 분할하여 CAN 프레임 내에서 MAC을 위한 공간을 줄이고, 더불어 분할된 MAC들 간에 선형 연산(linear operation)을 수행함으로써 분할된 MAC을 혼합하여 새로운 MAC을 만들어 전송할 것을 제안한다. 이를 통해 수신측에서는 송신측에서 사용한 선형 연산의 특성에 따라 분할 MAC 간의 관계를 이용하여 좀 더 효율적으로 인증을 수행할 수 있다.

[0025] 도 3은 본 발명의 일 실시예에 따른 분할 MAC 데이터의 혼합을 이용한 순차적 인증 방법의 일례를 나타낸다.

[0026] 도 3을 참조하면, 송신단에서는 메시지 1과 메시지 2를 이용하여 MAC 1 및 MAC 2를 각각 생성한다. MAC 1은 다시 MAC(1,A) 및 MAC(1,B)로 분할되고, MAC 2는 MAC(2,A) 및 MAC(2,B)로 분할된다. 여기서 각 분할 MAC의 크기는 동일한 것(즉, 메시지를 이용하여 생성된 MAC의 절반)이 바람직하다. 첫 번째 프레임에는 메시지 1과 그에 대한 인증용 MAC 데이터로 MAC(1,A)가 포함되고, 두 번째 프레임부터는 이전 프레임에 포함되는 메시지를 이용해 생성된 MAC의 분할 MAC들 중 이전 프레임에 포함되지 않은 분할 MAC(즉, 뒷 분할 MAC)과, 해당 프레임에 포함되는 메시지를 이용해 생성된 MAC의 분할 MAC들 중 첫 분할 MAC을 선형연산(여기서는 XOR)한 결과가 MAC 데이터로 포함된다. 예를 들어, 두 번째 프레임에는 메시지 2에 대한 MAC 데이터로 MAC(1,B)와 MAC(2,A)를 선형연산한 결과(즉, $MAC(1,B) \oplus MAC(2,A)$)가 포함된다.

[0027] 수신단에서는 첫 번째 프레임이 수신되면, 메시지 1을 이용하여 MAC 1을 생성하고, 그 첫 절반이 수신된 MAC(1,A)와 동일한지 여부로 메시지 1의 절반을 인증한다. 두 번째 프레임의 인증용 MAC 데이터(즉, $MAC(1,B) \oplus MAC(2,A)$)의 인증을 위해, 아래 수학식 1 및 수학식 2를 이용하여 MAC(1,B)와 MAC(2,A)가 각각 계산될 수 있다.

수학식 1

$$MAC(1,A) \oplus MAC(1,B) \oplus MAC(1,A) = MAC(1,B)$$

[0028]

수학식 2

$$MAC(1,B) \oplus MAC(2,A) \oplus MAC(1,B) = MAC(2,A)$$

[0029]

[0030] 즉, 수학식 1을 통해 MAC 1의 나머지 절반인 MAC(1,B)가 계산되고, 수학식 2를 통해 두 번째 프레임의 인증용 MAC 데이터($MAC(1,B) \oplus MAC(2,A)$)와 MAC(1,B)를 XOR하여 MAC(2,A)를 얻는다. MAC(2,A)는 메시지 2를 통해 계산된 MAC 2의 첫 절반과 비교하는 방법으로 인증이 수행될 수 있다. 물론, 이와 달리 계산된 MAC 2의 첫 절반과 계산된 MAC 1의 뒷 절반을 선형연산한 결과를 두 번째 프레임에 포함된 인증용 MAC 데이터와 비교할 수도 있다. 또는, 수학식 2를 변형하여 두 번째 프레임에 포함된 인증용 MAC 데이터와, 두 번째 메시지의 첫 절반을 XOR하여 MAC(1,B)를 얻을 수도 있다.

[0031] 따라서, 첫 프레임을 통해 메시지 1의 절반이 인증되고, 두 번째 프레임을 통해 메시지 1의 나머지 절반, 그리고 메시지 2의 절반이 인증될 수 있다.

[0032] 세 번째 이후는 두 번째와 유사하므로 명세서의 간명함을 위해 중복되는 설명은 생략하기로 한다.

[0033] 인증이 성공하는 경우 프레임에 실리는 인증용 MAC 데이터의 길이는 절반이면서도 실질적으로 두 배의 MAC 길이를 갖게 되는 장점이 생기게 된다. 즉, 절반의 용량으로 보안(즉, MAC의 길이)은 두 배로 향상된다.

- [0034] 다음으로, 본 발명의 일 실시예에 따른 분할된 MAC이 혼합되어 전송되는 두 프레임에서 적어도 일부의 인증이 실패한 경우 오류 판정 방법을 설명한다.
- [0035] 도 4는 수신단에서 수신된 두 개의 메시지의 인증 성공 여부의 일례를 나타낸다.
- [0036] 인증이 실패할 경우에는 확률에 따른 판정 규칙을 적용하여 인증 성공과 인증 실패가 결정될 수 있다. 예를 들어, 도 4와 같이 첫 번째 프레임의 인증은 성공했으나, 두 번째 프레임의 MAC 인증이 실패할 경우를 생각해 보자. 이러한 경우, MAC 1의 성분인 MAC(1,B)에 오류가 있을 수도 있고 MAC 2의 성분인 MAC(2,A)에 오류가 있을 수도 있다. 그런데, MAC 1의 절반, 즉, MAC(1,A)가 인증을 통과했다는 것은 첫 번째 MAC의 나머지 절반인 MAC(1,B)가 틀릴 가능성이 확률적으로 매우 낮다고 할 수 있다. 따라서 MAC(2,A)가 잘못되었다고 판정이 가능하다.
- [0037] 판정 규칙은 MAC 알고리즘의 특성에 기인할 수 있다. MAC 알고리즘은 입력에 따라 매우 랜덤한 메시지 인증 코드를 만들게 되는데, 앞 절반은 유지되면서 뒤 절반은 틀리게 되는 경우는 MAC 알고리즘 자체의 보안성에 문제가 있다는 의미가 된다. 이와 같이 여러 다른 상황에 대해서도 MAC 알고리즘의 특성을 고려하여 판정 규칙이 정의될 수 있다.
- [0038] 이하, 본 실시예에 따른 판정 규칙을 보다 상세히 설명한다.
- [0039] 전술한 바와 같이, MAC 알고리즘은 입력에 대해서 랜덤한 출력을 생성하게 되는데, 이 경우 입력이 한 비트라도 달라지면 랜덤한 위치의 절반 정도의 비트가 값이 바뀌게 된다. 따라서 MAC 크기를 b비트라 할 때, 입력에 한 비트 이상의 오류가 있는 경우, 평균 b/2비트에 오류가 발생한다. 그런데, 본 발명에 따르면 하나의 프레임에서 오류가 발생하면 이 프레임은 그 이후에 전달되는 다른 프레임의 인증용 MAC 데이터에도 영향을 준다.
- [0040] 0을 인증 성공(success) 1을 인증 실패(failure)라 하면, 일반적으로 연속된 첫 네 개의 프레임에 대해서 일반적으로 다음과 같은 형태의 오류가 주로 발생할 수 있다.
- [0041] 먼저, 인증 성공의 경우는 "0000..."이 된다.
- [0042] 다음으로, 연속된 두 개 이상의 프레임에 인증 실패가 발생한 경우는 아래와 같다.
- [0043] 1100...: 첫 번째 프레임 인증 실패
- [0044] 0110...: 두 번째 프레임 인증 실패
- [0045] 0011...: 세 번째 프레임 인증 실패
- [0046] 1110...: 첫 번째, 두 번째 프레임 인증 실패
- [0047] 0111...: 두 번째, 세 번째 프레임 인증 실패
- [0048] 1111...: 첫 번째, 두 번째, 세 번째 프레임 인증 실패
- [0049] 위의 결과에서와 같이, 궁극적으로는 어느 하나라도 인증이 실패하면 해당 구간에서의 인증이 실패하게 된다.
- [0050] 따라서, 특정 프레임 자체의 인증 여부보다 인증 실패 자체가 차량의 내부 통신망의 문제 혹은 공격자의 공격 등의 가능성이 높음을 의미하므로 어떤 패턴이든 인증 오류가 발생하게 되면, 수신단에 해당하는 제어기는 내부 시스템에 경고를 보낼 수가 있다.
- [0051] 한편, 예외적으로 1/2b의 낮은 확률로 다음과 같은 형태의 인증 실패가 발생할 수 있다.
- [0052] 0100: 첫 번째 혹은 두 번째 프레임의 인증 실패 (1/2b 확률)
- [0053] 0010: 두 번째 혹은 세 번째 프레임의 인증 실패 (1/2b 확률)
- [0054] 1011: 첫 번째 프레임의 인증 실패 (1/2b 확률) 후 세 번째 프레임의 인증 실패
- [0055] 0001...: 다섯 번째 프레임의 인증 결과에 따라 달라짐. 00011인 경우는 네 번째 프레임의 인증 실패, 00010인 경우는 1/2b의 확률로 세 번째 혹은 네 번째 프레임의 인증 실패
- [0056] 1101: 첫 번째 프레임의 인증 실패 후 다섯 번째 프레임의 인증 결과에 따라 달라짐. 11011인 경우는 추가로 네 번째 프레임의 인증 실패, 11010인 경우는 1/2b의 확률로 추가로 세 번째 혹은 네 번째 프레임의 인증 실패
- [0057] 상술한 바와 같은 분할 MAC의 혼합을 통한 인증 방법으로 CAN 프레임의 적은 영역만 인증을 위한 용도로 사용하

게 된다. 따라서, 한 프레임에 포함되는 인증용 MAC 데이터의 크기는 절반이나 수신단에서 연산을 통해 인증을 하여 실제로 전체 MAC을 전송하는 것과 같은 효과를 얻을 수 있다. 또한, 본 발명에 따른 인증 방식은 도 2와 같은 단순 분할 MAC 방식과 달리 모든 프레임에 대해서 동일한 수준의 인증을 제공한다.

[0058] 다음으로, 도 5를 참조하여 상술한 시간 동기화 방법을 수행할 수 있는 장치 구조를 설명한다. 도 5는 본 발명의 일 실시예에 따른 혼합 MAC 인증을 수행할 수 있는 장치 구조의 일례를 나타내는 블록 구성도이다.

[0059] 상술한 분할 MAC 인증 기법은 CAN 제어기(500)에서 수행될 수 있다. 물론, 네트워크 상의 모든 CAN 제어기에서 본 인증 기법이 사용될 수도 있고, 일부 CAN 제어기에서만 본 인증 기법이 사용될 수 있음은 물론이다.

[0060] 본 발명에 따른 CAN 제어기(500)는 메시지를 생성하거나 처리하는 메시지 관리 모듈(510), MAC 데이터를 생성하고 관리하여 분할 MAC 인증을 수행하는 인증 모듈(520), CAN 방식에 따른 통신을 송수신 모듈(530)을 포함할 수 있다. 물론, 도 5에 도시된 제어기는 본 발명의 수행에 반드시 필요한 요소만을 나타낸 것이어서, 필요에 따라 더 많은 구성요소가 포함될 수 있음은 물론이다.

[0061] 보다 상세히 각 구성 요소를 설명하면, 제어기(500)가 메시지를 네트워크에 전송하는 경우(즉, 송신단 역할) 메시지 관리 모듈(510)은 네트워크로 전송할 메시지를 생성한다. 인증 모듈(520)은 메시지 관리 모듈(510)에서 생성된 첫 메시지를 통해 MAC 1을 생성하고, 두 번째 메시지를 통해 MAC 2를 생성한다. 인증 모듈(520)은 다시 MAC 1의 뒷쪽 절반과 MAC 2의 앞쪽 절반을 선형 연산하여 두 번째 프레임에 포함될 인증용 MAC 데이터를 생성한다.

[0062] 송수신 모듈(530)은 첫 메시지를 MAC 1의 앞쪽 절반과 함께 첫 CAN 프레임을 통해 네트워크로 전송한다. 또한, 송수신 모듈(530)은 두 번째 메시지를 MAC 1의 뒷쪽 절반과 MAC 2의 앞쪽 절반을 선형연산한 결과와 함께 두 번째 CAN 프레임을 통해 네트워크로 전송한다. 두 번째 프레임 이후의 전송과정은 두 번째 프레임의 전송과정과 유사하므로 자세한 설명은 생략하기로 한다.

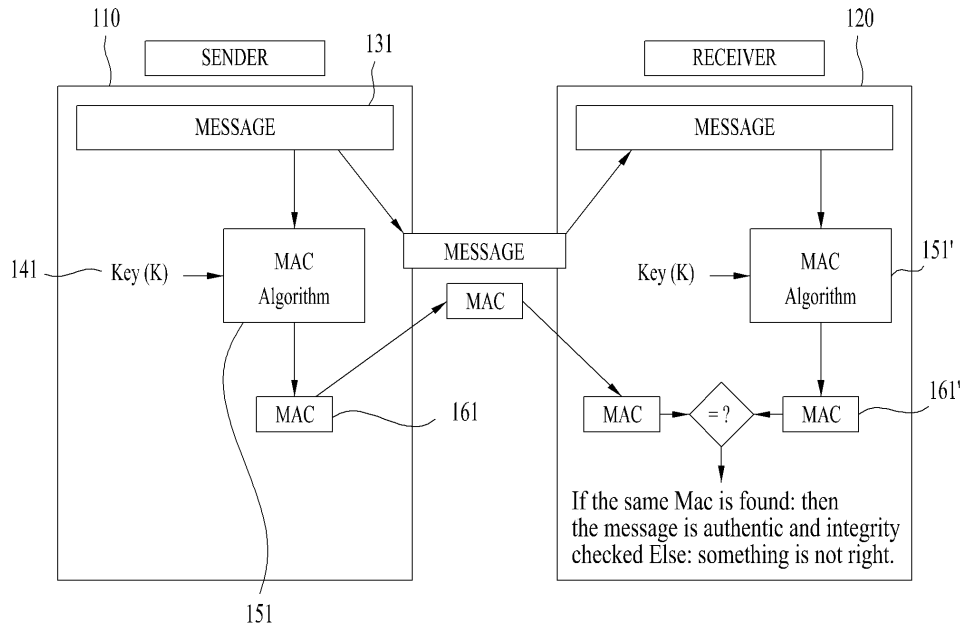
[0063] 제어기(500)가 메시지를 네트워크로부터 수신하는 경우(즉, 수신단 역할) 송수신 모듈(530)은 네트워크로부터 CAN 프레임들을 수신한다. 인증 모듈(520)은 첫 CAN 프레임을 통해 수신된 첫 메시지를 이용하여 MAC 1을 계산하고, 그의 앞쪽 절반과 첫 프레임에 포함된 인증용 MAC 데이터를 비교하여 첫 메시지의 절반을 인증한다. 이후 두 번째 프레임이 수신되면, 두 번째 메시지를 이용하여 MAC 2를 계산하고, 그 앞 절반과 앞에서 계산한 MAC 1의 뒷 절반을 선형연산하여 인증용 MAC 데이터를 인증할 수도 있다. 또는, 인증 모듈은 MAC 1의 뒷 절반을 선형 연산을 통해 계산하여 첫 메시지의 나머지 절반을 인증하고, 두 번째 프레임의 인증용 MAC 데이터와 MAC 1의 뒷 절반을 선형연산하여 MAC 2의 앞 절반을 계산하는 방법으로 두 번째 메시지의 절반을 인증할 수도 있다.

[0064] 인증이 완료된 메시지들은 메시지 관리 모듈(510)을 통해 해석되고 관리될 수 있다.

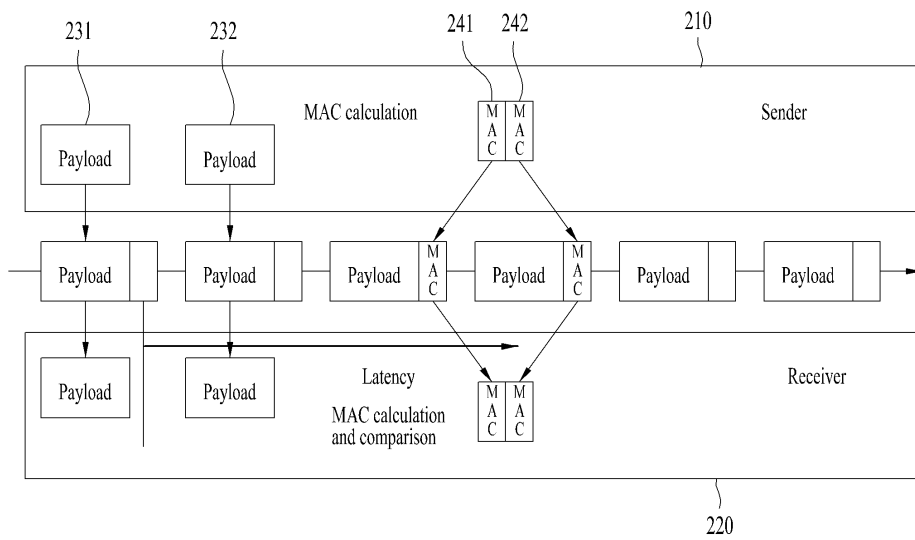
[0065] 상기와 같이 설명된 CAN 메시지 인증 방법은 상기 설명된 실시예들의 구성과 방법이 한정되게 적용될 수 있는 것이 아니라, 상기 실시예들은 다양한 변형이 이루어질 수 있도록 각 실시예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

도면

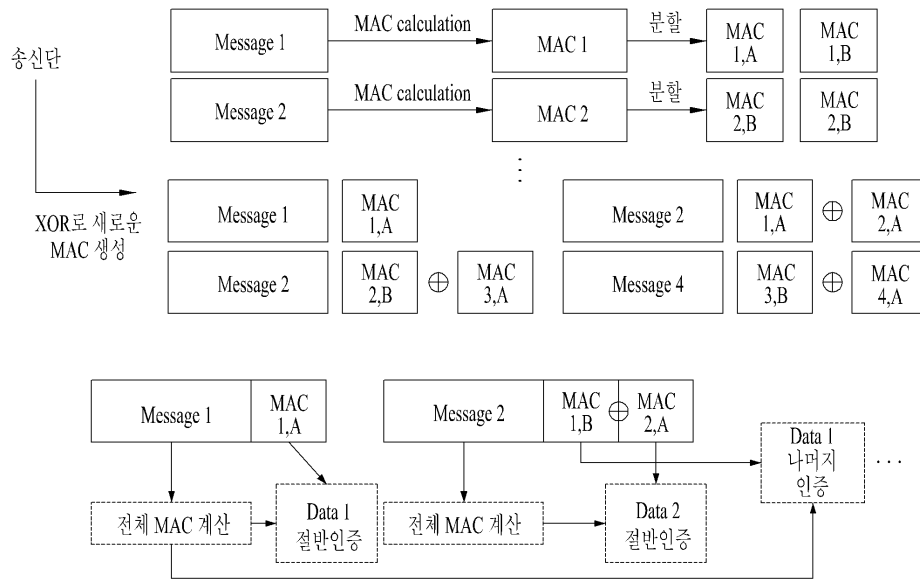
도면1



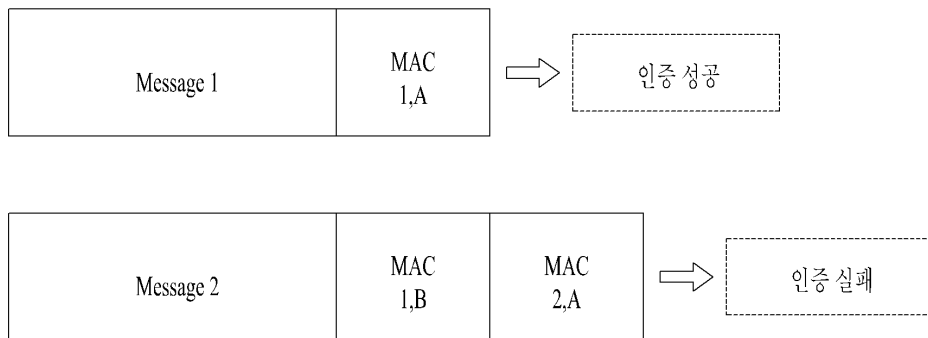
도면2



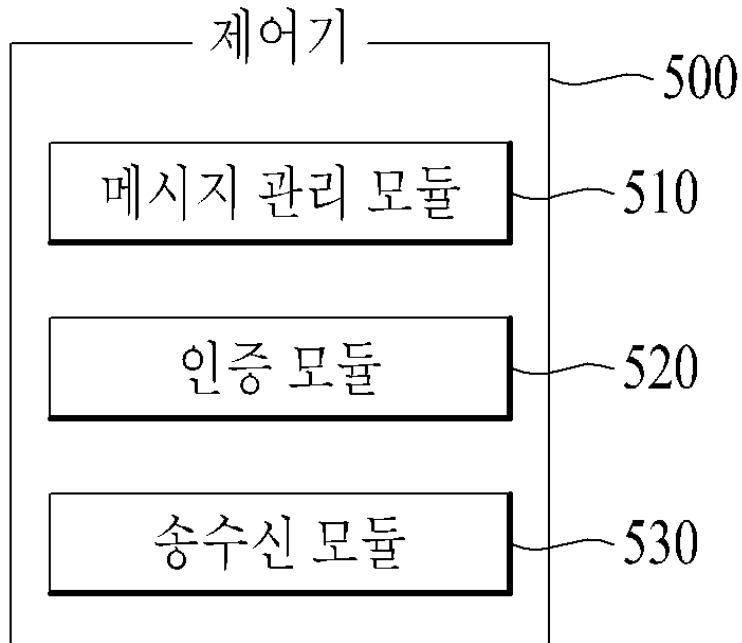
도면3



도면4



도면5



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제1항

【변경진】

"~ 단계를 포함하는, CAN 메시지 전송 방법."

【변경후】

"~ 단계를 포함하는, 메시지 전송 방법."