(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0021287
(43) 공개일자 2018년03월02일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/40* (2006.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 63/1425 (2013.01)
H04L 12/40104 (2013.01)
(21) 출원번호 10-2016-0104936
(22) 출원일자 2016년08월18일
심사청구일자 2016년08월18일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김휘강
서울특별시 서초구 태봉로2길 65 404동 302호 (우면동,네이처힐4단지)
이현승
경기도 고양시 덕양구 화신로 291,1011동 1502호 (화정동, 별빛마을10단지아파트)
정성훈
충청북도 청주시 청원구 율량로 135, 605동 1904호 (주성동, 대원칸타빌3차아파트)
(74) 대리인
김등용, 김홍석

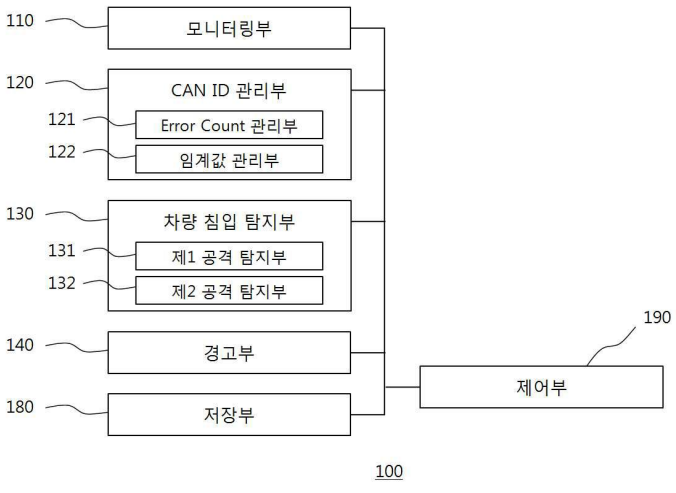
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **차량 침입 탐지 장치 및 방법**

(57) 요 약

차량의 침입 탐지 방법이 개시된다. 상기 침입 탐지 방법은 차량의 침입 탐지 장치에서 수행되고, 차량 내부 네트워크의 CAN 메시지들을 모니터링하는 단계, CAN 메시지의 CAN ID를 이용하여 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 카운트하는 단계, 상기 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 이용하여 엔트로피(H')를 계산하는 단계, 상기 엔트로피(H')가 미리 설정된 제1 공격에 대한 임계값보다 작은지 판단하는 단계. 및 상기 엔트로피(H')가 상기 제1 공격에 대한 임계값보다 작으면 운전자에게 제1 공격 발생에 대한 알림을 제공하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 67/12 (2013.01)
H04L 2012/40273 (2013.01)

명 세 서

청구범위

청구항 1

차량의 침입 탐지 장치에서 수행되는 CAN 메시지의 CAN ID 분석을 이용한 차량 침입 탐지 방법에 있어서,

차량 내부 네트워크의 CAN 메시지들을 모니터링하는 단계;

CAN 메시지의 CAN ID를 이용하여 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 카운트하는 단계;

상기 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 이용하여 엔트로피(H')를 계산하는 단계;

상기 엔트로피(H')가 미리 설정된 제1 공격에 대한 임계값보다 작은지 판단하는 단계; 및

상기 엔트로피(H')가 상기 제1 공격에 대한 임계값보다 작으면 운전자에게 제1 공격 발생에 대한 알림을 제공하는 단계;를 포함하는 침입 탐지 방법.

청구항 2

제1항에 있어서,

상기 엔트로피(H')는 아래의 수학식을 이용하여 계산하는 침입 탐지 방법.

[수학식]

$$H' = -\sum_{i=1}^{n} p_i \log p_i \quad , \quad (0 \le p_i \le 1)$$

(이때, n은 내부 네트워크에서 사용되는 CAN ID의 수를 의미하고, p_i는 특정 CAN ID를 가지는 메시지의 비율을 의미함)

청구항 3

제1항에 있어서,

상기 제1 공격에 대한 임계값은 제1 임계값 및 상기 제1 임계값보다 큰 제2 임계값을 포함하며,

신규의 CAN ID를 포함하는 CAN 메시지가 유입되지 아니한 경우, 상기 제1 임계값과 상기 엔트로피(H')를 비교하여 제1 공격을 탐지하고,

신규의 CAN ID를 포함하는 CAN 메시지가 유입된 경우, 상기 제2 임계값과 상기 엔트로피(H')를 비교하여 제1 공격을 탐지하는 침입 탐지 방법.

청구항 4

차량의 침입 탐지 장치에서 수행되는 CAN 메시지의 CAN ID 분석을 이용한 차량 침입 탐지 방법에 있어서,

차량 내부 네트워크의 CAN 메시지들을 모니터링하는 단계;

상기 차량 내부 네트워크에 에러 제어 메시지 발생 여부를 확인하는 단계;

상기 에러 제어 메시지와 관련된 CAN ID의 수집 가능 여부를 확인하는 단계;

상기 CAN ID의 수집이 가능한 경우, 해당 CAN ID에 대한 오류 발생 카운트(Error Count)를 증가시키는 단계;

특정 CAN ID에 대한 오류 발생 카운트(Error Count)가 미리 설정된 제2 공격에 대한 임계값보다 큰지 판단하는 단계; 및

상기 오류 발생 카운트(Error Count)가 상기 제2 공격에 대한 임계값보다 크면 운전자에게 제2 공격 발생에 대한 알림을 제공하는 단계;를 포함하는 침입 탐지 방법.

청구항 5

제4항에 있어서,

특정 CAN ID에 대한 에러 제어 메시지가 일정 시간 이상 발생하지 아니한 경우, 상기 CAN ID를 가진 ECU에 대한 공격이 발생하지 아니한 것으로 보고 오류 발생 카운트(Error Count)를 리셋(reset)하는 단계를 더 포함하는 침입 탐지 방법.

청구항 6

차량 내부 네트워크의 전체 CAN 메시지를 모니터링하는 모니터링부;

상기 모니터링부에서 모니터링한 CAN 메시지로부터 CAN ID를 획득하고 상기 CAN ID 및 상기 CAN ID 관련 정보를 관리하는 CAN ID 정보 관리부;

차량 침입 탐지를 위한 적어도 하나 이상의 임계값을 관리하는 임계값 관리부;

상기 CAN ID, 상기 CAN ID 관련 정보 및 상기 임계값을 이용하여 차량 침입 발생 여부를 판단하는 차량 침입 탐지부; 및

상기 차량 내부 네트워크에 대한 침입이 탐지된 경우, 상기 침입에 대한 알림을 제공하는 알람부;를 포함하며,

상기 CAN ID 정보 관리부는 차량 내부 네트워크에 존재하는 모든 ECU에서 사용되는 CAN ID 목록, 각각의 CAN ID에 대한 메시지 발생 수 및 각각의 CAN ID에 대한 오류 발생 카운트(Error Count)를 관리하고,

상기 임계값은 DoS 공격 탐지를 위한 제1 공격에 대한 임계값 및 메시지 주입 공격 탐지를 위한 제2 공격에 대한 임계값을 포함하는,

차량의 침입 탐지 장치.

청구항 7

제6항에 있어서,

상기 CAN ID 정보 관리부는 상기 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대응하는 메시지 발생 수를 이용하여 엔트로피(H')를 계산하고,

상기 차량 침입 탐지부는 상기 엔트로피(H')가 상기 제1 공격에 대한 임계값보다 작은지 판단하고,

상기 알람부는 상기 엔트로피(H')가 상기 제1 공격에 대한 임계값보다 작으면 운전자에게 DoS 공격 발생에 대한 알림을 제공하며,

상기 엔트로피(H')는 아래의 수학식을 이용하여 계산하는 차량의 침입 탐지 장치.

[수학식]

$$H' = -\sum_{i=1}^{n} p_i \log p_i \quad , \quad (0 \le p_i \le 1)$$

(이때, n은 내부 네트워크에서 사용되는 CAN ID의 수를 의미하고, p_i는 특정 CAN ID를 가지는 메시지의 비율을 의미함)

청구항 8

제6항에 있어서,

상기 차량 침입 탐지부는 특정 CAN ID에 대한 오류 발생 카운트(Error Count)가 상기 제2 공격에 대한 임계값보다 큰지 판단하고,

상기 알람부는 상기 오류 발생 카운트(Error Count)가 상기 제2 공격에 대한 임계값보다 크면 운전자에게 메시지 주입 공격 발생에 대한 알림을 제공하는 차량의 침입 탐지 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 개념에 따른 실시 예는 차량의 침입 탐지 장치 및 방법에 관한 것으로, 특히 차량 내부 네트워크의 CAN 메시지 ID 분석을 수행하여 메시지 주입 공격과 DoS 공격을 탐지하고 운전자에게 알리는 차량의 침입 탐지 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 본 발명은 차량 내부 네트워크 중 CAN에 대한 메시지 주입 공격 및 DoS 공격에 대해 CAN 메시지 ID를 분석하여 외부의 침입으로부터 자동차를 보호하기 위한 침입 탐지 기술을 제시한다.

[0003] IT 기술의 발전으로 인하여 자동차를 구성하는 각종 기계식 제어 시스템이 전자식으로 대체되는 비중이 늘고 있다. 특히, 차량 내 존재하는 ECU (Electric Computer Unit) 및 파워트레인(power train)을 구성하는 각종 모듈들은 차량 내부 구현의 간편화 및 오류 발생을 최소화하기 위해 CAN으로 연결된다.

[0004] CAN은 차량 내 장치가 서로 통신할 수 있도록 구현된 표준 프로토콜로, 많은 자동차에 구현되어 있다. 간단한 구현을 위해 통신을 수행하는 장치들은 모두 하나의 회선에 연결되어 있으며, CAN 버스(bus)에 전송된 메시지는 브로드캐스트 방식으로 차량 내 모든 ECU에 전달된다.

[0005] CSMA/CD+AMP 기술은 CAN으로 구현된 내부 네트워크에서 여러 노드가 동시에 송신할 데이터를 갖고 있을 때 회선 충돌을 방지하고 CAN 버스(bus)를 선점하기 위한 우선순위를 결정하는 기술이다. 보낼 메시지가 있는 여러 노드들은 동기화된 신호에 따라 동시에 CAN 버스로 메시지 송신을 시도하며, CAN 메시지의 앞쪽에 위치한 ID 필드의 값을 비트 단위로 비교한다. CAN에서는 메시지가 낮은 ID값을 가질수록 높은 우선순위를 가지고, 이 원칙에 따라 가장 우선순위가 높은(ID값이 낮은) 메시지가 CAN 버스를 선점한다. 그리고 CAN 버스를 선점한 메시지가 모두 전송되고 나면 다시 동기화된 신호에 따라 같은 작업을 반복한다. 그 결과, CAN 버스를 점유하려는 노드가 여러 개 있어도 CAN ID의 우선순위에 따라 회선 충돌 없이 안정적인 통신을 수행할 수 있다. 단, CSMA/CD+AMP 기술은 경쟁하는 메시지들의 ID가 다른 경우에만 메시지들의 우선순위를 가릴 수 있다.

[0006] CAN 메시지의 경쟁 ID(Arbitration ID, 이하 'CAN ID'라고도 함)를 이용한 우선순위 식별 방법을 상세히 설명하면 다음과 같다(도2 참고). 각 노드에서 전송되는 메시지는 우선순위를 포함하는 ID값을 갖고 있으며 두 개 이상의 노드에서 동시에 메시지를 전송하려 시도하면, 중재 단계(arbitration phase)에서 비트 단위로 비교를 수행한다. 이때 송신되는 메시지들은 반드시 동일한 타이밍에 메시지가 시작되므로, 중재 단계에서 같은 자리의 1 비트만을 검사할 수 있다. 만일 CAN ID의 특정 비트(bit)가 같은 값을 가지고 있다면 다음 bit의 검사를 수행한다. 그리고 비트(bit)가 다른 값을 가지고 있을 경우, 로우(Low)값을 가지는 메시지(들)는 계속 CAN 버스에 송신을 지속한다. CAN ID의 모든 비트(bit) 필드를 검사하면 결국 가장 낮은 ID값을 가진 메시지만이 메시지의 내용을 송신할 수 있게 된다. 중재 단계에서 경쟁에 밀린 메시지들은 다음 메시지 송신 타이밍에 다시 경쟁을 수행한다.

[0007] 브로드캐스팅 방식의 메시지 전달 특성상, 차량 내 CAN 버스와 연결된 ECU 및 모듈들은 모두 동일한 메시지를 수신받는다. ECU 및 모듈은 해당 메시지의 CAN ID를 검사하여, 메시지에 포함된 데이터를 처리해야 할지 혹은 메시지를 무시할지 결정한다.

[0008] 통신 기술의 발전으로 텔레매틱스 서비스가 발전하면서 운전자의 장치가 OBD-II (On-Board Diagnosis version II) 단자를 통해 CAN 네트워크와 직접적으로 연결되고 있다. 또한, CAN은 브로드캐스팅 프로토콜로, 메시지 암호화나 인증기능을 제공하지 않아 외부로부터 주입된 프레임을 식별하지 못하고 그대로 내부 네트워크의 모듈에 전달한다. 이로 인하여 차량이 텔레매틱스 단말기를 통해 외부의 공격으로부터 직접적인 영향을 받게 될 수 있는 문제점이 있다.

[0009] 따라서, 차량 내부 네트워크 중 CAN에 대한 메시지 주입 공격을 적은 연산량으로 신속하게 탐지할 수 있는 침입 탐지 방법이 필요하다. 본 발명에서는 차량 내부 네트워크 환경에서의 CAN 메시지 ID를 분석하여 OBD-II 단자를 이용한 패킷 주입 공격 또는 DoS 공격의 침입 탐지를 수행하는 장치 및 방법을 제안하고자 한다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) KR 10-1605783 B1

(특허문헌 0002) KR 10-1328389 B1

발명의 내용

해결하려는 과제

[0011] 본 발명이 이루고자 하는 기술적인 과제는 차량 내부 네트워크 환경에서 CAN 메시지 ID를 분석하여 차량에 악의적인 명령을 내리기 위한 패킷 주입 공격과, CAN 버스의 자원을 점유하여 차량의 기능을 무력화하는 DoS 공격을 탐지할 수 있는 차량 침입 탐지 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 본 발명의 실시 예에 따른 차량의 침입 탐지 방법은 차량의 침입 탐지 장치에서 수행되고, 차량 내부 네트워크의 CAN 메시지들을 모니터링하는 단계, CAN 메시지의 CAN ID를 이용하여 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 카운트하는 단계, 상기 차량 내부 네트워크에서 사용되는 모든 CAN ID 각각에 대한 메시지 발생 수를 이용하여 엔트로피(H')를 계산하는 단계, 상기 엔트로피(H')가 미리 설정된 제1 공격에 대한 임계값보다 작은지 판단하는 단계, 및 상기 엔트로피(H')가 상기 제1 공격에 대한 임계값보다 작으면 운전자에게 제1 공격 발생에 대한 알림을 제공하는 단계를 포함한다.

[0013] 본 발명의 실시 예에 따른 차량의 침입 탐지 장치는 차량 내부 네트워크의 전체 CAN 메시지를 모니터링하는 모니터링부, 상기 모니터링부에서 모니터링한 CAN 메시지로부터 CAN ID를 획득하고 관련 정보를 관리하는 CAN ID 정보 관리부, 차량 침입 탐지를 위한 적어도 하나 이상의 임계값을 관리하는 임계값 관리부, 상기 CAN ID 관련 정보 및 상기 임계값을 이용하여 차량 침입 여부를 탐지하는 차량 침입 탐지부, 상기 차량 내부 네트워크에 대한 침입이 탐지된 경우, 상기 침입에 대한 알림을 제공하는 알람부를 포함하며, 상기 CAN ID 정보 관리부는 차량 내부 네트워크에 존재하는 모든 ECU에서 사용되는 CAN ID 목록, 각각의 CAN ID에 대한 메시지 발생 수 및 각각의 CAN ID에 대한 오류 발생 카운트(Error Count)를 관리하고, 상기 임계값은 DoS 공격 탐지를 위한 제1 공격에 대한 임계값 및 메시지 주입 공격 탐지를 위한 제2 공격에 대한 임계값을 포함한다.

발명의 효과

[0014] 본 발명의 실시 예에 따른 차량 침입 탐지 장치 및 방법에 의할 경우, CAN 메시지의 ID를 분석하여, 신속하게 메시지 주입 공격 및 DoS 공격을 탐지하고, 이를 알릴 수 있는 효과가 있다.

[0015] 또한 본 발명의 실시 예에 따른 차량 침입 탐지 장치 및 방법은 메시지에 포함된 ID를 기반으로 분석을 수행하며, 메시지 ID가 나타내는 의미에 의존적이지 않으므로 차량 벤더(vender) 또는 차량 기종에 상관없이 저비용으로 침입 탐지를 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0016] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 침입 탐지 장치의 기능 블럭도이다.

도 2는 CAN 메시지 ID를 이용한 우선순위 식별 방법을 도시한다.

도 3은 도 1에 도시된 침입 탐지 장치를 이용한 차량의 침입 탐지 방법의 일 실시 예를 설명하기 위한 흐름도이다.

도 4는 차량 침입 탐지를 위한 CAN ID 및 CAN ID 관련 정보의 일 예를 도시한다.

도 5는 도 1에 도시된 침입 탐지 장치를 이용한 차량의 침입 탐지 방법의 다른 실시 예를 설명하기 위한 흐름도

이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0018] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0019] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0020] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0021] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0022] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0023] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다.

[0024] 도 1은 본 발명의 일 실시 예에 따른 침입 탐지 장치의 기능 블럭도이다.

[0025] 본 발명에 따른 침입 탐지 장치(100)는 차량 내부 네트워크 CAN의 메시지 ID를 분석하고, 이를 통하여 차량 침입 여부를 탐지할 수 있다. 또한, 침입 탐지 장치(100)는 침입 탐지 결과를 차량 내부 알람 장치 또는 미리 정해진 단말기로 송신할 수 있다.

[0026] 차량 침입의 신속한 탐지를 위하여 침입 탐지 장치(100)는 바람직하게는 차량 내부에 위치한다. 침입 탐지 장치(100)는 CAN 네트워크에서 게이트웨이(110)의 내부에 설치될 수도 있고, 독립된 개체로 버스에 연결되어 게이트웨이(110)와 통신할 수도 있다. 침입 탐지 장치(100)는 ECU일 수 있다. 이와는 달리, 침입 탐지 장치(100)는 차량 외부에 위치하는 별도의 서버일 수도 있다.

[0027] 침입 탐지 장치(100)는 게이트웨이 및 ECU들로부터 해당 CAN 네트워크 상의 모든 메시지를 모니터링할 수 있다.

[0028] 도 1을 참조하면, 침입 탐지 장치(100)는 모니터링부(110), CAN ID 정보 관리부(120), 임계값 관리부(130), 차량 침입 탐지부(140), 경고부(150), 저장부(180) 및 제어부(190) 중 적어도 하나 이상을 포함할 수 있다.

[0029] 모니터링부(110)는 차량 내부 네트워크의 전체 메시지를 모니터링하고, 차량 침입 탐지를 위한 필요한 정보를 수집할 수 있다.

[0030] CAN ID 정보 관리부(120)는 모니터링한 CAN 메시지의 CAN ID를 획득하고 분석하며, 차량 침입 탐지 관련 정보를 관리한다. 차량 침입 탐지를 위해 CAN ID 관리부(120)는 차량 내부 네트워크에 존재하는 모든 ECU에서 사용되는

CAN ID를 획득하고, CAN ID당 메시지 발생 수를 카운트한다. 그리고 획득한 CAN ID와 메시지 발생 수를 이용하여 엔트로피(H')을 구한다. 차량 네트워크에 DoS 공격이 발생하면 차량 내부 네트워크에 특정 CAN ID를 가지는 메시지의 비율이 압도적으로 높아지게 되며 그 결과 엔트로피가 낮아지게 되고, 이를 이용하여 차량 침입 탐지부(130)에서 DoS 공격을 탐지할 수 있다.

[0031] 또한, CAN ID 정보 관리부(120)는 에러 제어 메시지가 발생한 경우, 해당 CAN ID에 대응하는 에러 카운트(Error Count)를 증가시킬 수 있다.

[0032] 차량 침입 탐지부(130)는 상기 CAN ID 관련 정보를 분석하고 임계값과 비교하여 차량 침입 여부를 탐지한다. 본 발명의 일 실시에 따라 탐지하고자 하는 차량 침입에 의한 공격의 유형은 제1 공격 및 제2 공격으로 범주화될 수 있다. 상기 제1 공격은 CAN에 짧은 시간 대량의 메시지를 발생시켜 과부하를 발생시키는 DoS 공격을, 상기 제2 공격은 특정 CAN ID 메시지를 대량으로 CAN에 주입하여 오작동을 발생시키는 메시지 주입 공격을 의미할 수 있다.

[0033] CAN으로 구현된 차량 내부 네트워크에서의 DoS 공격은 기존 차량에 탑재된 ECU가 처리하는 CAN ID보다 더 높은 우선순위를 갖도록 메시지에 낮은 ID값을 설정하여 다량으로 송신하는 방법으로 발생하며, 메시지 주입 공격은 기존에 사용되던 CAN ID와 함께 공격할 내용을 메시지로 송신하는 방법으로 발생할 수 있다.

[0034] 제1 공격 탐지부(131)는 CAN ID 정보 관리부(120)에서 계산한 엔트로피가 미리 설정된 제1 공격에 대한 임계값보다 낮아지면 DoS 공격이 발생한 것으로 판단하고, 제2 공격 탐지부(132)는 해당 CAN ID에 대한 에러 카운트(Error Count)가 미리 설정된 제2 공격에 대한 임계값보다 높아지면 메시지 주입 공격이 발생한 것으로 판단한다.

[0035] 임계값 관리부(140)는 차량 침입 탐지를 위한 적어도 하나 이상의 임계값을 관리한다. 임계값 관리부(140)는 공격 유형별로 제1 공격에 대한 임계값과 제2 공격에 대한 임계값을 각각 설정할 수 있다. 또한, 탐지 성능 향상을 위해 새로 발견된 CAN ID의 우선순위가 차량에서 처리되는 CAN ID들의 우선 순위보다 높을 경우 DoS 공격이 더 쉽게 성공할 수 있으므로 CAN ID가 새로 발견된 경우, 제1 공격에 대한 임계값을 더 높게 설정할 수 있다. 또한, 임계값 관리부(140)는 CAN ID별로 임계값을 다르게 설정할 수도 있다.

[0036] CAN ID 분석을 통한 차량 공격 여부를 판단하는 방법은 아래의 침입 탐지 방법에 대한 설명에서 더욱 자세히 살펴보도록 한다.

[0037] 경고부(150)는 상기 침입이 탐지된 경우, 해당 차량의 알람 장치, 해당 차량의 운전자가 소지하고 있는 단말기, 또는 알림 제공을 위하여 운전자 또는 관리자에 의하여 미리 지정된 단말기 등에 상기 침입에 대한 알림을 제공한다. 예를 들어, 차량 침입 관련 정보를 포함하는 침입 알림 메시지를 송신하거나, 경고음을 발생시킬 수 있다.

[0038] 저장부(180)에는 각각의 CAN ID 관련 정보 및 침입 탐지를 위한 임계값이 저장되어 있다. CAN ID 관련 정보는 차량 내부 네트워크에 존재하는 모든 ECU에서 사용되는 CAN ID 목록, 해당 CAN ID의 메시지 발생 수, 해당 CAN ID를 가지는 메시지의 비율, 해당 CAN ID에 대한 오류 발생 카운트(Error Count) 정보 등을 포함할 수 있다. 또한, 본 명세서에서 저장부(180)라 함은, 각각의 저장부에 대응되는 정보를 저장하는 소프트웨어 및 하드웨어의 기능적 구조적 결합을 의미할 수 있다. 저장부(180)는 프로그램 저장부와 데이터 저장부를 포함할 수 있다. 상기 프로그램 저장부에는 침입 탐지 장치(100)의 동작을 제어하기 위한 프로그램들이 저장될 수 있다. 상기 데이터 저장부에는 상기 프로그램들을 수행하는 과정 중에 생성되는 데이터들이 저장될 수 있다.

[0039] 제어부(190)는 침입 탐지 장치(100)의 전반적인 동작을 제어한다. 즉, 모니터링(110), CAN ID 정보 관리부(120), 임계값 관리부(130), 차량 침입 탐지부(140), 경고부(150), 및 저장부(180)의 동작을 제어할 수 있다.

[0040] 도 1에 도시된 침입 탐지 장치의 구성들 각각은 기능 및 논리적으로 분리될 수 있음으로 나타내는 것이며, 반드시 각각의 구성이 별도의 물리적 장치로 구분되거나 별도의 코드로 작성됨을 의미하는 것이 아님을 본 발명의 기술분야의 평균적 전문가는 용이하게 추론할 수 있을 것이다.

[0041] 또한, 본 명세서에서 '-부'라 함은, 본 발명의 기술적 사상을 수행하기 위한 하드웨어 및 상기 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미할 수 있다. 예컨대, 상기 '-부'는 소정의 코드와 상기 소정의 코드가 수행되기 위한 하드웨어 리소스의 논리적인 단위를 의미할 수 있으며, 반드시 물리적으로 연결된 코드를 의미하거나, 한 종류의 하드웨어를 의미하는 것이 아니다.

[0042] 이하, 도 3 내지 도 5를 참조하여, 본 발명의 실시 예에 따른 침입 탐지 장치를 이용한 차량의 침입 탐지 방법

에 대하여 자세히 살펴보도록 한다.

[0043] 도 3은 도 1에 도시된 침입 탐지 장치를 이용한 차량의 침입 탐지 방법의 일 실시 예를 설명하기 위한 흐름도이다. 도 4는 차량 침입 탐지를 위한 CAN ID 및 CAN ID 관련 정보의 일 예를 도시한다.

[0044] 도 3을 참조하면, 침입 탐지 장치(100)의 모니터링부(110)는 차량 내부 네트워크의 CAN 메시지들을 수신하고(S110), CAN ID 분석을 통한 외부 공격을 탐지하기 위해 차량 내부 네트워크에 존재하는 모든 ECU에서 사용되는 CAN ID를 획득한다. 구체적으로, 수신된 CAN 메시지의 CAN ID가 신규의 CAN ID인 경우(S120), CAN ID를 차량 내부 네트워크의 CAN ID 목록에 저장(S130)하여 차량 내부 네트워크의 CAN ID 목록을 획득할 수 있다. 예를 들어, 차량 내에서 처리되는 CAN ID를 획득하기 위해 OBD-II 단자로 CAN ID가 '7DF' 인 메시지를 송신하거나 차량 내부 네트워크를 장시간 모니터링하여 테이블로 정리하는 방법 등을 사용할 수 있다.

[0045] 다음, DoS 공격을 탐지하기 위해 전체 메시지를 모니터링(S140)하며, 상기 차량 내부 네트워크에서 사용되는 메시지의 ID 목록을 이용하여 CAN ID당 메시지 발생 수를 카운트한다.

[0046] 다음, 획득한 CAN ID와 메시지 발생 수를 이용해 엔트로피(H')를 구하고, CAN ID 및 CAN ID 관련 정보를 저장부에 저장한다. CAN ID 관련 정보는 해당 CAN ID 사용 횟수, 해당 CAN ID를 갖는 메시지의 비율, 및 엔트로피(H')를 포함할 수 있다. 수집하는 CAN ID 및 CAN ID에 대응하는 관련 정보의 일 예는 도 4에 도시되어 있다. 도 4의 (c)와 같이, CAN ID '0x702'를 갖는 CAN 메시지가 다량 유입되면, 다양성 지수가 낮아지며 엔트포피(H')가 낮아진다.

[0047] 다음, 엔트로피(H')가 미리 설정된 임계값(threshold)보다 작은지 판단하여(S150), 엔트로피(H')가 임계값보다 낮아지면 운전자에게 DoS 공격 발생 경고를 알린다(S170). 엔트로피(H')를 구하기 위한 Shannon's diversity index는 아래의 수학식 1에 의해 정의될 수 있다.

수학식 1

[0048] $$H' = -\sum_{i=1}^{n} p_i \log p_i$$

[0049] n: 내부 네트워크에서 사용되는 CAN ID의 수

[0050] p_i: 특정 CAN ID를 가지는 메시지의 비율 ($(0 \le p_i \le 1)$)

[0051] 임계값은 차량마다 다르게 설정될 수 있다.

[0052] DoS 공격은 차량 내 ECU의 통신을 무력화하는 것이 목표이므로, 회선을 모두 점유할 수 있을 정도로 많은 양의 높은 우선순위를 갖는 메시지를 내부 네트워크로 주입한다. 차량 내부 네트워크에 특정 CAN ID를 가지는 메시지의 비율이 압도적으로 높아지게 되며 그 결과 엔트로피(H')가 낮아지게 되며, 엔트로피(H')가 미리 설정된 임계값(threshold)보다 작아지게 되면 DoS 공격이 발생한 것으로 판단하고 운전자 등에게 차량 침입 경고를 알린다. 예를 들어, 차량 침입이 탐지된 경우, 침입에 대한 알림 메시지를 해당 차량의 알람부, 해당 차량의 운전자가 소지하고 있는 단말기, 또는 알림 메시지 수신을 위하여 미리 설정된 단말기에 송신할 수 있으며, 알림 메시지는 침입(공격)의 유형에 대한 정보를 포함할 수 있다.

[0053] DoS 공격에 대한 보다 정확한 탐지를 위해, 해당 CAN ID에 대한 메시지가 가장 높은 비율을 차지하는지 판단하는 단계(S160)를 더 포함할 수 있다. 해당 CAN ID에 대한 메시지가 가장 높은 비율을 차지하는 경우 운전자에게 DoS 공격 발생 경고를 알릴 수 있다(S170).

[0054] 또한, 탐지 성능 향상을 위해, 새로 발견(유입)된 CAN ID의 우선순위가 차량에서 처리되는 기존의 CAN ID들의 우선순위보다 높을 경우 DoS 공격이 더 쉽게 성공할 수 있으므로 한 번도 사용되지 않았던 CAN ID가 발견된 경우, 임계값을 더 높여 탐지를 수행할 수 있다. 즉, 새로운 CAN ID가 발견되지 아니한 경우에 DoS 공격을 탐지하는 기존의 임계값(이하, '제1 임계값'이라 함)보다, 새로운 CAN ID가 발견된 경우에 DoS 공격을 탐지하는 임계값(이하, '제2 임계값'이라 함)을 높게 설정하여, 새로 발견한 CAN ID를 이용한 DoS 공격 탐지 민감도를 높일 수 있다.

[0055] 또한, 신규의 CAN ID의 우선순위가 종래의 CAN ID의 우선순위보다 낮은 경우에 사용하는 DoS 공격 탐지를 위한

임계값을 신규의 CAN ID의 우선순위가 종래의 CAN ID의 우선순위보다 낮은 경우에 사용하는 DoS 공격 탐지를 위한 임계값보다 높게 설정하여 DoS 공격을 탐지하는 것도 가능하다.

[0056] 도 5는 도 1에 도시된 침입 탐지 장치를 이용한 차량의 침입 탐지 방법의 다른 실시 예를 설명하기 위한 흐름도이다. 도 5는 메시지 주입 공격에 의한 차량 침입 여부를 탐지하는 방법의 일 실시 예를 도시한다.

[0057] 도 5를 참조하면, 침입 탐지 장치(100)는 차량 네트워크의 전체 메시지를 모니터링(S210)한다.

[0058] 메시지 주입 공격은 차량에서 실제로 사용되는 CAN ID(CAN 메시지의 중재 ID)와 공격 명령으로 구성된 메시지를 차량 내부 네트워크에 주입하는 방법으로 발생한다. 종래의 차량 내 ECU 및 모듈은 수신된 메시지의 CAN ID에 따라 아무런 검증 없이 공격 명령을 수행한다. 메시지 주입 공격은 차량에서 실제 사용되는 CAN ID를 이용하므로 차량이 주행하면서 발생되는 정상 메시지와 메시지 주입 공격으로 인한 메시지가 같은 CAN ID를 가진 채로 CAN 버스(bus)에서 경쟁을 하게 될 수 있다. 또한, 공격자는 효과적인 공격을 수행하기 위해 메시지를 지속적으로 주입하므로, 이러한 경쟁은 자주 발생하게 된다. CSMA/CD+AMP 기술은 회선 충돌을 방지하기 위해 CAN ID에 따라 메시지의 우선순위를 결정한다. 그러나 동일한 CAN ID를 가진 메시지가 동시에 송신되는 경우 중재 단계에서 충돌을 감지하지 못하므로 ID가 그대로 CAN bus에 전송되고, 데이터 전송 단계(data transmission phase)에서 CAN bus의 오류(error)가 발생한다. CAN bus 컨트롤러는 에러 제어 메시지를 생성한다. 에러 제어 메시지를 통해 오류 발생 사실을 내부 네트워크의 모든 ECU 및 모듈에 알리고 잠시 지연 시간을 가진 후, 통신을 재개한다.

[0059] 침입 탐지 장치(100)는 차량 네트워크의 전체 메시지를 모니터링(S210)을 수행하는 중에, 에러 제어 메시지가 발생하였는지를 확인하고(S220), 에러 제어 메시지가 발생한 경우, 오류와 연관된 CAN ID 수집이 가능지 여부를 판단한다(S230).

[0060] 오류와 연관된 CAN ID를 수집할 수 있는 경우, 해당 CAN ID에 대한 오류 발생 카운트(Error Count)를 증가시킨다(S240). 실시 예에 따라, 해당 CAN ID에 대한 에러 제어 메시지가 일정 시간 이상 발생하지 아니한 경우, 해당 차량 또는 해당 차량의 특정 CAN ID를 가진 ECU에 대한 공격(침입)이 발생하지 아니한 것으로 보고 오류 발생 카운트(Error Count)를 리셋(reset)하는 것도 가능하다.

[0061] 다음, 특정 CAN ID에 대한 오류 발생 카운트(Error Count)가 미리 설정된 제2 공격에 대한 임계값 초과 여부를 판단한다(S250). 이때, 제2 공격에 대한 임계값은 차량의 종류 또는 CAN ID별로 동일하게 또는 다르게 설정할 수 있다.

[0062] 특정 CAN ID에 대한 오류가 미리 설정된 제2 공격에 대한 임계값 이상 발생한 경우, 운전자에게 특정 CAN ID에 대응하는 ECU에 대한 메시지 주입 공격(제2 공격) 경고를 알린다(S270). CAN 버스에 전기적 잡음으로 인한 오류가 발생할 수 있지만 특정한 CAN ID와 관련된 메시지를 송신할 때만 오류가 발생할 가능성은 매우 낮으므로 제안된 방법은 오탐(false positive & false negative)없이 효과적으로 차량 침입 공격을 탐지할 수 있다.

[0063] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0064] 100 : 침입 탐지 장치 110 : 모니터링부

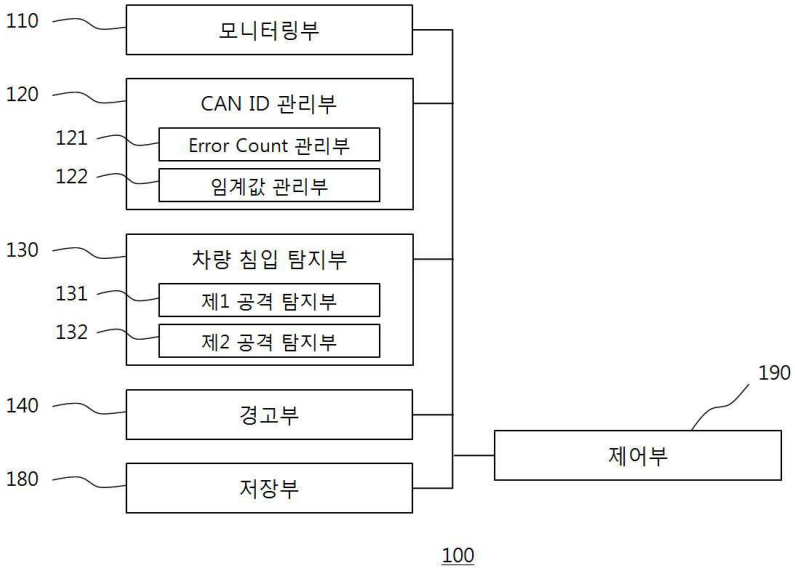
120 : CAN ID 정보 관리부 130 : 임계값 관리부

140 : 차량 침입 탐지부 150 : 경고부

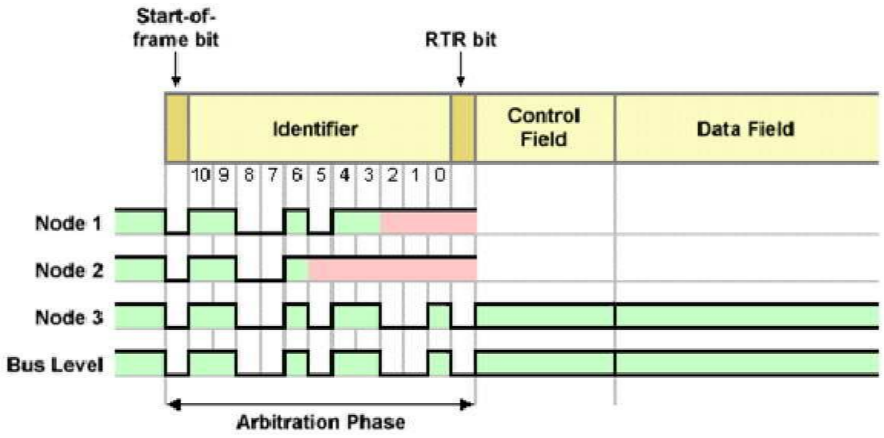
180 : 저장부 190 : 제어부

도면

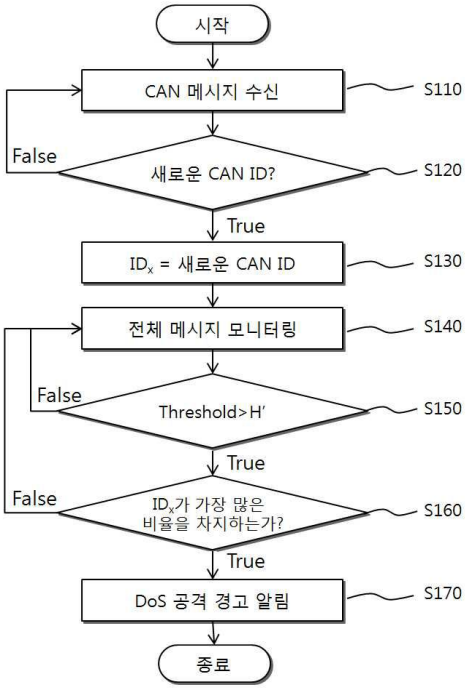
도면1


110
모니터링부
120
CAN ID 관리부
121
Error Count 관리부
122
임계값 관리부
130
차량 침입 탐지부
131
제1 공격 탐지부
132
제2 공격 탐지부
140
경고부
180
저장부
190
제어부
100

도면2


Start-of-frame bit
RTR bit
Identifier
Control Field
Data Field
10 9 8 7 6 5 4 3 2 1 0
Node 1
Node 2
Node 3
Bus Level
Arbitration Phase

도면3



도면4

(a) 기준

CAN ID	사용 횟수	p_i	logp_i	H'
0x701	2	0.5	-0.69	0.69
0x702	2	0.5	-0.69	

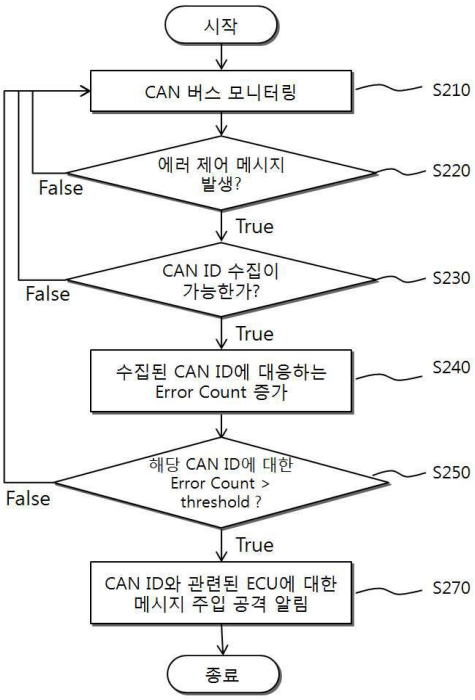
(b) 새로운 ID 유입

CAN ID	사용 횟수	p_i	logp_i	H'
0x701	2	0.33	-1.11	1.11
0x702	2	0.33	-1.11	
0x703	2	0.33	-1.11	

(c) 메시지 다량 유입

CAN ID	사용 횟수	p_i	logp_i	H'
0x701	2	0.2	-1.61	0.5
0x702	8	0.8	-0.22	

도면5


시작
CAN 버스 모니터링
S210
에러 제어 메시지 발생?
S220
False
True
CAN ID 수집이 가능한가?
S230
False
True
수집된 CAN ID에 대응하는 Error Count 증가
S240
해당 CAN ID에 대한 Error Count > threshold ?
S250
False
True
CAN ID와 관련된 ECU에 대한 메시지 주입 공격 알림
S270
종료