(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0088483
(43) 공개일자 2016년07월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 12/40* (2006.01)
(52) CPC특허분류
H04L 9/3223 (2013.01)
H04L 2012/40215 (2013.01)
(21) 출원번호 10-2015-0007411
(22) 출원일자 2015년01월15일
심사청구일자 2015년01월15일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
우사무엘
서울특별시 송파구 오금로53길 7 403호 (거여동,명산주택)
이정호
서울특별시 양천구 목동서로 70, 223동 1301호(목동, 목동2단지아파트)
이동훈
서울특별시 종로구 사직로8길 34 1404호 (내수동,경희궁의아침3단지)
(74) 대리인
김등용, 김홍석

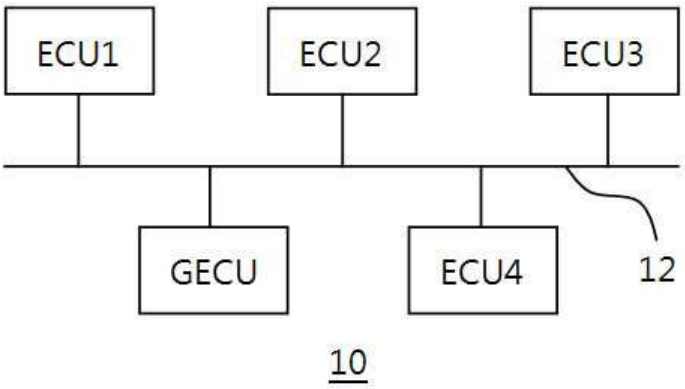
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **키 생성키 생성 방법 및 이를 이용한 데이터 프레임 인증 방법**

(57) 요 약

키 생성키 생성 방법이 개시된다. 상기 키 생성키 생성 방법은 게이트웨이 ECU(Electronic Control Unit)와 복수의 ECU들을 포함하는 통신 시스템에서의 키 생성키 생성 방법으로서, 상기 게이트웨이 ECU가 제1 질의값을 상기 복수의 ECU들 중 어느 하나의 ECU로 송신하는 단계, 상기 어느 하나의 ECU가 제2 질의값과 제1 응답값을 생성하고, 상기 제2 질의값과 상기 제1 응답값을 상기 게이트웨이 ECU로 송신하는 단계, 상기 게이트웨이 ECU가 상기 제1 응답값을 검증하고, 제2 응답값을 생성하여 생성된 상기 제2 응답값을 상기 어느 하나의 ECU로 송신하는 단계, 상기 어느 하나의 ECU가 상기 제2 응답값을 검증하는 단계, 및 상기 게이트웨이 ECU와 상기 어느 하나의 ECU 각각이 동일한 키 생성키를 생성하는 단계를 포함한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 2014-044-073-001
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송기술개발사업
연구과제명 자동차 전장 ECU간 보안전송기술 개발
기 여 율 1/1
주관기관 인포뱅크
연구기간 2014.04.01 ~ 2015.02.28

명 세 서

청구범위

청구항 1

게이트웨이 ECU(Electronic Control Unit)와 복수의 ECU들을 포함하는 통신 시스템에서의 키 생성키 생성 방법에 있어서,

상기 게이트웨이 ECU가 제1 질의값을 상기 복수의 ECU들 중 어느 하나의 ECU로 송신하는 단계;

상기 어느 하나의 ECU가 제2 질의값과 제1 응답값을 생성하고, 상기 제2 질의값과 상기 제1 응답값을 상기 게이트웨이 ECU로 송신하는 단계;

상기 게이트웨이 ECU가 상기 제1 응답값을 검증하고, 제2 응답값을 생성하여 생성된 상기 제2 응답값을 상기 어느 하나의 ECU로 송신하는 단계;

상기 어느 하나의 ECU가 상기 제2 응답값을 검증하는 단계; 및

상기 게이트웨이 ECU와 상기 어느 하나의 ECU 각각이 동일한 키 생성키를 생성하는 단계를 포함하는 키 생성키 생성 방법.

청구항 2

제1항에 있어서,

상기 통신 시스템은 CAN(Controller Area Network) 통신 시스템인, 키 생성키 생성 방법.

청구항 3

제1항에 있어서,

상기 키 생성키는 상기 제1 질의값을 입력으로 하는 키 생성함수의 결과값이고,

상기 키 생성함수는 상기 게이트웨이 ECU와 상기 복수의 ECU들이 공유하는 제2 대칭키를 키로 사용하는, 키 생성키 생성 방법.

청구항 4

제1항에 있어서,

상기 제1 질의값은 상기 게이트웨이 ECU에 의해 선택된 임의의 제1 난수이며, 상기 제2 질의값은 상기 어느 하나의 ECU에 의해 선택된 임의의 제2 난수인, 키 생성키 생성 방법.

청구항 5

제1항에 있어서,

상기 제1 응답값은 상기 게이트웨이 ECU의 ID, 상기 어느 하나의 ECU의 ID, 상기 제1 질의값, 및 상기 제2 질의값을 입력으로 하는 해쉬 함수의 결과값인, 키 생성키 생성 방법.

청구항 6

제1항에 있어서,

상기 제2 응답값은 상기 게이트웨이 ECU의 ID와 상기 제2 질의값을 입력으로 하는 해쉬 함수의 결과값인, 키 생성키 생성 방법.

청구항 7

제5항 또는 제6항에 있어서,

상기 해쉬 함수는 상기 게이트웨이 ECU와 상기 복수의 ECU들이 공유하는 제1 대칭키를 키로 사용하는 일 방향 해쉬 함수인, 키 생성키 생성 방법.

청구항 8

송신 ECU와 수신 ECU를 포함하는 통신 시스템에서의 데이터 프레임 인증 방법에 있어서,

상기 송신 ECU와 상기 수신 ECU 각각이 동일한 인증키를 생성하는 단계;

상기 송신 ECU가 메시지에 대한 데이터 프레임 인증 코드를 생성하는 단계;

상기 송신 ECU가 상기 메시지와 상기 데이터 프레임 인증 코드를 상기 수신 ECU로 송신하는 단계; 및

상기 수신 ECU가 상기 인증키를 이용하여 상기 데이터 프레임 인증 코드를 검증하는 단계를 포함하는 데이터 프레임 인증 방법.

청구항 9

제8항에 있어서,

상기 인증키는 키 생성키와 상기 송신 ECU가 상기 수신 ECU로 송신한 데이터 프레임의 송신 횟수를 입력으로 하는 키 생성 함수의 결과값이며,

상기 키 생성키는 제1항에 기재된 키 생성키 생성 방법을 통하여 상기 송신 ECU와 상기 수신 ECU에 의해 공유된, 데이터 프레임 인증 방법.

청구항 10

제8항에 있어서,

상기 통신 시스템은 CAN 통신 시스템이고,

상기 데이터 프레임 인증 코드는 CAN 데이터 프레임의 데이터 필드에 삽입되어 전송되는, 데이터 프레임 인증 방법.

청구항 11

제10항에 있어서,

상기 데이터 필드에 삽입되는 상기 데이터 프레임 인증 코드의 길이는 32 비트, 24 비트, 또는 12 비트인, 데이터 프레임 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 키 생성키 생성 방법에 관한 것으로, 특히 통신 시스템에 포함된 모든 ECU들이 동일한 키 생성키를 공유할 수 있고, 키 생성키와 일회성 인증키를 이용하여 데이터 프레임을 인증할 수 있는 키 생성키 생성 방법 및 이를 이용한 데이터 프레임 인증 방법에 관한 것이다.

배 경 기 술

[0002] 최근의 자동차들은 운전자와 승객에게 안전성과 편의성을 제공하기 위해 다양한 정보통신기술을 융합시키고 있다. 자동차에 정보통신기술을 효율적으로 융합시키기 위해서는 ECU(Electronic Control Unit)의 사용이 필수적으로 요구된다. 자동차 내부에 탑재되는 ECU는 도입 초기부터 지금까지 그 수요가 꾸준히 증가하여 최근에 개발되는 고급 자동차의 경우 약 70여개 이상의 ECU들이 자동차 내부에 탑재되고 있다. 자동차에 탑재되는 ECU들 사이의 효율적인 통신을 위하여 자동차 제조사에서는 CAN(Controller Area Network)을 사용하고 있다.

[0003] 그러나, CAN은 폐쇄적인 네트워크 환경만 고려하고 설계되어 정보보호 기능을 전혀 제공하지 않는다. 자동차에 정보통신기술의 융합이 가속화 되면서 CAN의 취약점을 이용한 각종 해킹 사례가 발표되고 있다. 이에, 정보통신기술 융합의 원활한 발전을 위해 안전한 CAN 통신 환경을 구축해야 할 필요성이 대두되고 있다.

[0004] CAN은 외부 전자파나 노이즈에 강한 장점을 갖고 있으며 이런 특성 때문에 차량 내부 네트워크 구축에 가장 큰 비중을 차지하고 있다. 하지만 보안적인 측면에서 CAN은 몇 가지 취약점을 갖고 있다. CAN은 브로드캐스트 통신 방식을 사용하기 때문에 데이터의 도청에 취약하다. 특히 최근 차량 기술의 동향은 외부 환경과의 통신을 지향하고 있기 때문에 현재의 CAN구조에서는 외부에서의 도청을 방지할 수 없다. 또한 CAN에는 도청으로 수집된 데이터에 대한 메시지 재전송공격을 방지 할 수 있는 보안 기법이 적용되어 있지 않다.

[0005] 위에 언급된 문제점을 해결하기 위해서 일반적인 IT환경에서는 메시지인증코드(Message Authentication Code; MAC)를 사용한다. 그러나 CAN 데이터 프레임 내부의 데이터 필드에는 MAC을 저장할 수 있는 가용공간이 충분하지 않다. 최근까지 발표된 대부분의 연구들은 CAN에서 MAC을 사용하기 위해 데이터 프레임 내부의 ID(identity 또는 identification)필드나 CRC(cyclical redundancy check)필드를 사용하는 방법을 제안하고 있다. 하지만 ID필드나 CRC필드는 변경 불가능한 필드이기 때문에 실제 자동차 환경에 적용할 수 없는 기법이다.

[0006] CAN 데이터 프레임의 제한적인 공간을 고려하여, 데이터와 MAC을 동시에 전송하기 위해서는 짧은 길이의 MAC을 사용해야한다. 그러나 짧은 길이의 MAC은 암호학적 안전성을 충분히 보장하지 않기 때문에 안전성을 보장하기 위한 추가적인 조치가 필요하다. 본 명세서에서는 짧은 길이의 MAC과 함께 MAC을 생성할 때 사용하는 인증키(Authentication Key)의 변경 주기를 빠르게 유지하여 암호학적 안전성을 보장하는 CAN 데이터 프레임 인증 기법을 제안한다.

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적인 과제는 시스템에 포함된 모든 ECU들이 동일한 키 생성키를 공유할 수 있고, 키 생성키와 일회성 인증키를 이용하여 데이터 프레임을 인증할 수 있는 키 생성키 생성 방법 및 이를 이용한 데이터 프레임 인증 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 본 발명의 실시 예에 따른 키 생성키 생성 방법은 게이트웨이 ECU(Electronic Control Unit)와 복수의 ECU들을 포함하는 통신 시스템에서의 키 생성키 생성 방법으로서, 상기 게이트웨이 ECU가 제1 질의값을 상기 복수의 ECU들 중 어느 하나의 ECU로 송신하는 단계, 상기 어느 하나의 ECU가 제2 질의값과 제1 응답값을 생성하고, 상기 제2 질의값과 상기 제1 응답값을 상기 게이트웨이 ECU로 송신하는 단계, 상기 게이트웨이 ECU가 상기 제1 응답값을 검증하고, 제2 응답값을 생성하여 생성된 상기 제2 응답값을 상기 어느 하나의 ECU로 송신하는 단계, 상기 어느 하나의 ECU가 상기 제2 응답값을 검증하는 단계, 및 상기 게이트웨이 ECU와 상기 어느 하나의 ECU 각각이 동일한 키 생성키를 생성하는 단계를 포함한다.

[0009] 또한, 본 발명의 실시 예에 따른 데이터 프레임 인증 방법은 송신 ECU와 수신 ECU를 포함하는 통신 시스템에서의 데이터 프레임 인증 방법으로서, 상기 송신 ECU와 상기 수신 ECU 각각이 동일한 인증키를 생성하는 단계, 상기 송신 ECU가 메시지에 대한 데이터 프레임 인증 코드를 생성하는 단계, 상기 송신 ECU가 상기 메시지와 상기 데이터 프레임 인증 코드를 상기 수신 ECU로 송신하는 단계, 및 상기 수신 ECU가 상기 인증키를 이용하여 상기 데이터 프레임 인증 코드를 검증하는 단계를 포함한다.

발명의 효과

[0010] 본 발명의 실시 예에 따른 키 생성키 생성 방법 및 데이터 프레임 인증 방법에 의하면, 메시지 재생공격 등을 이용한 해킹으로부터 통신 시스템을 보호할 수 있는 효과가 있다.

[0011] 또한, 본 발명은 일회성 인증키를 사용하여 짧은 메시지 인증 코드의 안전성을 강화할 수 있는 효과가 있다.

도면의 간단한 설명

[0012] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 의한 통신 시스템을 도시한다.

도 2는 도 1에 도시된 통신 시스템에서 키 생성키 생성 과정을 설명하기 위한 흐름도이다.

도 3은 도 1에 도시된 통신 시스템에서 데이터 프레임 인증과정을 설명하기 위한 흐름도이다.

도 4는 CAN 데이터 프레임 포맷을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0014] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0015] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0016] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[0017] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0018] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0019] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0020] 도 1은 본 발명의 일 실시 예에 의한 통신 시스템을 도시한다. 통신 시스템(10)은 차량용 통신 시스템을 의미할 수 있으며, 구체적으로는 CAN(Controller Area Network) 통신 시스템일 수 있다. 그러나, 본 발명이 통신 시스템(10)의 종류에 제한되는 것은 아니며, 실시 예에 따라 상기 통신 시스템은 CAN FD(CAN with Rlexible Data-Rate), Flexlay, LIN(Local Interconnect Network), 또는 MOST(Multimedia Oriented Systems Transport) 통신 시스템일 수도 있다.

[0021] 도 1을 참조하면, 통신 시스템(10)은 복수의 ECU(Electronic Control Unit)들과 버스(bus; 12)를 포함한다. 도 1에는 게이트웨이 ECU를 포함한 총 5 개의 ECU들만이 도시되어 있으나, 통신 시스템(10)에 포함된 ECU의 개수는 n(n은 2 이상의 자연수)일 수 있다.

[0022] 상기 복수의 ECU들은 게이트웨이 ECU(GECU), 제1 ECU(ECU1), 제2 ECU(ECU2), 제3 ECU(ECU3), 및 제4 ECU(ECU4)를 포함한다. 또한, 버스(12)는 두 개의 통신선으로 구현될 수도 있다.

[0023] 상기 복수의 ECU들 각각은 대응되는 전자 장치의 동작을 제어할 수 있으며, 버스(12)를 통하여 다른 ECU와 통신할 수 있다. 이때, 상기 복수의 ECU들 각각이 메시지를 송신하거나 수신하기 위해 송수신기를 포함할 수 있으며, 실시 예에 따라 상기 송수신기는 대응되는 ECU와 별도로 구현될 수도 있다.

[0024] 도 2는 도 1에 도시된 통신 시스템에서 키 생성키 생성 과정을 설명하기 위한 흐름도이다.

[0025] 키 생성키를 생성하기 전에 게이트웨이 ECU(GECU)를 포함한 모든 ECU들은 제1 대칭키와 제2 대칭키를 공유한다. 상기 제1 대칭키는 인증용 대칭키일 수 있으며, 상기 제2 대칭키는 키 생성용 대칭키일 수 있다. 또한, 상기 제1 대칭키와 상기 제2 대칭키는 안전한 환경에서 공유될 수 있다.

[0026] 도 2는 i 번째 세션에서 사용될 키 생성키(KGK_i)를 생성하는 과정을 게이트웨이 ECU와 제1 ECU를 중심으로 설명하고 있다. 키 생성키(KGK_i) 생성 과정은 게이트웨이 ECU(GECU)를 중심으로 모든 ECU가 순차적으로 진행한다. ECU의 ID 번호가 낮은 순서부터 순차적으로 진행될 수 있으며, 실시 예에 따라 미리 정해진 순서에 따라 진행될 수도 있다.

[0027] 키 생성키(KGK_i)는 i 번째 세션이 시작되기 전, 즉 i-1 번째 세션 중에 생성될 수 있으며, i 번째 세션에서 통신을 시작하기 전 i 번째 세션의 초기에 생성될 수도 있다. 키 생성키(KGK_i)의 생성 과정이 완료되면, 모든 ECU들은 동일한 키 생성키(KGK_i)를 공유할 수 있다. 또한, 키 생성키(KGK_i) 생성 과정에는 AKEP2(Authentication and Key Exchange Protocol Version2) 프로토콜이 이용될 수 있다.

[0028] 도 1과 도 2를 참조하면, 게이트웨이 ECU(GECU)가 제1 질의값을 생성한다(S110). 상기 제1 질의값은 임의의 난수(RA)일 수 있으며, 게이트웨이 ECU(GECU)는 임의의 난수(RA)를 선택함으로써 상기 제1 질의값을 생성할 수 있다. 또한, 게이트웨이 ECU(GECU)는 모든 ECU와 키 생성키를 생성하는 단계에서 동일한 난수(RA)를 선택함으로써, 모든 ECU가 동일한 키 생성키를 공유할 수 있도록 할 수 있다.

[0029] S120 단계에서, 게이트웨이 ECU(GECU)는 생성된 제1 질의값을 제1 ECU(ECU1)로 송신할 수 있다.

[0030] 상기 제1 질의값을 수신한 제1 ECU(ECU1)는 제2 질의값과 제1 응답값을 생성한다(S130). 제1 ECU(ECU1)는 임의의 난수(RB)를 선택함으로써 상기 제2 질의값을 생성할 수 있다. 제1 ECU(ECU1)는 아래의 수학식 1과 같이 게이트웨이 ECU(GECU)의 ID(ID_GECU), 제1 ECU(ECU1)의 ID(ID_ECU1), 제1 질의값(RA), 및 제2 질의값(RB)를 입력으로 하는 해쉬 함수(H_{SK_A}())를 연산함으로써 상기 제1 응답값을 생성할 수 있다. 이때, 해쉬 함수(H_{SK_A}())의 입력값들의 입력 순서는 실시 예에 따라 변화할 수 있으며, 상기 제1 응답값은 제1 메시지 인증 코드(MAC1)일 수 있다.

수학식 1

[0031] $$MAC1 = H_{SK_A}(ID_GECU \parallel ID_ECU1 \parallel RA \parallel RB)$$

[0032] 해쉬 함수(H_{SK_A}())는 제1 대칭키(SK_A)를 키로 사용하는 일 방향 해쉬 함수일 수 있다.

[0033] S140 단계에서, 제1 ECU(ECU1)는 생성된 제2 질의값과 제1 응답값을 게이트웨이 ECU(GECU)로 송신할 수 있다.

[0034] 상기 제2 질의값과 상기 제1 응답값을 수신한 게이트웨이 ECU(GECU)는 상기 제1 응답값을 검증하고 제2 응답값을 생성할 수 있다(S150). 상기 제1 응답값의 검증은 상기 수학식 1을 이용하여 수행될 수 있고, 상기 제2 응답값의 생성은 아래의 수학식 2를 이용하여 수행될 수 있다. 즉, 게이트웨이 ECU(GECU)는 게이트웨이 ECU(GECU)의 ID(ID_GECU)와 제2 질의값(RB)을 입력으로 하는 해쉬 함수(H_{SK_A})를 연산함으로써 제2 응답값을 생성할 수 있다. 상기 제2 응답값은 제2 메시지 인증 코드(MAC2)일 수 있다.

수학식 2

[0035] $$MAC2 = H_{SK_A}(ID_GECU \parallel RB)$$

[0036] S160 단계에서, 게이트웨이 ECU(GECU)는 상기 제2 응답값(MAC2)를 제1 ECU(ECU1)로 송신할 수 있다.

[0037] 제2 응답값(MAC2)를 수신한 제1 ECU(ECU1)는 제2 응답값(MAC2)을 검증하고, 키 생성키(KGK_i)를 생성할 수 있다(S170). 구체적으로, 제1 ECU(ECU1)은 상기 수학식 2를 이용하여 제2 응답값(MAC2)를 검증할 수 있고, 아래의 수학식 3을 이용하여 키 생성키(KGK_i)를 생성할 수 있다. 즉, 제1 ECU(ECU1)는 제2 대칭키(SK_G)를 키로 사용하는 키 생성함수(KDF_{SK_G}())에 제1 질의값(RA)을 입력으로 하여 키 생성키(KGK_i)를 생성할 수 있다.

수학식 3

[0038] $$KGK_i = KDF_{SK_G}(RA)$$

[0039] S180 단계에서, 게이트웨이 ECU(GECU)는 상기 수학식 3을 이용하여 키 생성키(KGK_i)를 생성할 수 있다.

[0040] 상기와 같은 과정을 통하여 게이트웨이 ECU(GECU)와 제1 ECU(ECU1)는 동일한 키 생성키(KGK_i)를 공유할 수 있다. 또한, 제2 ECU(ECU2), 제3 ECU(ECU3), 및 제4 ECU(ECU4) 또한 상기와 같은 과정을 통하여 동일한 키 생성키(KGK_i)를 공유할 수 있다. 다만, 키 생성키(KGK_i) 과정에서 게이트웨이 ECU(GECU)가 생성한 제1 질의값(RA)은 동일한 반면, 제2 ECU(ECU2), 제3 ECU(ECU3), 및 제4 ECU(ECU4) 각각이 생성하는 제2 질의값들은 상이할 수 있다. 또한, 각각의 검증 단계에서 검증에 실패한 경우 키 생성키의 생성 과정은 중단될 수 있다.

[0041] 도 3은 도 1에 도시된 통신 시스템에서 데이터 프레임 인증과정을 설명하기 위한 흐름도이다. 도 3은 통하여 i 번째 세션에서 j 번째 메시지를 송수신할 때의 과정을 설명하면 다음과 같다. 이때, 이용되는 데이터 프레임은 CAN 데이터 프레임일 수 있으나, 본 발명이 이에 제한되는 것은 아니다.

[0042] 송신 ECU(ECUS)와 수신 ECU(ECUR)는 키 생성키 생성 과정을 통해 i 번째 세션에서 사용할 키 생성키(KGK_i)를 공유하고 있다. 송신 ECU(ECUS)는 통신 시스템(10)에 포함된 ECU들 중 어느 하나의 ECU를 의미할 수 있으며, 수신 ECU(ECUR)는 통신 시스템(10)에 포함된 ECU들 중 다른 하나의 ECU를 의미할 수 있다. 또한, 송신 ECU(ECUS)와 수신 ECU(ECUR)는 송신 ECU(ECUS)가 i 번째 세션에서 송신한 데이터 프레임의 송신 횟수(C_i)를 관리하고 있으며, 송신 ECU(ECUS)와 수신 ECU(ECUR)가 관리하고 있는 송신 횟수(C_i)는 동기화된 값일 수 있다.

[0043] S210 단계와 S220 단계에서, 송신 ECU(ECUS)와 수신 ECU(ECUR)는 일회성 인증키(AK_ij)를 생성한다. 일회성 인증키(AK_ij)는 아래의 수학식 4를 이용하여 생성될 수 있다.

수학식 4

[0044] $$AK_ij = KDF_{SK_G}(KGK_i \,||\, C_i)$$

[0045] 즉, 송신 ECU(ECUS)와 수신 ECU(ECUR)는 제2 대칭키(SK_G)를 키로 사용하는 키 생성 함수($KDF_{SK_G}()$)에 키 생성키(KGK_i)와 송신 횟수(C_i)를 입력하여 일회성 인증키(AK_ij)를 생성할 수 있다.

[0046] S230 단계에서, 송신 ECU(ECUS)는 데이터 프레임(M_ij)를 송신하기 전에 아래의 수학식 5와 같이 데이터 프레임(M_ij)에 대한 데이터 프레임 인증 코드(MAC_ij)를 생성한다.

수학식 5

[0047] $$MAC_ij = H_{AK_ij}(M_ij)$$

[0048] 즉, 송신 ECU(ECUS)는 일회성 인증키(AK_ij)를 키로 사용하는 일방향 해쉬 함수($H_{AK_ij}()$)에 데이터 프레임(M_ij)를 입력함으로써 데이터 프레임 인증 코드(MAC_ij)를 생성할 수 있다.

[0049] S240 단계에서, 송신 ECU(ECUS)는 데이터 프레임(M_ij)을 데이터 프레임 인증 코드(MAC_ij)와 함께 수신 ECU(ECUR)로 송신한다.

[0050] 데이터 프레임(M_ij)과 데이터 프레임 인증 코드(MAC_ij)를 수신한 수신 ECU(ECUR)는 상기 수학식 5를 이용하여 데이터 프레임(M_ij)에 대한 데이터 프레임 인증 코드(MAC_ij)를 검증한다(S250).

[0051] 데이터 프레임(M_ij)과 데이터 프레임 인증 코드(MAC_ij)의 송수신 및 검증 과정이 모두 완료되면, 송신 ECU(ECUS)와 수신 ECU(ECUR)는 송신 횟수(C_i)를 1 만큼 증가시킨다(S260과 S270).

[0052] 상기와 같이 각 세션에서 데이터 프레임을 송수신할 때마다 일회성 인증키(AK_ij)를 생성함으로써, 메시지 인증

코드의 안전성을 강화할 수 있다.

[0053] 다만, i 번째 세션에서 송신 ECU(ECUS)와 수신 ECU(ECUR)가 관리하는 송신 횟수(C_i)는 유한한 크기를 갖는다. 이때, 송신 ECU(ECUS)가 송신 횟수(C_i)로 표현될 수 있는 범위보다 많은 데이터 프레임을 수신 ECU(ECUR)로 송신할 경우, 송신 횟수(C_i)는 초기화되고 초기값, 예컨대 0 부터 다시 관리될 것이다.

[0054] i 번째 세션에서 동일한 송신 횟수(C_i)가 발생할 경우 메시지 재생공격으로부터 안전성을 보장할 수 없다. 따라서, 메시지 재생공격으로부터 안전성을 보장하기 위해, 키 생성키에 대한 업데이트 과정이 필요할 수 있다.

[0055] i 번째 세션에서 송신 횟수(C_i)가 최대 표현 수치에 다다르기 전에 게이트웨이 ECU(GECU)를 포함한 ECU들은 키 생성키 업데이트 과정을 수행할 수 있다. 키 생성키 업데이트 과정은 도 2를 통하여 설명한 키 생성키 생성 과정과 동일할 수 있다. 키 생성키 업데이트 과정을 통하여 i+1 번째 세션에서 사용될 키 생성키(KGK_i+1)가 생성되면, i 번째 세션은 종료되고 i+1 번째 세션이 시작될 수 있다.

[0056] 도 4는 CAN 데이터 프레임 포맷을 도시한다.

[0057] 도 4를 참조하면, CAN 데이터 프레임의 데이터 페이로드는 8 바이트(byte)로 매우 제한적이다. 따라서, 본 발명에서는 64 비트(bit) 이하의 짧은 메시지 인증 코드(MAC)를 사용할 수 있다. 상기 메시지 인증 코드는 도 3을 통하여 설명한 데이터 프레임 인증 코드를 의미할 수 있다.

[0058] 8 바이트의 데이터 필드 중 32 비트, 24비트, 또는 12 비트가 상기 메시지 인증 코드를 전송하는데 사용될 수 있다. 그러나, 이와 같은 짧은 메시지 인증 코드를 사용할 경우 암호학적 안전성을 보장할 수 없다. 따라서, 본 발명에서는 32 비트, 24비트, 또는 12 비트의 길이를 갖는 메시지 인증 코드의 암호학적 안전성을 보장하기 위해 일회성 인증키를 사용할 수 있다.

[0059] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0060] 10 : 통신 시스템

12 : 버스

GECU : 게이트웨이 ECU

ECU1 : 제1 ECU

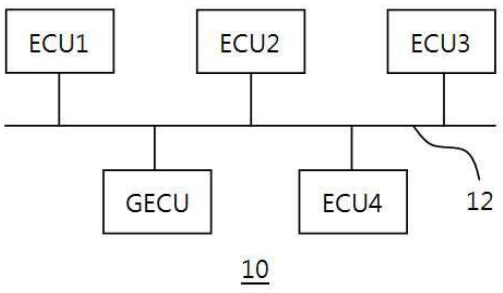
ECU2 : 제2 ECU

ECU3 : 제3 ECU

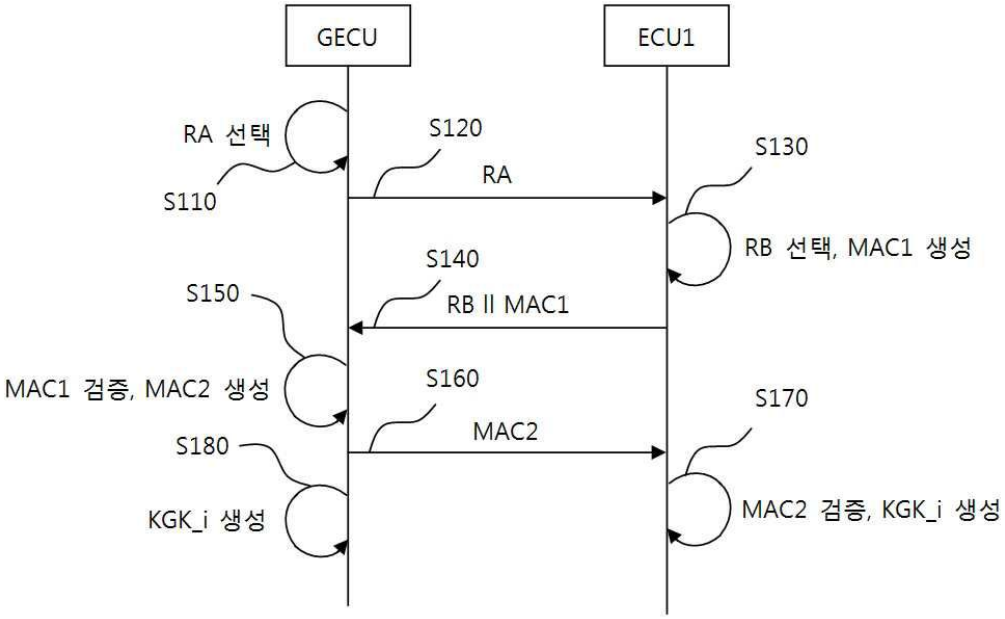
ECU4 : 제4 ECU

도면

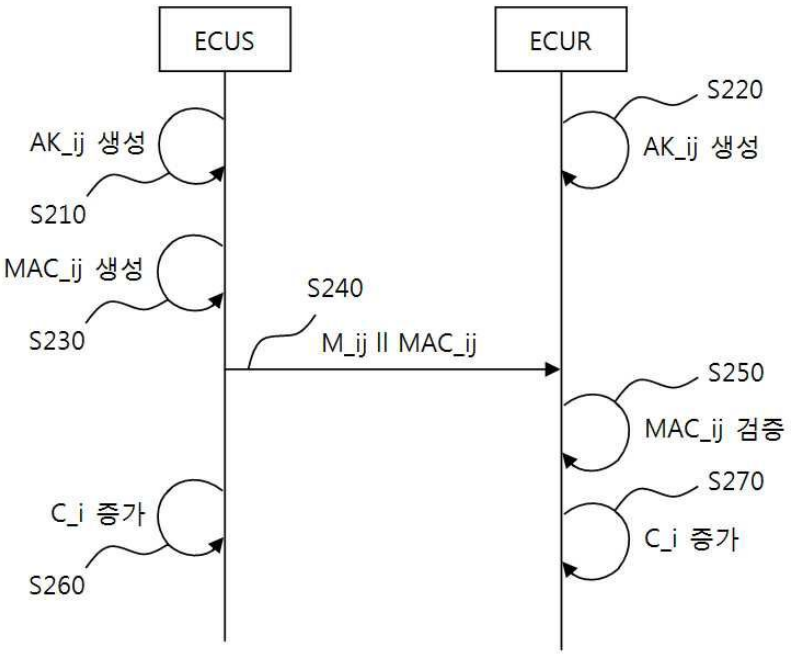
도면1



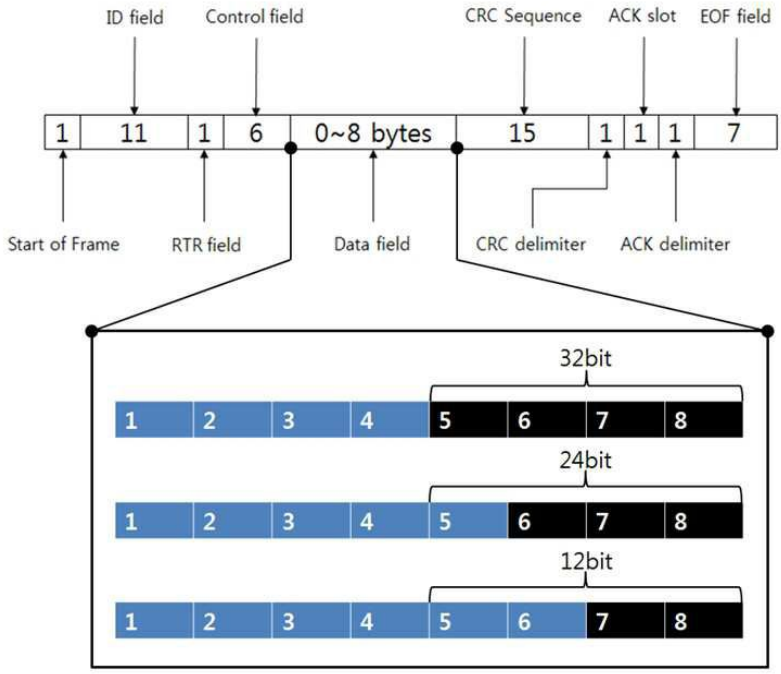
도면2


GECU
ECU1
RA 선택
S110
S120
RA
S130
RB 선택, MAC1 생성
S140
RB ll MAC1
S150
MAC1 검증, MAC2 생성
S160
MAC2
S170
S180
KGK_i 생성
MAC2 검증, KGK_i 생성

도면3


ECUS
ECUR
AK_ij 생성
S210
S220
AK_ij 생성
MAC_ij 생성
S230
S240
M_ij ll MAC_ij
S250
MAC_ij 검증
C_i 증가
S260
S270
C_i 증가

도면4


ID field
Control field
CRC Sequence
ACK slot
EOF field
1
11
1
6
0~8 bytes
15
1
1
1
7
Start of Frame
RTR field
Data field
CRC delimiter
ACK delimiter
32bit
1 2 3 4 5 6 7 8
24bit
1 2 3 4 5 6 7 8
12bit
1 2 3 4 5 6 7 8