(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년04월21일
(11) 등록번호 10-2242671
(24) 등록일자 2021년04월15일

(51) 국제특허분류(Int. Cl.)
H04L 12/40 (2006.01) *G06F 21/55* (2013.01)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 12/40104 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2019-0177894
(22) 출원일자 2019년12월30일
심사청구일자 2019년12월30일
(56) 선행기술조사문헌
Paper, W. Wu et al.: Sliding Window Optimized Information Entropy Analysis Method for Intrusion Detection on In-Vehicle Networks, IEEE Vol 6, 2018.08.13.*
Paper, Wang et. al., An Entropy Analysis based Intrusion Detection System for Controller Area Network in Vehicles, 2018 IEEE, 2019.01.21.*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
동국대학교 산학협력단
서울특별시 중구 필동로1길 30 내 (필동3가,동국대학교)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
임대운
서울특별시 은평구 진관2로 57-37, 243동 1001호 (진관동, 은평뉴타운우물골)
김영식
광주광역시 서구 풍암2로 66 금호2차아파트 201동 1005호
유기순
경상북도 안동시 녹전면 하이전길 9
(74) 대리인
김효성

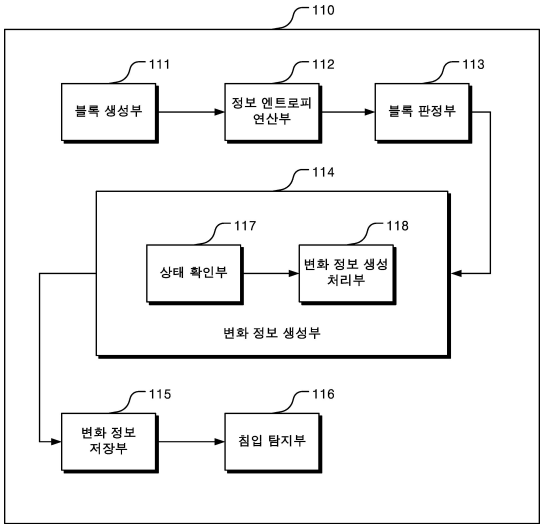
전체 청구항 수 : 총 10 항 심사관 : 이철수

(54) 발명의 명칭 **슬라이딩 윈도우를 이용한 메시지 검증 기반의 차량 내 보안 침입 탐지 장치 및 그 동작 방법**

(57) 요 약

슬라이딩 윈도우를 이용한 메시지 검증 기반의 차량 내 보안 침입 탐지 장치 및 그 동작 방법이 개시된다. 본 발명은 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임의 메시지 ID로 구성된 블록을 순차적으로 생성하고, 각 블록에서의 메시지 ID의 정보량을 표상하는 정보 엔트로피를 연산한 후 상기 연산된 정보 엔트로피를 기초로 이전 순번의 블록과 현재 순번의 블록 간의 비교를 수행하여 그 비교 결과를 기반으로 차량 내에 보안 침입이 발생하였는지 여부를 탐지하는 차량 내 보안 침입 탐지 장치 및 그 동작 방법을 제시함으로써, 차량 내의 외부 침입으로 인한 위험을 방지할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 63/123 (2013.01)
H04L 2012/40215 (2013.01)
H04L 2012/40273 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711092968
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	자율 주행차를 위한 침입 감내 핵심 요소 기술 개발
기 여 율	1/1
과제수행기관명	조선대학교 산학협력단
연구기간	2019.01.01 ~ 2019.12.31

명 세 서

청구범위

청구항 1

차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐(queue)에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성하는 블록 생성부;

현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산하는 정보 엔트로피 연산부;

상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행하는 블록 판정부;

상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성하는 변화 정보 생성부;

k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 상기 변화 정보 생성부에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장하는 변화 정보 저장부; 및

상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지하는 침입 탐지부

를 포함하고,

상기 침입 탐지부는

상기 변화 정보 큐에 저장된 k개의 변화 정보들이 상기 사전 설정된 패턴을 갖지 않는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록 중 상기 블록 판정부에서 정상 블록이 아닌 것으로 판정된 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해서만 보안 침입이 발생한 것으로 탐지하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 블록 판정부는

상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일한 경우, 상기 제1 블록을 정상 블록인 것으로 판정하고, 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일하지 않은 경우, 상기 제1 블록을 정상 블록이 아닌 것으로 판정하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치.

청구항 4

제1항에 있어서,

상기 변화 정보 생성부는

상기 제2 블록에서 상기 제1 블록으로의 변화 상태가 제1 변화 상태 - 상기 제1 변화 상태는 상기 제1 블록의 정보 엔트로피와 상기 제2 블록의 정보 엔트로피가 서로 동일한 경우의 상태를 나타냄 - 인지, 제2 변화 상태 - 상기 제2 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피를 초과하는 경우의 상태를 나타냄 - 인지, 제3 변화 상태 - 상기 제3 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의

정보 엔트로피 미만인 경우의 상태를 나타냄 - 인지 여부를 확인하는 상태 확인부; 및

상기 제1 변화 상태, 상기 제2 변화 상태, 상기 제3 변화 상태 및 상기 제1 블록이 정상 블록인지 아닌지에 대한 판정 결과로 조합 가능한 경우의 수에 따른 복수의 조건들 중 상기 블록 판정부를 통해 판정된 정상 블록인지 여부에 대한 판정 결과와 상기 상태 확인부에서 확인된 변화 상태에 매칭되는 제1 조건을 선택한 후 상기 제1 조건에 기초하여 상기 변화 정보의 생성을 처리하는 변화 정보 생성 처리부

를 포함하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치.

청구항 5

제4항에 있어서,

상기 변화 정보 생성 처리부는

상기 복수의 조건들 각각에 대응되는 미리 정해진 서로 다른 수치 값이 기록된 조건 테이블을 참조하여 상기 제1 조건에 따른 수치 값을 산출하고, 상기 제1 조건에 따른 수치 값을 상기 변화 정보로 생성하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치.

청구항 6

차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐(queue)에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성하는 단계;

현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산하는 단계;

상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행하는 단계;

상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성하는 단계;

k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 상기 변화 정보를 생성하는 단계에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장하는 단계; 및

상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지하는 단계

를 포함하고,

상기 탐지하는 단계는

상기 변화 정보 큐에 저장된 k개의 변화 정보들이 상기 사전 설정된 패턴을 갖지 않는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록 중 상기 판정을 수행하는 단계에서 정상 블록이 아닌 것으로 판정된 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해서만 보안 침입이 발생한 것으로 탐지하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 판정을 수행하는 단계는

상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일한 경우, 상기 제1 블록을 정상 블록인 것으로 판정하고, 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일하지 않은 경우, 상기 제1 블록을 정상 블록이 아닌 것으로 판정하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법.

청구항 9

제6항에 있어서,

상기 변화 정보를 생성하는 단계는

상기 제2 블록에서 상기 제1 블록으로의 변화 상태가 제1 변화 상태 - 상기 제1 변화 상태는 상기 제1 블록의 정보 엔트로피와 상기 제2 블록의 정보 엔트로피가 서로 동일한 경우의 상태를 나타냄 - 인지, 제2 변화 상태 - 상기 제2 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피를 초과하는 경우의 상태를 나타냄 - 인지, 제3 변화 상태 - 상기 제3 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피 미만인 경우의 상태를 나타냄 - 인지 여부를 확인하는 단계; 및

상기 제1 변화 상태, 상기 제2 변화 상태, 상기 제3 변화 상태 및 상기 제1 블록이 정상 블록인지 아닌지에 대한 판정 결과로 조합 가능한 경우의 수에 따른 복수의 조건들 중 상기 판정을 수행하는 단계를 통해 판정된 정상 블록인지 여부에 대한 판정 결과와 상기 확인하는 단계에서 확인된 변화 상태에 매칭되는 제1 조건을 선택한 후 상기 제1 조건에 기초하여 상기 변화 정보의 생성을 처리하는 단계

를 포함하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법.

청구항 10

제9항에 있어서,

상기 변화 정보의 생성을 처리하는 단계는

상기 복수의 조건들 각각에 대응되는 미리 정해진 서로 다른 수치 값이 기록된 조건 테이블을 참조하여 상기 제1 조건에 따른 수치 값을 산출하고, 상기 제1 조건에 따른 수치 값을 상기 변화 정보로 생성하는 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법.

청구항 11

제6항, 제8항, 제9항 또는 제10항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 12

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

발명의 설명

기 술 분 야

[0001] 본 발명은 메시지 검증 기반의 차량 내 보안 침입 탐지 장치 및 그 동작 방법에 대한 것이다.

배 경 기 술

[0002] 최근, 차량에 통신 모듈이 탑재되어, 네트워크를 통해 다른 차량들 또는 외부의 교통 시설들과 데이터를 송수신할 수 있는 커넥티드 카에 대한 연구가 지속되고 있다.

[0003] 아울러, 자율 주행 차량에 대한 관심이 증가됨에 따라, 자율 주행 차량에 적용되는 다양한 최신 기술들이 등장하고 있다.

[0004] 이렇게 첨단 기술이 탑재된 차량은 해당 차량이 스스로 주행 환경을 판단하여 차량 주행을 할 것인지 아니면, 멈출 것인지 등을 결정하는 기능을 제공하고 있다는 점에서 차량 주변 환경을 감지하기 위한 다양한 센서들이 탑재되고 있다.

[0005] 이러한 센서들로는 차량 주변에 장애물이 존재하는지 여부를 감지하기 위한 감지 센서, 차량의 현재 위치를 판단하기 위한 GPS 센서 등이 존재하며, 만약 감지 센서가 차량 주변에 장애물이 존재하는 것으로 감지하게 되면, 차량의 감속을 유도하기 위한 센싱 결과 값을 출력하고, 차량 주변에 장애물이 존재하지 않는 것으로 감지하면, 차량의 속도를 유지시키거나 가속을 유도하기 위한 센싱 결과 값을 출력하는 형태로 동작한다.

[0006] 참고로, 이러한 감지 센서들로는 초음파를 이용하여 장애물을 감지하는 초음파 센서, 카메라를 통해 촬영한 영상으로부터 오브젝트 추적을 수행하여 장애물을 감지하는 영상 감지 센서, 레이더(RADAR)를 이용하여 장애물을 감지하는 레이더 센서, 레이저 광을 이용하여 장애물을 감지하는 라이더(LiDAR) 센서 등이 활용되고 있다.

[0007] 네트워크 기능이 탑재된 차량들은 외부로부터 다양한 데이터를 수신하기 때문에 외부에서 인위적으로 차량의 제어 체계를 교란하기 위한 데이터를 전송하게 되면, 차량의 제어에 문제가 발생하게 되어 운전자에게 큰 위협이 될 수 있다.

[0008] 예컨대, 외부에서 차량에 탑재되어 있는 다양한 센서들에 대해 조작을 가하거나 차량의 ECU(Electronic Control Unit)에 대한 공격을 가함으로써, 운전자가 원하지 않는 형태로 차량을 제어함에 따라 대형 교통사고를 유발하는 문제를 일으킬 수 있다.

[0009] 따라서, 네트워크 기능이 탑재된 차량에 대해 외부로부터의 데이터 침입이 발생하였는지 여부를 탐지할 수 있는 기술에 대한 연구가 필요하다.

[0010] 특정 주행 환경 하에서 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들은 차량에 문제가 없는 한, 거의 매번 유사한 패턴으로 발생하기 때문에 CAN 통신 네트워크를 통해 발생할 수 있는 모든 종류의 프레임에 대한 메시지 ID의 발생 확률은 특정 확률 값으로 수렴하는 특징을 가지고 있다. 이로 인해, 특정 주행 환경 하에서 차량 내부에서 발생할 수 있는 CAN 프레임의 메시지 ID의 발생 확률과 연관된 정보량을 표상하는 정보 엔트로피(entropy)는 특정 값으로 수렴하게 된다. 여기서, 정보 엔트로피란 특정 확률을 갖는 사건들에 대한 불확실성 정도를 나타내는 정보량을 수치화한 것을 의미한다.

[0011] 앞서 언급한 바에 따라, 정상 상태의 차량에서는 특정 주행 조건별로 발생하는 메시지 ID의 종류가 규칙적인 특성을 가지고 있기 때문에 정보 엔트로피가 일정한 값으로 수렴하는 특징을 가지고 있다. 하지만, 공격자에 의해 차량 내부에 외부 데이터의 침입이 발생하게 되면, 각 프레임의 메시지 ID의 발생 확률이 달라지게 되어 정보 엔트로피 값에 대한 변화가 발생할 수 있다.

[0012] 따라서, 차량 내부에서 발생하는 CAN 프레임의 메시지 ID에 대한 정보량을 표상하는 정보 엔트로피의 확인을 통해 차량 내에 보안 침입이 발생하였는지 여부를 판단할 수 있는 기술을 도입함으로써, 차량 내의 외부 침입으로 인한 위험을 방지할 수 있는 기법에 대한 연구가 필요하다.

발명의 내용

해결하려는 과제

[0013] 본 발명은 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임의 메시지 ID로 구성된 블록을 순차적으로 생성하고, 각 블록에서의 메시지 ID의 정보량을 표상하는 정보 엔트로피를 연산한 후 상기 연산된 정보 엔트로피를 기초로 이전 순번의 블록과 현재 순번의 블록 간의 비교를 수행하여 그 비교 결과를 기반으로 차량 내에 보안 침입이 발생하였는지 여부를 탐지하는 차량 내 보안 침입 탐지 장치 및 그 동작 방법을 제시함으로써, 차량 내의 외부 침입으로 인한 위험을 방지할 수 있도록 한다.

과제의 해결 수단

[0014] 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치는 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐(queue)에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성하는 블록 생성부, 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산하는 정보 엔트로피 연산부, 상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행하는 블록 판정부, 상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성하는 변화 정보 생성부, k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수

있는 변화 정보 큐에 상기 변화 정보 생성부에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장하는 변화 정보 저장부 및 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지하는 침입 탐지부를 포함한다.

[0015] 또한, 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법은 차량 내부에서 발생하는 CAN 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성하는 단계, 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산하는 단계, 상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행하는 단계, 상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성하는 단계, k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 상기 변화 정보를 생성하는 단계에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장하는 단계 및 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지하는 단계를 포함한다.

발명의 효과

[0016] 본 발명은 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임의 메시지 ID로 구성된 블록을 순차적으로 생성하고, 각 블록에서의 메시지 ID의 정보량을 표상하는 정보 엔트로피를 연산한 후 상기 연산된 정보 엔트로피를 기초로 이전 순번의 블록과 현재 순번의 블록 간의 비교를 수행하여 그 비교 결과를 기반으로 차량 내에 보안 침입이 발생하였는지 여부를 탐지하는 차량 내 보안 침입 탐지 장치 및 그 동작 방법을 제시함으로써, 차량 내의 외부 침입으로 인한 위험을 방지할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0019] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0020] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아

울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0021] 도 1은 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 구조를 도시한 도면이다.

[0022] 도 1을 참조하면, 본 발명에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치(110)는 블록 생성부(111), 정보 엔트로피 연산부(112), 블록 판정부(113), 변화 정보 생성부(114), 변화 정보 저장부(115) 및 침입 탐지부(116)를 포함한다.

[0023] 블록 생성부(111)는 차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐(queue)에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성한다.

[0024] 정보 엔트로피 연산부(112)는 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산한다.

[0025] 정보 엔트로피란 특정 확률을 갖는 사건들에 대한 불확실성 정도를 나타내는 정보량을 수치화한 것을 의미한다. 관련해서, 이산 확률 변수에서 특정 값에 대한 확률을 나타내는 함수인 확률 질량 함수를 p(x)라고 하고, x의 개수가 K개라고 하였을 때, 상기 이산 확률 변수에 대한 정보 엔트로피 H[X]는 하기의 수학식 1과 같이 연산될 수 있다.

수학식 1

[0027]
$$H[X] = -\sum_{k=1}^{K} p(x_k)\log_2 p(x_k)$$

[0029] 이때, 본 발명의 일실시예에 따르면, 정보 엔트로피 연산부(112)는 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피로 레니(Renyi) 엔트로피를 사용할 수 있다.

[0030] 레니 엔트로피는 정보 엔트로피를 일반화한 것으로, 차수 α는 $\alpha \geq 0$고, $\alpha \neq 1$다. 레니 엔트로피 $H_\alpha(X)$는 하기의 수학식 2와 같이 정의된다.

수학식 2

[0032]
$$H_\alpha(X) = \frac{1}{1-\alpha}\log\left(\sum_{i=1}^{n} p_i^\alpha\right)$$

[0034] α에 따라 레니 엔트로피는 Hartley 엔트로피(Hartley entropy), 섀넌 엔트로피, 충돌 엔트로피(Colliison entropy), 최소 엔트로피(Min-entropy)로 계산될 수 있다.

[0035] 관련해서, 블록 생성부(111)와 정보 엔트로피 연산부(112)의 동작을 예를 들어 설명하면 다음과 같다.

[0036] 우선, n을 100이라고 하면, 블록 생성부(111)는 차량 내부에서 발생하는 CAN 프레임의 메시지 ID를 100개까지 상기 메시지 큐에 순차적으로 저장함으로써, 100개의 메시지 ID들로 구성된 블록을 하나씩 생성할 수 있다.

[0037] 이때, 정보 엔트로피 연산부(112)는 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도

에 따른 정보 엔트로피를 연산할 수 있다. 관련해서, 정보 엔트로피 연산부(112)는 상기 제1 블록에 포함되어 있는 100개의 메시지 ID들 중 서로 중복되지 않는 대표 메시지 ID를 선별할 수 있다. 만약, 100개의 메시지 ID들 중 20개의 메시지 ID들이 서로 중복되지 않는 대표 메시지 ID라고 하는 경우, 정보 엔트로피 연산부(112)는 20개의 메시지 ID들 각각이 상기 제1 블록 내에서 중복해서 존재하는 출연 빈도에 대한 비율을 산출한 후 상기 20개의 메시지 ID들 각각에서 산출된 비율을 이산 확률 변수의 각 확률로 취급해서 상기 수학식 1이나 상기 수학식 2와 같은 연산을 통해 상기 정보 엔트로피를 연산할 수 있다.

[0038] 블록 판정부(113)는 상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행한다.

[0039] 이때, 본 발명의 일실시예에 따르면, 블록 판정부(113)는 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일한 경우, 상기 제1 블록을 정상 블록인 것으로 판정하고, 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일하지 않은 경우, 상기 제1 블록을 정상 블록이 아닌 것으로 판정할 수 있다.

[0040] 변화 정보 생성부(114)는 상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성한다.

[0041] 이때, 본 발명의 일실시예에 따르면, 변화 정보 생성부(114)는 상태 확인부(117) 및 변화 정보 생성 처리부(118)를 포함할 수 있다.

[0042] 상태 확인부(117)는 상기 제2 블록에서 상기 제1 블록으로의 변화 상태가 제1 변화 상태인지, 제2 변화 상태인지, 제3 변화 상태인지 여부를 확인한다.

[0043] 여기서, 상기 제1 변화 상태는 상기 제1 블록의 정보 엔트로피와 상기 제2 블록의 정보 엔트로피가 서로 동일한 경우의 상태를 나타내고, 상기 제2 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피를 초과하는 경우의 상태를 나타내며, 상기 제3 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피 미만인 경우의 상태를 나타낸다.

[0044] 변화 정보 생성 처리부(118)는 상기 제1 변화 상태, 상기 제2 변화 상태, 상기 제3 변화 상태 및 상기 제1 블록이 정상 블록인지 아닌지에 대한 판정 결과로 조합 가능한 경우의 수에 따른 복수의 조건들 중 블록 판정부(113)를 통해 판정된 정상 블록인지 여부에 대한 판정 결과와 상태 확인부(117)에서 확인된 변화 상태에 매칭되는 제1 조건을 선택한 후 상기 제1 조건에 기초하여 상기 변화 정보의 생성을 처리한다.

[0045] 이때, 본 발명의 일실시예에 따르면, 변화 정보 생성 처리부(118)는 상기 복수의 조건들 각각에 대응되는 미리 정해진 서로 다른 수치 값이 기록된 조건 테이블을 참조하여 상기 제1 조건에 따른 수치 값을 산출하고, 상기 제1 조건에 따른 수치 값을 상기 변화 정보로 생성할 수 있다.

[0046] 관련해서, 상태 확인부(117)와 변화 정보 생성 처리부(118)의 동작에 대해 예를 들어 설명하면 다음과 같다.

[0047] 우선, 전술한 바와 같이, 블록 생성부(111)에서 100개의 메시지 ID들로 구성된 블록이 순차적으로 하나씩 생성된다고 가정하고, 상기 조건 테이블이 하기의 표 1과 같다고 가정하자.

표 1

[0049]

복수의 조건들	변화 상태	정상 블록인지 여부에 대한 판정 결과	수치 값
조건 1	제1 변화 상태	정상 블록	0
조건 2	제2 변화 상태	정상 블록	1
조건 3	제3 변화 상태	정상 블록	-1
조건 4	제2 변화 상태	비정상 블록	2
조건 5	제3 변화 상태	비정상 블록	-2

[0051] 이때, 상태 확인부(117)는 이전 순번에서 생성된 제2 블록에서 현재 순번에서 생성된 상기 제1 블록으로의 변화 상태가 상기 제1 변화 상태인지, 상기 제2 변화 상태인지, 상기 제3 변화 상태인지 여부를 확인할 수 있다.

[0052] 만약, 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피와 동일하다고 하는 경우, 상태 확인부(117)는 상기 변화 상태를 상기 제1 변화 상태로 확인할 수 있다.

[0053] 또한, 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피를 초과한다고 하는 경우, 상태 확인부

(117)는 상기 변화 상태를 상기 제2 변화 상태로 확인할 수 있다.

[0054] 또한, 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피 미만이라고 하는 경우, 상태 확인부(117)는 상기 변화 상태를 상기 제3 변화 상태로 확인할 수 있다.

[0055] 이렇게, 상기 변화 상태에 대한 확인이 완료되면, 변화 정보 생성 처리부(118)는 상기 표 1에서 나타낸 복수의 조건들 중 블록 판정부(113)를 통해 판정된 정상 블록인지 여부에 대한 판정 결과와 상태 확인부(117)에서 확인된 변화 상태에 매칭되는 제1 조건을 선택한 후 상기 제1 조건에 대응되는 수치 값을 변화 정보로 생성할 수 있다.

[0056] 관련해서, 블록 판정부(113)에서 상기 제1 블록이 정상 블록으로 판정되었고, 상태 확인부(117)에서 제2 변화 상태로 확인되었다고 하는 경우, 변화 정보 생성 처리부(118)는 상기 표 1을 참조하여 '1'이라고 하는 수치 값을 변화 정보로 생성할 수 있다.

[0057] 이와 달리, 블록 판정부(113)에서 상기 제1 블록이 비정상 블록으로 판정되었고, 상태 확인부(117)에서 제3 변화 상태로 확인되었다고 하는 경우, 변화 정보 생성 처리부(118)는 상기 표 1을 참조하여 '-2'라고 하는 수치 값을 변화 정보로 생성할 수 있다.

[0058] 변화 정보 저장부(115)는 k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 변화 정보 생성부(114)에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장한다.

[0059] 침입 탐지부(116)는 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지한다.

[0060] 예컨대, 블록 생성부(111)에서 100개의 메시지 ID들로 구성된 블록이 생성된다고 하고, 상기 변화 정보 큐에 '0, 0, 1, 0, 0, 1, 0, 0, 1'이라고 하는 변화 정보들이 저장되었다고 하며, '0, 0, 1, 0, 0, 1, 0, 0, 1'이 상기 사전 설정된 패턴이라고 가정하는 경우, 침입 탐지부(116)는 '0, 0, 1, 0, 0, 1, 0, 0, 1'이라고 하는 9개의 변화 정보들 각각이 생성되는데 사용된 현재 블록인 9개의 제1 블록을 각각 확인한 후 9개의 제1 블록에 각각 포함된 100개의 메시지 ID들을 확인하여 각 메시지 ID에 대응하는 CAN 프레임에 대해서 보안 침입이 발생한 것으로 탐지할 수 있다.

[0061] 여기서, 상기 사전 설정된 패턴은 차량 내에 보안 침입이 발생하였음을 지시하기 위한 미리 설정된 변화 정보들의 패턴을 의미하는 것으로, 개발자에 의해 사전 지정되는 정보이다.

[0062] 이때, 본 발명의 일실시예에 따르면, 침입 탐지부(116)는 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 상기 사전 설정된 패턴을 갖지 않는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록 중 블록 판정부(113)에서 정상 블록이 아닌 것으로 판정된 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해서만 보안 침입이 발생한 것으로 탐지할 수 있다.

[0063] 예컨대, 블록 생성부(111)에서 100개의 메시지 ID들로 구성된 블록이 생성된다고 하고, 상기 변화 정보 큐에 '0, 1, 1, 1, 0, 1, 0, 1, 1'이라고 하는 변화 정보들이 저장되었다고 하며, 해당 변화 정보들이 사전 설정된 패턴이 아닌 것이라고 가정하는 경우, 침입 탐지부(116)는 '0, 1, 1, 1, 0, 1, 0, 1, 1'이라고 하는 9개의 변화 정보들 각각이 생성되는데 사용된 현재 블록인 9개의 제1 블록을 각각 확인한 후 9개의 제1 블록 중 블록 판정부(113)에서 정상 블록이 아닌 것으로 판정된 블록만을 선별하여 상기 선별된 블록 각각에 포함된 100개의 메시지 ID에 대응하는 CAN 프레임에 대해서만 보안 침입이 발생한 것으로 탐지할 수 있다. 이때, 침입 탐지부(116)는 상기 9개의 제1 블록 중 블록 판정부(113)에서 정상 블록으로 판정된 블록에 포함된 메시지 ID에 대응하는 CAN 프레임에 대해서는 보안 침입이 발생하지 않은 정상 프레임으로 확인할 수 있다.

[0064] 도 2는 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법을 도시한 순서도이다.

[0065] 단계(S210)에서는 차량 내부에서 발생하는 CAN 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐에 상기 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성한다.

[0066] 단계(S220)에서는 현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산한다.

[0067] 단계(S230)에서는 상기 정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 상기 제1 블록이 정상 블록인지 여부에 대한 판정을 수행한다.

[0068] 단계(S240)에서는 상기 제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 확인한 후 상기 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 상기 제2 블록에서 상기 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성한다.

[0069] 단계(S250)에서는 k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 상기 변화 정보를 생성하는 단계에서 생성되는 상기 변화 정보를 순차적으로 하나씩 저장한다.

[0070] 단계(S260)에서는 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지한다.

[0071] 이때, 본 발명의 일실시예에 따르면, 단계(S260)에서는 상기 변화 정보 큐에 저장된 k개의 변화 정보들이 상기 사전 설정된 패턴을 갖지 않는 것으로 확인되는 경우, 상기 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 상기 제1 블록 중 상기 판정을 수행하는 단계에서 정상 블록이 아닌 것으로 판정된 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해서만 보안 침입이 발생한 것으로 탐지할 수 있다.

[0072] 또한, 본 발명의 일실시예에 따르면, 단계(S230)에서는 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일한 경우, 상기 제1 블록을 정상 블록인 것으로 판정하고, 상기 정보 엔트로피가 상기 미리 정해진 기준 엔트로피와 동일하지 않은 경우, 상기 제1 블록을 정상 블록이 아닌 것으로 판정할 수 있다.

[0073] 또한, 본 발명의 일실시예에 따르면, 단계(S240)에서는 상기 제2 블록에서 상기 제1 블록으로의 변화 상태가 제1 변화 상태(상기 제1 변화 상태는 상기 제1 블록의 정보 엔트로피와 상기 제2 블록의 정보 엔트로피가 서로 동일한 경우의 상태를 나타냄)인지, 제2 변화 상태(상기 제2 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피를 초과하는 경우의 상태를 나타냄)인지, 제3 변화 상태(상기 제3 변화 상태는 상기 제1 블록의 정보 엔트로피가 상기 제2 블록의 정보 엔트로피 미만인 경우의 상태를 나타냄)인지 여부를 확인하는 단계 및, 상기 제1 변화 상태, 상기 제2 변화 상태, 상기 제3 변화 상태 및 상기 제1 블록이 정상 블록인지 아닌지에 대한 판정 결과로 조합 가능한 경우의 수에 따른 복수의 조건들 중 상기 판정을 수행하는 단계를 통해 판정된 정상 블록인지 여부에 대한 판정 결과와 상기 확인하는 단계에서 확인된 변화 상태에 매칭되는 제1 조건을 선택한 후 상기 제1 조건에 기초하여 상기 변화 정보의 생성을 처리하는 단계를 포함할 수 있다.

[0074] 이때, 본 발명의 일실시예에 따르면, 상기 변화 정보의 생성을 처리하는 단계는 상기 복수의 조건들 각각에 대응되는 미리 정해진 서로 다른 수치 값이 기록된 조건 테이블을 참조하여 상기 제1 조건에 따른 수치 값을 산출하고, 상기 제1 조건에 따른 수치 값을 상기 변화 정보로 생성할 수 있다.

[0075] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법은 도 1을 이용하여 설명한 메시지 검증 기반의 차량 내 보안 침입 탐지 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0076] 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0077] 또한, 본 발명의 일실시예에 따른 메시지 검증 기반의 차량 내 보안 침입 탐지 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0078] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0079] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0080] 110: 메시지 검증 기반의 차량 내 보안 침입 탐지 장치

111: 블록 생성부 112: 정보 엔트로피 연산부

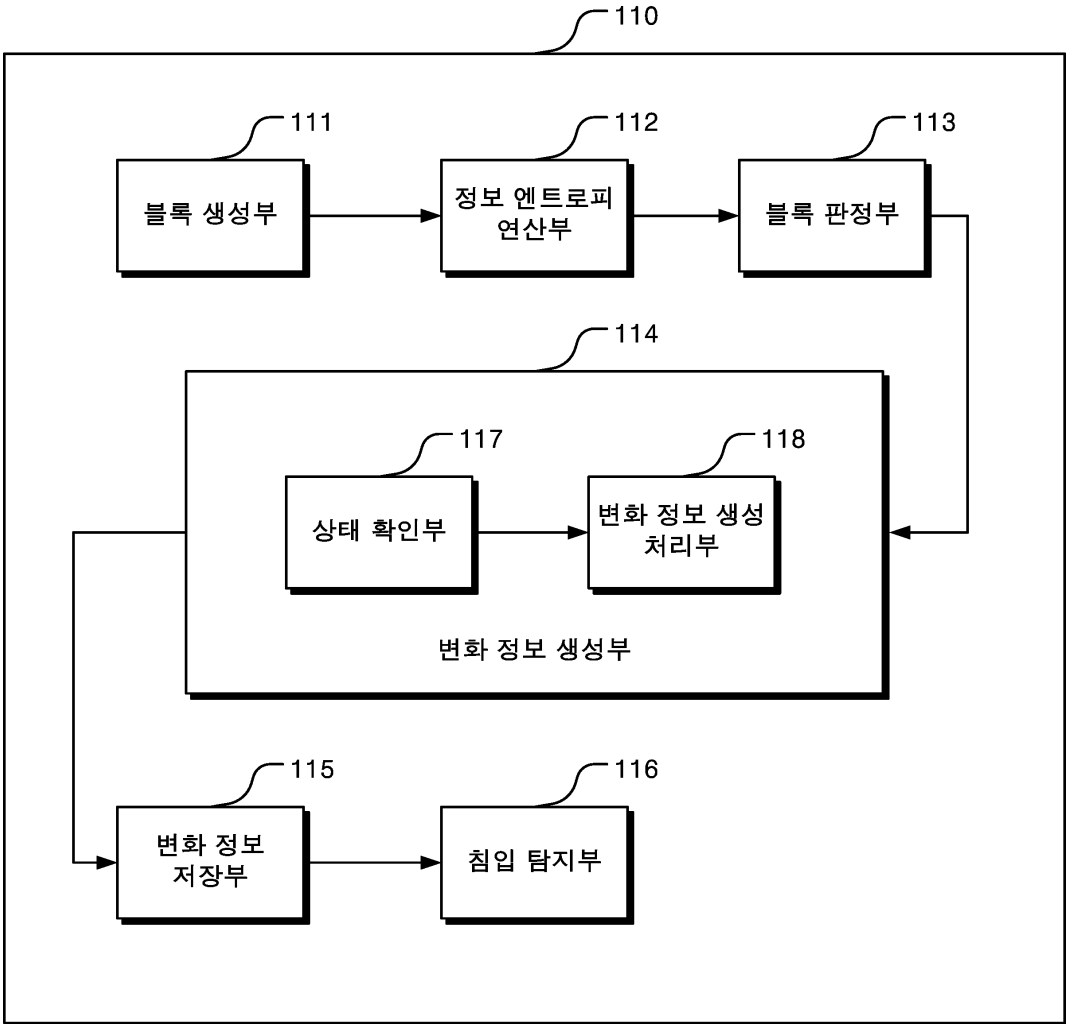
113: 블록 판정부 114: 변화 정보 생성부

115: 변화 정보 저장부 116: 침입 탐지부

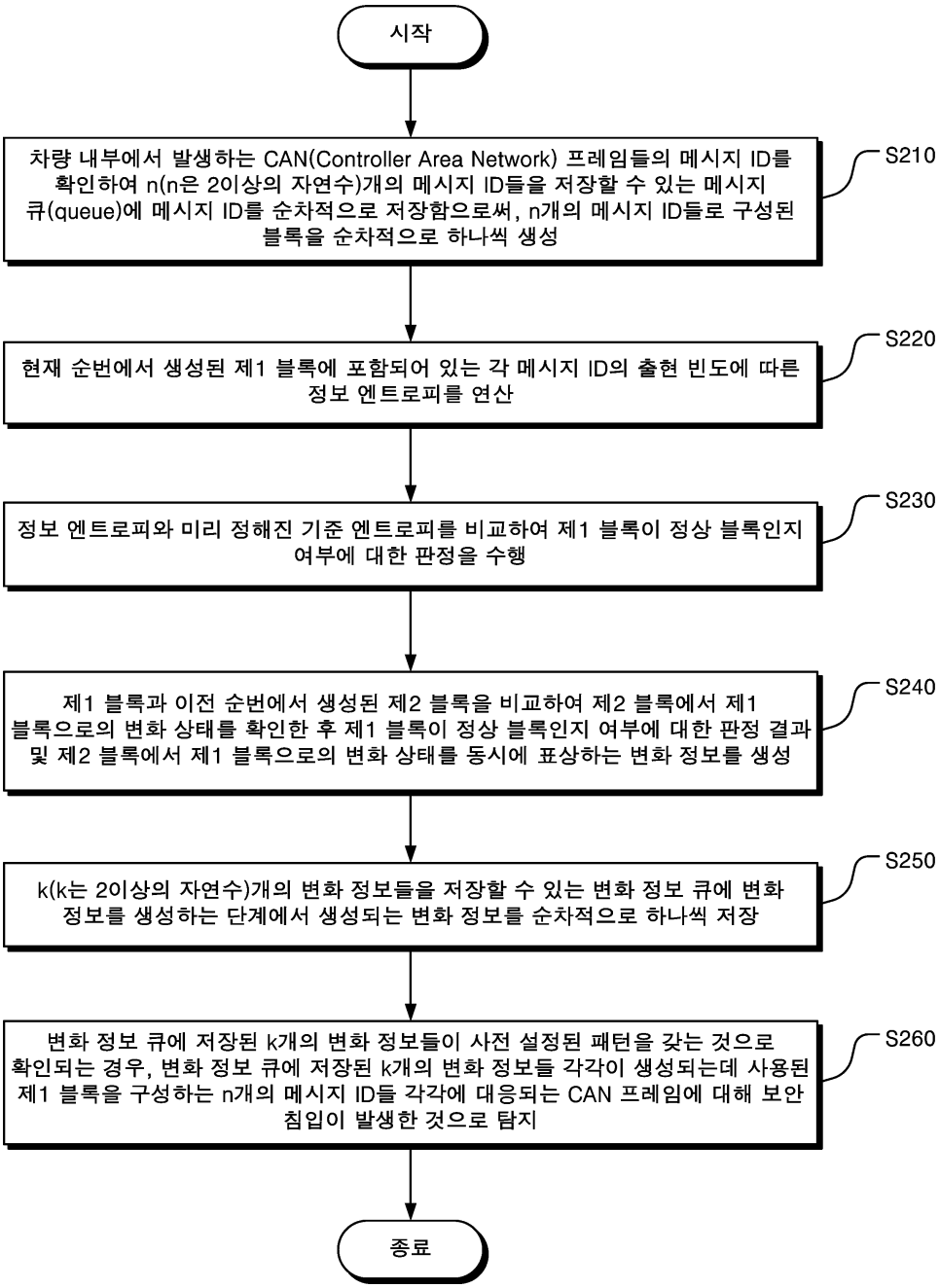
117: 상태 확인부 118: 변화 정보 생성 처리부

도면

도면1



도면2


시작
차량 내부에서 발생하는 CAN(Controller Area Network) 프레임들의 메시지 ID를 확인하여 n(n은 2이상의 자연수)개의 메시지 ID들을 저장할 수 있는 메시지 큐(queue)에 메시지 ID를 순차적으로 저장함으로써, n개의 메시지 ID들로 구성된 블록을 순차적으로 하나씩 생성
S210
현재 순번에서 생성된 제1 블록에 포함되어 있는 각 메시지 ID의 출현 빈도에 따른 정보 엔트로피를 연산
S220
정보 엔트로피와 미리 정해진 기준 엔트로피를 비교하여 제1 블록이 정상 블록인지 여부에 대한 판정을 수행
S230
제1 블록과 이전 순번에서 생성된 제2 블록을 비교하여 제2 블록에서 제1 블록으로의 변화 상태를 확인한 후 제1 블록이 정상 블록인지 여부에 대한 판정 결과 및 제2 블록에서 제1 블록으로의 변화 상태를 동시에 표상하는 변화 정보를 생성
S240
k(k는 2이상의 자연수)개의 변화 정보들을 저장할 수 있는 변화 정보 큐에 변화 정보를 생성하는 단계에서 생성되는 변화 정보를 순차적으로 하나씩 저장
S250
변화 정보 큐에 저장된 k개의 변화 정보들이 사전 설정된 패턴을 갖는 것으로 확인되는 경우, 변화 정보 큐에 저장된 k개의 변화 정보들 각각이 생성되는데 사용된 제1 블록을 구성하는 n개의 메시지 ID들 각각에 대응되는 CAN 프레임에 대해 보안 침입이 발생한 것으로 탐지
S260
종료