



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년05월02일
(11) 등록번호 10-1974411
(24) 등록일자 2019년04월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) H04L 12/40 (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/0631 (2013.01)
H04L 12/40104 (2013.01)
(21) 출원번호 10-2018-0138660
(22) 출원일자 2018년11월13일
심사청구일자 2018년11월13일
(56) 선행기술조사문헌
KR1020170032210 A*
(뒷면에 계속)

(73) 특허권자
동국대학교 산학협력단
서울특별시 중구 필동로1길 30 (필동3가, 동국대학교)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
임대운
서울특별시 은평구 진관2로 57-37, 243동 1001호
(진관동, 은평뉴타운우물골)
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
박경원
서울특별시 동대문구 장안벚꽃로 167 래미안장안 2차아파트 212동 101호
(74) 대리인
김효성

전체 청구항 수 : 총 10 항

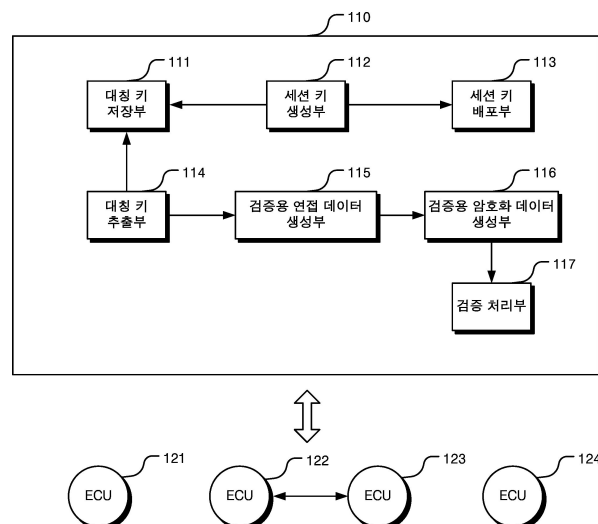
심사관 : 양종필

(54) 발명의 명칭 차량 내 보안 통신 지원 장치 및 그 동작 방법

(57) 요약

차량 내 보안 통신 지원 장치 및 그 동작 방법이 개시된다. 본 발명은 차량 내 탑재되어 있는 ECU(Electronic Control Unit)들 간의 메시지 송수신 과정에서 대칭키를 이용한 암호화 방식을 통해 전송측의 무결성을 검증할 수 있는 보안 프로토콜 기술을 제시함으로써, 제한된 연산능력을 갖춘 차량 통신 환경에서도 고도의 보안성이 유지될 수 있도록 지원할 수 있다.

대표도 - 도1



(52) CPC특허분류

H04L 9/0869 (2013.01)
H04L 2012/40273 (2013.01)
H04L 2209/84 (2013.01)

(56) 선행기술조사문헌

A. Menezes 외 2명, Handbook of Applied
 Cryptography, Chapter.1, CRC Press (1996.)
 KR101591323 B1
 KR1020050010860 A
 JP2010016522 A

*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	1711065844
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	자율 주행차를 위한 침입 감내 핵심 요소 기술 개발
기 여 율	1/1
주관기관	조선대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

데이터 암호화에 사용하기 위한 서로 다른 대칭 키를 저장하고 있는 복수의 ECU(Electronic Control Unit)들 간의 보안 통신을 지원하기 위한 차량 내 보안 통신 지원 장치에 있어서,

상기 복수의 ECU들 각각에 대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키를 서로 대응시켜 저장하고 있는 대칭 키 저장부;

상기 복수의 ECU들로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 수신되면, 제1 세션 키를 생성하고, 상기 대칭 키 저장부로부터 상기 복수의 ECU들 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 상기 복수의 ECU들 각각에 대응하는 대칭 키로 암호화하는 세션 키 생성부; 및

상기 복수의 ECU들 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송하는 세션 키 배포부

를 포함하고,

상기 복수의 ECU들 중 어느 하나인 제1 ECU는 상기 제1 ECU에 대응하는 제1 대칭 키로 암호화가 완료된 상기 제1 세션 키가 수신되면, 상기 제1 ECU에서 저장하고 있는 상기 제1 대칭 키로 상기 제1 세션 키에 대한 복호화를 수행하고, 상기 복수의 ECU들 중 제2 ECU에 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 복호화가 수행된 상기 제1 세션 키와 상기 제1 대칭 키를 기초로 상기 제1 메시지에 대한 암호화를 수행하여 상기 제2 ECU로 암호화가 수행된 상기 제1 메시지를 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리하는 차량 내 보안 통신 지원 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 제1 ECU는

상기 제2 ECU로 상기 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 랜덤 데이터를 랜덤하게 생성하고, 상기 제1 ECU에 대한 제1 식별자, 상기 제2 ECU에 대한 제2 식별자, 상기 랜덤 데이터 및 상기 제1 메시지를 순차적으로 연결(Concatenation)하여 제1 연결 데이터를 생성한 후 상기 제1 연결 데이터를 상기 제1 대칭 키로 암호화하여 제1 암호화 데이터를 생성하고,

상기 제1 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 순차적으로 연결하여 제2 연결 데이터를 생성한 후 상기 제2 연결 데이터를 상기 제1 세션 키로 암호화하여 제2 암호화 데이터를 생성하며,

상기 제2 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 순차적으로 연결하여 제3 연결 데이터를 생성한 후 상기 제3 연결 데이터를 상기 제2 ECU로 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리하는 차량 내 보안 통신 지원 장치.

청구항 4

제3항에 있어서,

상기 제2 ECU는

상기 제1 ECU로부터 상기 제3 연결 데이터가 수신되면, 상기 제3 연결 데이터로부터 상기 제1 메시지, 상기 랜

덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 각각 분리하고,

상기 제3 연결 데이터에 대한 분리가 완료되면, 상기 제3 연결 데이터에서 분리된 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터를 순차적으로 연결하여 제1 검증용 연결 데이터를 생성하고, 상기 제1 검증용 연결 데이터를 상기 제1 세션 키로 암호화하여 제1 검증용 암호화 데이터를 생성한 후 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는지 여부를 확인하며,

상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는 것으로 확인되면, 상기 차량 내 보안 통신 지원 장치로 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 전송하면서, 데이터 검증 요청을 전송하는 차량 내 보안 통신 지원 장치.

청구항 5

제4항에 있어서,

상기 차량 내 보안 통신 지원 장치는

상기 제2 ECU로부터 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터와 함께 상기 데이터 검증 요청이 수신되면, 상기 대칭 키 저장부로부터 상기 제1 식별자에 대응되어 저장되어 있는 상기 제1 대칭 키를 추출하는 대칭 키 추출부;

상기 제1 대칭 키가 추출되면, 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지 및 상기 랜덤 데이터를 순차적으로 연결하여 제2 검증용 연결 데이터를 생성하는 검증용 연결 데이터 생성부;

상기 제2 검증용 연결 데이터가 생성되면, 상기 제2 검증용 연결 데이터를 상기 제1 대칭 키로 암호화하여 제2 검증용 암호화 데이터를 생성하는 검증용 암호화 데이터 생성부; 및

상기 제2 검증용 암호화 데이터가 생성되면, 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는지 여부를 확인하여 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는 것으로 확인되면, 검증 성공 메시지를 생성하여 상기 제2 ECU에 전송하는 검증 처리부

를 더 포함하는 차량 내 보안 통신 지원 장치.

청구항 6

데이터 암호화에 사용하기 위한 서로 다른 대칭 키를 저장하고 있는 복수의 ECU(Electronic Control Unit)들 간의 보안 통신을 지원하기 위한 차량 내 보안 통신 지원 장치의 동작 방법에 있어서,

상기 복수의 ECU들 각각에 대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키를 서로 대응시켜 저장하고 있는 대칭 키 저장부를 유지하는 단계;

상기 복수의 ECU들로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 수신되면, 제1 세션 키를 생성하고, 상기 대칭 키 저장부로부터 상기 복수의 ECU들 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 상기 복수의 ECU들 각각에 대응하는 대칭 키로 암호화하는 단계; 및

상기 복수의 ECU들 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송하는 단계

를 포함하고,

상기 복수의 ECU들 중 어느 하나인 제1 ECU는 상기 제1 ECU에 대응하는 제1 대칭 키로 암호화가 완료된 상기 제1 세션 키가 수신되면, 상기 제1 ECU에서 저장하고 있는 상기 제1 대칭 키로 상기 제1 세션 키에 대한 복호화를 수행하고, 상기 복수의 ECU들 중 제2 ECU에 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 복호화가 수행된 상기 제1 세션 키와 상기 제1 대칭 키를 기초로 상기 제1 메시지에 대한 암호화를 수행하여 상기 제2 ECU로 암호화가 수행된 상기 제1 메시지를 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리하는 차량 내 보안 통신 지원 장치의 동작 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 제1 ECU는

상기 제2 ECU로 상기 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 랜덤 데이터를 랜덤하게 생성하고, 상기 제1 ECU에 대한 제1 식별자, 상기 제2 ECU에 대한 제2 식별자, 상기 랜덤 데이터 및 상기 제1 메시지를 순차적으로 연결(Concatenation)하여 제1 연결 데이터를 생성한 후 상기 제1 연결 데이터를 상기 제1 대칭 키로 암호화하여 제1 암호화 데이터를 생성하고,

상기 제1 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 순차적으로 연결하여 제2 연결 데이터를 생성한 후 상기 제2 연결 데이터를 상기 제1 세션 키로 암호화하여 제2 암호화 데이터를 생성하며,

상기 제2 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 순차적으로 연결하여 제3 연결 데이터를 생성한 후 상기 제3 연결 데이터를 상기 제2 ECU로 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리하는 차량 내 보안 통신 지원 장치의 동작 방법.

청구항 9

제8항에 있어서,

상기 제2 ECU는

상기 제1 ECU로부터 상기 제3 연결 데이터가 수신되면, 상기 제3 연결 데이터로부터 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 각각 분리하고,

상기 제3 연결 데이터에 대한 분리가 완료되면, 상기 제3 연결 데이터에서 분리된 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터를 순차적으로 연결하여 제1 검증용 연결 데이터를 생성하고, 상기 제1 검증용 연결 데이터를 상기 제1 세션 키로 암호화하여 제1 검증용 암호화 데이터를 생성한 후 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는지 여부를 확인하며,

상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는 것으로 확인되면, 상기 차량 내 보안 통신 지원 장치로 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 전송하면서, 데이터 검증 요청을 전송하는 차량 내 보안 통신 지원 장치의 동작 방법.

청구항 10

제9항에 있어서,

상기 차량 내 보안 통신 지원 장치의 동작 방법은

상기 제2 ECU로부터 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터와 함께 상기 데이터 검증 요청이 수신되면, 상기 대칭 키 저장부로부터 상기 제1 식별자에 대응되어 저장되어 있는 상기 제1 대칭 키를 추출하는 단계;

상기 제1 대칭 키가 추출되면, 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지 및 상기 랜덤 데이터를 순차적으로 연결하여 제2 검증용 연결 데이터를 생성하는 단계;

상기 제2 검증용 연결 데이터가 생성되면, 상기 제2 검증용 연결 데이터를 상기 제1 대칭 키로 암호화하여 제2 검증용 암호화 데이터를 생성하는 단계; 및

상기 제2 검증용 암호화 데이터가 생성되면, 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는지 여부를 확인하여 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는 것으로 확인되면, 검증 성공 메시지를 생성하여 상기 제2 ECU에 전송하는 단계

를 더 포함하는 차량 내 보안 통신 지원 장치의 동작 방법.

청구항 11

제6항, 제8항, 제9항 또는 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프

로그를 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

제6항, 제8항, 제9항 또는 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기술 분야

[0001] 본 발명은 차량 내 탑재되어 있는 ECU(Electronic Control Unit)들 간의 보안 통신이 가능하도록 지원하는 장치 및 그 동작 방법에 대한 것이다.

배경 기술

[0002] 최근, 차량에 다양한 전자 장비가 탑재됨에 따라, 이러한 전자 장비의 제어를 위한 다수의 ECU(Electronic Control Unit)들이 차량에 탑재되고 있는 추세이다.

[0003] 차량에서 사용되는 CAN 통신은 메시지 기반 프로토콜로 송신측이 메시지 기반으로 데이터를 생성하여 데이터 버스에 올리지만, 수신처를 별도로 지정하지 않음으로 인해 CAN 통신 버스에 연결되어 있는 ECU들은 모든 메시지를 수신할 수 있고, 각 ECU들은 메시지에 지정되어 있는 식별자를 보고 해당 메시지의 수신처를 판단하게 된다.

[0004] 이와 같이, CAN 통신의 메시지는 수신측과 송신측의 정보를 담고 있지 않기 때문에 악의적인 송신자에 의해서 변조된 메시지가 수신측에 수신되는 경우, 수신측에서는 공격자를 가려낼 방법이 없는 상황이다.

[0005] 차량에 탑재되어 있는 ECU들 간의 통신에 있어서, 보안을 강화하기 위해서 다양한 암호화 프로토콜의 도입을 고려할 수 있는데, 메시지 송신측의 무결성을 검증하기 위한 방식으로 비대칭키 기반의 암호화 알고리즘을 사용하는 방안을 고려할 수 있다.

[0006] 비대칭키 기반의 암호화 알고리즘은 수신측에 소정의 메시지가 수신되었을 때, 해당 메시지가 진정한 송신자에 의해서 전송된 메시지임을 검증하는데 활용할 수 있는 강력한 부인방지 알고리즘이지만, 공개키와 개인키를 이용한 암호화와 연산 과정이 다소 복잡하다는 점에서, 암호화에 많은 연산 자원을 할당하기 어려운 차량 환경에서는 비대칭키 기반의 암호화 알고리즘을 사용하기가 어려운 실정이다.

[0007] 따라서, 차량 내의 통신 시스템에서 비교적 간단한 연산이 수행되도록 하면서도 메시지 전송측의 무결성을 검증할 수 있는 보안 기술에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 차량 내 탑재되어 있는 ECU(Electronic Control Unit)들 간의 메시지 송수신 과정에서 대칭키를 이용한 암호화 방식을 통해 전송측의 무결성을 검증할 수 있는 보안 프로토콜 기술을 제시함으로써, 제한된 연산능력을 갖춘 차량 통신 환경에서도 고도의 보안성이 유지될 수 있도록 지원하고자 한다.

과제의 해결 수단

[0009] 본 발명의 일실시예에 따른 데이터 암호화에 사용하기 위한 서로 다른 대칭 키를 저장하고 있는 복수의 ECU(Electronic Control Unit)들 간의 보안 통신을 지원하기 위한 차량 내 보안 통신 지원 장치는 상기 복수의 ECU들 각각에 대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키를 서로 대응시켜 저장하고 있는 대칭 키 저장부, 상기 복수의 ECU들로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 수신되면, 제1 세션 키를 생성하고, 상기 대칭 키 저장부로부터 상기 복수의 ECU들 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 상기 복수의 ECU들 각각에 대응하는 대칭 키로 암호화하는 세션 키 생성부 및 상기 복수의 ECU들 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송하는 세션 키 배포부를 포함한다.

[0010] 또한, 본 발명의 일실시예에 따른 데이터 암호화에 사용하기 위한 서로 다른 대칭 키를 저장하고 있는 복수의 ECU들 간의 보안 통신을 지원하기 위한 차량 내 보안 통신 지원 장치의 동작 방법은 상기 복수의 ECU들 각각에

대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키를 서로 대응시켜 저장하고 있는 대칭 키 저장부를 유지하는 단계, 상기 복수의 ECU들로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 수신되면, 제1 세션 키를 생성하고, 상기 대칭 키 저장부로부터 상기 복수의 ECU들 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 상기 복수의 ECU들 각각에 대응하는 대칭 키로 암호화하는 단계 및 상기 복수의 ECU들 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송하는 단계를 포함한다.

발명의 효과

[0011] 본 발명은 차량 내 탑재되어 있는 ECU(Electronic Control Unit)들 간의 메시지 송수신 과정에서 대칭키를 이용한 암호화 방식을 통해 전송측의 무결성을 검증할 수 있는 보안 프로토콜 기술을 제시함으로써, 제한된 연산능력을 갖춘 차량 통신 환경에서도 고도의 보안성이 유지될 수 있도록 지원할 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0014] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0015] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0016] 도 1은 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 구조를 도시한 도면이다.

[0017] 도 1을 참조하면, 본 발명에 따른 차량 내 보안 통신 지원 장치(110)는 대칭 키 저장부(111), 세션 키 생성부(112) 및 세션 키 배포부(113)를 포함한다.

[0018] 우선, 본 발명에 따른 차량 내 보안 통신 지원 장치(110)는 차량 내부에 탑재될 수 있는 장치로, 상기 차량 내부에 탑재되어 있는 복수의 ECU들(121, 122, 123, 124) 간의 보안 통신을 지원하는 장치이다.

[0019] 그리고, 복수의 ECU들(121, 122, 123, 124) 각각에는 서로 다른 대칭 키가 미리 발급되어 저장되어 있고, 차량 내 보안 통신 지원 장치(110)에도 복수의 ECU들(121, 122, 123, 124) 각각에 대해서 발급된 대칭 키와 동일한 대칭 키가 미리 발급되어 있다. 이와 관련해서, 대칭 키 저장부(111)에는 복수의 ECU들(121, 122, 123, 124)

각각에 대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키가 서로 대응되어 저장되어 있다.

[0020] 예컨대, 대칭 키 저장부(111)에는 하기의 표 1과 같이 대칭 키가 저장되어 있을 수 있다.

표 1

ECU의 식별자	대칭 키
식별자 1	대칭 키 1
식별자 2	대칭 키 2
식별자 3	대칭 키 3
...	...

[0024] 이러한 상황 하에서, 복수의 ECU들(121, 122, 123, 134)로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 차량 내 보안 통신 지원 장치(110)에 수신되면, 세션 키 생성부(112)는 제1 세션 키를 생성하고, 대칭 키 저장부(111)로부터 복수의 ECU들(121, 122, 123, 134) 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 복수의 ECU들(121, 122, 123, 124) 각각에 대응하는 대칭 키로 암호화한다.

[0025] 그리고, 세션 키 배포부(113)는 복수의 ECU들(121, 122, 123, 124) 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송한다.

[0026] 예컨대, 상기 표 1과 같이 대칭 키 저장부(111)에 대칭 키가 저장되어 있다고 하는 경우, 세션 키 생성부(112)는 상기 제1 세션 키를 대칭 키 1, 대칭 키 2, 대칭 키 3으로 각각 암호화할 수 있다.

[0027] 그리고 나서, 세션 키 배포부(113)는 식별자 1을 갖는 ECU에 대해 상기 대칭 키 1로 암호화가 수행된 제1 세션 키를 전송할 수 있고, 식별자 2를 갖는 ECU에 대해 상기 대칭 키 2로 암호화가 수행된 제1 세션 키를 전송할 수 있으며, 식별자 3을 갖는 ECU에 대해 상기 대칭 키 3으로 암호화가 수행된 제1 세션 키를 전송할 수 있다.

[0028] 이렇게, 복수의 ECU들(121, 122, 123, 124) 각각에 각 ECU에 대응하는 대칭 키로 암호화가 수행된 상기 제1 세션 키가 수신되면, 복수의 ECU들(121, 122, 123, 124) 각각은 각 ECU에 저장되어 있는 대칭 키를 이용하여 상기 제1 세션 키에 대한 복호화를 수행한 후 상기 제1 세션 키와 각 ECU에 대응하는 대칭 키를 이용해서 복수의 ECU들(121, 122, 123, 124) 간의 암호화 통신을 수행할 수 있다.

[0029] 관련해서, 복수의 ECU들(121, 122, 123, 124) 중 어느 하나인 제1 ECU가 제2 ECU와 암호화 통신을 수행하는 과정에 대해 설명하면 다음과 같다. 여기서, 상기 제1 ECU는 도 1의 도면에서 도면부호 122로 표시한 ECU인 것으로 가정하고, 상기 제2 ECU는 도 1의 도면에서 도면부호 123으로 표시한 ECU인 것으로 가정하기로 한다.

[0030] 본 발명의 일실시예에 따르면, 제1 ECU(122)는 제1 ECU(122)에 대응하는 제1 대칭 키로 암호화가 완료된 상기 제1 세션 키가 차량 내 보안 통신 지원 장치(110)로부터 수신되면, 제1 ECU(122)에서 저장하고 있는 상기 제1 대칭 키로 상기 제1 세션 키에 대한 복호화를 수행할 수 있다.

[0031] 그리고, 제1 ECU(122)는 복수의 ECU들(121, 122, 123, 124) 중 제2 ECU(123)에 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 복호화가 수행된 상기 제1 세션 키와 상기 제1 대칭 키를 기초로 상기 제1 메시지에 대한 암호화를 수행하여 제2 ECU(123)로 암호화가 수행된 상기 제1 메시지를 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리할 수 있다.

[0032] 이때, 제1 ECU(122)의 동작을 보다 상세하게 설명하면 다음과 같다.

[0033] 우선, 제1 ECU(122)는 제2 ECU(123)로 상기 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 랜덤 데이터를 랜덤하게 생성하고, 제1 ECU(122)에 대한 제1 식별자, 제2 ECU(123)에 대한 제2 식별자, 상기 랜덤 데이터 및 상기 제1 메시지를 순차적으로 연결(Concatenation)하여 제1 연결 데이터를 생성한 후 상기 제1 연결 데이터를 상기 제1 대칭 키로 암호화하여 제1 암호화 데이터를 생성할 수 있다.

[0034] 여기서, '||'을 연결 기호라고 하였을 때, 상기 제1 연결 데이터는 '(제1 식별자 || 제2 식별자 || 랜덤 데이터 || 제1 메시지)'로 표현될 수 있다.

[0035] 이렇게, 상기 제1 암호화 데이터가 생성되면, 제1 ECU(122)는 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 순차적으로 연결하여 제2 연결 데이터를 생성한 후 상기 제2 연결 데이터를 상기 제1 세션 키

로 암호화하여 제2 암호화 데이터를 생성할 수 있다.

- [0036] 여기서, 상기 제2 연결 데이터는 '(제1 메시지 || 랜덤 데이터 || 제1 암호화 데이터)'로 표현될 수 있다.
- [0037] 그 이후, 제1 ECU(122)는 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 순차적으로 연결하여 제3 연결 데이터를 생성한 후 상기 제3 연결 데이터를 제2 ECU(123)로 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리할 수 있다.
- [0038] 즉, 제2 ECU(123)에 전송되는 상기 제3 연결 데이터는 '(제1 메시지 || 랜덤 데이터 || 제1 암호화 데이터 || 제2 암호화 데이터)'와 같이 표현될 수 있다.
- [0039] 이렇게, 제2 ECU(123)에 상기 제3 연결 데이터가 상기 제1 메시지에 대한 암호화 데이터로 수신되는 경우, 제2 ECU(123)는 상기 제1 메시지가 진정한 제1 ECU(122)에 의해서 발송된 메시지가 맞는지 확인하기 위한 검증 과정을 진행할 수 있다.
- [0040] 관련해서, 제2 ECU(123)는 상기 제3 연결 데이터가 수신되면, 상기 제3 연결 데이터로부터 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 각각 분리할 수 있다.
- [0041] 그리고, 상기 제3 연결 데이터에 대한 분리가 완료되면, 제2 ECU(123)는 상기 제3 연결 데이터에서 분리된 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터를 순차적으로 연결하여 제1 검증용 연결 데이터를 생성하고, 상기 제1 검증용 연결 데이터를 상기 제1 세션 키로 암호화하여 제1 검증용 암호화 데이터를 생성한 후 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는지 여부를 확인할 수 있다.
- [0042] 여기서, 상기 제1 검증용 암호화 데이터는 '(제1 메시지 || 랜덤 데이터 || 제1 암호화 데이터)'로 표현되는 제1 검증용 연결 데이터가 상기 제1 세션 키로 암호화된 데이터이고, 상기 제2 암호화 데이터는 '(제1 메시지 || 랜덤 데이터 || 제1 암호화 데이터)'로 표현되는 제2 연결 데이터가 상기 제1 세션 키로 암호화된 데이터이기 때문에, 상기 제1 검증용 암호화 데이터와 상기 제2 암호화 데이터가 서로 동일하다는 것은 제2 ECU(123)와 제1 ECU(122)가 서로 동일한 세션 키를 이용하여 데이터 암호화를 수행하였다는 것을 의미하게 된다.
- [0043] 따라서, 제2 ECU(123)는 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는 것으로 확인되면, 상기 제3 연결 데이터가 제1 ECU(122)로부터 정상적으로 발송된 데이터임을 1차적으로 확인한 후 차량 내 보안 통신 지원 장치(110)로 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 메시지 및 상기 제1 암호화 데이터를 전송하면서, 데이터 검증 요청을 전송할 수 있다.
- [0044] 이때, 본 발명의 일실시예에 따르면, 차량 내 보안 통신 지원 장치(110)는 제2 ECU(123)로부터 전송되는 데이터 검증 요청에 따른 데이터 검증을 수행하기 위한 구성으로, 대칭 키 추출부(114), 검증용 연결 데이터 생성부(115), 검증용 암호화 데이터 생성부(116) 및 검증 처리부(117)를 더 포함할 수 있다.
- [0045] 대칭 키 추출부(114)는 제2 ECU(123)로부터 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 메시지 및 상기 제1 암호화 데이터와 함께 상기 데이터 검증 요청이 수신되면, 대칭 키 저장부(111)로부터 제1 ECU(122)에 대한 식별자인 상기 제1 식별자에 대응되어 저장되어 있는 상기 제1 대칭 키를 추출한다.
- [0046] 검증용 연결 데이터 생성부(115)는 상기 제1 대칭 키가 추출되면, 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지 및 상기 랜덤 데이터를 순차적으로 연결하여 제2 검증용 연결 데이터를 생성한다.
- [0047] 검증용 암호화 데이터 생성부(116)는 상기 제2 검증용 연결 데이터가 생성되면, 상기 제2 검증용 연결 데이터를 상기 제1 대칭 키로 암호화하여 제2 검증용 암호화 데이터를 생성한다.
- [0048] 그리고, 검증 처리부(117)는 상기 제2 검증용 암호화 데이터가 생성되면, 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는지 여부를 확인하여 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는 것으로 확인되면, 검증 성공 메시지를 생성하여 제2 ECU(123)에 전송한다.
- [0049] 관련해서, 상기 제2 검증용 암호화 데이터는 '(제1 식별자 || 제2 식별자 || 제1 메시지 || 랜덤 데이터)'로 표현되는 제2 검증용 연결 데이터가 상기 제1 대칭 키로 암호화된 데이터이고, 상기 제1 암호화 데이터는 '(제1 식별자 || 제2 식별자 || 제1 메시지 || 랜덤 데이터)'로 표현되는 제1 연결 데이터가 상기 제1 대칭 키로 암호화된 데이터이기 때문에, 상기 제2 검증용 암호화 데이터와 상기 제1 암호화 데이터가 서로 동일하다는 것은 차량 내 보안 통신 지원 장치(110)와 제1 ECU(122)가 서로 동일한 대칭 키를 이용하여 데이터 암호화를 수행하였다는 것을 의미하게 된다.

- [0050] 따라서, 검증 처리부(117)는 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는 것으로 확인되면, 상기 제1 암호화 데이터가 제1 ECU(122)에 대응하는 진정한 대칭 키인 상기 제1 대칭 키를 기반으로 암호화된 것으로 판정하여 검증 성공 메시지를 생성한 후 상기 검증 성공 메시지를 제2 ECU(123)에 전송할 수 있다.
- [0051] 이를 통해, 제2 ECU(123)는 제1 ECU(122)로부터 수신한 '(제1 메시지 || 랜덤 데이터 || 제1 암호화 데이터 || 제2 암호화 데이터)'로 표현되는 상기 제3 연결 데이터가 제1 ECU(122)로부터 진정으로 발송된 것임을 파악하고, 상기 제3 연결 데이터에 포함되어 있는 상기 제1 메시지를 읽어들이어 상기 제1 메시지에 따른 동작을 수행할 수 있다.
- [0052] 도 2는 본 발명의 일실시예에 따른 데이터 암호화에 사용하기 위한 서로 다른 대칭 키를 저장하고 있는 복수의 ECU들 간의 보안 통신을 지원하기 위한 차량 내 보안 통신 지원 장치의 동작 방법을 도시한 순서도이다.
- [0053] 단계(S210)에서는 상기 복수의 ECU들 각각에 대한 식별자 및 각 ECU에 저장되어 있는 대칭 키와 동일한 대칭 키를 서로 대응시켜 저장하고 있는 대칭 키 저장부를 유지한다.
- [0054] 단계(S220)에서는 상기 복수의 ECU들로부터 ECU 간의 데이터 전송에 사용하기 위한 세션 키의 발급 요청이 수신되면, 제1 세션 키를 생성하고, 상기 대칭 키 저장부로부터 상기 복수의 ECU들 각각의 식별자에 대응되어 저장되어 있는 대칭 키를 추출한 후 상기 제1 세션 키를 상기 복수의 ECU들 각각에 대응하는 대칭 키로 암호화한다.
- [0055] 단계(S230)에서는 상기 복수의 ECU들 각각에 대해 각 ECU에 대응하는 대칭 키로 암호화가 완료된 상기 제1 세션 키를 전송한다.
- [0056] 이때, 본 발명의 일실시예에 따르면, 상기 복수의 ECU들 중 어느 하나인 제1 ECU는 상기 제1 ECU에 대응하는 제1 대칭 키로 암호화가 완료된 상기 제1 세션 키가 수신되면, 상기 제1 ECU에서 저장하고 있는 상기 제1 대칭 키로 상기 제1 세션 키에 대한 복호화를 수행하고, 상기 복수의 ECU들 중 제2 ECU에 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 복호화가 수행된 상기 제1 세션 키와 상기 제1 대칭 키를 기초로 상기 제1 메시지에 대한 암호화를 수행하여 상기 제2 ECU로 암호화가 수행된 상기 제1 메시지를 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리할 수 있다.
- [0057] 이때, 본 발명의 일실시예에 따르면, 상기 제1 ECU는 상기 제2 ECU로 상기 제1 메시지를 전송해야 하는 상황이 발생하는 경우, 랜덤 데이터를 랜덤하게 생성하고, 상기 제1 ECU에 대한 제1 식별자, 상기 제2 ECU에 대한 제2 식별자, 상기 랜덤 데이터 및 상기 제1 메시지를 순차적으로 연결하여 제1 연결 데이터를 생성한 후 상기 제1 연결 데이터를 상기 제1 대칭 키로 암호화하여 제1 암호화 데이터를 생성할 수 있다.
- [0058] 그리고, 상기 제1 ECU는 상기 제1 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 순차적으로 연결하여 제2 연결 데이터를 생성한 후 상기 제2 연결 데이터를 상기 제1 세션 키로 암호화하여 제2 암호화 데이터를 생성할 수 있다.
- [0059] 그리고, 상기 제1 ECU는 상기 제2 암호화 데이터가 생성되면, 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 순차적으로 연결하여 제3 연결 데이터를 생성한 후 상기 제3 연결 데이터를 상기 제2 ECU로 전송함으로써, 상기 제1 메시지에 대한 암호화 전송을 완료 처리할 수 있다.
- [0060] 이때, 본 발명의 일실시예에 따르면, 상기 제2 ECU는 상기 제1 ECU로부터 상기 제3 연결 데이터가 수신되면, 상기 제3 연결 데이터로부터 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터 및 상기 제2 암호화 데이터를 각각 분리하고, 상기 제3 연결 데이터에 대한 분리가 완료되면, 상기 제3 연결 데이터에서 분리된 상기 제1 메시지, 상기 랜덤 데이터, 상기 제1 암호화 데이터를 순차적으로 연결하여 제1 검증용 연결 데이터를 생성하고, 상기 제1 검증용 연결 데이터를 상기 제1 세션 키로 암호화하여 제1 검증용 암호화 데이터를 생성한 후 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는지 여부를 확인할 수 있다.
- [0061] 그리고, 상기 제2 ECU는 상기 제1 검증용 암호화 데이터가 상기 제2 암호화 데이터와 서로 일치하는 것으로 확인되면, 상기 차량 내 보안 통신 지원 장치로 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터를 전송하면서, 데이터 검증 요청을 전송할 수 있다.
- [0062] 이때, 본 발명의 일실시예에 따르면, 상기 차량 내 보안 통신 지원 장치의 동작 방법은 상기 제2 ECU로부터 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지, 상기 랜덤 데이터 및 상기 제1 암호화 데이터와 함께 상기 데이터 검증 요청이 수신되면, 상기 대칭 키 저장부로부터 상기 제1 식별자에 대응되어 저장되어 있는 상기 제1 대칭 키를 추출하는 단계, 상기 제1 대칭 키가 추출되면, 상기 제1 식별자, 상기 제2 식별자, 상기 제1 메시지 및 상기 랜덤 데이터를 순차적으로 연결하여 제2 검증용 연결 데이터를 생성하는 단계, 상기 제2 검증용 연결

데이터가 생성되면, 상기 제2 검증용 연결 데이터를 상기 제1 대칭 키로 암호화하여 제2 검증용 암호화 데이터를 생성하는 단계 및 상기 제2 검증용 암호화 데이터가 생성되면, 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는지 여부를 확인하여 상기 제2 검증용 암호화 데이터가 상기 제1 암호화 데이터와 서로 일치하는 것으로 확인되면, 검증 성공 메시지를 생성하여 상기 제2 ECU에 전송하는 단계를 더 포함할 수 있다.

[0063] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 동작 방법은 도 1을 이용하여 설명한 차량 내 보안 통신 지원 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0064] 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0065] 또한, 본 발명의 일실시예에 따른 차량 내 보안 통신 지원 장치의 동작 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 본 발명을 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.

[0066] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0067] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0068] 110: 차량 내 보안 통신 지원 장치

111: 대칭 키 저장부

112: 세션 키 생성부

113: 세션 키 배포부

114: 대칭 키 추출부

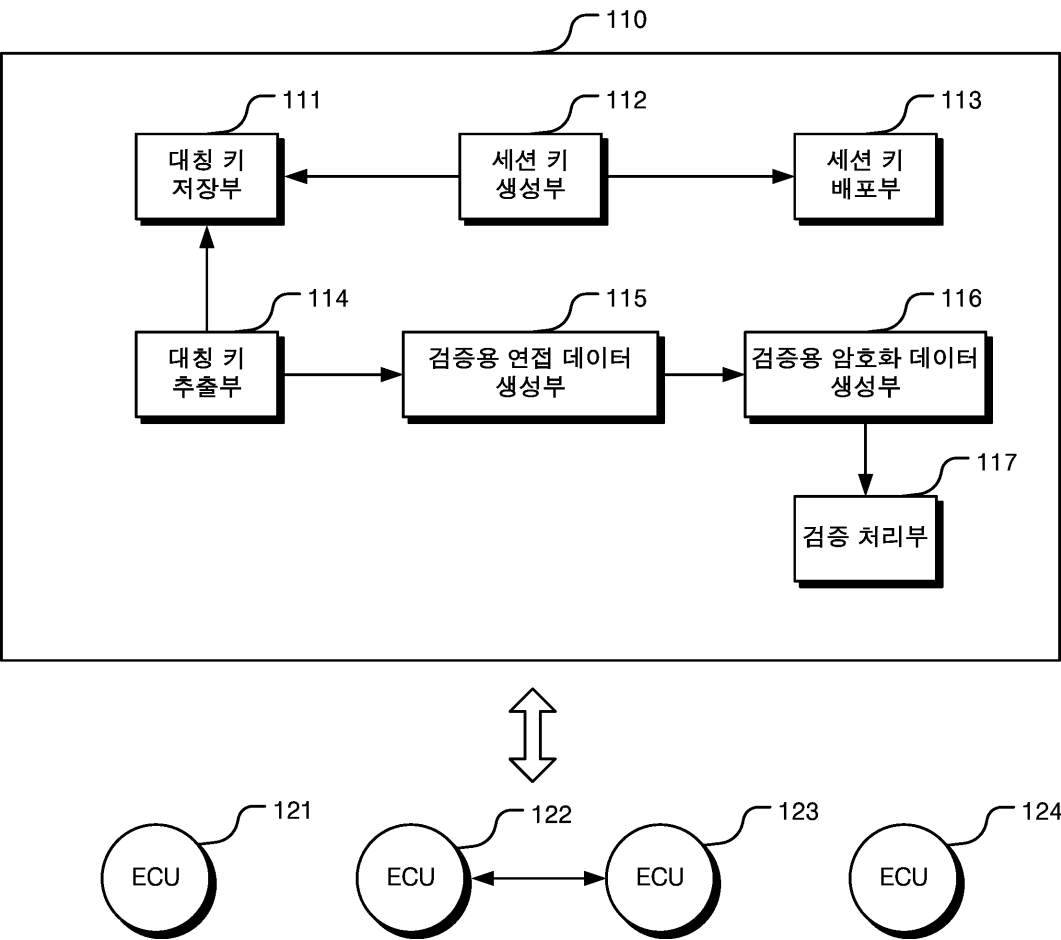
115: 검증용 언접 데이터 생성부 116: 검증용 암호화 데이터 생성부

117: 검증 처리부

121, 122, 123, 124: 복수의 ECU들

도면

도면1



도면2

