

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호

(43) 국제공개일
2019년 6월 27일 (27.06.2019) WIPO | PCT

WO 2019/124976 A1

- (51) 국제특허분류:
H04L 29/06 (2006.01) H04L 12/40 (2006.01)
- (21) 국제출원번호: PCT/KR2018/016243
- (22) 국제출원일: 2018년 12월 19일 (19.12.2018)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
62/607,595 2017년 12월 19일 (19.12.2017) US
- (71) 출원인: 현대자동차주식회사 (HYUNDAI MOTOR COMPANY) [KR/KR]; 06797 서울시 서초구 헌릉로 12, Seoul (KR). 기아자동차주식회사 (KIA MOTORS CORPORATION) [KR/KR]; 06797 서울시 서초구 헌릉로 12, Seoul (KR).
- (72) 발명자: 박승욱 (PARK, Seung Wook); 06797 서울시 서초구 헌릉로 12, Seoul (KR). 김세일 (KIM, Seil); 06797 서울시 서초구 헌릉로 12, Seoul (KR). 조아람 (CHO, Aram); 06797 서울시 서초구 헌릉로 12, Seoul (KR).
- (74) 대리인: 이철희 (LEE, Chulhee); 06229 서울시 강남구 도곡로33길 26, 베리타스빌딩 2-4층, Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT,

AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

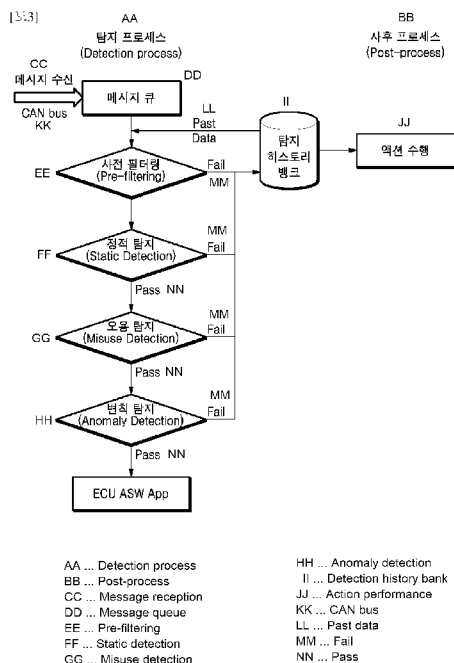
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(54) Title: SYSTEM AND METHOD FOR PROVIDING SECURE IN-VEHICLE NETWORK

(54) 발명의 명칭: 차량 내 네트워크에 보안을 제공하는 시스템 및 방법



(57) Abstract: The present invention pertains to a system and a method for providing a secure in-vehicle network. According to an aspect of the present invention, methods for efficiently operating a plurality of detection techniques are proposed in order to reduce the required system resources while maintaining strength with respect to detection of malicious messages.

(57) 요약서: 본 발명은 차량 내 네트워크에 보안을 제공하는 시스템 및 방법과 관련되어 있다. 본 발명의 일 측면에 따르면, 악의적 메시지 탐지에 대한 강인성을 유지하면서도 요구되는 시스템 자원을 줄이기 위해, 복수의 탐지 기법들을 효율적인 운용하는 방법들을 제안한다.

WO 2019/124976 A1

명세서

발명의 명칭: 차량 내 네트워크에 보안을 제공하는 시스템 및 방법 기술분야

- [1] 본 발명은 차량 내 네트워크에 보안을 제공하는 것과 관련되어 있다.

배경기술

- [2] 이 부분에 기술된 내용은 단순히 본 발명에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.
- [3] 침입 탐지 시스템(Intrusion Detection System: IDS)과 침입 방지 시스템 (Intrusion Protection System: IPS)은 네트워크 보안에 널리 사용되어 왔다. IDS는 네트워크 활동을 모니터링하고 의심스러운 행동을 감지한다. IPS는 탐지된 침입에 대응(예컨대 시스템에 영향을 줄 수 있는 신호를 차단)할 수 있는 기능 혹은 능력을 갖춘 시스템을 일컫는다. 대개 IDS와 IPS는 함께 사용되며, 이러한 시스템은 IDPS(Intrusion Detection and Prevention System)라고 지칭된다.
- [4] 차량에 탑재된 전자 제어 장치(ECU)들의 수가 크게 증가하고, 무선 네트워크를 통해 차량이 외부 네트워크와 연결됨에 따라, 차량의 내부 네트워크의 보안 위협을 탐지하고 대응하기 위해 IDS 혹은 IDPS가 도입되고 있는 추세이다.

발명의 상세한 설명

기술적 과제

- [5] 본 발명은 악의적 메시지 탐지에 대한 강인성을 유지하면서도 요구되는 시스템 자원을 줄일 수 있는 복수의 탐지 기법들의 효율적인 운용 방법들을 제안한다. 또한, 본 발명은 AUTOSAR(Automotive Open System Architecture) 기반의 소프트웨어 아키텍처에 IDS 혹은 IDPS를 탑재하기 위한 다양한 방법들을 제안한다.

과제 해결 수단

- [6] 본 발명의 일 측면에 의하면, 차량 내 네트워크로부터 수집된 새로운 네트워크 메시지가 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지인지 여부를 판단하는 단계; 및 상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지이면, 상기 새로운 네트워크 메시지에 대해, 복수의 탐지 기법의 적용을 스킵하고, 곧바로 상기 새로운 네트워크 메시지를 보안 위협 메시지로 간주하는 단계를 포함하는, 차량 내 네트워크에 보안을 제공하는 방법을 제공한다. 이에 따르면, 불필요한 탐지 프로세스를 스킵하여 전체 연산속도를 높임으로써 전체적인 탐지 효율을 향상시킬 수 있다.
- [7] 본 발명의 다른 측면에 의하면, 차량 내 네트워크로부터 수집되는 새로운 네트워크 메시지에 대해 적용할 복수의 탐지 기법들의 적용 순서를 결정하는 단계; 및 상기 새로운 네트워크 메시지에 대해, 상기 결정된 적용 순서에 따라 상기 복수의 탐지 기법들을 적용하여, 상기 새로운 네트워크 메시지가 보안 위협

메시지인지 여부를 결정하는 단계를 포함하는, 차량 내 네트워크에 보안을 제공하는 방법을 제공한다. 상기 복수의 탐지 기법들의 적용 순서는 상기 차량 내 네트워크로부터 기 수집된 적어도 하나의 네트워크 메시지에 대해 적용된 상기 복수의 탐지 기법들의 탐지 이력을 기초로 결정될 수 있다. 이에 따르면, 유사한 방식의 공격이 연속적으로 시도되는 경우에, 고정된 적용 순서를 사용하는 것에 비해, 빠르게 공격 메시지를 탐지할 수 있다.

- [8] 본 발명의 또 다른 측면에 의하면, 차량 내 네트워크로부터 수집된 네트워크 메시지에 대해, 복수의 탐지 기법들의 적용을 병렬적으로 개시하는 단계; 및 상기 복수의 탐지 기법들 중에서 어느 하나의 탐지 기법이 상기 수집된 네트워크 메시지를 보안 위협 메시지로 결정하는 것에 응답하여, 상기 수집된 네트워크 메시지에 대한 나머지 탐지 기법들의 적용을 중단하는 단계를 포함하는, 차량 내 네트워크에 보안을 제공하는 방법을 제공한다. 이에 따르면, 복수의 탐지 기법을 순차적으로 적용하는 것에 비해, 빠르게 탐지 절차를 완료할 수 있다.
- [9] 전술한 방법들은, 적어도 하나의 프로세서와 명령어들이 기록된 메모리를 포함하는 전자 장치에 의해 수행될 수 있다. 예컨대, 상기 명령어들은 상기 적어도 하나의 프로세서에 의해 실행될 때 상기 전자 장치로 하여금, 전술한 방법들을 수행하도록 한다.
- [10] 이와 같이, 제안된 방법들 및 전자 장치들에 따르면, 악의적 메시지 탐지에 대한 강인성은 유지하면서도 빠르게 공격 메시지를 탐지할 수 있고, 그에 따라 탐지에 필요한 시스템 자원을 줄일 수 있다.

도면의 간단한 설명

- [11] 도 1은 CAN 네트워크 상에서 IDS(혹은 IDPS)가 배치될 수 있는 위치들을 예시한 것이다.
- [12] 도 2는 IDPS의 예시적인 동작을 도시한 흐름도이다.
- [13] 도 3은 본 발명의 일 실시예에 따른, 히스토리 기반 탐지 프로세스 스킵 방법을 설명하기 위한 개념도이다.
- [14] 도 4는 본 발명의 일 실시예에 따른, 탐지 기법들의 적용 순서를 적응적으로 변경하는 기법의 일 예를 설명하기 위한 개념도이다.
- [15] 도 5는 본 발명의 일 실시예에 따른, 세 개의 상이한 탐지 기법들을 병렬적으로 적용하는 방법을 설명하기 위한 개념도이다.
- [16] 도 6은 본 발명의 일 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.
- [17] 도 7은 본 발명의 다른 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.
- [18] 도 8은 본 발명의 또 다른 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.
- [19] 도 9는 AUTOSAR 기반의 소프트웨어 아키텍처를 개략적으로 도시한

도면이다.

- [20] 도 10은 본 발명의 일 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [21] 도 11은 본 발명의 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [22] 도 12는 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [23] 도 13은 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [24] 도 14는 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [25] 도 15는 비트 스템핑(Bit Stumping)을 적용하기 위한 도 10의 소프트웨어 아키텍처의 변형예이다.

발명의 실시를 위한 형태

- [26] 이하, 본 발명의 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 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.
- [27] 또한, 본 발명의 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.
- [28]
- [29] 도 1은 CAN 네트워크 상에서 IDS(혹은 IDPS)가 배치될 수 있는 위치들(㉑, ㉒, ㉓, ㉔, ㉕)을 예시한 것이다. 센트럴 게이트웨이는 라우터 역할을 하는 센트럴 통신 노드이다. 센트럴 게이트웨이는 차량으로 들어오는 모든 데이터에 대한 게이트라고 볼 수 있다. 서브 게이트웨이는 파워 트레인, 샤시, 바디, 멀티미디어 등과 같은 특정 서브 시스템 도메인을 담당하는 로컬 통신 노드이다.
- [30] 각 위치 별 장단점은 다음과 같다.
- [31] ㉑ 센트럴 게이트웨이에 탑재: 외부와 모든 CAN 도메인이 연결되는 이곳에

IDPS를 설치하면, OBD 포트를 통해 CAN 네트워크로 들어오는 모든 공격을 탐지할 수 있다. 따라서 공격 의도를 가진 메시지를 미연에 파악할 수 있다. 그러나 너무 많은 데이터를 수집하면서, 내부 네트워크로 침입하려는 공격과 그렇지 않은 메시지를 구분하기 어렵기 때문에 공격에 효율적으로 대응하기 어렵다.

- [32] ㉑ 센트럴 게이트웨이 뒤: 센트럴 게이트웨이의 메시지 필터링을 거친 뒤의 메시지를 검사한다. ㉑를 지나기 전보다는 더 적은 수의, 그러나 더 강력한 의지를 가진 공격자를 탐지할 수 있다. 또한 CAN 백본망에 외부에서 직접 접근하여 악성 메시지를 주입하는 해킹을 탐지할 수 있다.
- [33] ㉒ 서버 게이트웨이에 탑재: 특정 CAN 도메인으로 송수신되는 CAN 메시지를 관리하는 곳에 IDPS를 설치하면, ㉑에서의 CAN 메시지와 특정 CAN 도메인에서 흐르고 있는 CAN 메시지 간의 불일치성을 쉽게 탐지할 수 있다. CAN 도메인 내부에서 다른 도메인으로 향하는 공격도 탐지할 수 있는 곳이므로 CAN 도메인 내부의 공격자도 일정 수준 이상 탐지할 수 있다.
- [34] ㉓ 서버 게이트웨이 뒤: 특정 악의적 메시지로 이중의 게이트웨이를 통과하여 시스템을 해킹하는 것은 쉽지 않다. 그러나 내부 제어기(ECU: Electronic Control Unit)가 공격자에 의해 손상되었거나 악의적 제어기가 교체되어 위장되었을 경우, 그리고 외부에서 직접 해당 CAN 버스에 연결한 경우 악의적인 메시지를 보내는 것이 여전히 가능하다. 따라서 본 설치 위치는 내부 제어기를 신뢰할 수 없어 제어기가 속한 특정 CAN 도메인의 네트워크 해킹을 감시하고자 할 때 설치할 수 있는 곳이다.
- [35] ㉔ 제어기에 탑재: 제어기는 네트워크상에 존재하는 모든 메시지를 수신하고 필요한 CAN 메시지의 ID를 확인하여 필요로 하는 메시지를 선택적으로 처리한다. 제어기는 제어기 외부에서 받은 CAN 상태 메시지와 명령 메시지의 컨텍스트를 분석한 뒤 구동한다. 이 때 제어기 외부와 내부 모두로부터 보호되어야 하기 때문에 높은 보안 수준을 필요로 한다. 제어기에 IDPS를 탑재하는 것은 제어기를 변조할 수 있는 매우 능력이 뛰어난 내부/외부 공격자로부터 제어기가 가진 중요 데이터의 손실이나 기능의 오동작을 막기 위함이다.
- [36] 도 2는 IDPS의 예시적인 동작을 도시한 흐름도이다.
- [37] IDPS는 차량의 시동이 켜지면 사전 프로세스(pre-process)를 수행하고, 그 후 차량 시동이 꺼질 때까지 탐지 프로세스(detection process)와 사후 프로세스(post-process)를 반복적으로 수행하도록 구성될 수 있다.
- [38] 사전 프로세스(pre-process)에서, IDPS가 재시작 되면 탐지 트리(detection tree)의 버전을 체크하고 현재 플래쉬 메모리에 저장된 IDPS 탐지 트리가 최신 버전이 아닐 경우, 예컨대, OTA 혹은 OBD 포트를 통해 다운 받은 최신 버전의 룰 셋으로 탐지 트리를 업데이트 한다. 이후 플래쉬 메모리에 저장된 암호화된 탐지 트리를 복호화하여 RAM 영역으로 로드한다. 사전 프로세스가 종료되면 IDPS의

실질적인 탐지 동작인 탐지 프로세스가 시작된다.

- [39] 탐지 프로세스(detection process)에서, IDPS는, 메시지 큐(Message Queue)에 새로운 CAN 메시지가 도착하면, 새로운 CAN 메시지가 보안 위협과 관련된 네트워크 메시지(이하 '보안 위협 메시지', '비정상 메시지', '악의적인 메시지', '공격 메시지', 혹은 '검사에 실패한 메시지'로도 지칭될 수 있음)인지 여부를 판단하기 위해, 정적 탐지(Static Detection), 오용 탐지(Misuse Detection), 및 변칙 탐지(Anomaly Detection) 기법을 순차적으로 수행할 수 있다. 각각의 기법에서는 다음과 같은 검사가 이루어진다.
- [40] 정적 탐지(Static Detection)는 메시지 ID, DLC(Data length code), 주기 등을 CAN 데이터베이스(CAN DB)에 명시된 값과 비교하여 CAN 메시지의 유효성을 검사하는 기법이다. 오용 탐지(Misuse Detection)는 차량 시스템의 취약점 분석을 통해 이미 알려진 공격 메시지를 탐지하는 기법으로서, 차량의 상태를 고려하지 않고 단순히 메시지 데이터의 내용이 악성 메시지 블랙리스트(Black List)로 분류될 경우 이를 탐지한다. 변칙 탐지(Anomaly Detection)는 차량의 상태를 기반하여 해당 메시지가 정상 메시지 범주 안에 있는 지 확인하는 기법으로서, 차량의 상태와 명령 메시지에 기반한 탐지 트리를 통해 이루어진다.
- [41] 사후 프로세스(post-process)에서는, CAN 메시지들에 대한 검사 결과에 따라 통과, 차단, 로깅(logging), 혹은 경고와 같은 액션이 취해진다. 예컨대, 탐지 로그가 원격 네트워크 상의 백-엔드 서버에 전송되도록, IDPS는, CAN 네트워크를 통해, 탐지 로그가 담긴 CAN 메시지를 원격 네트워크에 통신적으로 연결될 수 있는 게이트웨이 혹은 텔레매틱스 디바이스에 전달할 수 있다.
- [42] 전술한 침입 탐지 기법의 특성 및 장단점은 다음과 같다.
- [43] 정적 탐지(Static Detection)는 메시지의 ID, 메시지 길이, 메시지 전송 주기 등을 모니터링하여, 미리 정해놓은 규칙들과 비교하여 유효성 검사를 하는 기법이다. 따라서, 정적 탐지를 통해서 확인할 수 있는 것은 오직 제조사에서 미리 정하여 CAN DB에 저장해 놓은 '유효한 메시지 형식'에 맞는지의 유효성 검사뿐이다. 메시지 내에 들어 있는 악성 데이터 등은 탐지가 불가능하다.
- [44] 오용 탐지(Misuse Detection)는 시스템의 이미 알려진 취약점을 이용한 공격 방법 패턴이나 수단의 시그니처(signature)를 정의하고 그에 따른 트래픽의 비교를 통한 탐지 기법이다. 오용 탐지는 시그니처(signature) 기반의 탐지로도 불린다. 오용 탐지는 시스템의 자원을 적게 소모하고 탐지 확률이 높다는 장점이 있으나, 새로운 공격마다 새로운 시그니처를 정의해야 하므로 새로 출현한 공격에 대한 대처가 늦어질 수 있으며 많은 보안 인적 자원을 필요로 한다. 이 기법은 실제 공격을 놓칠 수 있는 거짓 음성(false negative; 2종 오류) 문제가 생길 수 있다.
- [45] 변칙 탐지(Anomaly Detection)는 네트워크 상에서의 일반적인 행동을 수집 및 분석하여 정상적인 패턴을 정의한 후 정상 패턴에서 일정한 임계치(threshold)를 벗어난 행동을 탐지하는 기법이다. 변칙 탐지는 프로파일(profile) 기반의

탐지으로도 불린다. 변칙 탐지의 경우 새로운 공격이 출현하였을 때에도 이러한 공격이 정상 패턴에서 벗어난 경우 탐지가 가능하며 오용 탐지 방법에 비해 보안 인적 자원의 비중이 적다. 그러나 많은 시스템 자원을 필요로 하며 설정된 임계치에 따라 거짓 양성(false positive, 1종 오류) 문제가 생길 수 있다.

- [46] 도 2의 예시된 동작에 따르면, 메시지 큐(Message Queue)에 쌓인 각 메시지는 세 가지 탐지 기법으로 구성된 탐지 프로세스(즉, 정적 탐지→오용 탐지→변칙 탐지)를 거치면서 그 메시지의 차단 혹은 통과가 결정된다. 또한, 정상적인 CAN 메시지 역시 세 가지 기법으로 구성된 탐지 프로세스를 거친 후에야 비로소 ECU의 응용 소프트웨어로 전달되게 된다.

[47]

- [48] 본 발명은 악의적 메시지 탐지에 대한 강인성을 유지하면서도 요구되는 시스템 자원을 줄이기 위해 복수의 탐지 기법들을 효율적인 운용하는 여러 방법들을 제안한다.

[49] 제 1 실시예 - 히스토리 기반 탐지 프로세스 스킵 방법

- [50] 본 방법은 차량 네트워크로부터 수집된 새로운 메시지가 이전에 수행된 탐지 프로세스를 통과하지 못한 보안 위협 메시지와 동일 또는 유사한 메시지일 경우에, 복수의 탐지 기법들의 적용을 스킵함으로써, 차단 결정과 차단 액션이 빠르게 수행될 수 있게 하는 것이다.

- [51] 도 3은 본 발명의 일 실시예에 따른, 히스토리 기반 탐지 프로세스 스킵 방법을 설명하기 위한 개념도이다.

- [52] IDPS는 정적 탐지, 오용 탐지, 및 변칙 탐지 단계를 거치면서 보안 위협 메시지로 결정된 메시지들(즉, failed messages)에 대한 기록이 저장되는 데이터베이스인 '탐지 히스토리 뱅크(detection history bank)'를 운용한다. IDPS는 새롭게 들어오는 메시지들에 대해 기존의 세 단계로 구성된 탐지 프로세스를 수행하기에 앞서, 탐지 히스토리 뱅크를 이용하여 사전 필터링(pre-filtering)을 수행한다.

- [53] 사전 필터링에서, 새로운 메시지를 탐지 히스토리 뱅크에 저장되어 있는 기록들과 비교하여, 새로운 메시지가 이전에 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지인지 판단한다. 새로운 메시지가 이전에 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지이면, 그 새로운 메시지에 대해서는 기존의 세 단계로 구성된 탐지 프로세스의 수행을 스킵하고, 그 새로운 메시지에 대한 기록을 탐지 히스토리 뱅크에 저장한 후 바로 차단 액션 단계로 진입한다. 즉, 새로운 메시지가 이전에 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지이면, 그 새로운 메시지는 보안 위협과 관련된 네트워크 메시지로 간주된다. 따라서 불필요한 탐지 기법들의 적용을 스킵하여 전체 연산속도를 높임으로써 시스템 전체의 스루풋(throughput)을 향상시킬 수 있다. 이하에서 설명하는 바와 같이, 메시지들이 동일하다는 의미는 비트 레벨에서 메시지 프레임 전체가 서로 동일함을 가리키며, 메시지들이 유사하다는 의미는 비트

레벨에서 메시지 프레임 구성하는 일부 필드가 동일함을 가리키는 것으로 이해될 수 있다.

[54] 보안 위협 메시지들에 대한 기록을 탐지 히스토리 뱅크에 저장하는 데에는 다양한 방식이 적용될 수 있다. 일 예로서, 저장 공간이 충분한 경우에 적합한 방식으로, 보안 위협 메시지의 프레임 전체를 탐지 히스토리 뱅크에 저장할 수 있다. 이 경우, 사전 필터링 단계에서는 새롭게 들어온 메시지와 비교 시 비트스트림 전체를 비교할 수도 있고, 프레임 내의 데이터 필드(data field), 중재 필드(arbitration field), 제어 필드(control field) 등 일부 필드를 선별적으로 비교할 수도 있다. 다른 예로서, 보안 위협 메시지의 프레임 내의 데이터 필드(data field), 중재 필드(arbitration field), 제어 필드(control field) 등 일부 필드만을 선별적으로 히스토리 뱅크에 저장할 수도 있다.

[55] 또한, 검색 효율성을 높이기 위해서, 탐지 히스토리 뱅크는 다음과 같이 운용될 수 있다. 예컨대, 탐지 히스토리 뱅크에 저장된 보안 위협 메시지마다 고유의 카운터(counter)가 할당될 수 있다. 새롭게 탐지된 보안 위협 메시지가 이미 히스토리 뱅크에 저장된 메시지와 동일하거나 유사할 때마다 그 메시지의 카운터는 1씩 증가된다. 탐지 히스토리 뱅크에서 메시지들은 카운터 값을 기준으로 내림차순으로 정렬될 수 있다. 따라서, 탐지 히스토리 뱅크에는, 차량 네트워크에 자주 출현하는 보안 위협 메시지에 대한 기록이 상위에, 가끔 출현하는 보안 위협 메시지에 대한 기록이 하위에 위치하게 된다. 이는 사전 필터링에서 탐지 히스토리 뱅크에 저장된 기록들에 대한 접근 속도를 향상시킨다.

[56]

[57] 제 2 실시예 - 시간적 연관성 기반 적응적 탐지

[58] 악의적인 공격은 시간에 따라 다른 공격 방식으로 시도되기 보다는, 일반적으로 유사한 방식의 공격이 연속적으로 시도될 가능성이 높다. 따라서, 전술한 세 가지 탐지 기법 중에서 어떤 탐지 기법이 공격 메시지를 탐지하였다면, 그 탐지 기법은 그 이후에 연이어 시도되는 공격 메시지들에 대해서도 탐지에 성공할 가능성이 높다. 이러한 시간적 연관성에 기반하여, 적응적으로 탐지 기법들의 적용 순서를 변경하는 기법을 제안한다.

[59] 도 4는 본 발명의 일 실시예에 따른 탐지 기법들의 적용 순서를 적응적으로 변경하는 기법의 일 예를 설명하기 위한 개념도이다. 도 4를 참조하면, $t=t_0$ 에서 메시지 큐로부터 출력된 제1메시지에 대해 "정적 탐지→오용 탐지→변칙 탐지" 순으로 탐지 절차가 수행된다. 제1메시지가 오용 탐지 단계에서 공격 메시지로 탐지되었다고 가정하자. 그러면 $t=t_0+1$ 에서 메시지 큐로부터 출력된 제2메시지에 대해서는 오용 탐지 기법이 정적 탐지 기법보다 먼저 적용된다. 만약 $t=t_0+1$ 에서 제2메시지가 변칙 탐지 단계에서 공격 메시지가 탐지되었다면, $t=t_0+2$ 에서 메시지 큐로부터 출력된 제3메시지에 대해 변칙 탐지 기법이 정적 탐지 기법과 그 적용 순서를 서로 자리바꿈하게 된다.

[60] 도 4의 예시에서는 이전 타이밍에서 보안 위협 메시지를 탐지한 기법에만 의존하여 탐지 기법들의 적용 순서가 뒤바뀌는 방식을 예로 들었지만, 각 탐지 기법마다 카운트를 할당하고, 어떤 기법에서 탐지가 성공할 때마다 관련된 카운터를 증가시키고, 누적된 카운터의 값에 따라 내림차순으로 탐지 기법들의 적용 순서를 정렬하는 방법도 가능하다.

[61]

[62] 제 3 실시예 - 병렬 프로세스 탐지 방법

[63] 본 방법은 복수의 탐지 기법들을 순차적으로 적용하는 대신에 병렬적으로 적용하는 것이다. 즉, 병렬 프로세싱을 통해 탐지 속도를 개선한다.

[64] 도 5는 본 발명의 일 실시예에 따른, 세 개의 상이한 탐지 기법들을 병렬적으로 적용하는 방법을 설명하기 위한 개념도이다. 도 5를 참조하면, 서로 상이한 탐지 기법들을 사용하는 세 개의 스레드(thread)가 동시에(concurrently) 실행되며, 메시지 큐에 저장되어 있던 CAN 메시지는 세 개의 스레드에 동시에 입력된다. 이로써 CAN 메시지에 대해 세 개의 상이한 탐지 기법들이 병렬적으로 적용된다. 도 5의 예시에서, 스레드 1는 정적 탐지를 수행하며, 스레드 2는 오용 탐지를 수행하며, 스레드 3는 변칙 탐지를 수행한다.

[65] 모든 스레드의 탐지 기법을 통과하면, CAN 메시지는 ECU의 응용 소프트웨어 컴포넌트로 전달된다. 어느 하나의 스레드의 탐지 기법이라도 통과하는 데 실패하면, CAN 메시지는 ECU의 응용 소프트웨어 컴포넌트로의 전달이 차단될 수 있다.

[66] 세 개의 스레드는 서로 상이한 탐지 기법을 사용하는 바, 프로세싱 속도 역시 서로 상이할 수 있다. 이에, 어느 하나의 스레드라도 먼저 fail이라는 결과가 나오면(즉, CAN 메시지가 어느 하나의 스레드의 탐지 기법이라도 통과하는 데 실패하면), 리소스를 낭비하지 않기 위해, 다른 스레드들의 동작을 중지시키고 바로 후처리(post process) 단계로 진입할 수 있도록 설계되는 것이 바람직하다. 이를 위해, 스레드들간에는 다른 스레드를 중지시키기 위한 시그널링, 즉 인터럽트 신호(interrupt signal)의 전송을 위한 채널이 제공될 수 있다.

[67] 세 개의 스레드는 처리하는 CAN 메시지의 'pass' 또는 'fail'을 알리는 파라미터(혹은 지시자)를 사용할 수 있다. 세 개의 스레드는 메시지 큐로부터 CAN 메시지가 입력되면, 파라미터 P1, P2, P3를 모두 0으로 설정할 수 있다. 각 스레드는, CAN 메시지가 자신의 탐지 기법을 통과하면, 파라미터 Px를 각각 1로 설정할 수 있다. 이후 모든 스레드가 종료된 후 모든 파라미터 Px값이 1일 경우에만 ECU의 응용 소프트웨어 컴포넌트로 CAN 메시지를 전달하게 될 수 있다.

[68] 이와 같이 CAN 메시지에 서로 상이한 기법들을 병렬적으로 적용함으로써, 도 2에 예시된 순차적인 적용 방식에 비해 전체 탐지 프로세스를 빠르게 완료할 수 있으며, 공격 메시지에 대한 빠른 대응이 가능하다.

[69]

- [70] 이하 도 6 내지 도 9를 참조하여, 전술한 방법들을 채용한 IDS 혹은 IDPS의 동작 방법들을 설명한다.
- [71] 도 6은 본 발명의 일 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.
- [72] 도 6에 도시된 바와 같이, IDS는 차량 내 네트워크로부터 수집된 새로운 네트워크 메시지가 보안 위협과 관련된 것으로 기 탐지된 네트워크 메시지와 동일 혹은 유사한 메시지인지 여부를 판단한다(S610). 이를 위해, IDS는, 기 탐지된 보안 위협 메시지를 식별하는 정보를 기록한 데이터베이스를 조회하여, 새로운 네트워크 메시지가 기 탐지된 보안 위협 메시지를 식별하는 정보에 상응하는 정보를 가지고 있는지 여부를 판단할 수 있다. 기 탐지된 보안 위협 메시지를 식별하는 정보는 보안 위협 메시지의 프레임 전체 또는 프레임의 일부 필드일 수 있다.
- [73] 새로운 네트워크 메시지가 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지가 아니면(S620에서 '아니오'), IDS는, 새로운 네트워크 메시지에 대해 복수의 탐지 기법들을 적용하여, 새로운 네트워크 메시지가 보안 위협과 관련된 네트워크 메시지인지 여부를 결정한다(S630). 복수의 탐지 기법들은 정적 탐지, 오용 탐지, 및 변칙 탐지를 포함한다.
- [74] 새로운 네트워크 메시지가 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지이면(S620에서 '예'), IDS는, 새로운 네트워크 메시지에 대해, 상기 복수의 탐지 기법의 적용을 스킵하고, 곧바로 새로운 네트워크 메시지를 보안 위협과 관련된 네트워크 메시지로 결정(간주)한다(S640).
- [75] 도 7은 본 발명의 다른 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.
- [76] 도 7을 참조하면, IDS는 차량 내 네트워크로부터 수집된 네트워크 메시지들 중에서 보안 위협과 관련된 네트워크 메시지의 탐지에 성공한 탐지 성공 이력을 기초로, 차량 내 네트워크로부터 수집되는 새로운 네트워크 메시지에 대해 적용할 복수의 탐지 기법들의 적용 순서를 결정한다(S710). 복수의 탐지 기법들은 정적 탐지, 오용 탐지, 및 변칙 탐지를 포함한다. IDS는 보안 위협과 관련된 네트워크 메시지를 탐지하는 데에 성공한 탐지 기법이 다른 탐지 기법들에 비해 우선 적용되도록 복수의 탐지 기법들의 적용 순서를 변경할 수 있다. IDS는, 각 탐지 기법 별로, 보안 위협과 관련된 네트워크 메시지를 탐지하는 데 성공한 누적 횟수를 카운트하고, 각 탐지 기법별 누적 횟수의 내림차순으로 탐지 기법들을 적용순서를 변경할 수 있다.
- [77] IDS는, 차량 내 네트워크로부터 수집되는 새로운 네트워크 메시지에 대해, 결정된 적용 순서에 따라 상기 탐지 기법들을 적용하여, 새로운 네트워크 메시지가 보안 위협과 관련된 네트워크 메시지인지 여부를 결정한다(S720).
- [78] 도 8은 본 발명의 또 다른 실시예에 따른 IDS(혹은 IDPS)의 동작 방법을 도시한 흐름도이다.

- [79] IDS는, 차량 내 네트워크로부터 수집된 네트워크 메시지에 대해, 복수의 탐지 기법들의 적용을 병렬적으로 개시한다(S810). 이는, 일 예로서, 서로 상이한 탐지 기법들을 사용하는 복수의 스레드(thread)들을 동시에(concurrently) 실행하고, 수집된 네트워크 메시지를 복수의 스레드에 각각 입력함으로써 달성될 수 있다. 복수의 탐지 기법들은 정적 탐지, 오용 탐지, 및 변칙 탐지를 포함한다.
- [80] 병렬적으로 적용된 복수의 탐지 기법들 중에서 어느 하나의 탐지 기법이 수집된 네트워크 메시지를 보안 위협과 관련된 네트워크 메시지로 결정하는 것에 응답하여, IDS는 수집된 네트워크 메시지에 대한 나머지 탐지 기법들의 적용을 중단한다(S820). 이를 위해, 일 예로서, 수집된 네트워크 메시지를 보안 위협과 관련된 네트워크 메시지로 결정한 스레드는 다른 스레드들에게 인터럽트 신호를 전송하고, 다른 스레드들은 인터럽트 신호의 수신에 응답하여 자신의 실행을 종료한다.
- [81] 상기 복수의 탐지 기법들 모두가 상기 네트워크 메시지를 보안 위협과 관련된 네트워크 메시지가 아니라고 결정하는 것에 응답하여, IDS는 상기 네트워크 메시지가 애플리케이션 영역으로 전달되는 것을 허용할 수 있다.
- [82]
- [83] 이하에서는, 위와 같은 IDPS 혹은 IDS를 AUTOSAR (Automotive Open System Architecture) 기반의 소프트웨어 아키텍처를 가지는 전자 제어 장치(Electronic Control Unit: ECU)에 구현하기 위한 다양한 방법들을 기술한다.
- [84] 먼저, 도 9를 참조하여, ECU의 AUTOSAR 기반의 소프트웨어 아키텍처를 간략히 살펴본다. 도 9는 AUTOSAR 기반의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.
- [85] AUTOSAR의 소프트웨어 아키텍처는 크게 응용 소프트웨어(Application Software: ASW) 계층, 런-타임 환경(Run Time Environment: RTE) 및 기본 소프트웨어(Basic Software: BSW) 계층으로 구분된 계층화된 구조를 가진다. 즉, RTE 개념을 도입하여 응용 소프트웨어와 하드웨어 관련 소프트웨어인 BSW를 분리함으로써, 하드웨어에 독립적인 응용 소프트웨어를 개발할 수 있게 한다. 특히, BSW는 서비스 계층(Services Layer), ECU 추상화 계층(ECU Abstraction Layer: EAL), 마이크로컨트롤러 추상화 계층(Microcontroller Abstraction Layer: MCAL), CDD(Complex Device Driver) 계층으로 세분화되어 구성된다.
- [86] Service 계층은 메모리, 통신 네트워크, 시스템 등의 서비스 기능을 수행하는 모듈들이 존재한다. 통신 네트워크 서비스 측면에서, 하부의 통신 하드웨어에 대한 의존성이 제거한 통일된 인터페이스를 제공하기 위해, CAN/LIN/FlexRay 통신 네트워크에 대한 NM(Network manager), SM(State Manager), TP(Transport), DCOM(Diagnostic Communication Manager), COM(Communication), PDU Router(PDUR) 등의 모듈들이 존재한다. 특히 메시지들로 구성된 신호들의 라우팅을 담당하는 PDUR 상위에 COM(Communication) 모듈이 존재하고 이는 RTE에 통일된 통신 방식을 제공한다.

- [87] MCAL 영역은, 하드웨어 의존성이 가진 소프트웨어 모듈들로서, OSI의 데이터 링크 계층의 통신 드라이버, ADC, PWM, DIO 등의 아날로그 디지털 I/O 드라이버, EEPROM, Flash 등의 메모리 드라이버, 주변장치 마이크로 컨트롤러의 장치 드라이버 등으로 구성된다. CDD 영역은, 표준화 되지 못한, 파워트레인의 연료주사, 전자밸브 제어, 미션 제어 등의 영역에서 사용된다.
- [88] BSW의 각 층을 이루고 있는 여러 모듈들 중에서 통신에 관련된 모듈들의 집합을 통신 스택(Communication Stack: Com-Stack)이라고 부른다. 도 6에는, 이해의 편의를 위해, Com-Stack 중에서도 CAN(Controller Area Network) 관련 모듈들 위주로 도시되어 있다. CAN 메시지의 전달에 관여되는 BSW의 모듈들은 COM(Communication), PDU Router(Protocol Data Unit Router: PDUR), CAN Interface(CAN IF), CAN Driver(CAN Drv) 등이다.
- [89] ASW 계층의 소프트웨어 컴포넌트(즉, ECU APP)가 CAN 네트워크에 데이터를 보내는 경우, 데이터는 RTE, COM, PduR, 및 CAN IF를 거친 후 CAN Drv에서 CAN Bus로 전송된다. 이렇게 전송된 데이터는 CAN Bus에 연결되어 있는 모든 ECU의 CAN Drv에서 수신하게 되며, CAN Drv는 CAN ID(Message ID)를 확인하여 자신이 수신해야 할 데이터이면 CAN IF, PDUR, COM, 및 RTE를 거쳐 응용 소프트웨어 컴포넌트(ECU APP)로 전달하게 된다.
- [90]
- [91] 이제, 도 9에 예시된 AUTOSAR 기반의 소프트웨어 아키텍처에 대해 IDPS를 탑재하기 위한 다양한 방법들을 설명한다. 이하에서 설명되는 방법들은 IDS를 탑재하는 데에도 실질적으로 동일하게 적용될 수 있다.
- [92] 전술한 정적 탐지(Static detection)는 메시지(message) 단위로 수행되며, 오용 탐지(Misuse detection)와 변칙 탐지(anomaly detection)는 시그널(signal) 단위로 수행된다. 또한, 오용 탐지(Misuse detection)와 변칙 탐지(anomaly detection)는 정적 탐지에 대비되는 동적 탐지로 지칭될 수 있다. 이하의 설명에서, 용어 '정적 탐지'와 '메시지 단위의 탐지'는 상호 호환적으로 사용될 수 있으며, 용어 '동적 탐지'와 '시그널 단위의 탐지'는 상호 호환적으로 사용될 수 있다.
- [93] 제 1 실시예 - 병렬 탐지 후 차단 신호 전송 방법
- [94] 도 10은 본 발명의 일 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다. 도 10에 도시된 바와 같이, 본 실시예에서, 정적 탐지(메시지 단위의 탐지)를 수행하는 IDPS 모듈이 CDD 영역에 탑재된다. 동적 탐지(시그널 단위의 탐지)를 수행하는 IDPS 모듈은 CDD 영역 혹은 ASW 영역에 탑재될 수 있다.
- [95] 본 실시예에서, Com-Stack상의 전형적인 CAN 메시지 처리 절차는 그대로 유지되고, MCAL 영역의 CAN Drv에서 CDD 영역의 IDPS 모듈로 CAN 메시지를 전달하면서 탐지가 시작된다. CDD 영역의 IDPS 모듈에 CAN 메시지가 전달되면 IDPS 모듈은 정적 탐지를 수행한다. 만약 CDD 영역에 IDPS의 동적 탐지 모듈이 포함되어 있다면, 정적 탐지와 동적 탐지가 동시에 수행될 수 있다. 정적 및 동적

탐지에서 CAN 메시지가 보안 위협과 관련된 메시지로 판단되면, IDPS 모듈은 PDUR 모듈로 메시지 차단 요청 신호를 전달한다.

- [96] CAN 메시지 처리 절차에 따라 CAN 메시지가 CAN IF로부터 PDUR 모듈로 전달 되기 전에 메시지 차단 요청 신호가 PDUR 모듈에 도착한다면, CAN 메시지는 PDUR 모듈에서 차단될 수 있다. 반면, 메시지 차단 요청 신호보다 CAN 메시지가 PDUR에 먼저 도착하면, CAN 메시지의 차단은 이루어지지 않는다.
- [97] 본 실시예의 기법은 CAN 메시지 처리 절차를 그대로 유지하므로, CAN 메시지 처리 절차에 지연을 가하지 않고도, 보안 위협 메시지의 차단을 가능하게 한다. 그러나 동적 탐지를 수행하기 위한 CDD 영역의 리소스 부하가 크다. 또한 IDPS에서 PDUR 모듈로 메시지 차단 요청 신호를 전송하기 위해 추가적인 인터페이스가 필요하다. 그리고 보안 위협 메시지의 차단을 이루기 위해서는 PDUR 모듈에 CAN 메시지가 도착하기 전에 메시지 차단 요청 신호가 먼저 도착해야 한다. 따라서 탐지 처리가 오래 걸리면 차단이 불가능할 수 있다.
- [98]
- [99] 제 2 실시예 - 병렬 탐지 전용 방법
- [100] 도 11은 본 발명의 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다. 도 11에 도시된 바와 같이, 본 실시예에서, CAN 메시지들이 큐잉되는 IDPS 메시지 큐가 CDD 영역에 형성되고, 정적 탐지와 동적 탐지를 수행하는 IDPS 탐지 모듈이 응용 소프트웨어(ASW) 영역에 탑재된다.
- [101] 본 실시예에서는 Com-Stack상의 전형적인 CAN 메시지 처리 절차는 그대로 유지되고, MCAL영역의 CAN Driver에서 CDD영역의 IDPS 큐잉 모듈로 CAN 메시지를 전달된다. IDPS 메시지 큐에 CAN 메시지가 저장되면, ASW 영역의 IDPS 탐지 모듈은 메시지 큐로부터 CAN 메시지를 전달받아 탐지를 수행한다. ASW 영역의 IDPS 탐지 모듈들은 정적 탐지와 동적 탐지를 동시에 수행할 수 있다. 본 방법은 메시지 지연이 없다는 장점이 있으나 탐지만 가능하다는 단점이 있다.

[102]

[103] 제 3 실시예 - 메시지 인터럽트 차단 방식

[104] 도 12는 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.

[105] 본 실시예에서는, Com-Stack상의 CAN 메시지 처리 절차에서 MCAL 영역의 CAN Drv에서 EAL영역의 CAN IF로 전달되는 CAN 메시지를 CDD영역의 IDPS가 인터럽트 하면서 탐지가 시작된다. CDD영역의 IDPS 탐지 모듈에 CAN 메시지가 전달되면 IDPS탐지 모듈은 정적 탐지를 수행한다. IDPS의 동적 탐지 모듈은 CDD 영역 혹은 ASW 영역에 임베딩(embedding)될 수 있는 바, 만약 CDD 영역에 IDPS의 동적 탐지 모듈이 포함되어 있다면, CDD 영역에서는 정적

탐지와 동적 탐지가 동시에 수행될 수 있다. 정적 및/또는 동적 탐지에서 보안 위협 메시지를 탐지하면 IDPS 탐지 모듈은 EAL 영역의 CAN IF 모듈로 CAN 메시지를 전달하지 않는다. CAN 메시지가 전달되지 않으므로 기존 CAN 메시지 처리 절차가 더 이상 수행되지 않는다.

- [106] 본 실시예의 구현 예는 보안 위협 메시지의 차단 성공 확률이 높은 장점이 있다. 그러나 인터럽트 사용에 따른 메시지 지연이 발생하고 IDPS에서 CAN IF로 CAN 메시지 전달을 위해 추가적인 인터페이스가 필요하다. 또한 CDD 영역에서 동적 탐지가 가능하나 부하가 크다는 단점이 있다.

[107]

[108] 제 4 실시예 - AutoSAR 모듈 수정 방법

- [109] 도 13은 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.

- [110] 본 실시예에서는 기존 AUTOSAR 플랫폼에서 정의된 CAN IF 모듈에서 정적 탐지를 수행하고 COM 서비스 모듈에서 동적 탐지를 수행한다. 본 방법은 AUTOSAR 플랫폼의 Com-Stack을 구성하는 표준화된 모듈(즉, CAN IF 및 COM)을 변형하므로 CDD 영역을 사용하는 경우와 달리 인터럽트가 불필요하며, 보안 위협 메시지의 탐지 및 차단이 가능하다는 장점이 있다. 그러나 전체 메시지 처리 절차에 지연이 발생할 수 있으며 AUTOSAR 플랫폼의 표준화된 모듈(즉, CAN IF 및 COM) 내부에 IDPS 모듈 구현을 위해서 관련 파티들과의 협업이 필요하다.

[111]

[112] 제 5 실시예 - 멀티코어 전용 드라이버 사용 방법

- [113] 도 14는 본 발명의 또 다른 실시예에 따른 IDPS가 탑재된 ECU의 소프트웨어 아키텍처를 개략적으로 도시한 도면이다.

- [114] 본 실시예에서는 Com-Stack상의 CAN 메시지 처리 절차는 그대로 진행되고 MCAL 영역의 CAN Drv에서 IDPS 전용 코어(제 2 코어)의 공유 메모리(shared memory)로 CAN 메시지를 전달하면서 탐지가 시작된다. CAN 메시지가 전달되면 IDPS는 정적 탐지 및 동적 탐지를 (동시에) 수행한다. 본 실시예의 장점은 CAN 메시지 처리 절차에 지연을 부가하지 않으며, 별도 코어(제 2 코어)를 이용하므로 기존의 CAN 메시지 처리 절차가 진행되는 제 1 코어에 부하를 적게 준다는 장점이 있다. 그러나 구현에 따른 비용이 높으며 탐지만 가능하다는 단점이 있다.

[115]

[116] 제 6 실시예 - Bit Stumping을 통한 보안 위협 메시지 차단 방법

- [117] 비트 스템핑(Bit Stumping)은 보안 위협 메시지를 탐지하였을 때 기존의 점유된 버스상에 강제로 신호를 송신하여 메시지 프레임 오류를 유발함으로써 보안 위협 메시지를 무효화 시키는 차단 방법으로 사용할 수 있다. 이러한 보안 위협 메시지 차단 방법은 도 10 내지 도 14를 참조하여 설명한 방법들과 각각 결합

가능하다.

- [118] 도 15는 비트 스템핑(Bit Stumping)을 적용하기 위한 도 10의 소프트웨어 아키텍처(제 1 실시예)의 변형예이다. Bit Stumping을 사용하기 위해서는, 도 15에 보인 바와 같이, IDPS에서 CAN 버스로 연결되는 추가적인 하드웨어(즉, 입출력 포트(I/O 포트))가 필요하다.
- [119]
- [120] 전술한 예시적인 실시예들은 많은 상이한 방식으로 구현될 수 있다는 것을 이해해야 한다. 일부 예들에서, 본 개시에서 설명된 다양한 방법들, 장치들, 시스템들은 프로세서, 메모리, 통신 인터페이스 등을 가지는 전자 제어 장치, 게이트웨이 등에 의해 구현되거나 이들에 포함될 수도 있다. 예컨대, 전자 제어 장치는 소프트웨어 명령어들을 프로세서에 로딩한 다음, 본 개시에 설명된 기능을 수행하기 위해 명령어들을 실행함으로써 상술한 방법을 실행하는 장치로 기능할 수 있다.
- [121] 한편, 본 개시에서 설명된 다양한 방법들은 하나 이상의 프로세서에 의해 관독되고 실행될 수 있는 비일시적 기록매체에 저장된 명령어들로 구현될 수도 있다. 비일시적 기록매체는, 예를 들어, 컴퓨터 시스템에 의하여 관독가능한 형태로 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 예를 들어, 비일시적 기록매체는 EPROM(erasable programmable read only memory), EEPROM(Electrically Erasable Programmable Read-Only Memory), 플래시 메모리, 광학 드라이브, 자기 하드 드라이브, 솔리드 스테이트 드라이브(SSD)와 같은 저장매체를 포함한다.
- [122] 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.
- [123] CROSS-REFERENCE TO RELATED APPLICATION
- [124] 본 특허출원은, 본 명세서에 그 전체가 참고로서 포함되는, 2017년 12월 19일 미국에 출원한 US 62/607,595에 대해 우선권을 주장한다.

청구범위

- [청구항 1] 차량 내 네트워크에 보안을 제공하는 방법에 있어서,
 차량 내 네트워크로부터 수집된 새로운 네트워크 메시지가 기 탐지된
 보안 위협 메시지와 동일 혹은 유사한 메시지인지 여부를 판단하는 단계;
 및
 상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지와 동일
 혹은 유사한 메시지이면, 상기 새로운 네트워크 메시지에 대해, 복수의
 탐지 기법의 적용을 스킵하고, 곧바로 상기 새로운 네트워크 메시지를
 보안 위협 메시지로 간주하는 단계
 를 포함하는, 방법.
- [청구항 2] 제 1 항에 있어서,
 상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지와 동일
 혹은 유사한 메시지가 아니면, 상기 새로운 네트워크 메시지에 대해 상기
 복수의 탐지 기법들을 적용하여, 상기 새로운 네트워크 메시지가 보안
 위협 메시지인지 여부를 결정하는 단계를 더 포함하는, 방법.
- [청구항 3] 제 2 항에 있어서,
 상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지와 동일
 혹은 유사한 메시지인지 여부를 판단하는 단계는,
 상기 기 탐지된 보안 위협 메시지를 식별하는 정보를 기록한
 데이터베이스를 조회하는 단계;
 상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지를
 식별하는 정보에 상응하는 정보를 가지고 있는지 여부를 판단하는 단계
 를 포함하는 것을 특징으로 하는, 방법.
- [청구항 4] 제 3 항에 있어서,
 상기 새로운 네트워크 메시지를 상기 보안 위협 메시지로 결정하거나
 간주하는 것에 응답하여, 상기 데이터베이스를 업데이트하는 단계를 더
 포함하는 것을 특징으로 하는, 방법.
- [청구항 5] 제 3 항에 있어서,
 상기 데이터베이스에 기록된 상기 기 탐지된 보안 위협 메시지를
 식별하는 정보는,
 상기 기 탐지된 보안 위협 메시지의 프레임 전체 또는 프레임의 일부
 필드인 것을 특징으로 하는, 방법.
- [청구항 6] 제 1 항에 있어서,
 상기 차량 내 네트워크는 CAN(Controller Area Network) 네트워크인 것을
 특징으로 하는, 방법.
- [청구항 7] 제 1 항에 있어서,
 상기 복수의 탐지 기법들은,

- 정적 탐지(static detection), 오용 탐지(misuse detection), 및 변칙 탐지(anomaly detection)를 포함하는 것을 특징으로 하는, 방법.
- [청구항 8] 차량 내 네트워크에 보안을 제공하는 방법에 있어서,
 차량 내 네트워크로부터 수집되는 새로운 네트워크 메시지에 대해 적용할 복수의 탐지 기법들의 적용 순서를 결정하는 단계; 및
 상기 새로운 네트워크 메시지에 대해, 상기 결정된 적용 순서에 따라 상기 복수의 탐지 기법들을 적용하여, 상기 새로운 네트워크 메시지가 보안 위협 메시지인지 여부를 결정하는 단계
 를 포함하는, 방법.
- [청구항 9] 제 8 항에 있어서,
 상기 복수의 탐지 기법들의 적용 순서는,
 상기 차량 내 네트워크로부터 기 수집된 적어도 하나의 네트워크 메시지에 대해 적용된 상기 복수의 탐지 기법들의 탐지 이력을 기초로 결정되는 것을 특징으로 하는, 방법.
- [청구항 10] 제 8 항에 있어서,
 상기 복수의 탐지 기법들의 적용 순서를 결정하는 단계는,
 상기 보안 위협 메시지를 탐지하는 데에 성공한 탐지 기법이 다른 탐지 기법들에 비해 우선 적용되도록 상기 복수의 탐지 기법들의 적용 순서를 변경하는 단계를 포함하는 것을 특징으로 하는, 방법.
- [청구항 11] 제 8 항에 있어서,
 상기 복수의 탐지 기법들의 적용 순서를 결정하는 단계는,
 각 탐지 기법 별로, 상기 보안 위협 메시지를 탐지하는 데 성공한 누적 횟수를 카운트하는 단계; 및
 상기 각 탐지 기법별 누적 횟수의 내림 차순으로, 상기 복수의 탐지 기법들을 적용순서를 변경하는 단계
 를 포함하는, 방법.
- [청구항 12] 제 8 항에 있어서,
 상기 복수의 탐지 기법들은,
 정적 탐지, 오용 탐지, 및 변칙 탐지를 포함하는 것을 특징으로 하는, 방법.
- [청구항 13] 차량 내 네트워크에 보안을 제공하는 방법에 있어서,
 차량 내 네트워크로부터 수집된 네트워크 메시지에 대해, 복수의 탐지 기법들의 적용을 병렬적으로 개시하는 단계; 및
 상기 복수의 탐지 기법들 중에서 어느 하나의 탐지 기법이 상기 수집된 네트워크 메시지를 보안 위협 메시지로 결정하는 것에 응답하여, 상기 수집된 네트워크 메시지에 대한 나머지 탐지 기법들의 적용을 중단하는 단계
 를 포함하는, 방법.
- [청구항 14] 제 13 항에 있어서,

상기 복수의 탐지 기법들 모두가 상기 네트워크 메시지를 보안 위협 메시지가 아니라고 결정하는 것에 응답하여, 상기 네트워크 메시지가 응용 소프트웨어로 전달되는 것을 허용하는 단계를 더 포함하는, 방법.

[청구항 15] 제 13 항에 있어서,
상기 복수의 탐지 기법들의 적용을 병렬적으로 개시하는 단계는, 서로 상이한 탐지 기법들을 사용하는 복수의 스레드(thread)들을 동시에(concurrently) 실행하는 단계; 및
상기 수집된 네트워크 메시지를 상기 복수의 스레드에 각각 입력하는 단계를 포함하는 것을 특징으로 하는, 방법.

[청구항 16] 제 15 항에 있어서,
상기 복수의 스레드들 각각은,
상기 수집된 네트워크 메시지를 보안 위협 메시지로 결정하는 것에 응답하여 다른 스레드들에게 인터럽트 신호를 전송하고, 다른 스레드들로부터 수신되는 인터럽트 신호에 응답하여 자신의 실행을 종료하도록 구성된 것을 특징으로 하는, 방법.

[청구항 17] 제 13 항에 있어서,
상기 복수의 탐지 기법들은,
정적 탐지, 오용 탐지, 및 변칙 탐지를 포함하는 것을 특징으로 하는, 방법.

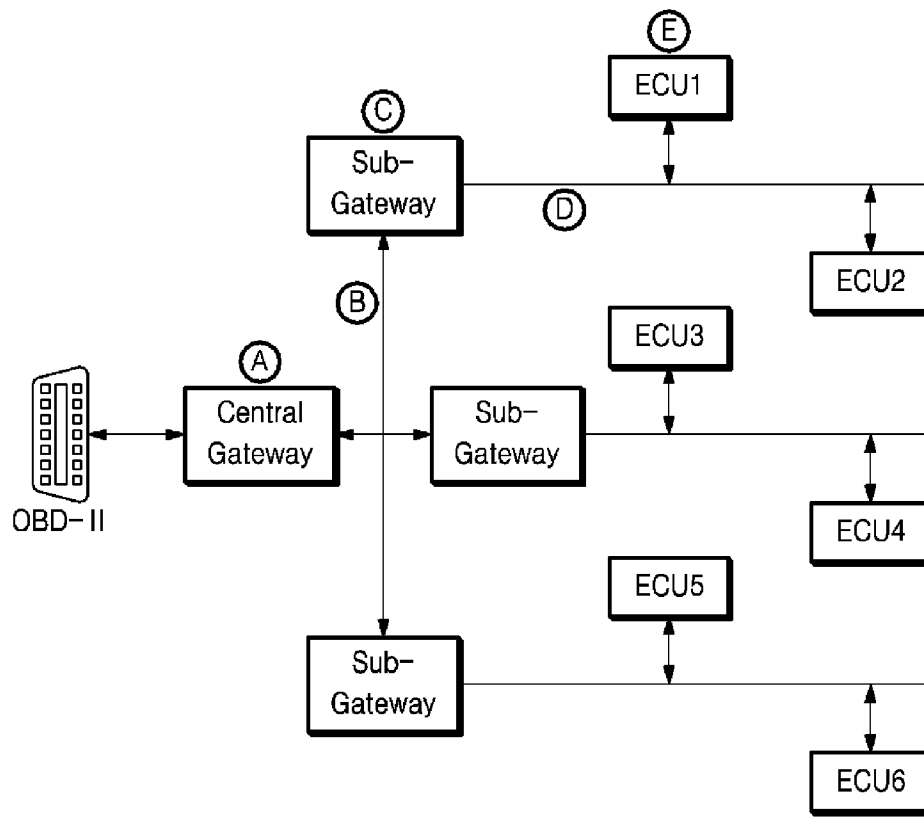
[청구항 18] 차량 내 네트워크에 보안을 제공하는 전자 장치로서,
하나 이상의 프로세서; 및
명령어들이 저장된 메모리를 포함하되, 상기 명령어들은 상기 하나 이상의 프로세서에 의해 실행될 때 상기 전자 장치로 하여금,
차량 내 네트워크로부터 수집된 새로운 네트워크 메시지가 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지인지 여부를 판단하는 단계; 및
상기 새로운 네트워크 메시지가 상기 기 탐지된 보안 위협 메시지와 동일 혹은 유사한 메시지이면, 상기 새로운 네트워크 메시지에 대해, 복수의 탐지 기법의 적용을 스킵하고, 곧바로 상기 새로운 네트워크 메시지를 보안 위협 메시지로 간주하는 단계를 수행하도록 하는, 전자 장치.

[청구항 19] 차량 내 네트워크에 보안을 제공하는 전자 장치로서,
하나 이상의 프로세서; 및
명령어들이 저장된 메모리를 포함하되, 상기 명령어들은 상기 하나 이상의 프로세서에 의해 실행될 때 상기 전자 장치로 하여금,
차량 내 네트워크로부터 수집되는 새로운 네트워크 메시지에 대해 적용할 복수의 탐지 기법들의 적용 순서를 결정하는 단계; 및

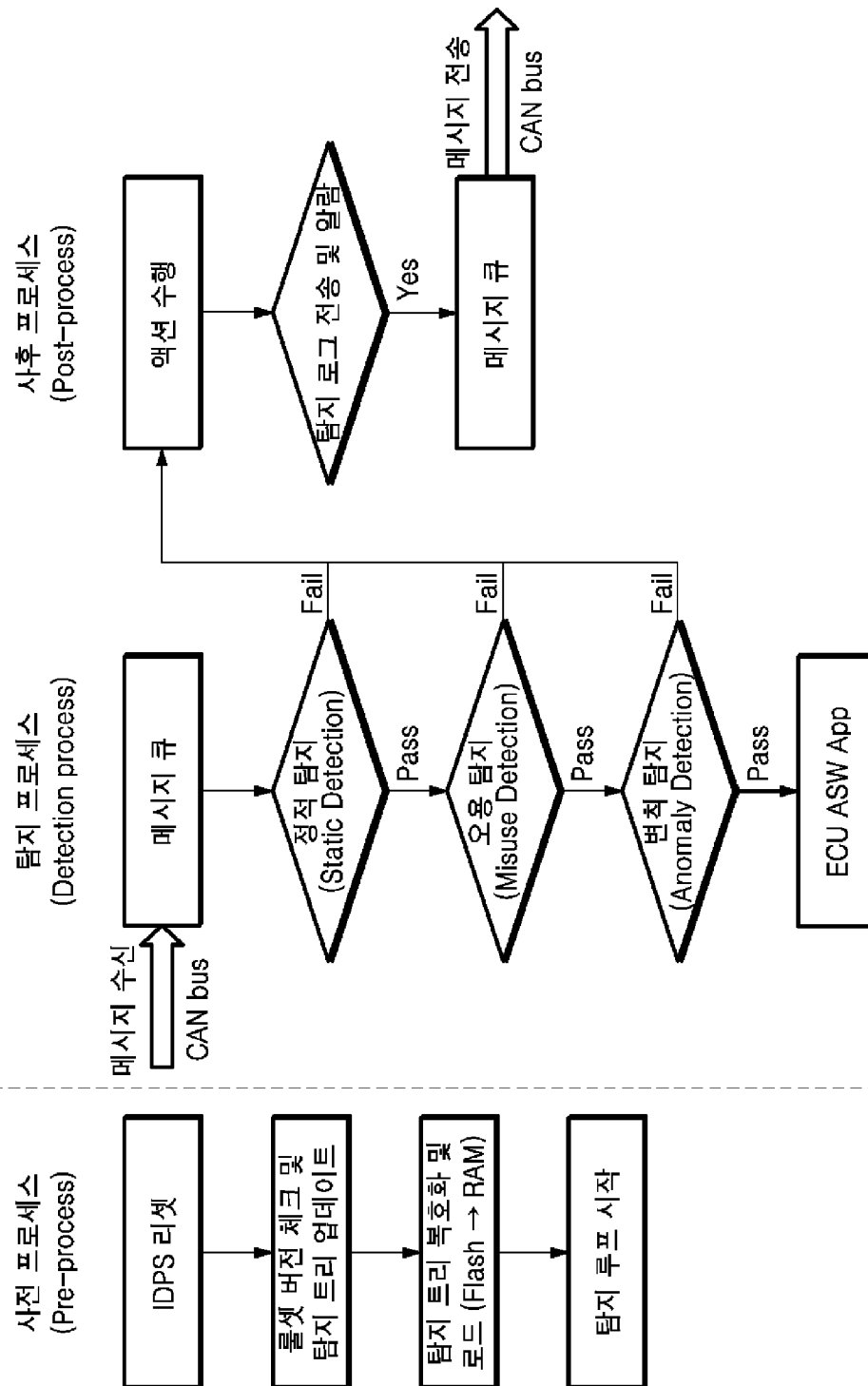
상기 새로운 네트워크 메시지에 대해, 상기 결정된 적용 순서에 따라 상기 복수의 탐지 기법들을 적용하여, 상기 새로운 네트워크 메시지가 보안 위협 메시지인지 여부를 결정하는 단계
를 수행하도록 하는, 전자 장치.

- [청구항 20] 차량 내 네트워크에 보안을 제공하는 전자 장치로서,
하나 이상의 프로세서; 및
명령어들이 저장된 메모리를 포함하되, 상기 명령어들은 상기 하나 이상의 프로세서에 의해 실행될 때 상기 전자 장치로 하여금,
차량 내 네트워크로부터 수집된 네트워크 메시지에 대해, 복수의 탐지 기법들의 적용을 병렬적으로 개시하는 단계; 및
상기 복수의 탐지 기법들 중에서 어느 하나의 탐지 기법이 상기 수집된 네트워크 메시지를 보안 위협 메시지로 결정하는 것에 응답하여, 상기 수집된 네트워크 메시지에 대한 나머지 탐지 기법들의 적용을 중단하는 단계
를 수행하도록 하는, 전자 장치.

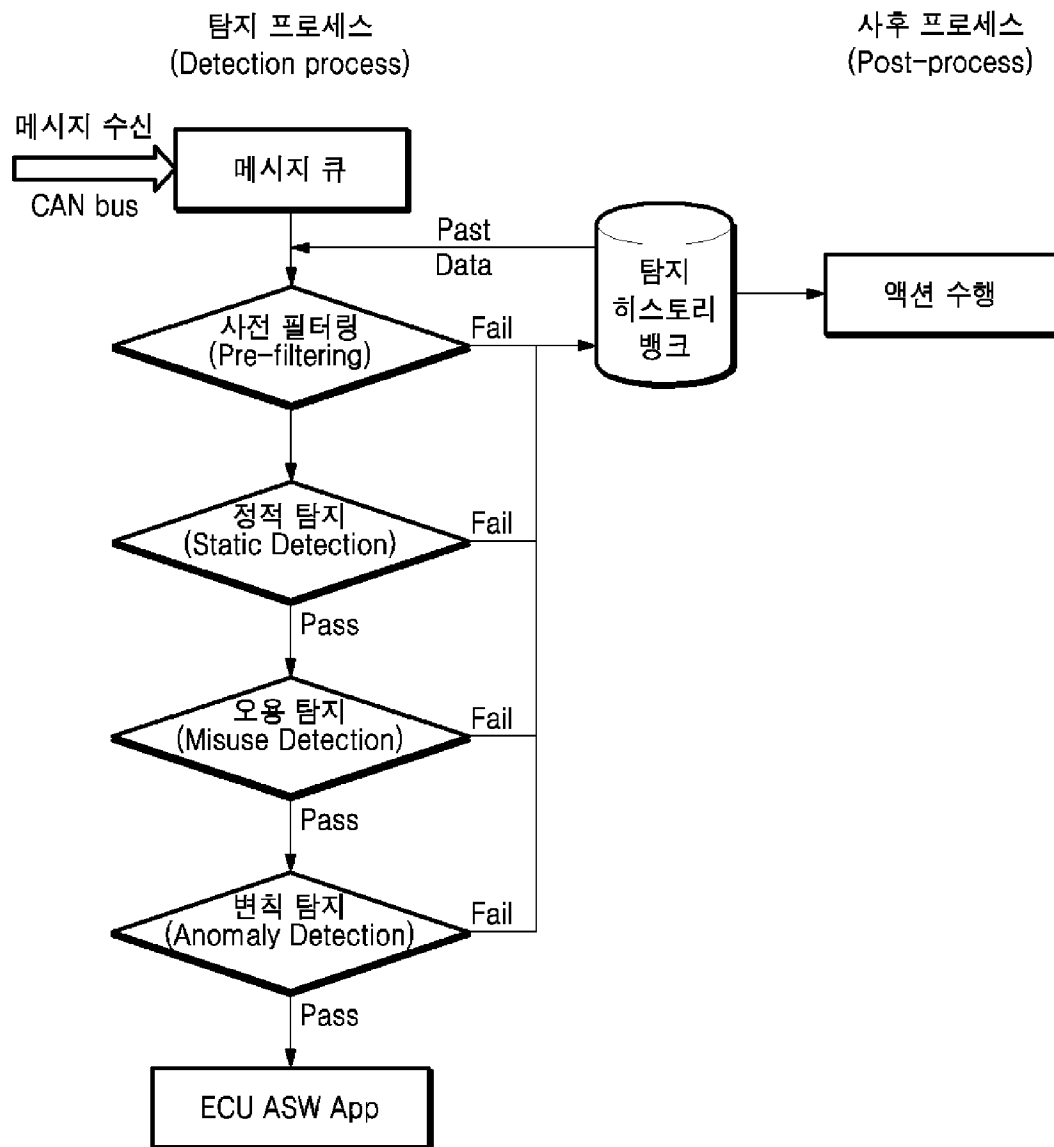
[도 1]



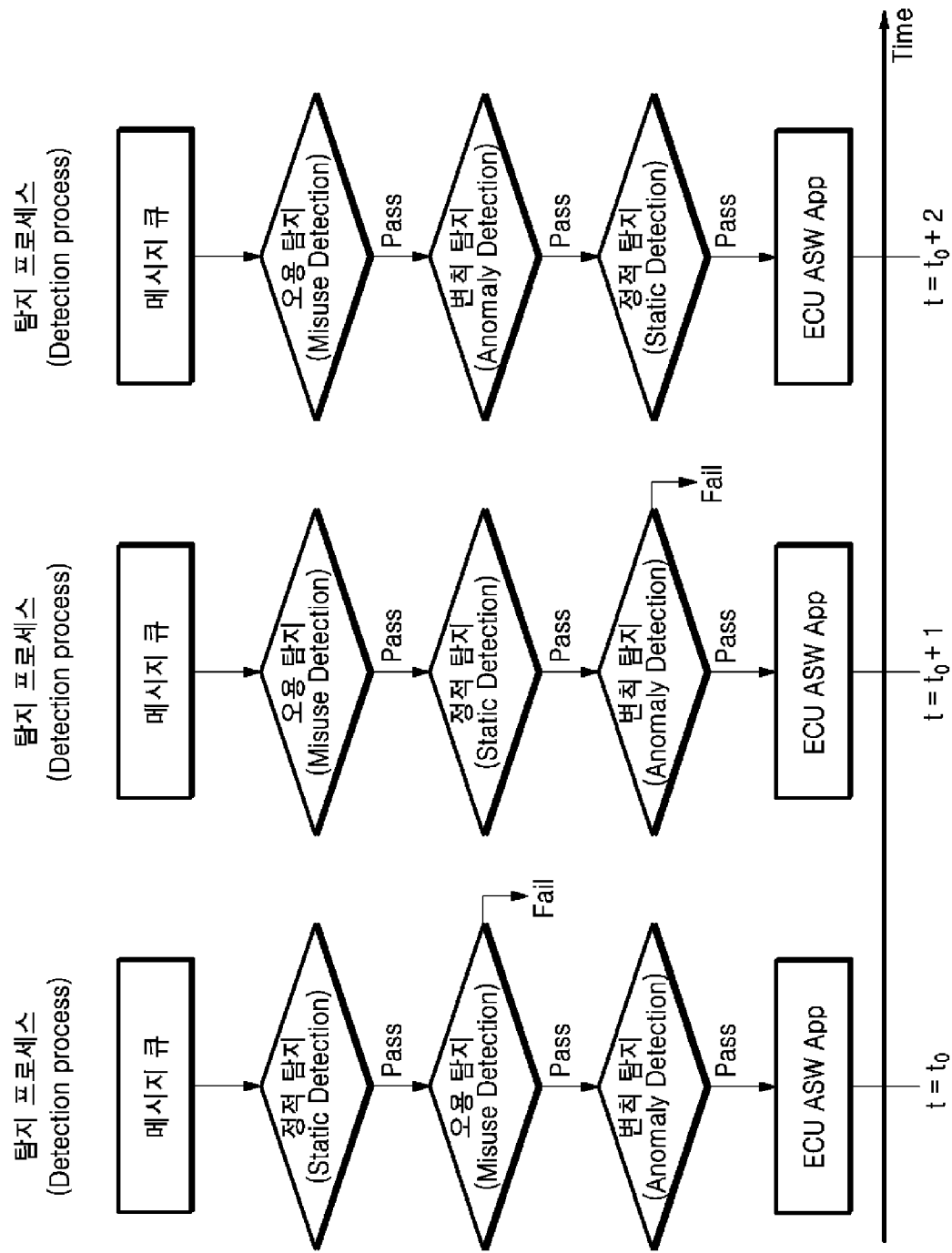
[도2]



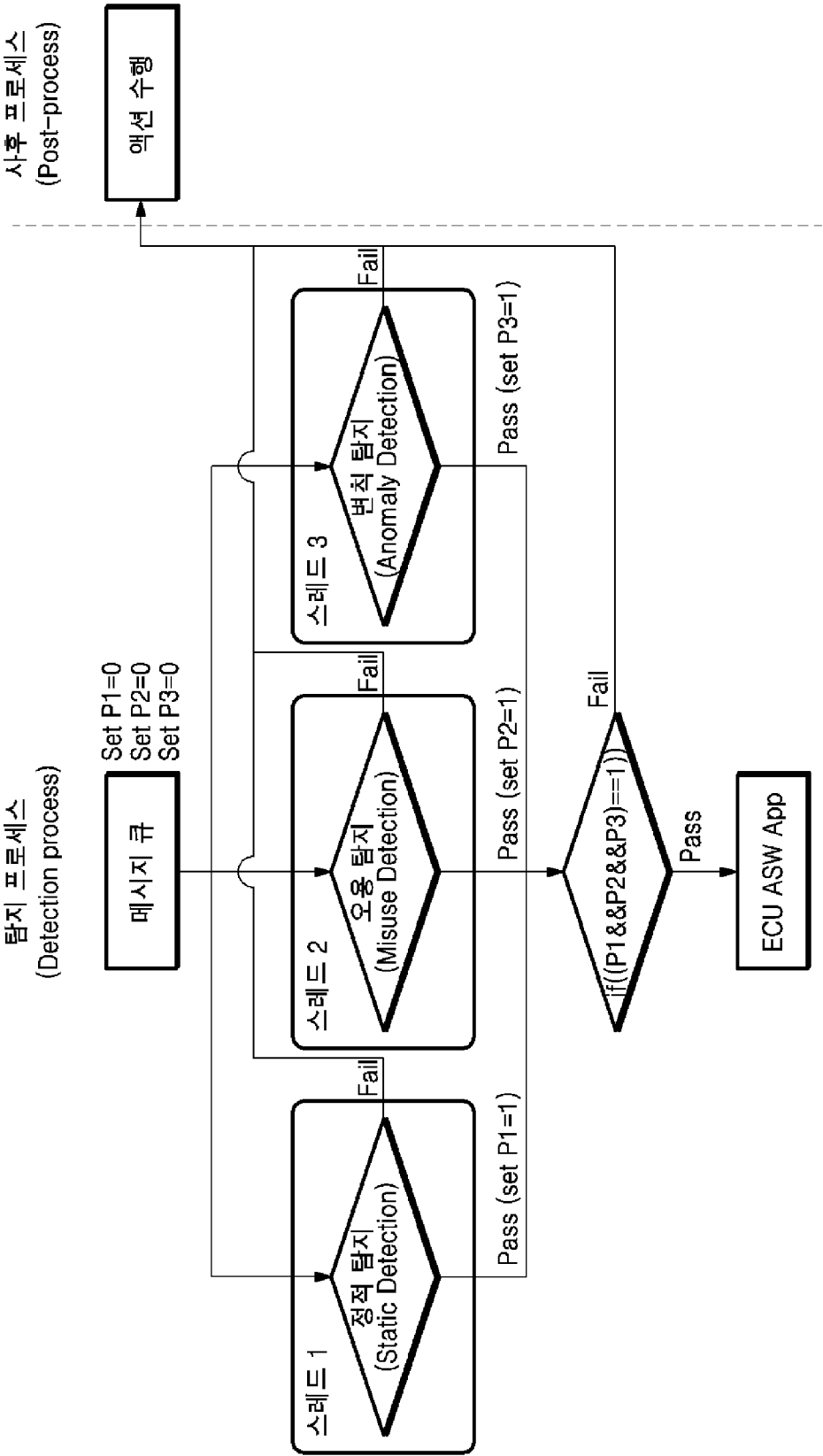
[도3]



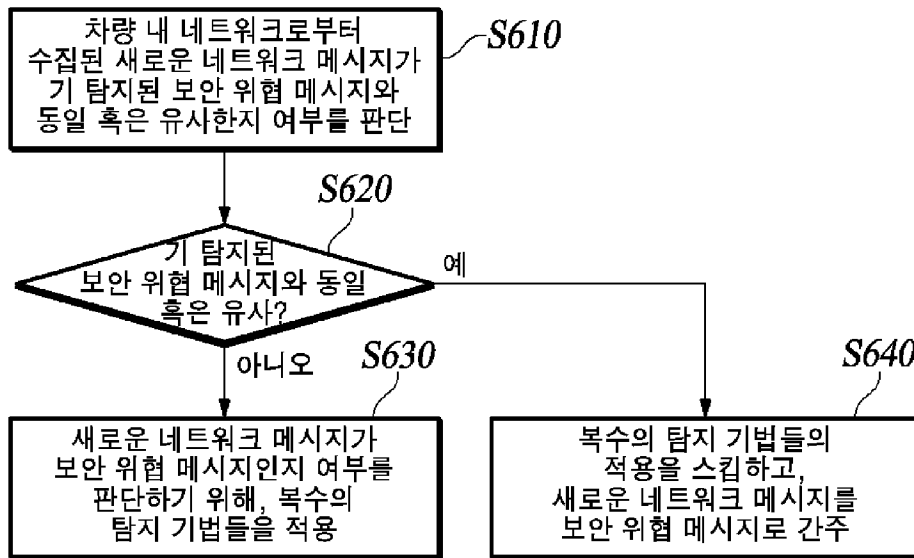
[도 4]



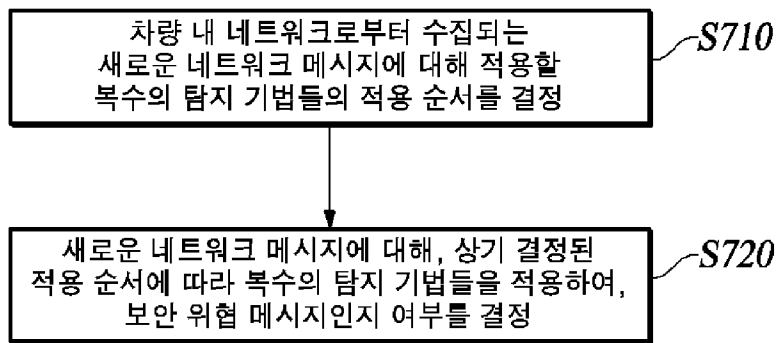
[도5]



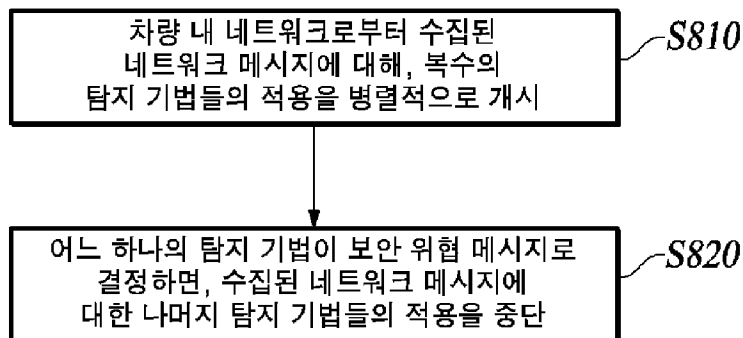
[도6]



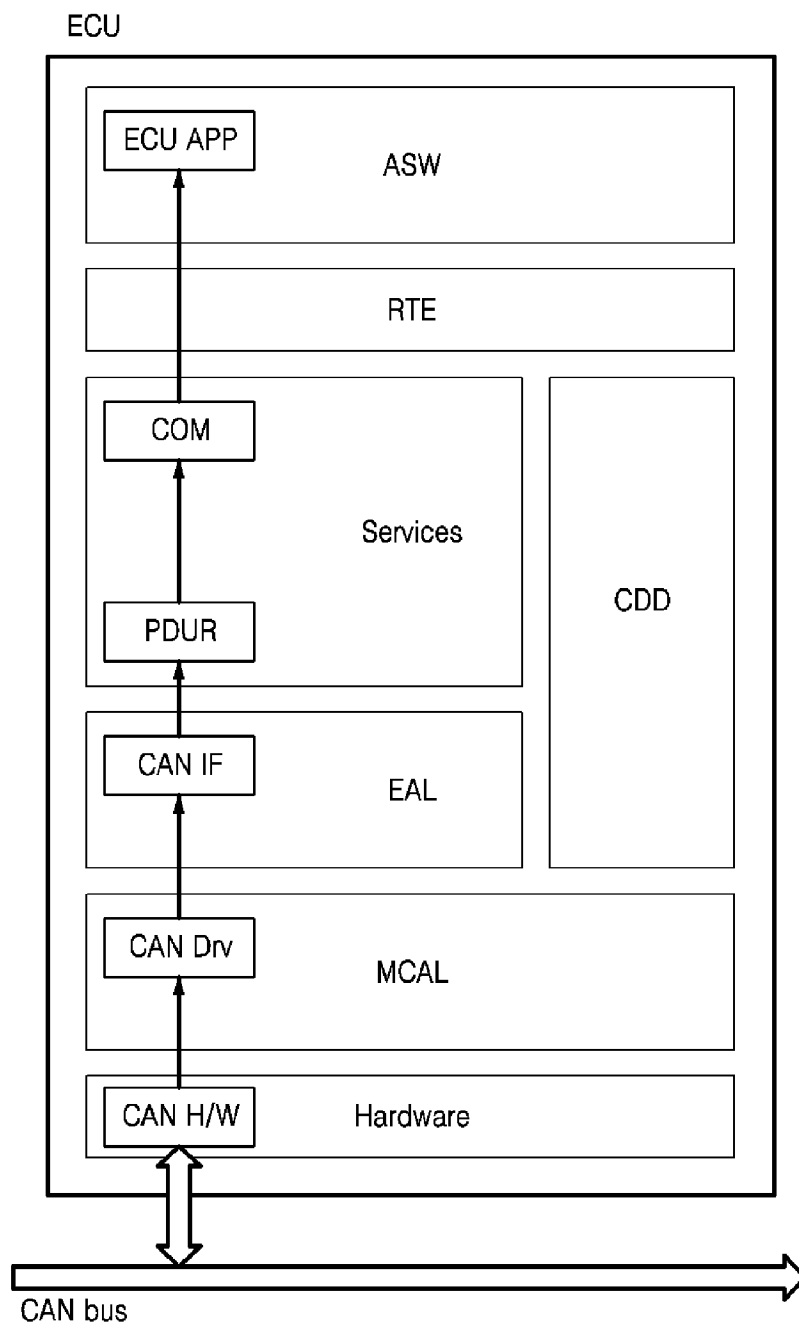
[도7]



[도8]

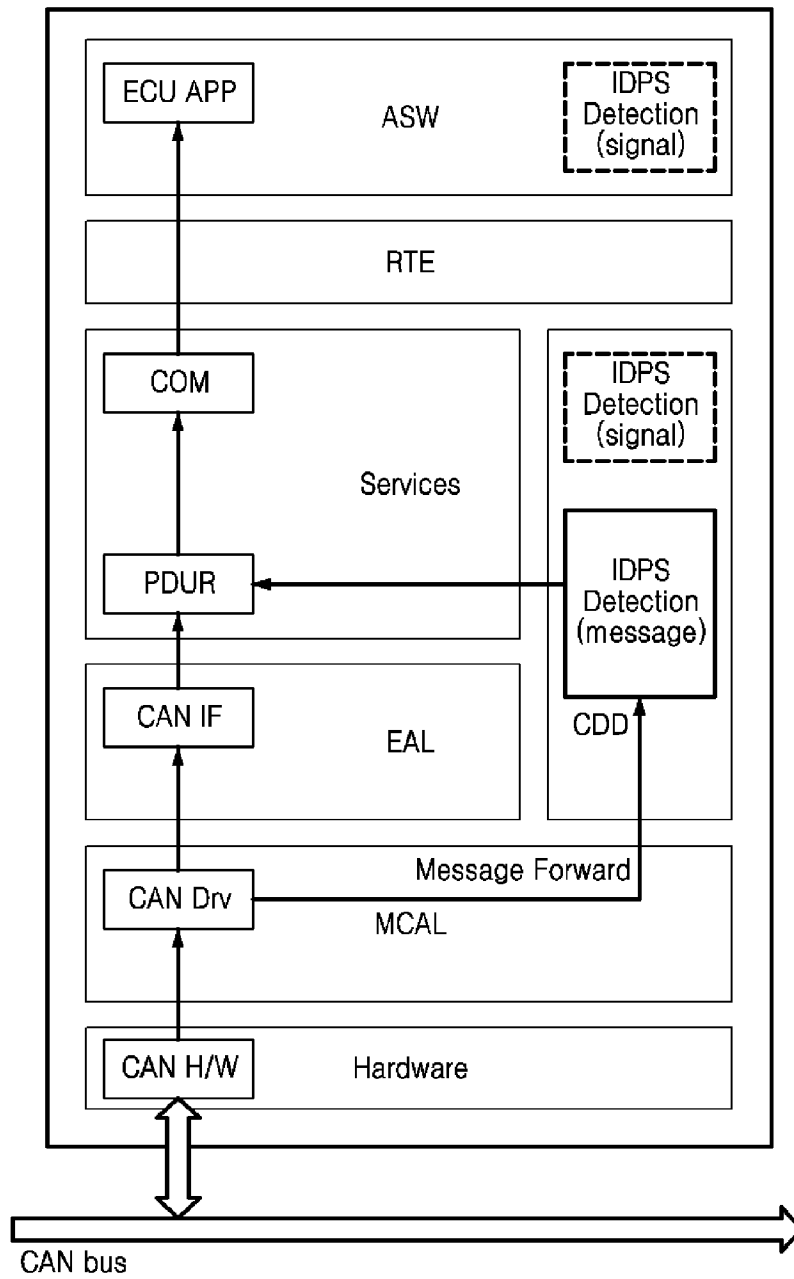


[도9]

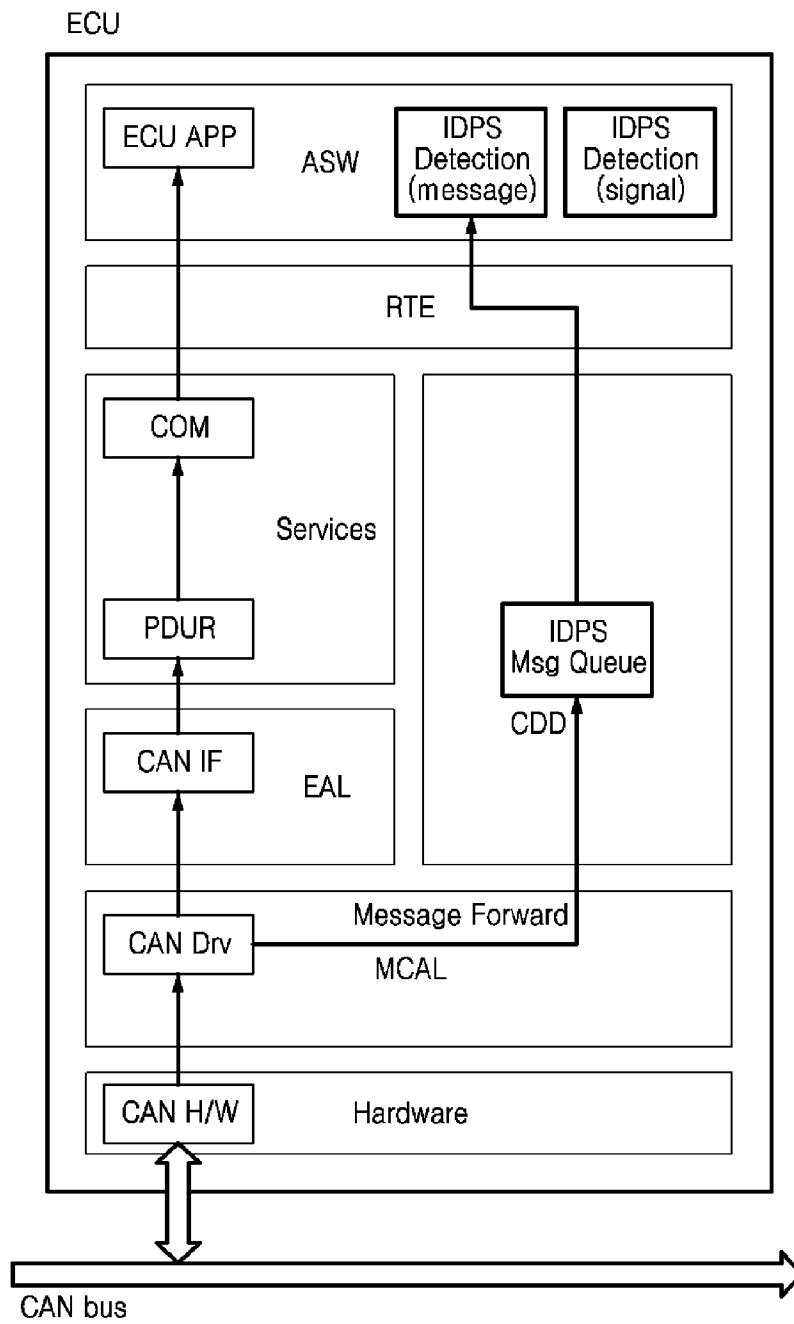


[도10]

ECU

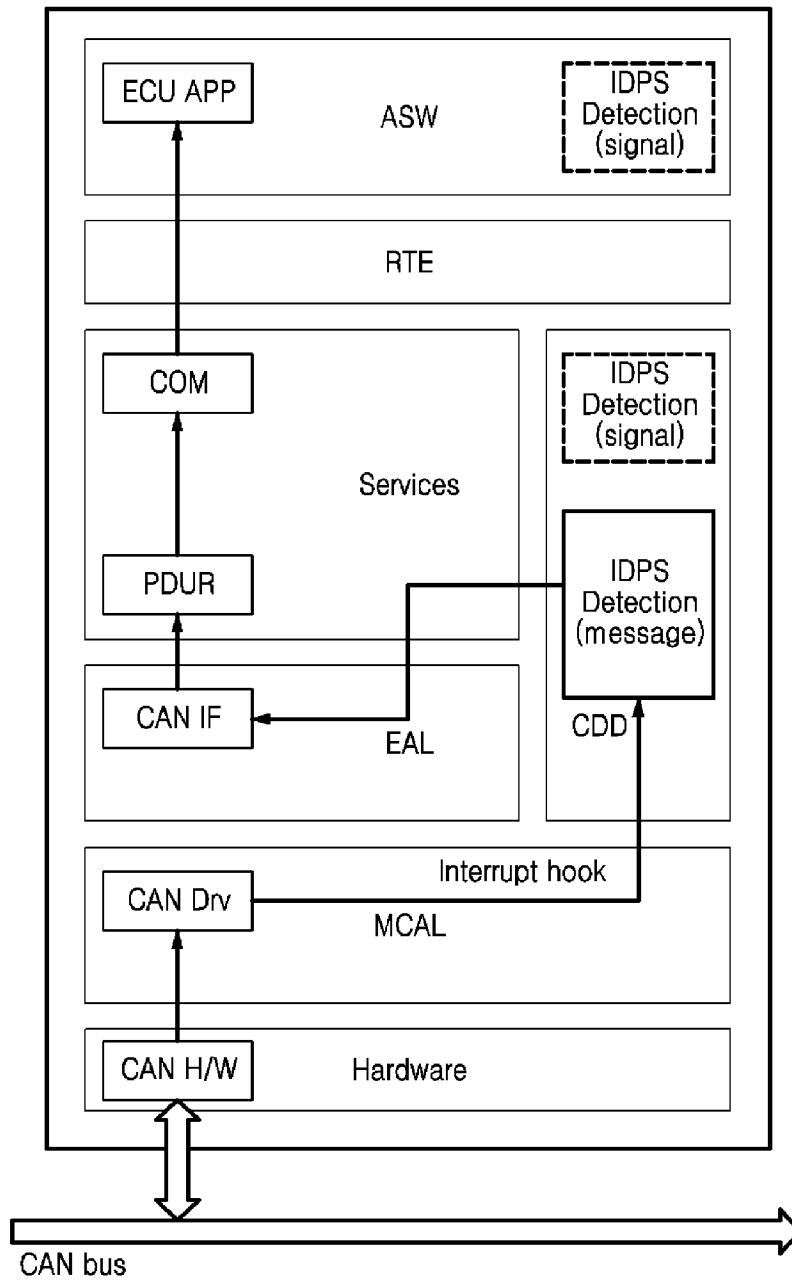


[도11]

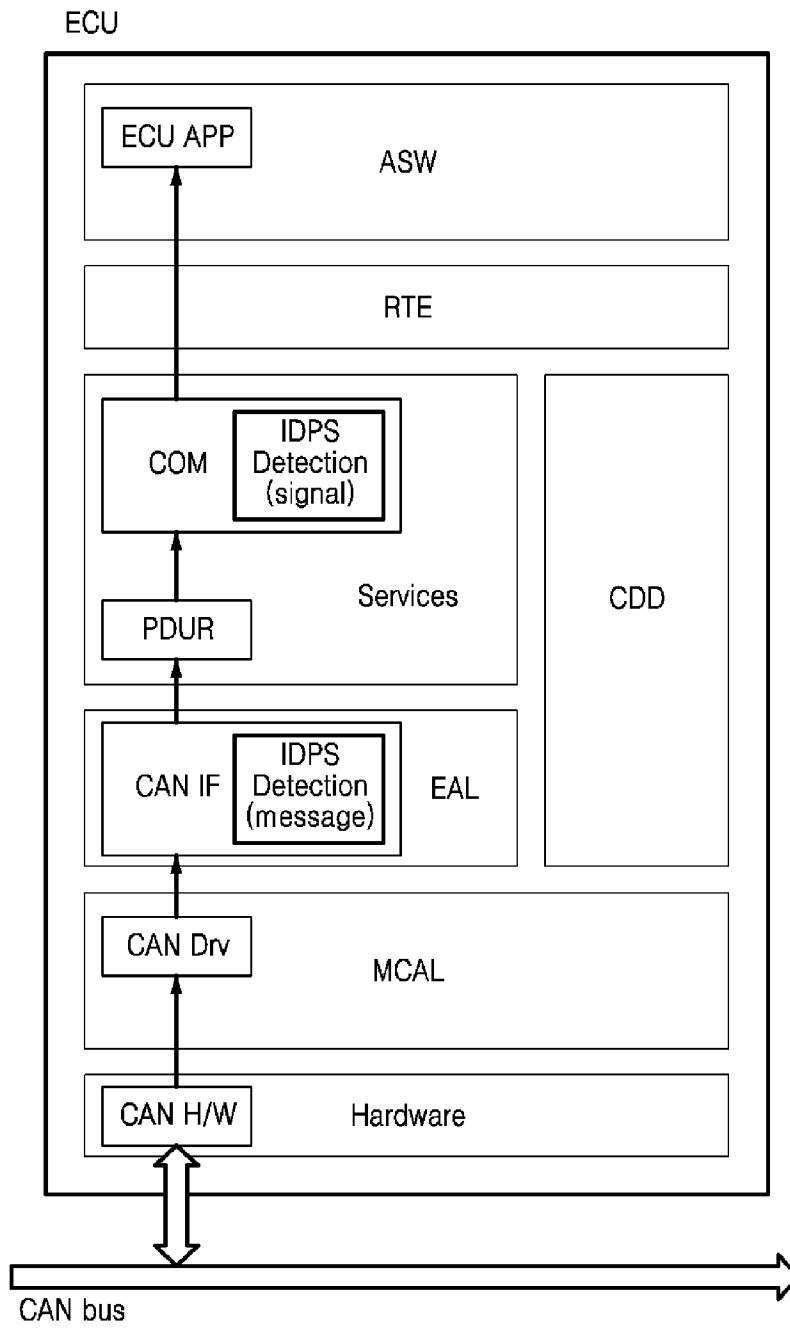


[도 12]

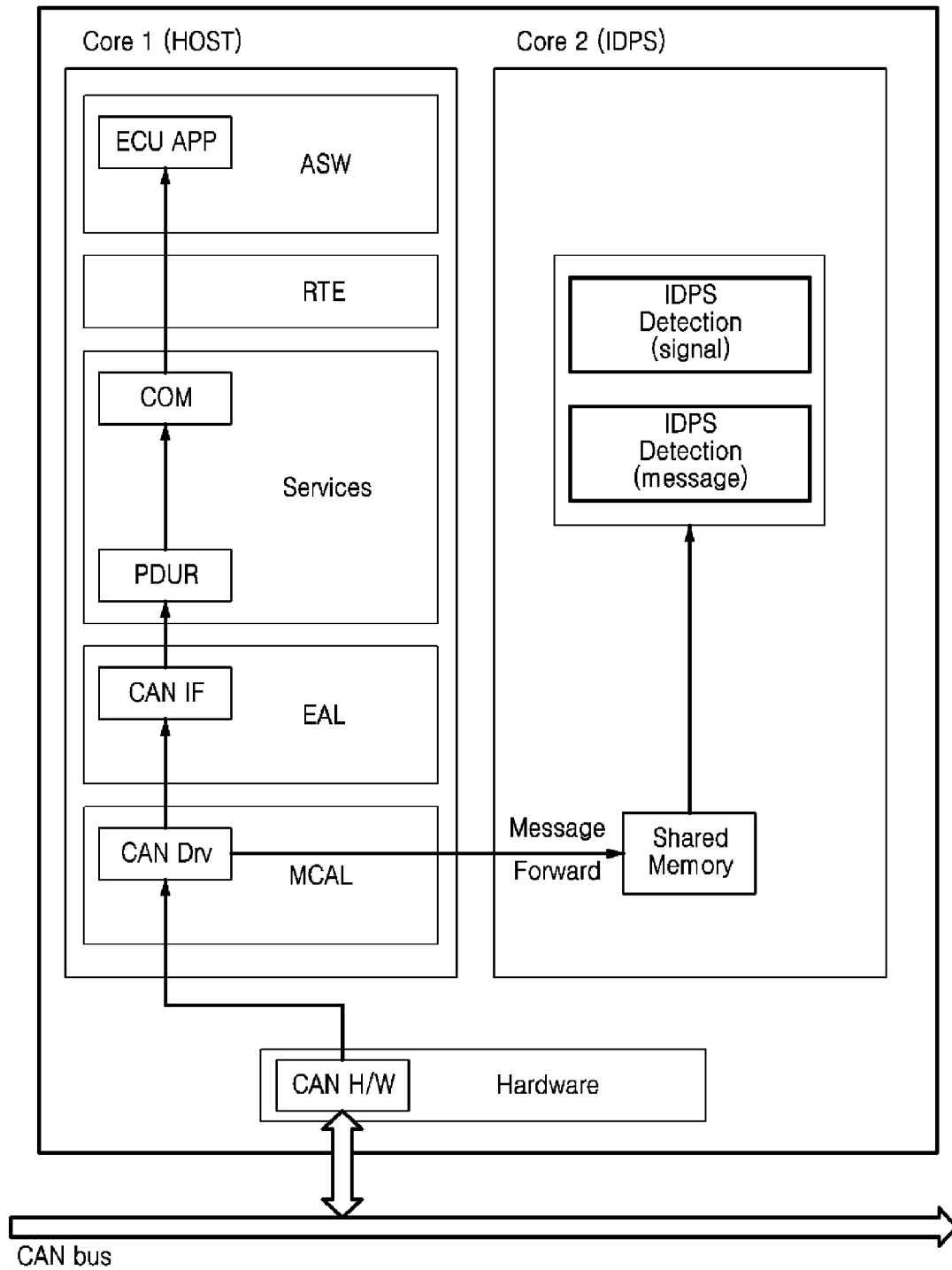
ECU



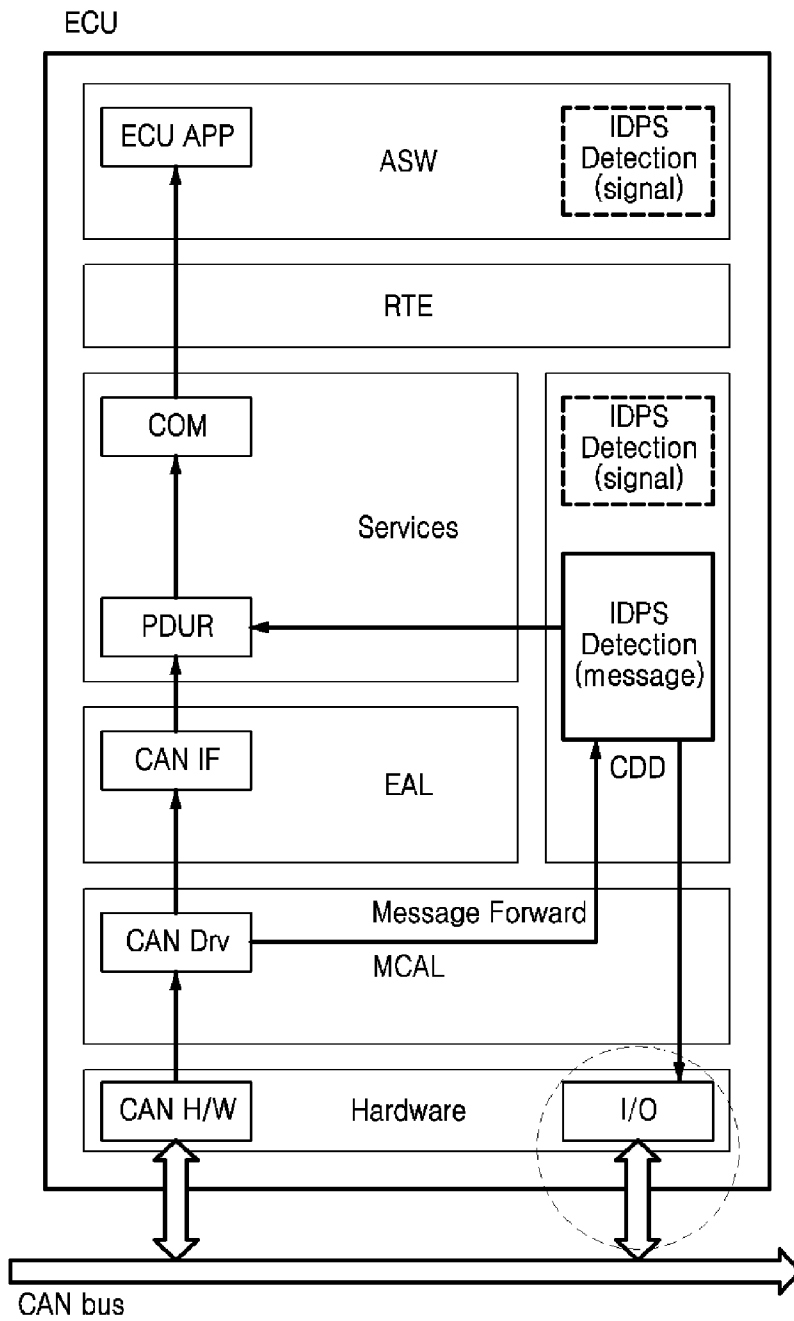
[도13]



[도14]
ECU



[도15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2018/016243**A. CLASSIFICATION OF SUBJECT MATTER****H04L 29/06(2006.01)i, H04L 12/40(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/06; G06F 1/12; G06F 21/55; H04L 29/08; H04L 12/40

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: intrusion detection, vehicle, CAN, network, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016-0205117 A1 (GM GLOBAL TECHNOLOGY OPERATIONS LLC.) 14 July 2016 See claim 1 and paragraph [0015].	1-6,18
Y		7-17,19,20
Y	KR 10-2015-0073176 A (TOWER-SEC LTD.) 30 June 2015 See claim 2 and paragraph [0463].	7-12,17,19
Y	US 2017-0013005 A1 (ARGUS CYBER SECURITY LTD.) 12 January 2017 See paragraph [0034].	13-17,20
A	US 2013-0227689 A1 (TT GOVERNMENT SOLUTIONS, INC.) 29 August 2013 See claims 1-9 and figure 1A.	1-20
A	US 2017-0286675 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 05 October 2017 See claims 1-7 and figure 5.	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

19 MARCH 2019 (19.03.2019)

Date of mailing of the international search report

25 MARCH 2019 (25.03.2019)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex Daejeon Building 4, 189, Cheongsu-ro, Seo-gu,
Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2018/016243

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2016-0205117 A1	14/07/2016	CN 105791266 A DE 102015122823 A1 US 9578047 B2	20/07/2016 28/07/2016 21/02/2017
KR 10-2015-0073176 A	30/06/2015	CN 105050868 A CN 105050868 B EP 2909065 A1 HK 1214216 A1 IL 238359 A IL 238359 B IL 238359 D0 JP 2016-502697 A MX 2015004828 A MX 356554 B US 2015-0271201 A1 US 2017-0149820 A1 US 9560071 B2 WO 2014-061021 A1	11/11/2015 21/12/2018 26/08/2015 22/07/2016 30/06/2015 30/04/2018 30/06/2015 28/01/2016 08/01/2016 04/06/2018 24/09/2015 25/05/2017 31/01/2017 24/04/2014
US 2017-0013005 A1	12/01/2017	EP 3113529 A1 US 2016-0381059 A1 US 2016-0381066 A1 US 2016-0381067 A1 US 2016-0381068 A1	04/01/2017 29/12/2016 29/12/2016 29/12/2016 29/12/2016
US 2013-0227689 A1	29/08/2013	EP 2815282 A1 EP 2815360 A1 EP 2948882 A1 JP 06277137 B2 JP 06359463 B2 JP 2015-510127 A JP 2015-513828 A JP 2016-511966 A US 10097417 B2 US 2013-0226485 A1 US 2014-0204799 A1 US 2016-0021059 A1 US 2017-0142067 A9 US 9110101 B2 US 9696346 B2 US 9733274 B2 WO 2013-123434 A1 WO 2013-123441 A1 WO 2014-116964 A1	24/12/2014 24/12/2014 02/12/2015 07/02/2018 18/07/2018 02/04/2015 14/05/2015 21/04/2016 09/10/2018 29/08/2013 24/07/2014 21/01/2016 18/05/2017 18/08/2015 04/07/2017 15/08/2017 22/08/2013 22/08/2013 31/07/2014
US 2017-0286675 A1	05/10/2017	EP 3437301 A2 KR 10-2018-0123557 A WO 2017-173087 A2 WO 2017-173087 A3	06/02/2019 16/11/2018 05/10/2017 23/08/2018

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i, H04L 12/40(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 29/06; G06F 1/12; G06F 21/55; H04L 29/08; H04L 12/40

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 침입탐지, 차량, CAN, 네트워크, 보안

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	US 2016-0205117 A1 (GM GLOBAL TECHNOLOGY OPERATIONS LLC) 2016.07.14 청구항 1 및 단락 [0015] 참조.	1-6, 18
Y		7-17, 19, 20
Y	KR 10-2015-0073176 A (타워-섹 리미티드) 2015.06.30 청구항 2 및 단락 [0463] 참조.	7-12, 17, 19
Y	US 2017-0013005 A1 (ARGUS CYBER SECURITY LTD.) 2017.01.12 단락 [0034] 참조.	13-17, 20
A	US 2013-0227689 A1 (TT GOVERNMENT SOLUTIONS, INC.) 2013.08.29 청구항 1-9 및 도 1A 참조.	1-20
A	US 2017-0286675 A1 (THE REGENTS OF THE UNIVERSITY OF MICHIGAN) 2017.10.05 청구항 1-7 및 도 5 참조.	1-20

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2019년 03월 19일 (19.03.2019)

국제조사보고서 발송일

2019년 03월 25일 (25.03.2019)

ISA/KR의 명칭 및 우편주소



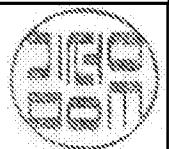
대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

김성우

전화번호 +82-42-481-3348



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2016-0205117 A1	2016/07/14	CN 105791266 A DE 102015122823 A1 US 9578047 B2	2016/07/20 2016/07/28 2017/02/21
KR 10-2015-0073176 A	2015/06/30	CN 105050868 A CN 105050868 B EP 2909065 A1 HK 1214216 A1 IL 238359 A IL 238359 B IL 238359 D0 JP 2016-502697 A MX 2015004828 A MX 356554 B US 2015-0271201 A1 US 2017-0149820 A1 US 9560071 B2 WO 2014-061021 A1	2015/11/11 2018/12/21 2015/08/26 2016/07/22 2015/06/30 2018/04/30 2015/06/30 2016/01/28 2016/01/08 2018/06/04 2015/09/24 2017/05/25 2017/01/31 2014/04/24
US 2017-0013005 A1	2017/01/12	EP 3113529 A1 US 2016-0381059 A1 US 2016-0381066 A1 US 2016-0381067 A1 US 2016-0381068 A1	2017/01/04 2016/12/29 2016/12/29 2016/12/29 2016/12/29
US 2013-0227689 A1	2013/08/29	EP 2815282 A1 EP 2815360 A1 EP 2948882 A1 JP 06277137 B2 JP 06359463 B2 JP 2015-510127 A JP 2015-513828 A JP 2016-511966 A US 10097417 B2 US 2013-0226485 A1 US 2014-0204799 A1 US 2016-0021059 A1 US 2017-0142067 A9 US 9110101 B2 US 9696346 B2 US 9733274 B2 WO 2013-123434 A1 WO 2013-123441 A1 WO 2014-116964 A1	2014/12/24 2014/12/24 2015/12/02 2018/02/07 2018/07/18 2015/04/02 2015/05/14 2016/04/21 2018/10/09 2013/08/29 2014/07/24 2016/01/21 2017/05/18 2015/08/18 2017/07/04 2017/08/15 2013/08/22 2013/08/22 2014/07/31
US 2017-0286675 A1	2017/10/05	EP 3437301 A2 KR 10-2018-0123557 A WO 2017-173087 A2 WO 2017-173087 A3	2019/02/06 2018/11/16 2017/10/05 2018/08/23