(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년06월22일
(11) 등록번호 10-2411797
(24) 등록일자 2022년06월17일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *G06F 8/65* (2018.01)
H04L 12/40 (2006.01) *H04L 9/32* (2006.01)
H04L 9/40 (2022.01)
(52) CPC특허분류
H04L 9/0877 (2013.01)
G06F 8/65 (2013.01)
(21) 출원번호 10-2021-0186802
(22) 출원일자 2021년12월24일
심사청구일자 2021년12월24일
(56) 선행기술조사문헌
JP2017059211 A*
KR1020200061702 A*
JP2021179935 A*
KR101673310 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
쌍용자동차 주식회사
경기도 평택시 동삭로 455-12 (칠괴동)
(72) 발명자
선진
경기도 평택시 이충로 16 휴먼시아추담마을아파트 403동 805호
백은기
경기도 평택시 지제동삭2로 177
(뒷면에 계속)
(74) 대리인
김병진

전체 청구항 수 : 총 3 항 심사관 : 나용수

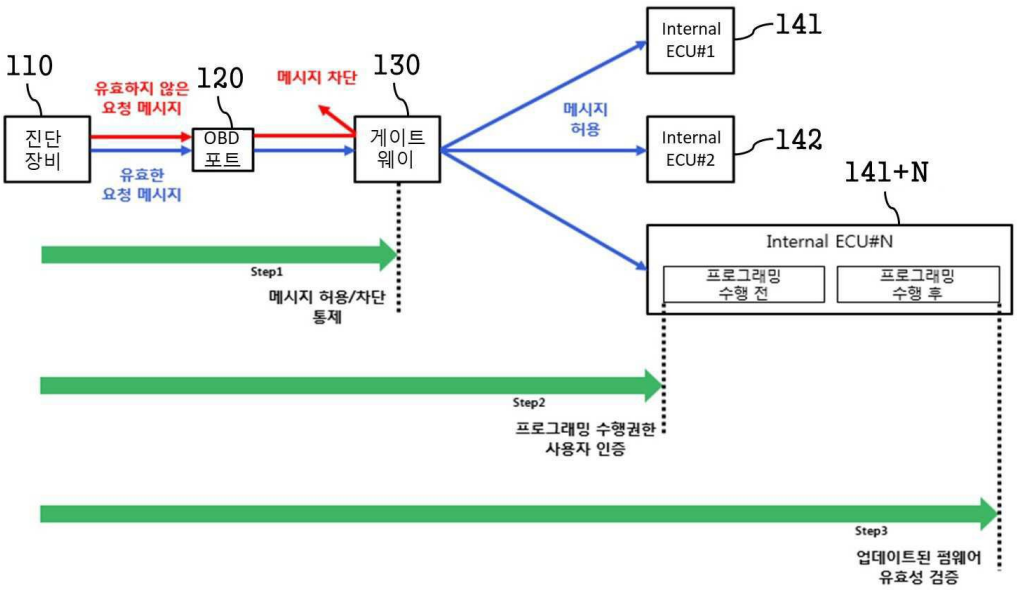
(54) 발명의 명칭 **하드웨어 기반의 차량 사이버보안시스템**

(57) 요 약

차량의 전자제어장치(ECU) 간 네트워크 장치의 게이트웨이에서 암호화 보안 키를 이용하여 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하도록 하여, 사이버 보안 애플리케이션이 설치되지 않은 제어기의 사이버 보안이 이루어지도록 함으로써 사이버 보안을 위한 원가를 절감할 수 있도록 한 하드웨어 기반의 차량 사이버보안시스템

(뒷면에 계속)

대 표 도 - 도4



에 관한 것으로서, 외부의 보안 키 관리 시스템에서 유선으로 전송된 보안 키를 전달하는 진단 포트(OBD 포트), 외부의 보안 키 관리 시스템으로부터 무선으로 전송된 보안 키를 수신하여 전달하거나 외부 장치와 무선 연결을 위한 커넥티비티 장비, 진단 포트 및/또는 커넥티비티 장비와 접속되며, 하나 이상의 제어기(ECU)를 통신으로 연결하며, 데이터 형태의 보안 키를 별도의 저장 매체에 저장하고, 진단 포트 또는 커넥티비티 장비를 통해 업데이트 데이터 수신 시 별도의 저장매체에 저장한 보안 키와 외부 보안 키 관리 시스템에서 할당받은 보안 키 정보를 비교하여 일치하는 경우에만 업데이트 데이터를 연결된 전자제어장치로 전달하는 게이트웨이를 포함하여, 하드웨어 기반의 차량 사이버보안시스템을 구축한다.

(52) CPC특허분류
H04L 12/40104 (2013.01)
H04L 63/123 (2013.01)
H04L 9/0894 (2013.01)
H04L 9/3234 (2013.01)
H04L 9/3263 (2013.01)
H04L 2012/40215 (2013.01)
H04L 2012/40273 (2013.01)
H04L 2209/80 (2013.01)
H04L 2209/84 (2013.01)

(72) 발명자
이훈
경기도 성남시 분당구 장미로 101 장미마을
이원재
경기도 성남시 분당구 동판교로 155 봇들마을7단지 아파트 709동 701호

명 세 서

청구범위

청구항 1

외부의 보안 키 관리 시스템에서 유선으로 전송된 보안 키를 전달하는 진단 포트(OBD 포트);

외부의 보안 키 관리 시스템으로부터 무선으로 전송된 보안 키를 수신하여 전달하거나 외부 장치와 무선 연결을 위한 커넥티비티 장비;

상기 진단 포트 및/또는 커넥티비티 장비와 접속되며, 하나 이상의 제어기(ECU)를 통신으로 연결하며, 데이터 형태의 보안 키를 별도의 저장 매체에 저장하고, 상기 진단 포트 또는 커넥티비티 장비를 통해 업데이트 데이터 수신 시 상기 별도의 저장매체에 저장한 보안 키와 상기 외부 보안 키 관리 시스템에서 할당받은 보안 키 정보를 비교하여 일치하는 경우에만 업데이트 데이터를 연결된 제어기인 전자제어장치로 전달하는 게이트웨이를 포함하고,

상기 게이트웨이는 소프트웨어 업데이트를 관리하는 소프트웨어 업데이트 관리 모듈을 포함하며,

상기 게이트웨이의 업데이트 관리 모듈은,

외부 보안 키 관리시스템에서 진단장비용 인증서를 발급받아 그 인증서 검증을 통해 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하며,

상기 제어기는 상기 게이트웨이를 통해 외부 장치의 접근 시 상기 외부 보안 키 관리시스템에서 제공한 인증서를 이용한 접근자의 인증을 통해 1차 보안 기능을 수행하고, 업데이트된 펌웨어의 유효성 검증을 통해 2차 보안 기능을 수행하는 것을 특징으로 하는 하드웨어 기반의 차량 사이버보안시스템.

청구항 2

청구항 1에서, 상기 게이트웨이는 사이버 보안 위협 모니터링 및 사고대응용 CAN-IDS 솔루션을 구비한 것을 특징으로 하는 하드웨어 기반의 차량 사이버보안시스템.

청구항 3

청구항 1에서, 상기 게이트웨이는,

소프트웨어 업데이트 관리를 위한 리프로그래밍 수행 모듈;

소프트웨어 펌웨어를 저장하는 소프트웨어 펌웨어 저장소를 포함하며,

상기 소프트웨어 펌웨어 저장소는 데이터 형태의 보안 키를 별도로 저장하는 것을 특징으로 하는 하드웨어 기반의 차량 사이버보안시스템.

청구항 4

삭제

청구항 5

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 하드웨어 기반의 차량 사이버보안시스템에 관한 것으로, 특히 차량의 전자제어장치(ECU) 간 네트워크 장치의 게이트웨이에서 암호화 보안 키를 이용하여 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하도록 하여, 사이버 보안 애플리케이션이 설치되지 않은 제어기의 사이버 보안이 이루어지도록 함으로써 사이버 보안을 위한 원가를 절감할 수 있도록 한 하드웨어 기반의 차량 사이버보안시스템에 관한 것이다.

배 경 기 술

[0002] IT 기술이 지속적으로 발전하면서 가전기기는 물론 차량 역시 다양한 IT 기기들이 탑재되고 있다. 차량에 IT 기기들이 탑재되기 시작하면서 차량 내의 전자제어장치인 ECU(Electronic Control Unit)도 다양한 기능을 지원하기에 이르렀고 탑재되는 수량 또한 증가하고 있으며, 필요에 따라 차량의 적재적소에 분산 배치되어 있다.

[0003] 차량 내에 분산 배치된 ECU들은 상호 유기적으로 작용하여 동작해야 하기 때문에 이들은 기본적으로 통신을 통해 상호 상태를 인지해야 한다. 이를 위해서 차량 내 수십 개의 ECU들은 차량용 네트워크로 연결되어 있다. 주지한 바와 같이 차량용 네트워크는 CAN(Controller Area Network)이 사실상 표준 역할을 하면서 다양한 통신방식(LIN, MOST, Flexray, CAN-FD, Ethernet, Bluetooth 등)으로 확대되고 있다.

[0004] 차량에 탑재되는 통신 노드들의 수가 증대되고 있다는 점, 자율주행 적용으로 기존에 비해 상대적으로 더 많은 통신 부하를 처리해야 한다는 점, 유무선 외부 네트워크와의 연결됨에 따라 차량의 내부 네트워크의 보안 위험이 증가하고 있으며, 사이버 해킹에 대한 차량 보호의 중요성이 대두하고 있다.

[0005] 차량용 전자제어장치가 Hacking 공격을 당하여 악의적으로 작동하는 경우, 운전자와 탑승자의 안전에는 치명적이고 심각한 결과를 초래할 수 있고, 일부 제어장치에 자행되는 불법적인 데이터 튜닝과 변경 등을 방지할 수 있는 신뢰성 높은 보안기술 적용이 필수적이라고 할 수 있다.

[0006] 향후 개발되는 차량은 차량의 제어기술의 발달로 인하여 각종 편의적인 커넥티드 카 서비스 및 자율주행 서비스가 상용화될 시점이 도래하고 있는 동시에 사이버해킹 공격 가능성과 무단 차량 제어 위험성 또한 커지고 있는 실정이다.

[0007] 도 1은 과학기술정보통신부와 정보통신기술진흥센서에서 제공한 지능형 자동차 보안 대응 방안 보고서(2017)에서 발췌한 내용으로서, 자동차 보안 위협에 대해 공격 경로가 다양함을 알 수 있다.

[0008] 이러한 사이버 보안 위협으로부터 차량용 전자제어장치(Engine Control Unit; ECU) 내부의 보호해야 하는 자산은 크게 두 가지의 형태로 구분(식별)이 가능하다.

[0009] 하나는 소프트웨어 형태의 펌웨어이고, 다른 하나는 제어기 간의 통신 메시지이다. 현재, 차량용 전자제어장치의 자산을 보호하기 위한 기술적인 방안은 전자식제어장치의 내부의 보안 시스템 구성의 기반이 되는 플랫폼을 구축하고, 인증을 통한 사용자 접근 통제, 인가된 펌웨어만 업데이트 가능, 펌웨어 무결성 입증, 전자제어장치 간 통신 메시지 보호 등 보안 어플리케이션이 적용되고 있다.

[0010] 권한에 따라 전자제어장치의 프로그램 모드, 진단 모드 등 모드를 변경할 수 있는 기능을 허용해주는 것이 사용자 인증이며, 사용자 인증과정으로 씨드 엔 키 (Seed & Key)방식이 현재 적용되고 있다.

[0011] 도 2는 씨드 엔 키 방식의 보안 애플리케이션의 예시이다.

[0012] Seed & Key 방식은 전자제어장치와 진단 툴 간에 사전에 프로그램된 Seed 값에 대하여 이미 프로그램된 Key 값과 차량의 전자제어장치에서 계산한 Key 값을 비교하여 인증하는 방법으로, Seed 값은 요청할 때마다 변경되는 Random(난수) 함수를 사용한다. 그러나 약속된 Key가 외부에 노출되면 공개 알고리즘을 이용하여 누구나 그 데이터를 확인할 수 있는 구조이므로 보안성이 취약하다고 할 수 있다.

[0013] 결론적으로, 국제 표준 Key(암호) 알고리즘은 전자제어장치의 Core 성능에 따라 암호 알고리즘 연산처리에 적합하지 않은 경우가 많아서 엔진 제어 및 스마트키 전자제어장치 등 특정 제어장치에만 적용하고 있으므로, 암호 알고리즘 연산처리 수행시간을 최대한 단축할 수 있는 하드웨어 기반의 보안 모듈이 필요한 것이다.

[0014] 이러한 이유로 유럽에서는 도 3과 같은 EVITA(E-safety Vehicle Intrusion Protected Application) 프로젝트를 수행하였고, 자동차 사이버 보안을 위한 차세대 솔루션으로 하드웨어 기반의 모듈이 제안되었고, 최근에는 대부분의 차량용 마이크로프로세서에는 하드웨어 기반의 모듈이 기본적으로 탑재되고 있다고 할 수 있다.

[0015] 따라서 차량용 전자제어장치(Electronic Control Unit; ECU) 보안 기술의 하나로 진단 포트(On-Board-Diagnosis; OBD)를 통한 접속(Interface) 침투 그리고 무선 통신을 통한 접속 침투를 통하여 해킹(Hacking)하

여 전자제어장치의 펌웨어(소프트웨어)를 무단으로 변조하거나 임의로 조작하여 차량의 이상 작동을 야기할 수 있는 위협에 대하여 이를 방지하거나 완화할 수 있는 확률 높은 보안 시스템이 필요하다.

선행기술문헌

특허문헌

[0016] (특허문헌 0001) 대한민국 등록특허 10-1714525(2017.03.03. 등록)(차량 해킹 방지 방법 및 그를 위한 장치 및 시스템)

(특허문헌 0002) 대한민국 등록특허 10-2156261(2020.09.09. 등록)(차량에 대한 공격의 검출 및 예방을 위한 디바이스)

(특허문헌 0003) 대한민국 등록특허 10-1972457(2019.04.19. 등록)(CAN 통신 기반 해킹공격 탐지 방법 및 시스템)

(특허문헌 0004) 대한민국 등록특허 10-2262711(2021.06.03. 등록)(차량용 무선신호 해킹방지 방법 및 장치)

(특허문헌 0005) 대한민국 공개특허 10-2019-0116192(2019.10.14. 공개)(자율주행 차량 해킹 대응 방법 및 그 장치)

(특허문헌 0006) 대한민국 등록특허 10-2317862(2021.10.20. 등록)(블록체인을 이용한 원격 주행차의 해킹방지 방법)

(특허문헌 0007) 대한민국 등록특허 10-2312891(2021.10.07. 등록)(전파 및 음파를 활용한 차량의 해킹 방지 시스템의 스마트 제어 방법)

발명의 내용

해결하려는 과제

[0017] 따라서 본 발명은 상기와 같은 일반적인 차량의 통신을 통한 접속 침투를 통하여 해킹(Hacking)하여 전자제어장치의 펌웨어(소프트웨어)를 무단으로 변조하거나 임의로 조작하여 차량의 이상 작동을 야기할 수 있는 위협 문제를 해결하기 위해서 제안된 것으로서, 차량의 전자제어장치(ECU) 간 네트워크 장치의 게이트웨이에서 암호화 보안 키를 이용하여 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하도록 하여, 사이버 보안 애플리케이션이 설치되지 않은 제어기의 사이버 보안이 이루어지도록 함으로써 사이버 보안을 위한 원가를 절감할 수 있도록 한 하드웨어 기반의 차량 사이버보안시스템을 제공하는 데 그 목적이 있다.

[0018] 본 발명의 다른 목적은 게이트웨이를 통해 외부 장치의 접근 시 제어기에서 외부 보안 키 관리시스템에서 제공한 인증서를 이용한 접근자의 인증을 통해 1차 보안 기능을 수행하고, 업데이트된 펌웨어의 유효성 검증을 통해 2차 보안 기능을 수행하여 사이버 보안을 강화할 수 있는 하드웨어 기반의 차량 사이버보안시스템을 제공하는 것이다.

과제의 해결 수단

[0019] 상기한 바와 같은 목적을 달성하기 위하여, 본 발명에 따른 "하드웨어 기반의 차량 사이버보안시스템"은,

[0020] 외부의 보안 키 관리 시스템에서 유선으로 전송된 보안 키를 전달하는 진단 포트(OBD 포트);

[0021] 외부의 보안 키 관리 시스템으로부터 무선으로 전송된 보안 키를 수신하여 전달하거나 외부 장치와 무선 연결을 위한 커넥티비티 장비;

[0022] 상기 진단 포트 및/또는 커넥티비티 장비와 접속되며, 하나 이상의 제어기(ECU)를 통신으로 연결하며, 데이터 형태의 보안 키를 별도의 저장 매체에 저장하고, 상기 진단 포트 또는 커넥티비티 장비를 통해 업데이트 데이터 수신 시 상기 별도의 저장매체에 저장한 보안 키와 상기 외부 보안 키 관리 시스템에서 할당받은 보안 키 정보를 비교하여 일치하는 경우에만 업데이트 데이터를 연결된 전자제어장치로 전달하는 게이트웨이를 포함하는 것을 특징으로 한다.

[0023] 상기에서 게이트웨이는 사이버 보안 위협 모니터링 및 사고대응용 CAN-IDS 솔루션을 구비한 것을 특징으로

한다.

[0024] 상기에서 게이트웨이는,

[0025] 소프트웨어 업데이트 관리를 위한 리프로그래밍 수행 모듈;

[0026] 소프트웨어 업데이트를 관리하는 소프트웨어 업데이트 관리 모듈; 및

[0027] 소프트웨어 펌웨어를 저장하는 소프트웨어 펌웨어 저장소를 포함하며,

[0028] 상기 소프트웨어 펌웨어 저장소는 데이터 형태의 보안 키를 저장하는 것을 특징으로 한다.

[0029] 상기에서 게이트웨이의 업데이트 관리 모듈은,

[0030] 외부 보안 키 관리시스템에서 진단장비용 인증서를 발급받아 그 인증서 검증을 통해 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하는 것을 특징으로 한다.

[0031] 상기에서 제어기는,

[0032] 상기 게이트웨이를 통해 외부 장치의 접근 시 상기 외부 보안 키 관리시스템에서 제공한 인증서를 이용한 접근자의 인증을 통해 1차 보안 기능을 수행하고, 업데이트된 펌웨어의 유효성 검증을 통해 2차 보안 기능을 수행하는 것을 특징으로 한다.

발명의 효과

[0033] 본 발명에 따르면 다수의 제어기(전자제어장치)의 통신을 연결해주는 게이트웨이에서 암호화된 보안 키(인증서)를 이용하여 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한하도록 하여 차량 사이버보안시스템의 원가를 절감하도록 도모해주는 효과가 있다.

[0034] 또한, 본 발명에 따른 차량의 전자제어장치 간 또는 외부 장치와 차량의 전자제어장치의 통신을 연결해주는 게이트웨이에서 암호화된 보안 키를 이용하여 메시지의 허용 및 차단을 통제함으로써, 사이버 보안 애플리케이션이 없는 전자제어장치의 사이버 보안을 구현해주는 효과가 있다.

도면의 간단한 설명

[0035] 도 1은 자동차 보안 위협에 대한 공격 경로 예시도,

도 2는 씨드 엔 키 방식이 사용자 인증과정 예시도,

도 3은 기존 하드웨어 기반의 자동차 사이버 보안 모듈의 예시도,

도 4는 본 발명에 따른 하드웨어 기반의 차량 사이버보안시스템의 구성도,

도 5는 본 발명에 따른 하드웨어 기반의 차량 사이버보안시스템이 무선 통신(OTA)에 적용된 예시도,

도 6은 본 발명에 따른 하드웨어 기반의 차량 사이버보안시스템이 진단 포트(OBD 포트)를 통해 유선으로 적용된 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0036] 이하 본 발명의 바람직한 실시 예에 따른 하드웨어 기반의 차량 사이버보안시스템을 첨부된 도면을 참조하여 상세하게 설명한다.

[0037] 이하에서 설명되는 본 발명에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 안되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념으로 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다.

[0038] 따라서 본 명세서에 기재된 실시 예와 도면에 도시된 구성은 본 발명의 바람직한 실시 예에 불과할 뿐이고, 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원 시점에서 이들을 대체할 수 있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해하여야 한다.

[0039] 도 4는 본 발명의 바람직한 실시 예에 따른 하드웨어 기반의 차량 사이버보안시스템의 구성도이고, 도 5는 본 발명에 따른 하드웨어 기반의 차량 사이버보안시스템이 무선 통신(OTA)에 적용된 예시 도이며, 도 6은 본 발명에 따른 하드웨어 기반의 차량 사이버보안시스템이 진단 포트(OBD 포트)를 통해 유선으로 적용된 예시도로서,

진단 장비(110), 진단 포트(OBD 포트)(120), 게이트웨이(130), 복수의 전자제어장치(141 - 141+N), 커넥티비티 장비(160)를 포함할 수 있다.

[0040] 진단 장비(110)는 외부의 보안 키 관리 시스템과 연결되어 차량 진단 등을 수행하는 역할을 한다.

[0041] 진단 포트(120)는 외부의 보안 키 관리 시스템에서 진단 장비(110)를 통해 유선으로 전송된 보안 키를 게이트웨이(130)에 전달하며, 진단을 위한 메시지 등을 상기 게이트웨이(130)를 통해 전자제어장치에 전달하는 역할을 한다.

[0042] 커넥티비티 장비(160)는 외부의 보안 키 관리 시스템(150)으로부터 무선으로 전송된 보안 키를 수신하여 상기 게이트웨이(130)에 전달하거나 외부 장치와 무선 연결을 위한 역할을 한다. 이러한 커넥티비티 장비(160)는 외부의 장치와 무선 통신을 위한 LTE 모뎀, 서비스를 수행하는 서비스 모듈을 포함할 수 있다.

[0043] 게이트웨이(130)는 상기 진단 포트(120) 및/또는 커넥티비티 장비(160)와 접속되며, 하나 이상의 제어기(ECU)(141 - 141+N)를 통신으로 연결하며, 데이터 형태의 보안 키를 별도의 저장 매체에 저장하고, 상기 진단 포트(120) 또는 커넥티비티 장비(160)를 통해 업데이트 데이터 수신 시 상기 별도의 저장매체에 저장한 보안 키와 상기 외부 보안 키 관리 시스템에서 할당받은 보안 키 정보를 비교하여 일치하는 경우에만 업데이트 데이터를 연결된 전자제어장치(ECU)로 전달하는 역할을 한다.

[0044] 이러한 게이트웨이(130)는 사이버 보안 위협 모니터링 및 사고대응용 CAN-IDS 솔루션(134)을 구비할 수 있다.

[0045] 또한, 상기 게이트웨이(130)는 소프트웨어 업데이트를 수행하는 리프로그래밍 수행 모듈(131), 소프트웨어 업데이트를 관리하는 소프트웨어 업데이트 관리 모듈(132), 및 소프트웨어(SW) 펌웨어(F/W)를 저장하는 소프트웨어 펌웨어 저장소(eMMC)(133)를 포함하며, 상기 소프트웨어 펌웨어 저장소(133)는 데이터 형태의 보안 키를 저장할 수 있다.

[0046] 상기 게이트웨이(130)의 소프트웨어 업데이트 관리 모듈(132)은 외부 보안 키 관리시스템에서 진단장비용 인증서를 발급받아 그 인증서 검증을 통해 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한할 수 있다.

[0047] 제어기인 전자제어장치(141 - 141+N)는 대응하게 연결된 장치를 제어하며, 진단 요청에 따라 진단을 수행하고 진단 수행 결과를 제공하거나, 외부 장치(서버)와 접속하여 데이터를 송수신하며, 업데이트 펌웨어를 이용하여 업데이트를 수행하는 역할을 한다.

[0048] 이러한 전자제어장치인 제어기는 상기 게이트웨이(130)를 통해 외부 장치의 접근 시 상기 외부 보안 키 관리시스템(150)에서 제공한 인증서를 이용한 접근자의 인증을 통해 1차 보안 기능을 수행하고, 업데이트된 펌웨어의 유효성 검증을 통해 2차 보안 기능을 수행할 수 있다.

[0049] 이와 같이 구성된 본 발명의 바람직한 실시 예에 따른 하드웨어 기반의 차량 사이버보안시스템의 동작을 구체적으로 설명하면 다음과 같다.

[0050] 먼저, 사이버 보안을 위해, 보안키 관리 시스템(150)에서는 사이버 보안을 위한 인증서(보안 키)를 발급하여 진단 장비(110), 진단 포트(120)를 통해 게이트웨이(130)에 전달하거나, 무선 이동 통신을 통해 커넥티비티 장비(160)를 통해 게이트웨이(CGW)(130)에 전달한다.

[0051] 게이트웨이(130)는 진단 포트(120) 또는 커넥티비티 장비(160)를 통해 전달되는 사이버 보안을 위한 인증서인 보안 키를 데이터 형태로 수신하여 소프트웨어 펌웨어 저장소(133)에 저장하며, 아울러 사이버 보안 애플리케이션이 구비된 제어기(ECU)에도 해당 인증서를 전달한다.

[0052] 이후, 진단 포트(120)를 통해 유선으로 특정 제어기의 펌웨어 업데이트 파일이 전달되거나 외부 장치가 접근을 하면, 소프트웨어 업데이트 관리모듈(132)에서 소프트웨어 펌웨어 저장소(eMMC)(133)에 별도로 저장한 암호화된 보안 키(인증서)를 이용하여 접근자를 인증한다.

[0053] 이때, 수신된 제어기 업데이트 데이터에 포함된 외부 보안키 관리 시스템(150)에서 할당받은 보안 키와 상기 소프트웨어 펌웨어 저장소(133)에 별도로 저장한 보안 키의 정보가 일치하면, 수신한 업데이트 파일을 대응하는 제어기(예를 들어, 141)에 전달한다.

[0054] 만약, 수신된 제어기 업데이트 데이터에 포함된 외부 보안키 관리 시스템(150)에서 할당받은 보안 키와 상기 소프트웨어 펌웨어 저장소(133)에 별도로 저장한 보안 키의 정보가 일치하지 않으면, 수신한 업데이트 데이터가 유효하지 않은 것으로 판단을 하고, 메시지를 차단한다.

[0055] 이로써 사이버 보안 애플리케이션이 설치되지 않은 제어기에 허가받지 않은 사용자가 접근하여 탑승자의 안전에 치명적이거나 심각한 결과를 초래하거나 불법적인 데이터 튜닝과 변경 등을 하는 사이버 해킹을 게이트웨이에서 차단할 수 있다.

[0056] 게이트웨이에서 사이버 보안 기능을 수행함으로써, 기존 사이버 보안 애플리케이션이 설치되지 않은 제어기(전자제어장치)의 사이버 보안 기능을 향상함으로써, 사이버 보안 애플리케이션이 설치된 제어기로 교체하지 않고서도 사이버 보안 문제를 해결할 수 있어, 제어기 교체에 따른 비용을 해결할 수 있다.

[0057] 한편, 무선을 통해 외부 장치가 커넥티비티 장비(160)를 통해 차량 제어기에 접근하는 경우, 게이트웨이(130)에 설치된 CAN-IDS 솔루션(134)을 이용하여 사이버 보안 위협 모니터링 및 사고대응을 1차적으로 할 수 있다.

[0058] 그러나 이러한 사이버 보안 위협 모니터링 및 사고 대응 기능을 통해서도 외부 사이버 보안 위협에 대응하지 못하여, 업데이트 데이터나 해킹을 위한 외부 장치의 데이터가 특정 제어기(예를 들어, 141+N)에 전송된 경우, 제어기(141+N)는 업데이트 파일을 설치하기 이전에 상기 외부 보안 키 관리시스템(150)에서 제공한 인증서를 이용하여 접근자의 인증을 통해 1차 보안 기능을 수행한다. 인증되지 않은 접근자일 경우, 업데이트 파일을 설치하지 않거나 폐기하여 사이버 보안 기능을 수행한다.

[0059] 아울러 1차 보안 기능을 통과하여 업데이트 파일이 설치된 경우에는, 다시 2차적으로 업데이트된 펌웨어의 유효성 검증을 통해 2차 보안 기능을 수행한다.

[0060] 이로써 사이버 보안의 신뢰성을 극대화할 수 있다.

[0061] 이상 상술한 본 발명에 따르면 차량의 전자제어장치(ECU) 간 네트워크 장치에서 특정 제어장치에만 하드웨어 기반의 보안모듈이 구성된 상태에서, 게이트웨이에서 암호화된 보안 키(인증서)를 이용하여 제어장치 간 진단이나 보안 Flash를 위한 통신을 제한함으로써, 사이버 보안 애플리케이션이 설치되지 않은 제어기의 사이버 보안을 도모할 수 있어, 차량 사이버보안시스템의 원가를 절감할 수 있다.

[0062] 이상 본 발명자에 의해서 이루어진 발명을 상기 실시 예에 따라 구체적으로 설명하였지만, 본 발명은 상기 실시 예에 한정되는 것은 아니고 그 요지를 이탈하지 않는 범위에서 여러 가지로 변경 가능한 것은 이 기술분야에서 통상의 지식을 가진 자에게 자명하다.

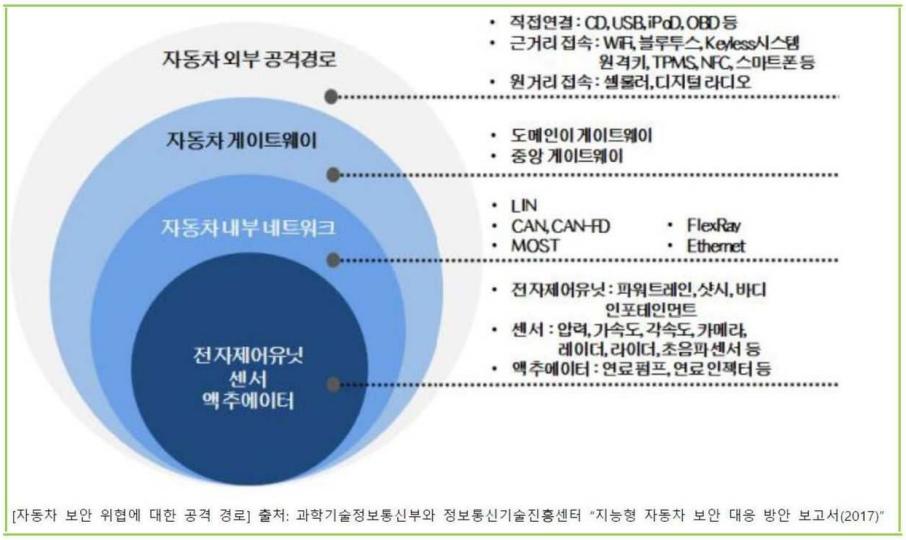
부호의 설명

[0063]

110: 진단 장비
120: 진단 포트(OBD 포트)
130: 게이트웨이
131: 리프로그래밍 수행 모듈
132: 소프트웨어 업데이트 관리모듈
133: 소프트웨어 펌웨어 저장소
141 - 141+N: 제어기(전자제어장치)
150: 보안키 관리 시스템
160: 커넥티비티 장비

도면

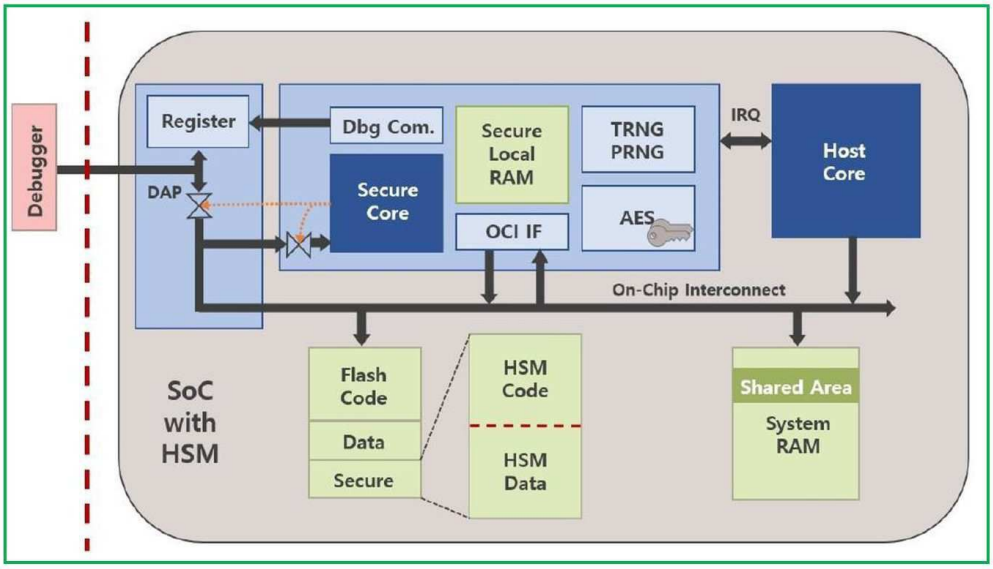
도면1



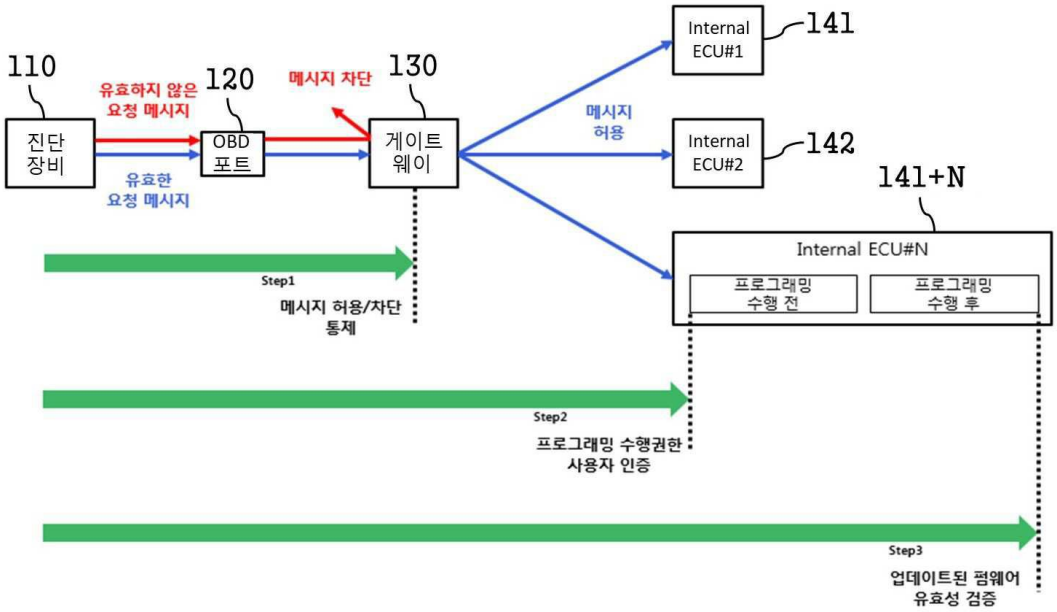
[자동차 보안 위협에 대한 공격 경로] 출처: 과학기술정보통신부와 정보통신기술진흥센터 "지능형 자동차 보안 대응 방안 보고서(2017)"

도면2

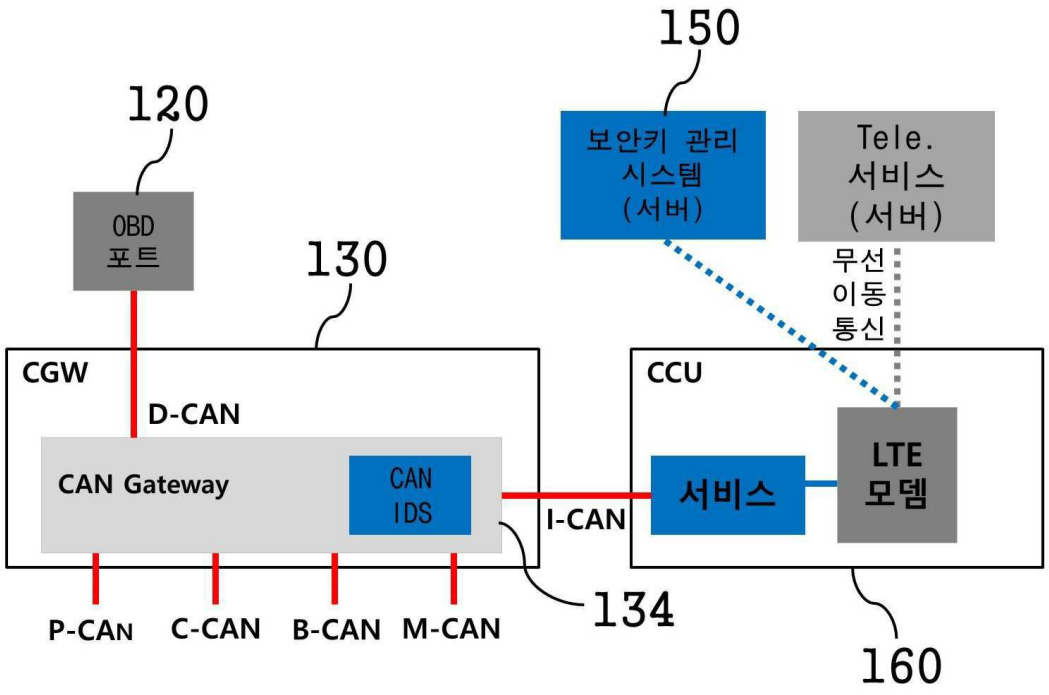
도면3



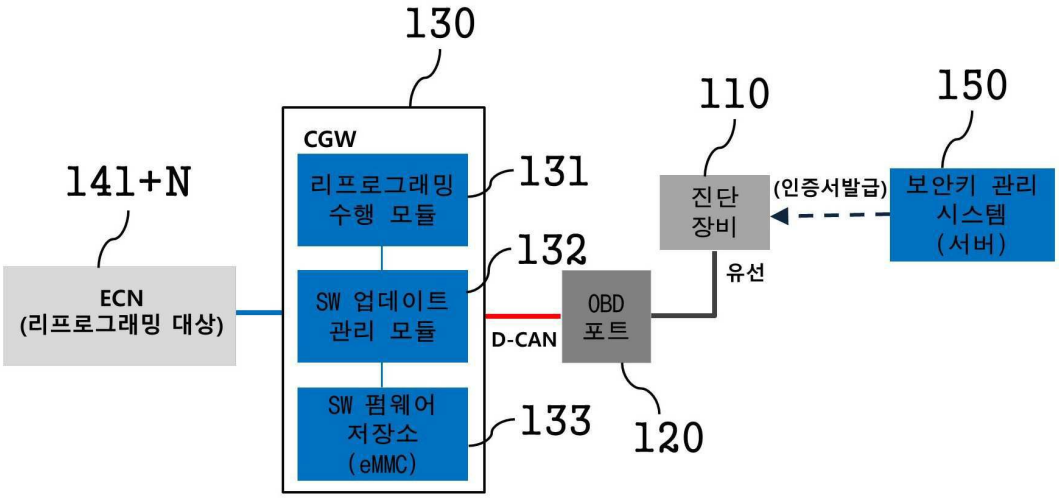
도면4


110
진단 장비
유효하지 않은 요청 메시지
유효한 요청 메시지
120
OBD 포트
메시지 차단
130
게이트 웨이
메시지 허용
Internal ECU#1
141
Internal ECU#2
142
141+N
Internal ECU#N
프로그래밍 수행 전
프로그래밍 수행 후
Step1
메시지 허용/차단 통제
Step2
프로그래밍 수행권한 사용자 인증
Step3
업데이트된 펌웨어 유효성 검증

도면5


150
보안키 관리 시스템 (서버)
Tele. 서비스 (서버)
120
OBD 포트
130
무선 이동 통신
CGW
D-CAN
CAN Gateway
CAN IDS
I-CAN
CCU
서비스
LTE 모뎀
P-CAN
C-CAN
B-CAN
M-CAN
134
160

도면6


130
CGW
141+N
ECN
(리프로그래밍 대상)
리프로그래밍
수행 모듈
131
SW 업데이트
관리 모듈
132
SW 펌웨어
저장소
(eMMC)
133
D-CAN
OBD
포트
120
110
진단
장비
(인증서발급)
150
보안키 관리
시스템
(서버)
유선