(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021 년 8 월 19 일 (19.08.2021)

WIPO | PCT

(10) 국제공개번호
WO 2021/162473 A1

(51) 국제특허분류:
H04L 12/40 (2006.01) *H04L 29/06* (2006.01)
B60R 25/30 (2013.01)

(21) 국제출원번호: PCT/KR2021/001826

(22) 국제출원일: 2021 년 2 월 10 일 (10.02.2021)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2020-0018611 2020 년 2 월 14 일 (14.02.2020) KR
10-2021-0019258 2021 년 2 월 10 일 (10.02.2021) KR

(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: 김태근 (**KIM, Tae Guen**); 18111 경기도 오산시 문시로 183-19, 104-1602, Gyeonggi-do (KR). 조아람 (**CHO, A Ram**); 17064 경기도 용인시 기흥구 중부대로 375, 102-2506, Gyeonggi-do (KR). 박승욱 (**PARK, Seung Wook**); 16803 경기도 용인시 수지구 태봉로 17, 403동 302호, Gyeonggi-do (KR). 임화평 (**LIM, Wha Pyeong**); 18271 경기도 화성시 남양읍 역골로 49번길 29 202호, Gyeonggi-do (KR).

(74) 대리인: 이철희 (**LEE, Chulhee**); 06229 서울시 강남구 도곡로33길 26, 베리타스빌딩 2-4층, Seoul (KR).

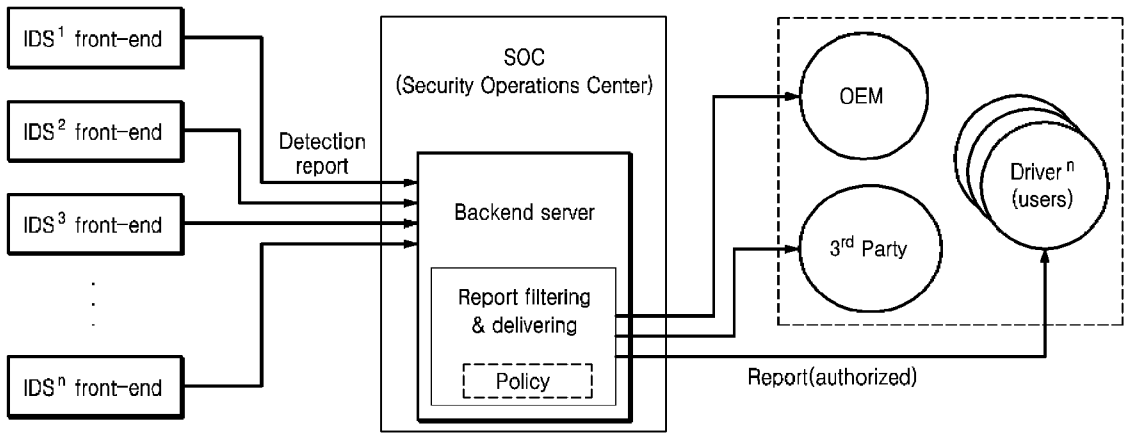
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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), 유

(54) **Title:** SYSTEM AND METHOD FOR DETECTING INTRUSION INTO IN-VEHICLE NETWORK

(54) **발명의 명칭:** 차량 내 네트워크에 대한 침입 탐지를 위한 시스템 및 방법

[도4]



(57) **Abstract:** The present invention relates to detection of intrusion into an in-vehicle network. The present disclosure proposes methods for efficiently managing multiple detection techniques which can reduce a required system resource while maintaining the architecture of an intrusion detection system (IDS) suitable to be mounted in a vehicle and robustness to a detected attack message or security event. In addition, the present disclosure proposes methods for determining severity and reliability of a detected security event and determining an action for the detected event on the basis of the determined severity and reliability.

(57) **요약서:** 본 발명은 본 발명은 차량 내 네트워크에 대한 침입 탐지에 관련되어 있다. 본 개시는 차량에 탑재하기에 적합한 침입 탐지 시스템(IDS)의 아키텍처와 공격 메시지 혹은 보안 이벤트 탐지에 대한 강인성을 유지하면서도 요구되는 시스템 자원을 줄일 수 있는 복수의 탐지 기법들의 효율적인 운용 방법들을 제시한다. 또한, 본 개시는 탐지된 보안 이벤트의 심각도와 신뢰도를 판단하고, 이를 기초로 탐지 이벤트에 대한 액션을 결정하는 방법들을 제시한다.

[다음 쪽 계속]

WO 2021/162473 A1

럽 (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))

명세서

발명의 명칭: 차량 내 네트워크에 대한 침입 탐지를 위한 시스템 및 방법

기술분야

[1] 본 발명은 차량 내 네트워크에 대한 침입 탐지에 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. IDS는 IPS는 탐지된 침입에 대응(예컨대 시스템에 영향을 줄 수 있는 신호를 차단)할 수 있는 기능 혹은 능력을 갖출 수도 있다. 차량에 탑재된 전자 제어 장치(ECU)들의 수가 크게 증가하고, 유선 및 무선 네트워크를 통해 차량이 외부 네트워크와 연결됨에 따라, 차량의 내부 네트워크의 보안 위협을 탐지하고 대응하기 위해 IDS가 도입되고 있는 추세이다.

발명의 상세한 설명

기술적 과제

[4] 본 개시는 차량에 탑재하기에 적합한 침입 탐지 시스템(IDS)의 아키텍처와 공격 메시지 혹은 보안 이벤트 탐지에 대한 강인성을 유지하면서도 요구되는 시스템 자원을 줄일 수 있는 복수의 탐지 기법들의 효율적인 운용 방법들을 제시한다. 또한, 본 개시는 탐지된 보안 이벤트의 심각도와 신뢰도를 판단하고, 이를 기초로 탐지 이벤트에 대한 액션을 결정하는 방법들을 제시한다.

기술적 해결방법

[5] 본 개시의 일 측면에 의하면, 차량 내 네트워크에서 침입을 탐지하기 위한 침입 탐지 시스템은, 차량 내 네트워크로부터 수집되는 네트워크 메시지들을 메시지 큐에 저장하기 위한 메시지 큐 모듈; 복수의 탐지 기법들에 사용되는 탐지 룰들(detection rules)의 집합인 룰-셋(ruleset)을 안전하게 저장하기 위한 저장소; 보안 이벤트들을 탐지하기 위해 상기 수집된 네트워크 메시지에 대해 상기 복수의 탐지 기법들을 적용하고, 탐지된 보안 이벤트들 각각에 대해 심각도 점수와 신뢰도 점수를 결정하도록 구성된 룰 엔진; 및 상기 보안 이벤트들의 탐지에 응답하여 탐지 리포트들을 원격의 백앤드 서버에 전송하기 위한 인터페이스 매니저를 포함한다.

[6] 상기 침입 탐지 시스템의 실시예들은 다음의 특징들을 하나 이상 더 포함할 수 있다.

[7] 일부 실시예에서, 상기 심각도 점수는 관련된 보안 이벤트가 차량 혹은

운전자의 안전에 얼마나 위험한지를 나타내는 값이며, 관련된 보안 이벤트의 검출에 성공한 탐지 룰에 대해 미리 정의된 중요도를 기초로 결정될 수 있다.

[8] 일부 실시예에서, 상기 신뢰도 점수는 관련된 보안 이벤트가 실제 공격일 가능성을 나타내는 값이며, 관련된 보안 이벤트의 특성과 상기 차량 내 네트워크의 정상적인 특성 간의 차이에 기초하여 결정될 수 있다. 예를 들어, 네트워크 메시지들이 정상 전송 주기와는 상이한 주기로 전송되는 보안 이벤트에 대해, 상기 신뢰도 점수는 상기 정상 전송 주기로부터 벗어난 편차를 기초로 결정될 수 있다.

[9] 일부 실시예에서, 상기 룰 엔진은, 상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트에 대한 액션을 결정할 수 있다.

[10] 일부 실시예에서, 상기 인터페이스 매니저는, 상기 심각도 점수와 상기 신뢰도 점수를 기초로, 상기 탐지 리포트들의 전송 순서 혹은 전송 타이밍을 결정하도록 구성될 수 있다.

[11] 일부 실시예에서, 상기 인터페이스 매니저는 상기 심각도 점수와 상기 신뢰도 점수를 기초로 관련된 보안 이벤트의 우선순위를 결정하고, 상기 우선 순위가 미리 정의된 값보다 높은 보안 이벤트에 대해서는 탐지 리포트를 실시간으로 상기 백엔드 서버로 전달하며, 그렇지 않은 보안 이벤트에 대해서는 탐지 리포트를 유휴 시간 동안에 상기 백엔드 서버로 전달하도록 구성될 수 있다.

[12] 일부 실시예에서, 상기 인터페이스 매니저는 상기 보안 이벤트들의 탐지 순서대로 상기 탐지 리포트를 상기 백엔드 서버로 전송하되, 미리 정의된 시간 구간 동안에 복수의 보안 이벤트가 탐지된 경우에, 상기 심각도 점수와 상기 신뢰도 점수를 기초로 각 보안 이벤트의 우선 순위를 결정하고, 각 보안 이벤트에 대한 탐지 리포트를 상기 우선 순위에 따라 상기 백엔드 서버로 전송하도록 구성될 수 있다.

[13] 본 개시의 다른 측면에 의하면, 차량 내 네트워크에서 침입을 탐지하기 위한 침입 탐지 시스템에 의해 수행되는 방법이 제시된다. 상기 방법은 차량 내 네트워크로부터 수집되는 네트워크 메시지들을 메시지 큐에 저장하는 단계; 보안 이벤트들을 탐지하기 위해 상기 수집된 네트워크 메시지에 대해 복수의 탐지 기법들을 적용하는 단계, 상기 복수의 탐지 기법들은 탐지 룰들(detection rules)의 집합인 룰-셋(ruleset)을 이용함; 탐지된 보안 이벤트들 각각에 대해 심각도 점수와 신뢰도 점수를 결정하는 단계; 및 상기 보안 이벤트들의 탐지에 응답하여, 탐지 리포트들을 원격의 백엔드 서버에 전송하는 단계를 포함한다.

[14] 이러한 침입 탐지 시스템 및 그 동작 방법은 제한된 처리 능력과 제한된 네트웍 대역폭을 가진 차량 환경에서 위협적인 공격에 대해 신속한 대응을 가능하게 한다.

도면의 간단한 설명

[15] 도 1은 CAN 네트워크 상에서 IDS가 배치될 수 있는 위치들을 예시한 것이다.

[16] 도 2는 본 발명의 일 실시예에 따른 차량 내 네트워크에서 보안 이벤트를 탐지하기 위한 IDS의 기능적인 블록도이다.

[17] 도 3은 본 발명의 일 실시예에 따른, IDS의 예시적인 동작을 도시한 흐름도이다.

[18] 도 4는 본 발명의 일 실시예에 따른 차량들로부터 탐지된 보안 이벤트들이 원격 서버에서 수집되고 배포되는 방식을 보이는 개념도이다.

[19] 도 5는 본 발명에서 사용될 수 있는 예시적인 탐지 리포트의 메시지 포맷을 보인다.

발명의 실시를 위한 형태

[20] 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.

[21] 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.

[22] 도 1은 차량의 CAN 네트워크 상에서 IDS가 배치될 수 있는 위치들 {(a),(b), (c), (d), (e)}을 예시한 것이다. 센트럴 게이트웨이(central gateway; CGW)는 차량 내 여러 도메인들간에 데이터를 전달하는 라우터 역할을 수행하고, 외부 네트워크와 차량 내 네트워크 간의 통신에 대한 게이트 역할을 하는 센트럴 통신 노드이다. 센트럴 게이트웨이(CGW)는 차량으로 들어오는 모든 데이터에 대한 게이트라고 볼 수 있다. 서브 게이트웨이(sub-gatewary)는 파워 트레인, 새시, 바디, 인포테인먼트(Infotainment) 등과 같은 특정 기능 도메인을 담당하는 로컬 통신 노드이다. 도 1에서는 각 기능 도메인에서 ECU(Electronic Control Unit)들이 CAN 버스에 연결되는 것을 전제하고 있으나, 일부 기능 도메인에서 다른 통신 프로토콜(예컨대, LIN, FlexRay, Ethernet 등)을 사용하는 버스에 연결될 수도 있을 것이다.

[23] 각 위치 별 장단점은 다음과 같다.

[24] **(a) 센트럴 게이트웨이에 탑재 -** 외부와 모든 CAN 도메인이 연결되는 이곳에

IDS을 설치하면, OBD 포트를 통해 CAN 네트워크로 들어오는 모든 공격을 탐지할 수 있다. 따라서 공격 의도를 가진 메시지가 CAN 네트워크에 영향을 미치기에 앞서 미연에 파악할 수 있다. 그러나 다른 위치들에 비해 매우 많은 메시지를 처리하여야 하므로, 내부 네트워크로 침입하려는 공격과 그렇지 않은 메시지를 구분하기 어렵기 때문에 공격에 효율적으로 대응하기 어렵다.

[25] **(b) 센트럴 게이트웨이 뒤** - 센트럴 게이트웨이의 메시지 필터링을 거친 뒤의 메시지를 검사한다. (a)를 지나기 전보다는 더 적은 수의, 그러나 더 강력한 의지를 가진 공격자를 탐지할 수 있다. 또한 CAN 버스에 외부에서 직접 접근하여 악성 메시지를 주입하는 해킹을 탐지할 수 있다.

[26] **(c) 서브 게이트웨이에 탑재** - 특정 CAN 도메인으로 송수신되는 CAN 메시지를 관리하는 곳에 IDS를 설치하면, (b)에서의 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.

[27] **(d) 서브 게이트웨이 뒤** - 특정 악의적 메시지로 이중의 게이트웨이를 통과하여 시스템을 해킹하는 것은 쉽지 않다. 그러나 내부 제어기(ECU)가 공격자에 의해 손상되었거나 악의적 제어기가 교체되어 위장되었을 경우, 그리고 외부에서 직접 해당 도메인의 CAN 버스에 연결한 경우, 해당 도메인 내의 CAN 버스에 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 고려될 수 있는 위치이다.

[28] (e) **ECU에 탑재** - ECU는 네트워크상에 존재하는 모든 메시지를 수신하고 필요한 CAN 메시지의 ID를 확인하여 필요로 하는 메시지를 선택적으로 처리한다. 제어기는 제어기 외부로부터 받은 CAN 상태 메시지와 CAN 명령 메시지의 컨텍스트(context)를 분석한 뒤 구동한다. 따라서, ECU는 외부와 내부 모두로부터 보호되어야 하기 때문에 높은 보안 수준을 필요로 한다. ECU에 IDS를 탑재하는 것은 ECU를 변조할 수 있는 매우 능력이 뛰어난 내부/외부 공격자로부터 ECU가 가진 중요 데이터의 손실이나 기능의 오동작을 막기 위함이다.

[29] 도 1에 예시된 위치에 IDS가 배치될 수 있는 위치들 {(a),(b), (c), (d), (e)} 중 적어도 하나의 위치에 복수의 IDS이 배치될 수도 있다. 예컨대, 센트럴 게이트웨이와 복수의 서브 게이트웨이에 각각 IDS가 임베딩될 수도 있으며, 센트럴 게이트웨이와 주요 ECU에 각각 IDS가 임베딩될 수도 있다. 또한, 각 도메인에는 도메인 레벨의 모니터링을 수행하는 전용 전자 제어 장치가 설치될 수도 있다. 이들 IDS는 상호 보완적으로 네트워크를 모니터링하고 공격 시도를 탐지하여, 차량 네트워크의 보안을 강화할 수 있을 것이다.

[30] 도 2는 본 발명의 일 실시예에 따른 차량 내 네트워크에서 보안 이벤트를 탐지하기 위한 IDS의 기능적인 블록도이다.

[31] 도 2에 예시된 바와 같이, 침입 탐지 시스템(IDS)는 메시지 큐 모듈(message queue module; 20), 룰 엔진(rule engine; 30), 암호화 모듈(crypto module; 40), 인터페이스 매니저(interface manager; 50), 및 저장소(storage; 60)를 포함할 수 있다. 도 2에 예시된 침입 탐지 시스템(IDS)은 도 1에 예시된 게이트웨이(들) 혹은 ECU(들)에 임베드되거나, 차량 네트워크에 연결된 전용 전자 제어 장치로 구현될 수 있다.

[32] 메시지 큐 모듈(20)은 CAN 버스에서 수집된 모든 CAN 트래픽 데이터를 메시지 큐(message queue)에 저장한다. 수집된 트래픽 데이터에 대한 IDS의 다른 모듈들의 요청은 메시지 큐 모듈(20)에 의해 처리된다.

[33] 룰 엔진(혹은 '탐지 엔진'으로도 지칭될 수 있음; 30)은 IDS의 본질적인 기능인 탐지자(detector) 및 응답자(responder)로서 동작하는 모듈이다. 룰 엔진(30)의 기능은, 크게, 사전 프로세스(pre-process; 31), 탐지 프로세스(detection process; 32), 사후 프로세스(post process; 33)로 구분될 수 있다.

[34] 사전 프로세스(pre-process; 31)에서, 룰 엔진(30)은 다양한 수단들(예컨대, 백-엔드 서버(backend server), USB 메모리 스틱, SD 카드 등)을 통해 획득된 탐지 룰-셋(detection ruleset; 10)으로 저장소(60)에 저장된 룰-셋을 업데이트하거나 IDS를 리셋한다. 탐지 룰-셋은 탐지 프로세스에서 수행되는 복수의 탐지 기법들이 보안 위협과 관련된 네트워크 메시지를 탐지하는 데에 사용하는 미리 정의된 룰들의 집합이다. 탐지 프로세스(detection process; 32)에서, 룰 엔진(30)은 복수의 탐지 기법들을 이용하여, 주행 중에 보안 위협과 관련된 네트워크 메시지를 탐지함으로써 보안 이벤트의 발생을 탐지한다. 사후 프로세스(post process; 33)에서, 룰 엔진(30)은 탐지된 보안 위협 메시지를 어떻게 처리할지 결정한다. 예컨대, 탐지된 악성 메시지를 드랍(drop)하거나, 로깅(logging) 혹은 알람을 생성할 수 있다. 룰 엔진(30)은 보안 이벤트가 발생하면(즉, 보안 위협 메시지가 탐지되면), 보안 이벤트에 대한 심각도 점수와 신뢰도 점수를 결정할 수 있다.

[35] 암호화 모듈(40)은 룰-셋과 탐지 로그를 암호화하거나 복호화하고, 관련된 키들을 관리한다.

[36] 인터페이스 매니저(50)는, 백엔드 서버로부터 새로운 룰-셋(10)을 다운로드하거나 탐지 로그 혹은 탐지 결과를 백엔드 서버에 전송하기 위해, 백엔드 서버와의 통신 연결을 관리한다. 탐지 룰-셋과 탐지 로그는 암호화 엔진에 의해 암호화되어 저장소(60; 예컨대, 플래쉬 메모리)에 안전하게 저장된다. 저장소(60)는 차량 내 네트워크 상의 다른 노드에 의해 제공될 수도 있다. 이 경우, 인터페이스 매니저(50)는 다른 노드에 위치한 저장소(60)와의 통신 연결도 관리할 수 있다.

[37] 도 3은 본 발명의 일 실시예에 따른 IDS의 예시적인 동작을 도시한 흐름도이다.

[38] IDS는 차량의 시동이 켜지면 사전 프로세스(pre-process)을 수행하고, 그 후 차량 시동이 꺼질 때까지 탐지 프로세스(detection process)와 사후

프로세스(post-process)를 반복적으로 수행하도록 구성될 수 있다.

[39] 사전 프로세스(pre-process)에서, IDS가 재시작 되면 탐지 룰-셋의 버전을 체크하고 현재 저장소에 저장된 탐지 룰-셋이 최신 버전이 아닐 경우, 예컨대, OTA을 통해 다운받은 혹은 OBD 포트를 통해 수신된 최신 버전의 탐지 룰-셋으로 업데이트할 수 있다. 이후 IDS는 저장소에 저장된 암호화된 룰-셋을 복호화하여 내부 메모리(RAM)로 로드한다. 사전 프로세스가 종료되면 IDS의 실질적인 탐지 동작인 탐지 프로세스가 시작된다.

[40] 탐지 프로세스(detection process)에서, IDS는, 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', 혹은 '공격 메시지'로도 지칭될 수 있음)인지 여부를 판단하기 위해, 오용 탐지(misuse detection), 시그니처 탐지(signature detection), 및 이상 탐지(anomaly detection) 기법을 순차적으로 수행할 수 있다.

[41] 사후 프로세스(post-process)에서는, CAN 메시지들에 대한 검사 결과에 따라 통과, 차단, 로깅(logging), 혹은 경고와 같은 액션이 취해진다. 보안 이벤트가 발생하면(즉, 보안 위협 메시지가 탐지되면), IDS는, 공격 소스를 식별하거나, 공격의 심각도를 분류하거나, 기능 안전에 대한 영향을 분석할 수도 있다. 또한, IDS는, 예컨대 보안 이벤트에 대한 탐지 로그가 원격 네트워크 상의 백-엔드 서버에 전송되도록, 원격 네트워크에 통신적으로 연결될 수 있는 게이트웨이 혹은 텔레매틱스 디바이스에 CAN 네트워크를 통해(혹은 별도의 통신 라인을 통해) 탐지 로그가 담긴 메시지(이하 '탐지 리포트' 혹은 '탐지 리포트 메시지'로 지칭됨)를 전달할 수도 있다.

[42] 전술한 침입 탐지 기법의 특성 및 장단점은 다음과 같다.

[43] 오용 탐지(Misuse Detection)는 CAN 메시지의 ID, CAN 메시지의 길이(Data length code: DLC), 메시지 전송 주기 등을 CAN 데이터베이스에 명시된 값들과 비교하여 CAN 메시지의 유효성(validity) 검사를 하는 기법이다. 즉, 시그니처 탐지에서는 수집된 CAN 메시지가 제조사에서 미리 정해 놓은 '유효한 메시지 형식'에 맞는지 미리 정의된 룰들에 따라 체크된다.

[44] 시그니처 탐지는, 시그니처 탐지 및 이상 탐지에 비해, 시스템 자원을 적게 소모한다. 다만, 유효성 검사만으로는 메시지 내에 들어 있는 악성 데이터 등은 탐지가 불가능하다.

[45] 시그니처 탐지(Signature Detection)는, 차량 시스템의 취약점 분석을 통해 미리 정의해 둔(즉, 이미 알려진), 공격 패턴을 탐지하는 기법이다. 이러한 공격 패턴은 시그니처(signature)라고도 불린다. 시그니처 탐지는, 차량의 상태를 고려하지 않고, 악의적인 메시지의 시그니처들이 수록된 블랙리스트(Black List)를 체크하여, 수집된 메시지가 악의적인 메시지인지 판단한다.

[46] 시그니처 탐지는 시스템의 자원을 적게 소모하고 탐지 확률이 높다는 장점이 있으나, 새로운 공격마다 새로운 시그니처를 정의해야 하므로 새로 출현한

공격에 대처하기 위해서는 많은 시간과 보안 인적 자원을 필요로 한다. 이 기법은 실제 공격을 놓칠 수 있는 거짓 음성(false negative; 2종 오류) 문제가 생길 수 있다.

[47] 이상 탐지(Anomaly Detection)는 차량의 상태를 기반하여 해당 메시지가 정상 메시지 범주 안에 있는 지를 확인하는 기법으로서, 차량의 상태와 명령 메시지에 기반한 탐지 룰들에 기초하여 이루어진다. 이상 탐지는 네트워크 상에서의 일반적인 행동을 수집 및 분석하여 정상적인 패턴('프로파일'로도 불릴 수 있음)을 정의한 후 정상 패턴에서 일정한 임계치(threshold)를 벗어난 행동을 탐지하는 기법이다. 이상 탐지는 프로파일(profile) 기반의 탐지로도 불린다. 예를 들어, 이상 탐지는 CAN 메시지에 포함된 데이터의 변화율이 정상 범위를 초과하거나 특정 기간에 상관 관계가 높은 두 신호가 갑자기 상관 관계가 해제되는 행위를 탐지할 수 있다.

[48] 이상 탐지의 경우 알려지지 않은 새로운 공격이 출현하였을 때에도 이러한 공격이 정상 패턴에서 벗어난 경우 탐지가 가능하며 시그니처 탐지 방법에 비해 보안 인적 자원의 비중이 적다. 그러나 많은 시스템 자원을 필요로 하며 설정된 임계치에 따라 정상적인 활동을 침입으로 식별하는 거짓 양성(false positive, 1종 오류) 문제가 생길 수 있다.

[49] 전술한 바와 같이, 탐지 룰-셋은 탐지 프로세스에서 수행되는 복수의 탐지 기법들이 보안 위협과 관련된 네트워크 메시지를 탐지하는 데에 사용하는 미리 정의된 룰들의 집합이다. 탐지 룰-셋은 오용 탐지에 사용되는 오용 룰-셋(misuse ruleset), 시그니처 룰-셋(signature ruleset), 및 이상 룰-셋(anomaly ruleset)을 포함할 수 있다.

[50] 표 1 내지 표 3은 예시적인 탐지 룰-셋의 구조들을 보인다. 표 1은 CAN 데이터베이스에 기초하여 정의된 기본적인 룰-셋들을 예시하고, 표 2는 신호들 간의 상관 계수 맵을 예시하며, 표 3은 시그너처 탐지에 사용되는 미리 알려진 공격 패턴인 시그니처를 예시한다. 표 1에서 CAN ID, DLC, Signal ID, Signal value 및 Bus ID는 오용 탐지에 사용될 수 있으며, 표 1에 정의된 범위를 벗어난 값들을 가지는 메시지는 비정상으로 간주될 수 있다. 표 1에 예시된 Message rate, Signal value change rate, Correlated Signal ID와 표 2에 예시된 신호들간의 상관 계수들은 이상 탐지에 사용될 수 있다.

[51] [표1]

CAN ID	DLC	Signal ID	Signal value	Bus ID	Message rate	Signal value change rate	Correlated Signal ID
0x01	0x08	0x10	0x00~0xFF	0x01	90ms ~ 100ms	10% ~ 20%	0x30
0x02	0x08	0x20	0x00~0x80	0x02	90ms ~ 100ms	10% ~ 20%	-
…	…	…	…	…	…	…	…

[52]

[표2]

Signal ID	0x01	0x02	0x03	0x04	…
0x01	1	0.5	0.9	0.6	…
0x02	0.5	1	0.7	-0.9	…
0x03	0.9	0.7	1	-0.5	…
0x04	0.6	-0.9	-0.5	1	…
…	…	…	…	…	…

[53] [표3]

No	Signature pattern
1	ff 00 01 86 a5
2	75 05 a6 f5 a2
3	00 40 45 00 00
4	ff 31 c3 77 45 65 c5
…	…

[54] 도 3의 예시된 동작에 따르면, 메시지 큐(Message Queue)에 쌓인 각 메시지는 세 가지 탐지 기법으로 구성된 탐지 프로세스(즉, 오용 탐지 --> 시그니처 탐지 --> 이상 탐지)를 거치면서 그 메시지의 차단 혹은 통과가 결정된다. 따라서, 예시된 탐지 프로세스에서, 정상적인 CAN 메시지 역시 세 가지 기법으로 구성된 탐지 프로세스를 거친 후에 비로소 IDS가 탑재된 게이트웨이 혹은 ECU의 응용 소프트웨어로 전달된다. 또한, 적용된 탐지 기법이 CAN 메시지를 보안 위협 메시지로 결정하면, 해당 CAN 메시지에 대한 나머지 탐지 기법들의 적용은 바이패스된다.

[55] 따라서, 탐지 효율이 높고 요구되는 컴퓨팅 파워와 소요시간이 적은 탐지 기법들이 먼저 적용될수록, 전체적인 탐지 프로세스의 효율이 증가할 것이다. 예시된 탐지 프로세스는 낮은 컴퓨팅 파워와 적은 소요시간이 예상되는 기법들을 먼저 적용하도록 구성되었음에 주목한다. 이러한 탐지 프로세스의 구성을 통해, 악의적 메시지의 탐지에 대한 강인성을 유지하면서도, 전체적인 탐지 프로세스의 효율을 높일 수 있다.

[56] 도 3의 예시된 IDS의 동작에서는, 탐지 프로세스에서 세 가지 탐지 기법(즉, 오용 탐지, 시그니처 탐지, 이상 탐지)을 모두 사용되고 있다. 그러나, IDS가 배치된 위치에 따라, 세 가지 탐지 기법들 중에서 일부 기법이 생략될 수 있다. 예컨대, 이상 탐지에는 많은 컴퓨팅 파워와 시간이 소요되는 바, ECU에 임베딩된 IDS의 탐지 프로세스에서는 오용 탐지만 사용되거나, 오용 탐지와 시그니처 탐지만 사용될 수도 있다. 반면, 상대적으로 높은 컴퓨팅 파워를 가지는 (센트럴/서브) 게이트웨이에 임베딩된 IDS의 탐지 프로세스에서는 세

가지 탐지 기법이 모두 사용될 수도 있다. 다른 예로, 센트럴 게이트웨이에서는 세 가지 탐지 기법이 모두 사용되고, 서브 게이트웨이에서는 오용 탐지와 시그니처 탐지만이 사용되고, ECU에서는 오용 탐지만이 사용될 수도 있다.

[57] 도 4는 본 발명의 일 실시예에 따른 차량들로부터 탐지된 보안 이벤트들이 원격 서버에서 수집되고 배포되는 방식을 보이는 개념도이다.

[58] 각 차량은 IDS에서 탐지된 보안 이벤트를, 보안 이벤트들을 관리하고 분석하는 보안 운영 센터(security operations center; SOC)로 전달할 수 있다. 각 차량의 IDS는 탐지 리포트를 생성할 수 있다. 탐지 리포트는 기밀성과 무결성을 유지하기 위해 보안 채널을 통해 보안 운영 센터의 백엔드 서버로 전송될 수 있다. 탐지 리포트는 다음과 같은 항목들을 포함할 수 있다.

[59] - 차량 식별 번호(Vehicle Identification Number; VIN)

[60] - 이벤트 탐지 시점에서의 차량 상태(예컨대, 변속기 제어 유닛에서 제공되는 차량 속도, 엔진 제어 유닛에서 제공되는 엔진 냉각수 온도, 차체 제어 유닛에서 제공되는 스티어링 휠 각도 등)

[61] - 이벤트 타임스탬프(이벤트 날짜, 이벤트 시간)

[62] - 탐지된 이벤트에 관련된 탐지 룰을 식별하는 룰 식별자(Rule ID)

[63] - 탐지된 이벤트에 관련된 CAN 메시지에서 취득된 CAN ID

[64] - 탐지된 이벤트에 관련된 CAN 메시지의 내용(contents)

[65] 도 5는 본 발명에서 사용될 수 있는 예시적인 탐지 리포트의 메시지 포맷을 보인다.

[66] 도 5에 보인 바와 같이, 탐지 리포트 메시지는 Tag, LEN, VIN, Vehicle status, Event date, Event time, Rule ID, CAN ID 및 Message contents 필드들로 구성될 수 있다. 탐지 리포트에서, 데이터의 기밀성을 보장하기 위해, Tag 필드 및 LEN 필드를 제외한 나머지 필드들의 데이터가 암호화될 수 있다. Tag 필드는 본 메시지가 탐지 리프트 메시지임을 식별하기 위한 값이 들어가며, LEN 필드에는 암호화되는 필드들(VIN 필드부터 메시지 내용 필드)의 데이터 길이를 나타내는 값이 들어가며, 보안 운영 센터의 백엔드 서버에서 각 데이터 항목을 파싱하는 데 이용될 수 있다. 또한 탐지 리포트의 무결성을 보장하기 위해, 태그 및 길이 데이터 필드를 포함한 전체 필드들에 대한 디지털 서명을 생성하여 탐지 보고서에 덧붙여질 수 있다.

[67] 보안 운영 센터는 보안 전문가에 의해 관리되는 보안 정보 및 이벤트 관리 시스템을 포함한 백엔드 서버를 운영하고, 각 차량의 IDS에 의해 생성된 보안 이벤트들을 수집하고 통계적으로 분석할 수 있다. 보안 운영 센터는 수집된 탐지 리포트들과 관련 정보(예를 들어, 보안 위협의 수준, 추천하는 액션)를 차량 제조사(OEM), 차량 운전자, 차량 소유자, 제3자 등 데이터 액세스 권한을 가진 이해 관계자들에게 제공할 수 있다. 제3자에는 보험 회사 또는 주행 데이터 분석 서비스 제공자가 포함될 수 있다.

[68] IDS는 탐지된 보안 이벤트들에 심각도 점수와 신뢰도 점수를 결정할 수 있다.

심각도 점수는 보안 이벤트가 차량 혹은 운전자의 안전에 얼마나 위험한지를 나타내는 값이다. 심각도 점수는 보안 이벤트가 위반한 특정 탐지 룰의 중요도에 따라 결정될 수 있다. 각 탐지 룰의 중요도는 보안 전문가에 의해 미리 정의될 수 있다. 신뢰도 점수는 IDS에 의해 탐지된 보안 이벤트가 실제 공격일 가능성을 나타내는 값이다. 신뢰도 점수는 IDS에 의해 탐지 룰의 위반이 탐지될 때마다 동적으로 계산되며, 탐지 룰의 위반의 정도(예컨대, 차량 내 네트워크의 정상적인 특성으로부터 벗어난 편차)를 기초로 결정될 수 있다. 예를 들어, 정상 메시지 전송 주기를 위반한 2개의 의심 메시지가 탐지되었고, 각 의심 메시지의 전송 주기가 정상 전송 주기로부터 벗어난 편차가 각각 10ms와 20ms인 경우에, IDS는 10ms 차이를 보이는 메시지보다 20ms 차이를 보이는 의심 메시지에 더 큰 신뢰도 점수를 부여할 수 있다. 다른 예로, IDS는 의심 메시지에 포함된 데이터 혹은 데이터의 변화율이 정상 범위를 더 크게 초과할수록 더 큰 신뢰도 점수를 부여할 수 있다.

[69] IDS는 심각도 점수와 신뢰도 점수를 기초로, 보안 이벤트에 대한 액션을 결정할 수도 있다. 예를 들어, 차량의 안전에 심각한 영향을 줄 수 있는 높은 심각도 점수를 갖는 보안 이벤트가 탐지되었을 때, IDS는 차량의 주행을 즉시 중지할 것을 권고하는 알람을 운전자에게 제공할 수도 있다. 다른 일 예로, 낮은 신뢰도 점수를 갖는 보안 이벤트들이 지속적으로 탐지되는 경우에, IDS는 차량의 정비 혹은 검사를 권고하는 알람을 운전자에게 제공할 수도 있다. 또 다른 일 예로, 낮은 심각도 점수를 갖는 보안 이벤트들이 탐지된 경우에, 그 탐지 결과를 로그에 기록하되, 운전자에게는 아무런 알람도 제공하지 않을 수도 있다. 보안 이벤트에 대한 빈번한 알람은 운전자로 하여금 중요한 알람을 간과하게 만들 수 있다.

[70] IDS는 관련된 보안 이벤트의 심각도 점수와 신뢰도 점수에 기초하여, 탐지 리포트들의 전달 순서의 우선 순위를 결정할 수도 있다. 전달 순서의 우선 순위는 보안 이벤트의 심각도 점수와 신뢰도 점수에 따라 결정될 수 있다. 예를 들어, 우선 순위는 심각도 점수와 신뢰도 점수의 합산, 가중합, 혹은 평균을 이용하여 산술적으로 결정될 수 있다. 일부 실시예에서, IDS는 관련된 보안 이벤트의 탐지 순서에 따라 탐지 리포트들을 백엔드 서버에 전달하되, 단기간에 여러 보안 이벤트들이 탐지된 경우에, 탐지된 보안 이벤트들의 우선 순위에 따라 관련된 탐지 리포트들을 보안 운영 센터의 백엔드 서버에 전달할 수도 있다.

[71] IDS는 관련된 보안 이벤트의 심각도 점수와 신뢰도 점수 혹은 우선 순위에 기초하여, 탐지 리포트들의 전달 타이밍을 결정할 수도 있다. 예컨대, IDS는 산출된 우선순위(혹은 심각도 점수)가 미리 정의된 값보다 높은 보안 이벤트에 대해서는 탐지 리포트를 실시간으로(즉, 탐지 즉시) 보안 운영 센터의 백엔드 서버로 전달하고, 그렇지 않은 보안 이벤트에 대해서는 탐지 리포트를 비실시간으로(즉, 유휴 시간 동안에) 보안 운영 센터의 백엔드 서버로 전달할 수도 있다.

[72] 전술한 리포팅 방식들은, 제한된 처리 능력과 제한된 네트웍 대역폭을 가진 차량 환경에서, 위협적인 공격에 대해 신속한 대응을 가능하게 한다.

[73] 예컨대, 우선 순위에 기초하여 탐지 리포트들의 전달 순서를 결정함으로써, 우선순위가 높은(즉, 위협적인) 공격의 발생을 보안 운영 센터에 보다 신속하게 알릴 수 있으며, 보안 운영 센터가 위협 상황에서 벗어날 수 있도록 운전자 등에게 빠르게 가이드할 수 있게 한다. 차량에서 발생하는 공격에 대해 위협의 정도와 상관없이 순차적으로 리포팅을 하는 방식은, 큰 위협이 없는 이벤트들을 리포팅하느라 위협적인 공격에 대한 리포팅이 늦어질 수 있어, 운전자의 위협 대응력이 크게 떨어질 수 있다.

[74] 일부 실시예에서, IDS는 심각도 점수, 신뢰도 점수, 혹은 우선 순위에 기초하여 보안 운영 센터의 백엔드 서버로의 탐지 리포트 전달을 생략할지 여부를 결정할 수도 있다. 예를 들어, 차량의 IDS는 미리 정의된 값보다 낮은 심각도 점수를 가지는 보안 이벤트에 대해 탐지 리포트 전달을 생략할 수도 있다. 다른 예로, 미리 정의된 값보다 높은 심각도 점수를 가지는 보안 이벤트에 대해서는, 그 신뢰도 점수와 무관하게, 보안 운영 센터의 백엔드 서버로 탐지 리포트를 전달할 수도 있다. 일부 실시예에서, 미리 정의된 값보다 낮은 심각도 점수를 가지는 보안 이벤트들에 대해, IDS는 전술한 포맷의 탐지 리포트 대신에 이벤트들에 대한 요약된 탐지 정보를 백엔드 서버에 전송할 수도 있다. 이는 차량의 제한된 리소스를 효율적으로 사용할 수 있게 하며, 다수의 차량들로부터 탐지 리포트를 수신하여야 하는 백엔드 서버의 부하를 경감할 수 있다.

[75] 전술한 예시적인 실시예들은 많은 상이한 방식들로 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.

[76] 한편, 본 개시에서 설명된 다양한 방법들은 하나 이상의 프로세서에 의해 판독되고 실행될 수 있는 비일시적 기록매체에 저장된 명령어들로 구현될 수도 있다. 비일시적 기록매체는, 예를 들어, 컴퓨터 시스템에 의하여 판독가능한 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.

[77] 이상의 설명은 본 발명의 실시예들의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이

가능할 것이다. 따라서, 본 실시예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다.

[78] [CROSS-REFERENCE TO RELATED APPLICATION]

[79] 본 특허출원은, 본 명세서에 그 전체가 참고로서 포함되는, 2020년 2월 14일자로 한국에 출원한 특허출원번호 제10-2020-0018611호 및 2021년 2월 10일자로 한국에 출원한 특허출원번호 제10-2021-0019258호에 대해 우선권을 주장한다.

청구범위

[청구항 1] 차량 내 네트워크에서 침입을 탐지하기 위한 침입 탐지 시스템으로서,
차량 내 네트워크로부터 수집되는 네트워크 메시지들을 메시지 큐에 저장하기 위한 메시지 큐 모듈;
복수의 탐지 기법들에 사용되는 탐지 룰들(detection rules)의 집합인 룰-셋(ruleset)을 안전하게 저장하기 위한 저장소;
보안 이벤트들을 탐지하기 위해 상기 수집된 네트워크 메시지에 대해 상기 복수의 탐지 기법들을 적용하고, 탐지된 보안 이벤트들 각각에 대해 심각도 점수와 신뢰도 점수를 결정하도록 구성된 룰 엔진; 및
상기 보안 이벤트들의 탐지에 응답하여 탐지 리포트들을 원격의 백엔드 서버에 전송하기 위한 인터페이스 매니저
포함하는, 침입 탐지 시스템.

[청구항 2] 제1항에 있어서,
상기 심각도 점수는,
관련된 보안 이벤트가 차량 혹은 운전자의 안전에 얼마나 위험한지를 나타내는 값이며, 관련된 보안 이벤트의 검출에 성공한 탐지 룰에 대해 미리 정의된 중요도를 기초로 결정되는 것인, 침입 탐지 시스템.

[청구항 3] 제1항에 있어서,
상기 신뢰도 점수는,
관련된 보안 이벤트가 실제 공격일 가능성을 나타내는 값이며, 관련된 보안 이벤트의 특성과 상기 차량 내 네트워크의 정상적인 특성 간의 차이에 기초하여 결정되는 것인, 침입 탐지 시스템.

[청구항 4] 제3항에 있어서,
네트워크 메시지들이 정상 전송 주기와는 상이한 주기로 전송되는 보안 이벤트에 대해, 상기 신뢰도 점수는 상기 정상 전송 주기로부터 벗어난 편차를 기초로 결정되는 것인, 침입 탐지 시스템.

[청구항 5] 제1항에 있어서,
상기 룰 엔진은,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트에 대한 액션을 결정하도록 구성된, 침입 탐지 시스템.

[청구항 6] 제1항에 있어서,
상기 인터페이스 매니저는,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 상기 탐지 리포트들의 전송 순서를 결정하도록 구성된, 침입 탐지 시스템.

[청구항 7] 제1항에 있어서,
상기 인터페이스 매니저는,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 상기 탐지 리포트들의

전송 타이밍을 결정하도록 구성된, 침입 탐지 시스템.

[청구항 8] 제1항에 있어서,
상기 인터페이스 매니저는,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트의 우선순위를 결정하고, 상기 우선 순위가 미리 정의된 값보다 높은 보안 이벤트에 대해서는 탐지 리포트를 실시간으로 상기 백엔드 서버로 전달하며, 그렇지 않은 보안 이벤트에 대해서는 탐지 리포트를 유휴 시간 동안에 상기 백엔드 서버로 전달하도록 구성된, 침입 탐지 시스템.

[청구항 9] 제1항에 있어서,
상기 인터페이스 매니저는,
상기 보안 이벤트들의 탐지 순서대로 상기 탐지 리포트를 상기 백엔드 서버로 전송하되,
미리 정의된 시간 구간 동안에 복수의 보안 이벤트가 탐지된 경우에, 상기 심각도 점수와 상기 신뢰도 점수를 기초로 각 보안 이벤트의 우선 순위를 결정하고, 각 보안 이벤트에 대한 탐지 리포트를 상기 우선 순위에 따라 상기 백엔드 서버로 전송하도록 구성된, 침입 탐지 시스템.

[청구항 10] 제1항에 있어서,
상기 인터페이스 매니저는,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트에 대한 탐지 리포트의 전송을 생략할 지 여부를 결정하도록 구성된, 침입 탐지 시스템.

[청구항 11] 차량 내 네트워크에서 침입을 탐지하기 위한 침입 탐지 시스템에 의해 수행되는 방법으로서,
차량 내 네트워크로부터 수집되는 네트워크 메시지들을 메시지 큐에 저장하는 단계;
보안 이벤트들을 탐지하기 위해 상기 수집된 네트워크 메시지에 대해 복수의 탐지 기법들을 적용하는 단계, 상기 복수의 탐지 기법들은 탐지 룰들(detection rules)의 집합인 룰-셋(ruleset)을 이용함;
탐지된 보안 이벤트들 각각에 대해 심각도 점수와 신뢰도 점수를 결정하는 단계; 및
상기 보안 이벤트들의 탐지에 응답하여, 탐지 리포트들을 원격의 백엔드 서버에 전송하는 단계
를 포함하는, 방법.

[청구항 12] 제11항에 있어서,
상기 심각도 점수는,
관련된 보안 이벤트가 차량 혹은 운전자의 안전에 얼마나 위험한지를 나타내는 값이며, 관련된 보안 이벤트의 검출에 성공한 탐지 룰에 대해 미리 정의된 중요도를 기초로 결정되는 것인, 방법.

[청구항 13] 제11항에 있어서,
상기 신뢰도 점수는,
관련된 보안 이벤트가 실제 공격일 가능성을 나타내는 값이며, 관련된 보안 이벤트의 특성과 상기 차량 내 네트워크의 정상적인 특성 간의 차이에 기초하여 결정되는 것인, 방법.

[청구항 14] 제13항에 있어서,
네트워크 메시지들이 정상 전송 주기와는 상이한 주기로 전송되는 보안 이벤트에 대해, 상기 신뢰도 점수는 상기 정상 전송 주기로부터 벗어난 편차를 기초로 결정되는 것인, 방법.

[청구항 15] 제11항에 있어서,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트에 대한 액션을 결정하는 단계를 더 포함하는, 방법.

[청구항 16] 제11항에 있어서,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 상기 탐지 리포트들의 전송 순서를 결정하는 단계를 더 포함하는, 방법.

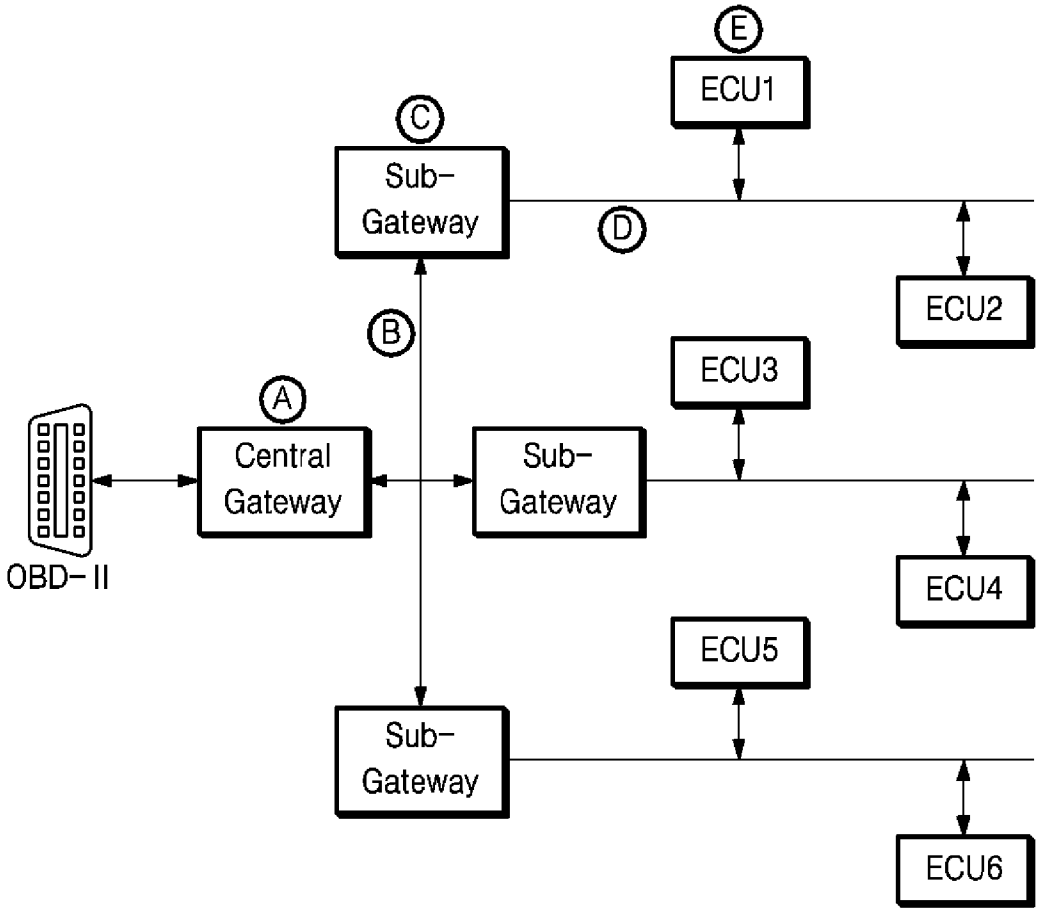
[청구항 17] 제11항에 있어서,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 상기 탐지 리포트들의 전송 타이밍을 결정하는 단계를 더 포함하는, 방법.

[청구항 18] 제11항에 있어서,
상기 심각도 점수와 상기 신뢰도 점수를 기초로 결정되는 우선순위로, 관련된 보안 이벤트에 대한 탐지 리포트를 실시간으로 상기 백엔드 서버에 전달할지 여부를 결정하는 단계를 더 포함하고,
상기 우선 순위가 미리 정의된 값보다 높은 보안 이벤트에 대한 탐지 리포트는 실시간으로 상기 백엔드 서버로 전달되며, 상기 우선 순위가 미리 정의된 값보다 높지 않은 보안 이벤트에 대한 탐지 리포트는 유휴 시간 동안에 상기 백엔드 서버로 전달되는 것인, 방법.

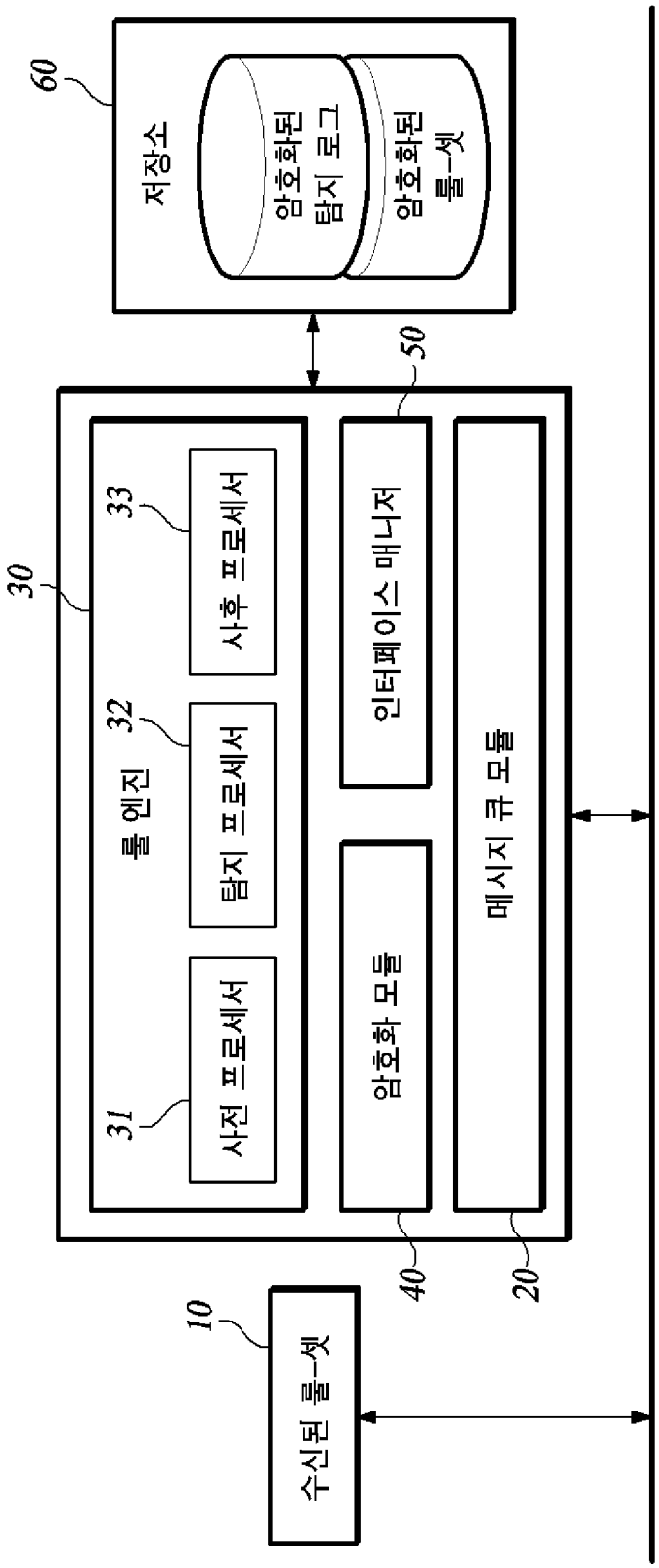
[청구항 19] 제11항에 있어서,
상기 탐지 리포트들을 원격의 백엔드 서버에 전송하는 단계는,
상기 보안 이벤트들의 탐지 순서대로 상기 탐지 리포트를 상기 백엔드 서버로 전송하되,
미리 정의된 시간 구간 동안에 복수의 보안 이벤트가 탐지된 경우에, 상기 심각도 점수와 상기 신뢰도 점수를 기초로 각 보안 이벤트의 우선 순위를 결정하고, 각 보안 이벤트에 대한 탐지 리포트를 상기 우선 순위에 따라 상기 백엔드 서버로 전송하도록 구성된, 방법.

[청구항 20] 제11항에 있어서,
상기 심각도 점수와 상기 신뢰도 점수를 기초로, 관련된 보안 이벤트에 대한 탐지 리포트의 전송을 생략할 지 여부를 결정하는 단계를 더 포함하는, 방법.

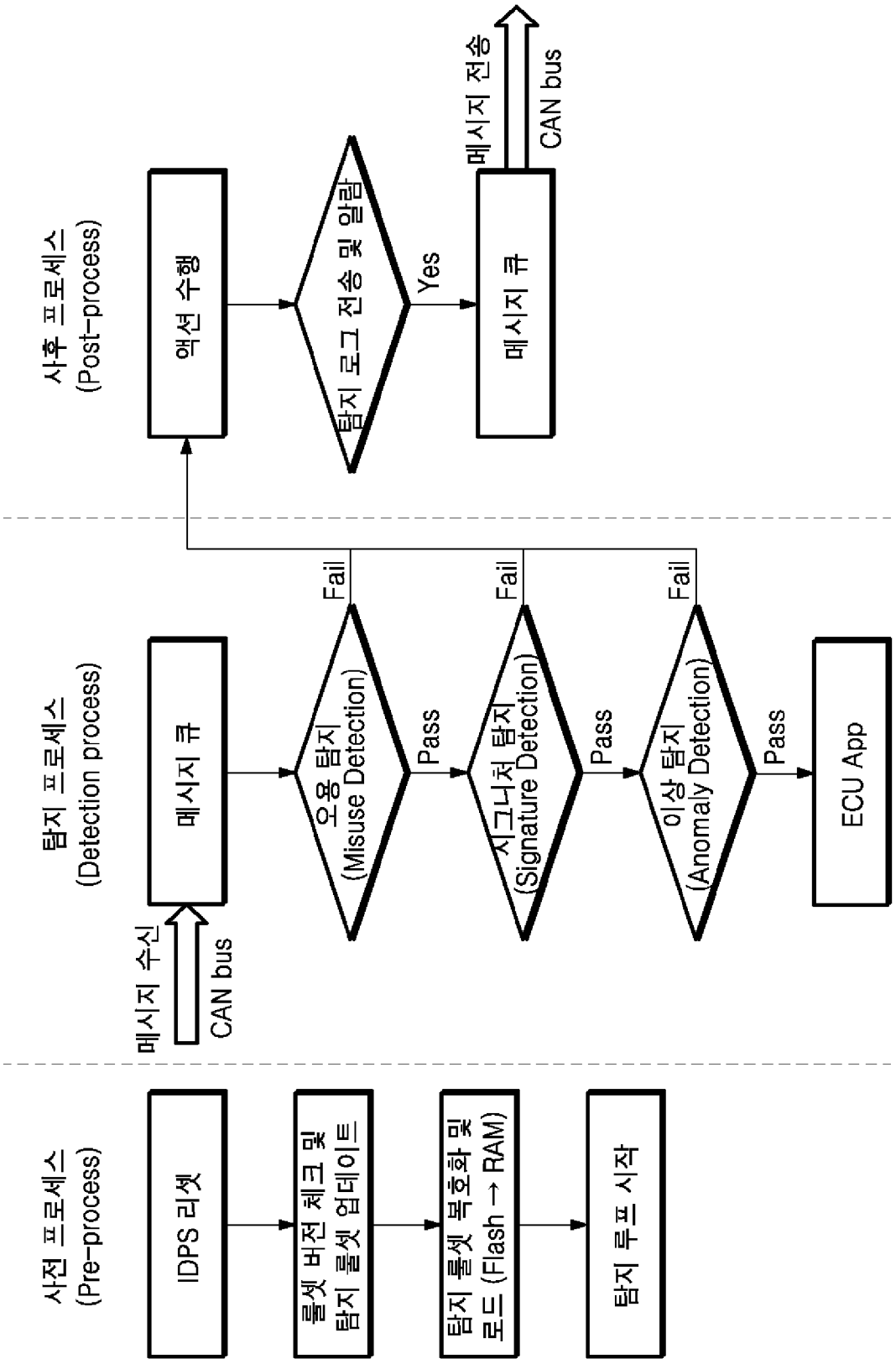
[도1]


E
ECU1
C
Sub-
Gateway
D
ECU2
B
ECU3
A
Central
Gateway
Sub-
Gateway
OBD-II
ECU4
ECU5
Sub-
Gateway
ECU6

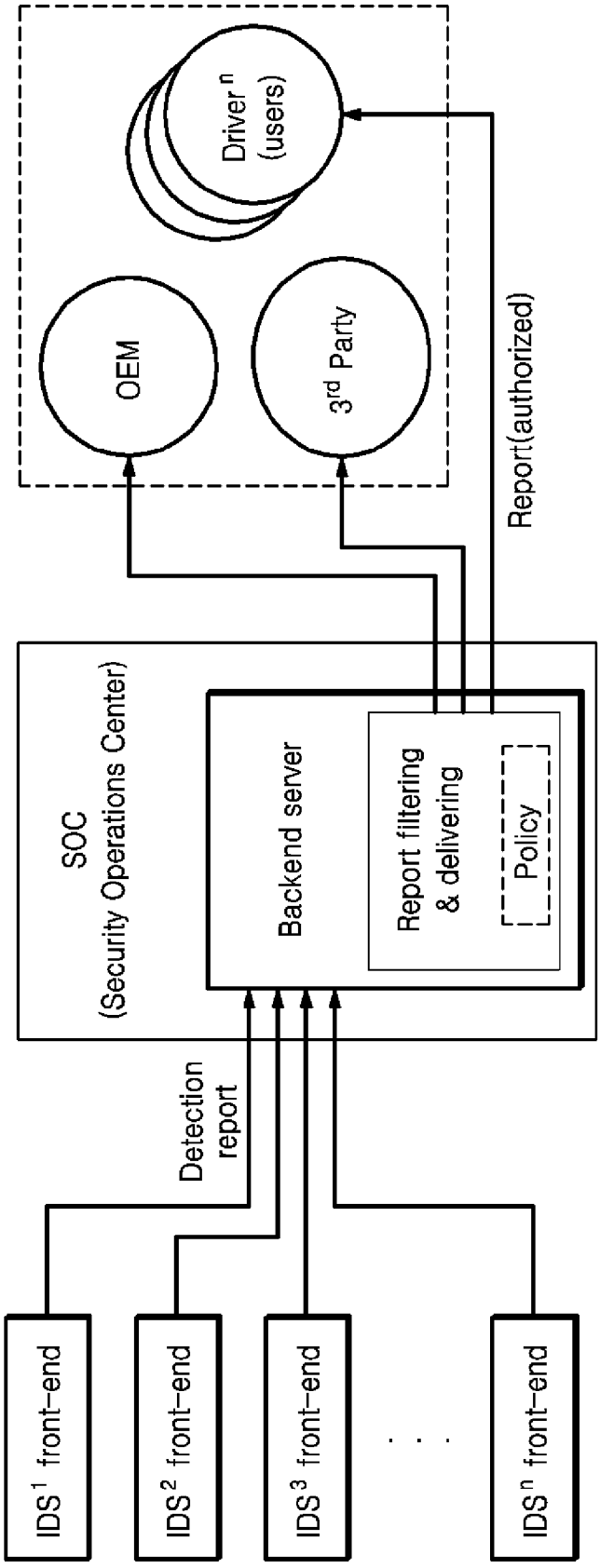
[도2]


60
저장소
암호화된 탐지 로그
암호화된 룰-셋
50
30
룰 엔진
33
사후 프로세서
32
탐지 프로세서
31
사전 프로세서
인터페이스 매니저
암호화 모듈
메시지 큐 모듈
40
20
10
수신된 룰-셋

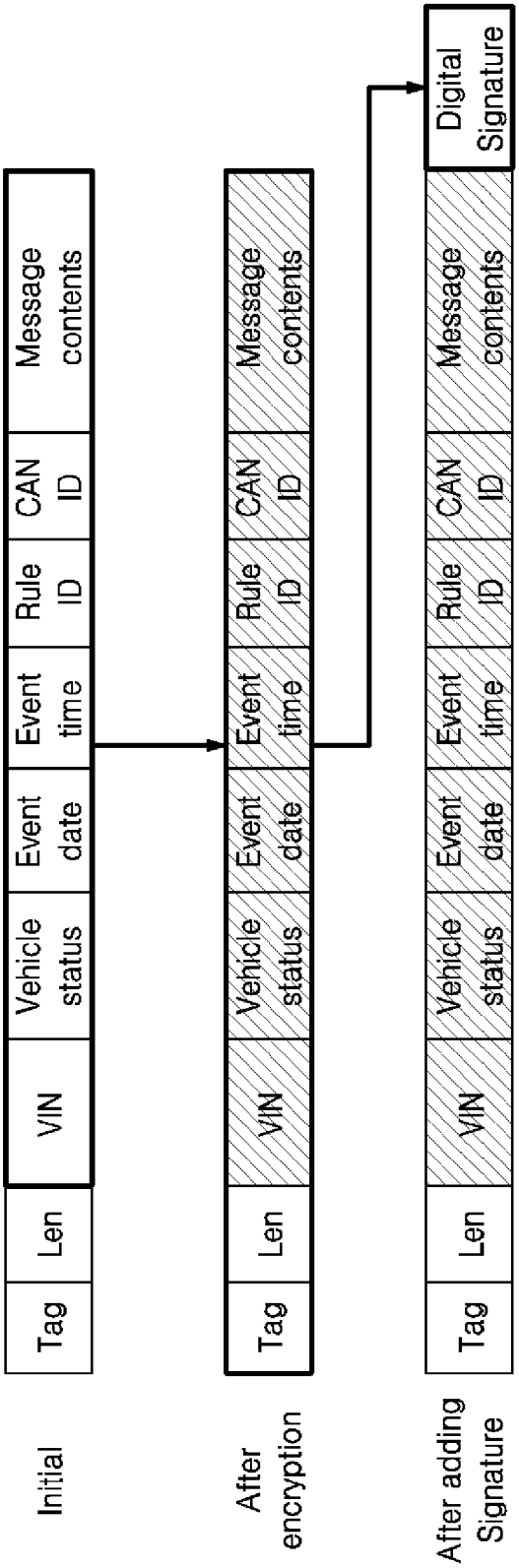
[도3]


사전 프로세스
(Pre-process)
IDPS 리셋
룰셋 버전 체크 및
탐지 룰셋 업데이트
탐지 룰셋 복호화 및
로드 (Flash → RAM)
탐지 루프 시작
탐지 프로세스
(Detection process)
메시지 수신
CAN bus
메시지 큐
오용 탐지
(Misuse Detection)
Fail
Pass
시그니처 탐지
(Signature Detection)
Fail
Pass
이상 탐지
(Anomaly Detection)
Fail
Pass
ECU App
사후 프로세스
(Post-process)
액션 수행
탐지 로그 전송 및 알람
Yes
메시지 큐
메시지 전송
CAN bus

[도4]


Driver n (users)
OEM
3rd Party
Report(authorized)
SOC (Security Operations Center)
Backend server
Report filtering & delivering
Policy
Detection report
IDS 1 front-end
IDS 2 front-end
IDS 3 front-end
IDS n front-end

[도5]


Initial
Tag
Len
VIN
Vehicle status
Event date
Event time
Rule ID
CAN ID
Message contents
After encryption
Tag
Len
VIN
Vehicle status
Event date
Event time
Rule ID
CAN ID
Message contents
After adding Signature
Tag
Len
VIN
Vehicle status
Event date
Event time
Rule ID
CAN ID
Message contents
Digital Signature

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2021/001826

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/40(2006.01)i; **B60R 25/30**(2013.01)i; **H04L 29/06**(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 12/40(2006.01); H04L 12/26(2006.01); H04L 29/06(2006.01); H04L 9/08(2006.01)

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: 침입 탐지 시스템(intrusion detection system), 탐지 룰들(detection rules), 신뢰도(reliability), 심각도(severity), 백엔드 서버(backend server)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2018-0021287 A (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 02 March 2018 (2018-03-02) See paragraphs [0030]-[0044]; claim 1; and figures 1 and 3.	1-20
A	KR 10-1638613 B1 (HYUNDAI MOTOR COMPANY et al.) 11 July 2016 (2016-07-11) See paragraphs [0026]-[0027]; claim 1; and figure 2.	1-20
A	WO 2019-146976 A1 (HYUNDAI MOTOR COMPANY et al.) 01 August 2019 (2019-08-01) See paragraphs [0035]-[0049]; claim 1; and figures 2-3.	1-20
A	WO 2019-231135 A1 (LG ELECTRONICS INC.) 05 December 2019 (2019-12-05) See paragraphs [0047]-[0060]; claim 1; and figures 2-4.	1-20
A	KR 10-1902823 B1 (KOREA AUTOMOTIVE TECHNOLOGY INSTITUTE) 01 October 2018 (2018-10-01) See paragraphs [0124]-[0131]; claim 1; and figure 11.	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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
28 May 2021	**28 May 2021**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2021/001826

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-2018-0021287 A	02 March 2018	KR 10-1853676 B1	03 May 2018
KR 10-1638613 B1	11 July 2016	CN 106059987 A	26 October 2016
		CN 106059987 B	21 February 2020
		US 2016-0308887 A1	20 October 2016
WO 2019-146976 A1	01 August 2019	CN 111434090 A	17 July 2020
		DE 112019000485 T5	22 October 2020
		JP 2021-510478 A	22 April 2021
		KR 10-2020-0103643 A	02 September 2020
		US 2021-0075807 A1	11 March 2021
WO 2019-231135 A1	05 December 2019	KR 10-2021-0003261 A	11 January 2021
KR 10-1902823 B1	01 October 2018	KR 10-1781135 B1	22 September 2017
		KR 10-1907011 B1	11 October 2018
		KR 10-2018-0109642 A1	08 October 2018

국 제 조 사 보 고 서

국제출원번호
PCT/KR2021/001826

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/40(2006.01)i; **B60R 25/30**(2013.01)i; **H04L 29/06**(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 12/40(2006.01); H04L 12/26(2006.01); H04L 29/06(2006.01); H04L 9/08(2006.01)

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: 침입 탐지 시스템(intrusion detection system), 탐지 룰들(detection rules), 신뢰도(reliability), 심각도(severity), 백엔드 서버(backend server)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2018-0021287 A (고려대학교 산학협력단) 2018.03.02 단락 [0030]-[0044]; 청구항 1; 및 도면 1, 3	1-20
A	KR 10-1638613 B1 (현대자동차주식회사 등) 2016.07.11 단락 [0026]-[0027]; 청구항 1; 및 도면 2	1-20
A	WO 2019-146976 A1 (현대자동차주식회사 등) 2019.08.01 단락 [0035]-[0049]; 청구항 1; 및 도면 2-3	1-20
A	WO 2019-231135 A1 (엘지전자 주식회사) 2019.12.05 단락 [0047]-[0060]; 청구항 1; 및 도면 2-4	1-20
A	KR 10-1902823 B1 (자동차부품연구원) 2018.10.01 단락 [0124]-[0131]; 청구항 1; 및 도면 11	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
"D" 본 국제출원에서 출원인이 인용한 문헌
"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌
"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌
"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌
"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌
"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.
"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2021년05월28일(28.05.2021)	**2021년05월28일(28.05.2021)**

ISA/KR의 명칭 및 우편주소

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

팩스 번호 **+82-42-481-8578**

심사관

김성희

전화번호 **+82-42-481-3516**

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2021/001826

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2018-0021287 A	2018/03/02	KR 10-1853676 B1	2018/05/03
KR 10-1638613 B1	2016/07/11	CN 106059987 A	2016/10/26
		CN 106059987 B	2020/02/21
		US 2016-0308887 A1	2016/10/20
WO 2019-146976 A1	2019/08/01	CN 111434090 A	2020/07/17
		DE 112019000485 T5	2020/10/22
		JP 2021-510478 A	2021/04/22
		KR 10-2020-0103643 A	2020/09/02
		US 2021-0075807 A1	2021/03/11
WO 2019-231135 A1	2019/12/05	KR 10-2021-0003261 A	2021/01/11
KR 10-1902823 B1	2018/10/01	KR 10-1781135 B1	2017/09/22
		KR 10-1907011 B1	2018/10/11
		KR 10-2018-0109642 A1	2018/10/08