



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년03월10일
(11) 등록번호 10-1371902
(24) 등록일자 2014년03월03일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) H04L 12/851 (2013.01)
(21) 출원번호 10-2012-0144900
(22) 출원일자 2012년12월12일
심사청구일자 2012년12월12일
(56) 선행기술조사문헌
KR1020000072707 A
KR1020100041533 A

(73) 특허권자
현대자동차주식회사
서울특별시 서초구 현릉로 12 (양재동)
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
(72) 발명자
안현수
경기 화성시 현대연구소로 150, (장덕동, 현대
기아자동차남양연구소)
이정희
서울 관악구 양지7길 38, 3층 (신림동)
(뒷면에 계속)
(74) 대리인
특허법인태평양

전체 청구항 수 : 총 12 항

심사관 : 전용해

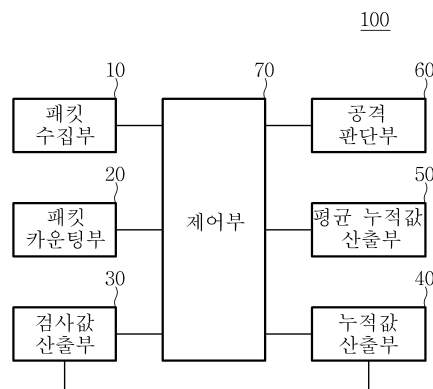
(54) 발명의 명칭 차량 네트워크 공격 탐지 장치 및 그 방법

(57) 요약

본 발명은 차량 네트워크 공격 탐지 장치 및 그 방법에 관한 것으로, 차량 네트워크 버스에 연결되어 있는 각 장치(ID)별로 패킷을 누적 카운팅하고, 패킷을 누적 카운팅할 때마다 검사값(S)을 누적하여 누적값을 산출하며, 상기 누적값을 누적 카운팅으로 나눈 평균 누적값이 제 1 임계치를 초과하지 않는 경우에 공격이 발생한 것으로 판단하는 차량 네트워크 공격 탐지 장치 및 그 방법을 제공하고자 한다.

이를 위하여, 본 발명은 패킷 전송에 대한 우선순위가 정해진 장치들이 차량 네트워크 버스에 연결되어 있는 차량 네트워크 환경에 있어서, 상기 차량 네트워크 버스를 통해 전달되는 패킷을 수집하는 패킷 수집부; 상기 패킷 수집부가 수집한 패킷의 수를 누적 카운팅하는 패킷 카운팅부; 동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출하는 검사값 산출부; 상기 검사값 산출부가 산출한 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출하는 누적값 산출부; 상기 누적값 산출부가 산출한 누적값을 상기 패킷 카운팅부가 누적 카운팅한 값으로 나누어 평균 누적값을 산출하는 평균 누적값 산출부; 및 상기 평균 누적값 산출부가 산출한 평균 누적값을 기반으로 공격 발생 여부를 판단하는 공격 판단부를 포함한다.

대표도 - 도1



(72) 발명자

이병욱

경기 화성시 현대연구소로 150, (장덕동, 현대기
아자동차남양연구소)

배현철

경기 수원시 영통구 청명로 132, 337동 1302호 (영
통동, 청명마을3단지아파트)

노종선

서울 강남구 광평로10길 15, 109동 406호 (일원동,
상록수아파트)

김지엽

서울특별시 용산구 한강로1가 대우월드마크 OAK
1805호

우준영

서울 서초구 사평대로 240, 501동 101호 (반포동,
미도2차아파트)

조창민

서울 서초구 서초대로1길 30, 106동 902호 (방
배동, 방배현대홈타운)

김영식

광주 서구 풍암2로 36, 105동 903호 (풍암동, 주은
모아아파트)

문영식

서울 관악구 낙성대역길 58, 애당 403호 (봉천동)

특허청구의 범위

청구항 1

패킷 전송에 대한 우선순위가 정해진 장치들이 차량 네트워크 버스에 연결되어 있는 차량 네트워크 환경에 있어서,

상기 차량 네트워크 버스를 통해 전달되는 패킷을 수집하는 패킷 수집부;

상기 패킷 수집부가 수집한 패킷의 수를 누적 카운팅하는 패킷 카운팅부;

동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출하는 검사값 산출부;

상기 검사값 산출부가 산출한 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출하는 누적값 산출부;

상기 누적값 산출부가 산출한 누적값을 상기 패킷 카운팅부가 누적 카운팅한 값으로 나누어 평균 누적값을 산출하는 평균 누적값 산출부; 및

상기 평균 누적값 산출부가 산출한 평균 누적값을 기반으로 공격 발생 여부를 판단하는 공격 판단부를 포함하는 차량 네트워크 공격 탐지 장치.

청구항 2

제 1 항에 있어서,

상기 공격 판단부는,

상기 평균 누적값이 임계치를 초과하지 않은 경우에 공격이 발생한 것으로 판단하는 것을 특징으로 하는 차량 네트워크 공격 탐지 장치.

청구항 3

제 1 항에 있어서,

상기 패킷 카운팅부는,

상기 패킷 수집부가 수집한 패킷을 ID별로 분류한 후 각 ID별로 패킷의 수를 누적 카운팅하는 것을 특징으로 하는 차량 네트워크 공격 탐지 장치.

청구항 4

제 1 항에 있어서,

상기 패킷 카운팅부는,

상기 패킷 수집부가 수집한 패킷을 ID별로 분류한 후, 소정의 우선순위를 갖는 ID의 패킷을 대상으로 각 ID별로 누적 카운팅하는 것을 특징으로 하는 차량 네트워크 공격 탐지 장치.

청구항 5

제 1 항에 있어서,

상기 검사값 산출부는

현재 시간(t_c)과 직전에 해당 ID의 패킷이 발생한 시간(t_{ID})과의 차이를 기반으로 검사값을 생성하는 것을 특징

으로 하는 차량 네트워크 공격 탐지 장치.

청구항 6

제 5 항에 있어서,

상기 검사값 산출부는,

하기의 [수학식 A]를 이용하여 검사값(S)을 산출하는 것을 특징으로 하는 차량 네트워크 공격 탐지 장치.

[수학식 A]

$$S = \log_2(t_c - t_{ID})$$

청구항 7

패킷 전송에 대한 우선순위가 정해진 장치들이 차량 네트워크 버스에 연결되어 있는 차량 네트워크 환경에 있어서,

패킷 수집부가 상기 차량 네트워크 버스를 통해 전달되는 패킷을 수집하는 단계;

패킷 카운팅부가 상기 수집된 패킷의 수를 누적 카운팅하는 단계;

검사값 산출부가 동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출하는 단계;

누적값 산출부가 상기 산출된 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출하는 단계;

평균 누적값 산출부가 상기 산출된 누적값을 상기 누적 카운팅한 값으로 나누어 평균 누적값을 산출하는 단계; 및

공격 판단부가 상기 산출된 평균 누적값을 기반으로 공격 발생 여부를 판단하는 단계

를 포함하는 차량 네트워크 공격 탐지 방법.

청구항 8

제 7 항에 있어서,

상기 공격 판단 단계는,

상기 평균 누적값이 임계치를 초과하지 않은 경우에 공격이 발생한 것으로 판단하는 것을 특징으로 하는 차량 네트워크 공격 탐지 방법.

청구항 9

제 7 항에 있어서,

상기 패킷 카운팅 단계는,

상기 패킷 수집부가 수집한 패킷을 ID별로 분류한 후 각 ID별로 패킷의 수를 누적 카운팅하는 것을 특징으로 하는 차량 네트워크 공격 탐지 방법.

청구항 10

제 7 항에 있어서,

상기 패킷 카운팅 단계는,

상기 패킷 수집부가 수집한 패킷을 ID별로 분류한 후, 소정의 우선순위를 갖는 ID의 패킷을 대상으로 각 ID별로 누적 카운팅하는 것을 특징으로 하는 차량 네트워크 공격 탐지 방법.

청구항 11

제 7 항에 있어서,

상기 검사값 산출 단계는

현재 시간(t_c)과 직전에 해당 ID의 패킷이 발생한 시간(t_{ID})과의 차이를 기반으로 검사값을 생성하는 것을 특징으로 하는 차량 네트워크 공격 탐지 방법.

청구항 12

제 11 항에 있어서,

상기 검사값 산출 단계는,

하기의 [수학식 B]를 이용하여 검사값(S)을 산출하는 것을 특징으로 하는 차량 네트워크 공격 탐지 방법.

[수학식 B]

$$S = \log_2(t_c - t_{ID})$$

명세서

기술분야

[0001] 본 발명은 차량 네트워크 공격 탐지 장치 및 그 방법에 관한 것으로, 더욱 상세하게는 차량 네트워크에 대한 외부의 임의적 공격을 사전에 탐지하는 기술에 관한 것이다.

배경기술

[0002] 일반적으로 차량의 내부 네트워크는 외부 네트워크와 독립적으로 운영되어 왔기 때문에, 차량의 내부 네트워크 정보에 대한 보호 수단이 전혀 마련되어 있지 않다.

[0003] 최근 들어 무선통신망(3G/4G) 또는 블루투스 등과 같은 외부 네트워크와의 연결이 가능해지고, 차량 진단 기기와의 연결이 가능해짐에 따라 차량의 내부 네트워크에 악영향이 발생할 가능성이 있다. 즉, 외부 네트워크의 악의적인 공격자가 차량의 내부 네트워크를 교란시킬 경우, 차량 운행에 심각한 문제를 야기하여 탑승자의 안전을 위협할 수 있게 되었다.

[0004] 한편, 인터넷 패킷은 동일 IP 주소를 갖더라도 시간에 따라 패킷의 특징(패킷의 크기, 지연시간, 발생빈도 등)이 다르고, 아울러 규칙적이지 않고 랜덤한 특성을 갖는다. 따라서, 범용 네트워크 공격 탐지 기술은 단위 시간당 수신 패킷 수에 근거하여 공격 여부를 판단한다.

[0005] 반면, 차량 네트워크에서 발생하는 트래픽은 ID별로 패킷 발생 빈도가 다르지만, 각 ID별 트래픽의 발생은 비교적 규칙적으로 생성된다. 이때 두 패킷이 동시에 발생한 경우에는 우선순위에 의해 전송 순서를 결정한다.

[0006] 따라서, 고속으로 발생하는 패킷 ID를 대상으로, 상기 ID보다 높은 우선순위의 패킷을 상기 ID를 가지는 패킷의 발생 빈도와 유사한 빈도로 네트워크에 주입하는 공격에 대해서, 단위 시간당 수신 패킷 수를 기반으로 한 분석으로는 공격을 감지할 수 없다.

[0007] 즉, 우선 순위가 높은 공격용 ID가 우선순위가 낮은 정상 ID 대신 네트워크에 주입이 되기 때문에, 전체 패킷 수에서는 큰 차이가 나지 않으면서도 차량용 네트워크에 대한 서비스 거부 공격이 가능하다. 이 경우, 단순히 패킷 수를 카운팅하는 방식으로는 공격을 감지할 수 없다.

[0008] 이에, 인터넷 침입 탐지에 사용되는 방식과 다른 차량용 트래픽에 적합한 트래픽 분석 방안이 요구된다.

발명의 내용

해결하려는 과제

[0009] 상기와 같은 요구에 부응하기 위하여, 본 발명은 차량 네트워크 버스에 연결되어 있는 각 장치(ID)별로 패킷을 누적 카운팅하고, 패킷을 누적 카운팅할 때마다 검사값(S)을 누적하여 누적값을 산출하며, 상기 누적값을 누적 카운팅으로 나눈 평균 누적값이 제 1 임계치를 초과하지 않는 경우에 공격이 발생한 것으로 판단하는 차량 네트워크 공격 탐지 장치 및 그 방법을 제공하는데 그 목적이 있다.

[0010] 또한, 본 발명은 차량 네트워크 버스에 연결되어 있는 장치(ID)들 중에서 소정의 우선순위 범위에 포함되는 각 장치별로 패킷을 누적 카운팅하고, 패킷을 누적 카운팅할 때마다 검사값(S)을 누적하여 누적값을 산출하며, 상기 누적값을 누적 카운팅으로 나눈 평균 누적값이 제 3 임계치를 초과하지 않는 경우에 공격이 발생한 것으로 판단하는 차량 네트워크 공격 탐지 장치 및 그 방법을 제공하는데 다른 목적이 있다.

[0011] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 또 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타난 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 장치는, 패킷 전송에 대한 우선순위가 정해진 장치들이 차량 네트워크 버스에 연결되어 있는 차량 네트워크 환경에 있어서, 상기 차량 네트워크 버스를 통해 전달되는 패킷을 수집하는 패킷 수집부; 상기 패킷 수집부가 수집한 패킷의 수를 누적 카운팅하는 패킷 카운팅부; 동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출하는 검사값 산출부; 상기 검사값 산출부가 산출한 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출하는 누적값 산출부; 상기 누적값 산출부가 산출한 누적값을 상기 패킷 카운팅부가 누적 카운팅한 값으로 나누어 평균 누적값을 산출하는 평균 누적값 산출부; 및 상기 평균 누적값 산출부가 산출한 평균 누적값을 기반으로 공격 발생 여부를 판단하는 공격 판단부를 포함한다.

[0013] 또한 상기 목적을 달성하기 위한 본 발명의 방법은, 패킷 전송에 대한 우선순위가 정해진 장치들이 차량 네트워크 버스에 연결되어 있는 차량 네트워크 환경에 있어서, 패킷 수집부가 상기 차량 네트워크 버스를 통해 전달되는 패킷을 수집하는 단계; 패킷 카운팅부가 상기 수집된 패킷의 수를 누적 카운팅하는 단계; 검사값 산출부가 동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출하는 단계; 누적값 산출부가 상기 산출된 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출하는 단계; 평균 누적값 산출부가 상기 산출된 누적값을 상기 누적 카운팅한 값으로 나누어 평균 누적값을 산출하는 단계; 및 공격 판단부가 상기 산출된 평균 누적값을 기반으로 공격 발생 여부를 판단하는 단계를 포함한다.

발명의 효과

[0014] 상기와 같은 본 발명은, 차량 네트워크 버스에 대한 외부의 공격을 사전에 감지함으로써, 차량의 오작동을 유발하여 정상적인 운행을 방해하려는 시도를 사전에 차단할 수 있도록 하는 효과가 있다.

[0015] 또한, 본 발명은 차량 네트워크 버스에 추가적인 데이터를 주입하지 않고 외부의 공격을 탐지함으로써, 차량 내부 통신의 부하를 최소화할 수 있는 효과가 있다.

[0016] 또한, 본 발명은 차량 내부 통신을 분석하고자 하는 시도(랜덤 패킷의 주입을 통한 분석 시도)를 사전에 감지함으로써, 추가적인 공격 가능성을 차단할 수 있도록 하는 효과가 있다.

도면의 간단한 설명

- [0017] 도 1 은 본 발명에 따른 차량 네트워크 공격 탐지 장치에 대한 일실시에 구성도,
 도 2a 는 본 발명이 적용되는 차량 네트워크 버스에 대한 일예시도,
 도 2b 는 본 발명이 적용되는 차량 네트워크 버스에 대한 다른 예시도,
 도 3 은 본 발명에 따른 차량 네트워크 공격 탐지 원리에 대한 일예시도,
 도 4 는 본 발명에 따른 차량 네트워크 공격 탐지 방법에 대한 일실시에 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0018] 상술한 목적, 특징 및 장점은 첨부된 도면을 참조하여 상세하게 후술되어 있는 상세한 설명을 통하여 보다 명확해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세히 설명하기로 한다.
- [0019] 도 1 은 본 발명에 따른 차량 네트워크 공격 탐지 장치에 대한 일실시에 구성도이다.
- [0020] 도 1에 도시된 바와 같이, 본 발명에 따른 차량 네트워크 공격 탐지 장치는, 패킷 수집부(10), 패킷 카운팅부(20), 검사값 산출부(30), 누적값 산출부(40), 평균 누적값 산출부(50), 공격 판단부(60), 및 제어부(70)를 포함한다.
- [0021] 이러한 구성요소들을 포함하는 차량 네트워크 공격 탐지 장치(ADS)는, 도 2a에 도시된 바와 같이 차량 네트워크의 게이트웨이 내에 구현될 수도 있고, 도 2b에 도시된 바와 같이 차량 네트워크 버스에 연결된 별개의 장치로서 구현될 수도 있다.
- [0022] 상기 각 구성요소들에 대해 살펴보면, 먼저 패킷 수집부(10)는 차량 네트워크 버스를 통해 전달되는 패킷을 수집한다. 이때, 차량 네트워크에 연결된 각 장치(ECU)들에는 고유 ID가 부여되어 있으며, 각 장치들은 자신의 ID가 삽입된 패킷을 차량 네트워크로 전송한다.
- [0023] 다음으로, 패킷 카운팅부(20)는 패킷 수집부(10)가 수집한 패킷의 수를 누적 카운팅한다. 즉, 패킷 카운팅부(20)는 패킷 수집부(10)가 수집한 패킷을 ID별로 분류한 후 각 ID별로 패킷의 수를 누적 카운팅한다.
- [0024] 또한, 패킷 카운팅부(20)는 제어부(70)의 제어하에 패킷 수집부(10)가 수집한 패킷을 ID별로 분류한 후, 소정의 우선순위를 갖는 ID의 패킷을 대상으로 각 ID별로 누적 카운팅할 수도 있다.
- [0025] 다음으로, 검사값 산출부(30)는 현재 시간(t_c)과 직전에 해당 ID의 패킷이 발생한 시간(t_{ID})과의 차이를 기반으로 검사값(S)을 생성한다. 즉, 검사값 산출부(30)는 하기의 [수학식 1]를 이용하여 검사값(S)을 산출한다.
- [0026] [수학식 1]
- [0027]
$$S = \log_2(t_c - t_{ID})$$
- [0028] 검사값 산출부(30)는 ID별로 패킷이 발생한 시간을 갱신한다.
- [0029] 다음으로, 누적값 산출부(40)는 검사값 산출부(30)가 산출한 검사값을 직전에 산출된 검사값과 합하여 누적값($A=A+S$)을 산출한다. 여기서, A는 누적값을 의미한다.
- [0030] 다음으로, 평균 누적값 산출부(50)는 누적값 산출부(30)가 산출한 누적값을 패킷 카운팅부(20)가 카운팅한 값(해당 ID의 누적 패킷 수)으로 나누어 평균 누적값을 산출한다.
- [0031] 다음으로, 공격 판단부(70)는 평균 누적값 산출부(50)가 산출한 평균 누적값이 임계치를 초과하지 않으면 공격이 발생한 것으로 판단한다.
- [0032] 한편, 제어부(70)는 상기 각 구성요소들을 제어한다. 특히, 제어부(70)는 차량 네트워크 공격 탐지 정책에 따라 상기 각 구성요소들을 개별 제어할 수 있다.
- [0033] 예를 들어, 차량 네트워크 버스에 연결되어 있는 모든 장치들을 대상으로 각 장치별로 공격 여부를 탐지하는 경

우, 제어부(70)는 그에 상응하도록 제어 기능을 수행한다.

- [0034] 다른 예로, 차량 네트워크 버스에 연결되어 있는 장치들 중에서 소정의 우선순위 범위에 포함되는 장치들을 대상으로 각 장치별로 공격 여부를 탐지하는 경우, 제어부(70)는 그에 상응하도록 제어 기능을 수행한다.
- [0035] 본 발명은 특정 ID를 가지는 패킷이 직전에 발생한 시간과 현재 다시 발생한 시간과의 차이에 로그(log)를 취해서 누적한 누적값을 이용한다.
- [0036] 부연 설명하자면, 동일한 ID의 패킷이 다시 발생할 때까지의 시간 차이는 해당 ID의 패킷이 발생하는 확률 값과 밀접한 관계가 있다. 즉, 발생 빈도가 높은 ID(발생 확률이 높은 ID)는 시간 차이가 짧고, 발생 빈도가 낮은 ID(발생 확률이 낮은 ID)는 시간 차이가 크다.
- [0037] 발생 빈도가 높은 ID는 시간 차이가 짧으므로 작은 값이 자주 더해지고, 빈도가 낮은 ID는 시간 차이가 크기 때문에 큰 값이 드물게 더해진다.
- [0038] 이런 값들을 누적한 후에 해당 ID의 전체 패킷 발생 횟수로 나누게 되면 평균적인 기대값(이하, 평균 누적값)을 얻을 수 있고, 이를 이용하여 외부의 공격 여부를 판단할 수 있다.
- [0039] 이하, 도 3을 참조하여 차량 네트워크 공격 탐지 장치가 차량 네트워크에 대한 외부의 공격을 탐지하는 원리에 대해 살펴보기로 한다.
- [0040] 도 3에 도시된 바와 같이, 정상적인 트래픽으로서, ID=2인 패킷이 2ms마다 발생한다고 가정한다. 이때, 외부의 공격자는 우선순위 공격으로서, 정상적인 트래픽의 발생 주기에 맞춰 ID=2인 패킷보다 우선순위가 높은 패킷(ID=1)을 주입하여 정상 패킷(ID=2)의 전송을 방해한다고 가정한다.
- [0041] 이 경우, 전체 패킷의 총 수는 8개로 동일하기 때문에 패킷의 수를 검사하는 종래의 방식으로는 공격 여부를 파악할 수 없다.
- [0042] 그러나, 본 발명은 누적 평균값에 있어서 다음과 같은 차이가 발생하게 되어, 차량 네트워크에 대한 공격 여부를 파악할 수 있다.
- [0043] 정상적인 트래픽의 경우, 평균 누적값은 $(\log_2 10^{-3} + 7 \times \log_2 2 \times 10^{-3})/8 = -9.09$ 가 된다.
- [0044] 반면, 우선순위 공격의 경우, 평균 누적값은 $(\log_2 10^{-3} + \log_2 3 \times 10^{-3} + 5 \times \log_2 2 \times 10^{-3} + \log_2 14 \times 10^{-3})/8 = -8.67$ 이 된다.
- [0045] 도 4는 본 발명에 따른 차량 네트워크 공격 탐지 방법에 대한 일실시에 흐름도이다.
- [0046] 먼저, 패킷 수집부(10)가 차량 네트워크 버스를 통해 전달되는 패킷을 수집한다(401).
- [0047] 이후, 패킷 카운팅부(20)가 패킷 수집부(10)가 수집한 패킷의 수를 누적 카운팅한다(402). 이때, 패킷 카운팅부(20)는 패킷 수집부(10)가 수집한 패킷을 ID별로 분류한 후 각 ID별로 패킷의 수를 누적 카운팅할 수도 있고, 패킷 수집부(10)가 수집한 패킷을 ID별로 분류한 후, 소정의 우선순위를 갖는 ID의 패킷을 대상으로 각 ID별로 누적 카운팅할 수도 있다.
- [0048] 이후, 검사값 산출부(30)가 동일 ID 패킷의 발생 시간차를 기반으로 검사값을 산출한다(403).
- [0049] 이후, 누적값 산출부(40)가 검사값 산출부(30)가 산출한 검사값을 직전에 산출된 검사값과 합하여 누적값을 산출한다(404).
- [0050] 이후, 평균 누적값 산출부(50)가 누적값 산출부(40)가 산출한 누적값을 상기 누적 카운팅한 값으로 나누어 평균 누적값을 산출한다(405).
- [0051] 이후, 공격 판단부(60)가 평균 누적값 산출부(50)가 산출한 평균 누적값을 기반으로 공격 발생 여부를 판단한다(406).
- [0052] 이러한 과정은 하나의 패킷이 발생할 때마다, 즉 하나의 패킷이 카운팅될 때마다 한 번씩 수행되어 차량 네트워크에 대한 공격 여부를 판단한다.
- [0053] 한편, 전술한 바와 같은 본 발명의 방법은 컴퓨터 프로그램으로 작성이 가능하다. 그리고 상기 프로그램을 구성하는 코드 및 코드 세그먼트는 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기

작성된 프로그램은 컴퓨터가 읽을 수 있는 기록매체(정보저장매체)에 저장되고, 컴퓨터에 의하여 판독되고 실행됨으로써 본 발명의 방법을 구현한다. 그리고 상기 기록매체는 컴퓨터가 판독할 수 있는 모든 형태의 기록매체를 포함한다.

[0054] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

부호의 설명

- [0055]
- 10 : 패킷 수집부

20 : 패킷 카운팅부

30 : 검사값 산출부

50 : 평균 누적값 산출부

70 : 제어부

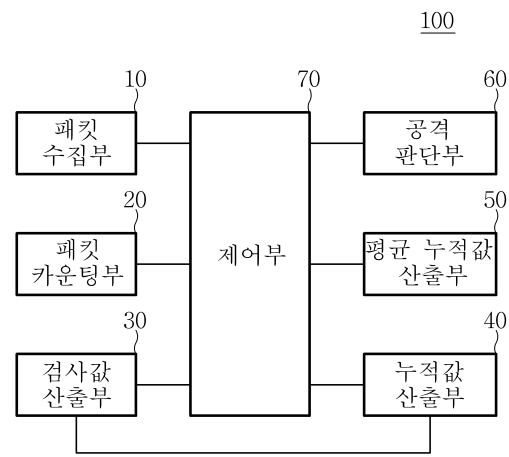
20 : 패킷 카운팅부

40 : 누적값 산출부

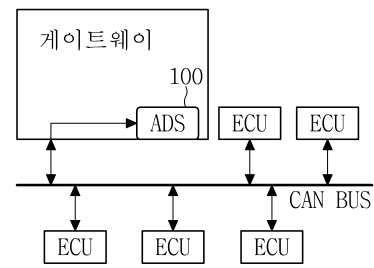
60 : 공격 판단부

도면

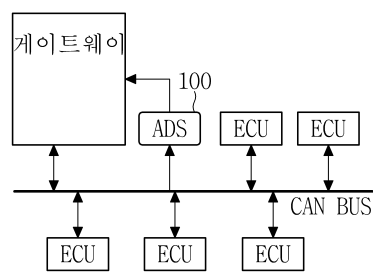
도면1



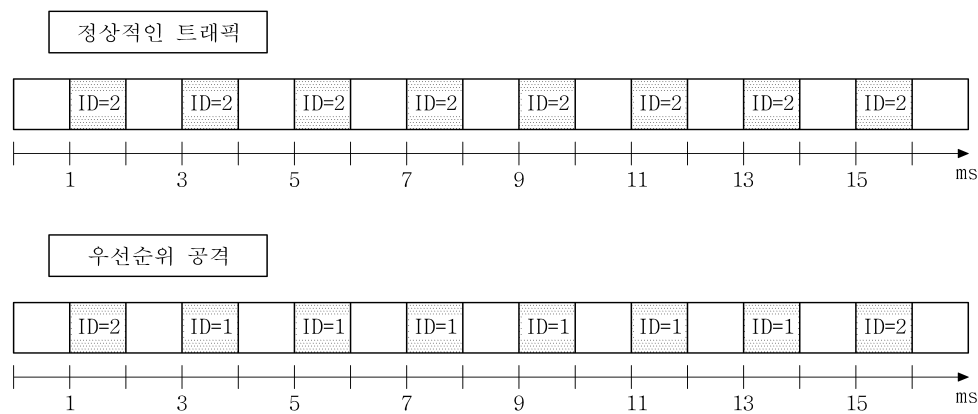
도면2a



도면2b



도면3



도면4

