(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0064859
(43) 공개일자 2018년06월15일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 12/24* (2006.01)
(52) CPC특허분류
H04L 63/1425 (2013.01)
H04L 41/145 (2013.01)
(21) 출원번호 10-2016-0165268
(22) 출원일자 2016년12월06일
심사청구일자 2016년12월06일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
유인태
경기도 용인시 기흥구 덕영대로 1871, 106동 501호 (하갈동, 청명호수마을 신안인스빌1단지)
선경희
경기도 안산시 상록구 부곡로5안길 10-1, 502호
박현선
경기도 수원시 팔달구 정조로 687 1404호
(74) 대리인
김홍석, 김등용

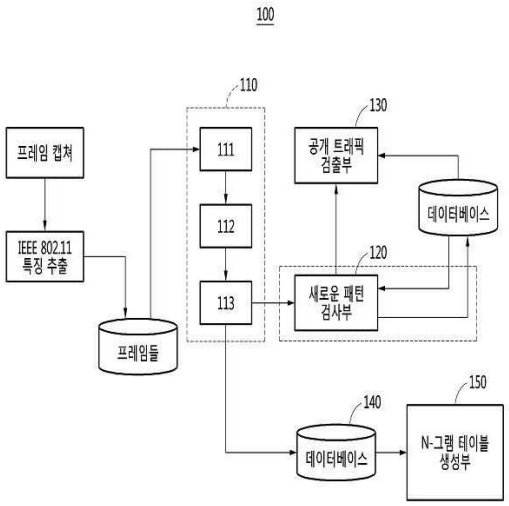
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **무선 트래픽의 패턴 분석 장치 및 방법**

(57) 요 약

본 발명은 무선 트래픽의 패턴을 분석하는 장치 및 방법에 관한 것으로서, 무선 랜(LAN) 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지하기 위해 패턴을 분석하여 확률적으로 해당 패턴이 정상 패턴인지 공격 패턴인지 판단하는 기술적 사상을 개시한다.

대 표 도



(52) CPC특허분류
H04L 63/20 (2013.01)

명 세 서

청구범위

청구항 1

무선 트래픽을 수신하고, 상기 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류하는 수신부; 및

트레이닝 기간 동안에 정상 모델로부터 생성된 N 그램 테이블을 참고하여, 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 새로운 패턴 검사부

를 포함하는 무선 트래픽의 패턴 분석 장치.

청구항 2

제1항에 있어서,

상기 정상 모델에 N 그램 모델을 적용하여 상기 정상 모델에 존재하는 패턴으로부터 상기 N 그램 테이블을 생성하는 N-그램 테이블 생성부

를 더 포함하는 무선 트래픽의 패턴 분석 장치.

청구항 3

제1항에 있어서,

상기 새로운 패턴 검사부는,

크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 확률을 계산하는 무선 트래픽의 패턴 분석 장치.

청구항 4

제1항에 있어서,

상기 새로운 패턴 검사부는,

상기 분류된 패턴에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단하는 무선 트래픽의 패턴 분석 장치.

청구항 5

제1항에 있어서,

상기 새로운 패턴 검사부는,

상기 분류된 패턴에서, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단하는 무선 트래픽의 패턴 분석 장치.

청구항 6

제1항에 있어서,

상기 새로운 패턴 검사부는,

상기 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단하는 무선 트래픽의 패턴 분석 장치.

청구항 7

제1항에 있어서,

상기 새로운 패턴 검사부는,

상기 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단하는 무선 트래픽의 패턴 분석 장치.

청구항 8

정상 모델로부터 패턴들을 분류하는 분류부;

상기 분류된 패턴들 중에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 계산하고, 상기 제1 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 계산하며, 전체 프레임 중에서 상기 제1 프레임이 나올 확률을 계산하는 계산부; 및

상기 계산 결과를 고려하여 패턴의 확률 값이 특정 임계값 이상인 경우 정상 패턴으로 판단하여 정상 모델에 추가하여 정상 모델을 개선시키는 개선부

를 포함하는 것을 특징으로 하는 무선트래픽의 패턴 분석 장치

청구항 9

정상 모델에 N 그램 모델을 적용하여 상기 정상 모델에 존재하는 패턴으로부터 상기 N 그램 테이블을 생성하는 단계;

무선 트래픽을 수신하고, 상기 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류하는 단계; 및

상기 생성된 N 그램 테이블을 참고하여, 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

청구항 10

제9항에 있어서,

상기 정상 여부를 판단하는 단계는,

크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 확률을 계산하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

청구항 11

제10항에 있어서,

상기 각 패턴에 대한 확률을 계산하는 단계는,

상기 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 상기 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을

정상 패턴으로 판단하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

청구항 12

제9항에 있어서,

상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는,

상기 분류된 패턴에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

청구항 13

제9항에 있어서,

상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는,

상기 분류된 패턴에서, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

청구항 14

제9항에 있어서,

상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는,

상기 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단하는 단계

를 포함하는 무선 트래픽의 패턴 분석 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 무선 트래픽의 패턴을 분석하는 장치 및 방법에 관한 것으로서, 무선 랜(LAN) 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지하기 위해 패턴을 분석하여 확률적으로 해당 패턴이 정상 패턴인지 공격 패턴인지 판단하는 기술적 사상을 개시한다.

배 경 기 술

[0003] 트래픽은 전신, 전화 등의 통신 시설에서 통신의 흐름을 의미하는 것으로서, 크게 유선 트래픽과 무선 트래픽으로 분류될 수 있다.

[0004] 그 중에서 무선 트래픽은 통신 선로가 무선 채널로 대체된다는 점에서 매우 효율적인 시스템이나 무선 트래픽에 노이즈가 발생하거나 공격이 발생한 경우, 데이터의 신뢰도가 상당히 낮아질 수 있는 문제가 있다.

[0005] 오늘날의 무선 랜을 이용하는 기술은 이동성은 물론 전송 효율 특성의 향상으로 인하여 다양한 모바일 장치를 위한 네트워크 서비스 환경을 제공하고 있다. 그러나, 이러한 서비스 확장으로 인하여 보안 측면에서의 문제 또한 매우 심각하게 고려해야 할 사항이 되었다.

[0006] 무선 트래픽의 신뢰도 문제를 보완하기 위한 다양한 기술들 개발되고 있다.

[0007] 일반적인 무선 침입 탐지 시스템은 트레이닝 단계에서 대량의 무선 트래픽을 수집하여 정상 모델을 만들고, 새로운 무선 트래픽이 감지되면 기존에 만들어진 정상 모델과 비교하여 정상모델에 없는 트래픽일 경우 이를 비정상적인 트래픽으로 판단한다. 그러나 이 방식은 실제로 감지한 트래픽이 정상적인 트래픽임에도 불구하고 비정상적인 것으로 판단하는 FPR(False Positive Rate) 값이 높아진다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국특허출원 제2008-0043643호 "SNMP 기반의 트래픽 공격 탐지 장치 및 방법"

(특허문헌 0002) 한국특허출원 제2002-0070686호 "분산 서비스 거부 공격 대응 시스템 및 방법"

발명의 내용

해결하려는 과제

[0010] 본 발명은 무선 랜 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지하는 것을 목적으로 한다.

[0011] 본 발명은 정상적인 트래픽임에도 불구하고 비정상적인 트래픽으로 분류될 확률을 줄이는 것을 목적으로 한다.

과제의 해결 수단

[0013] 일실시예에 따른 무선 트래픽의 패턴 분석 장치는 무선 트래픽을 수신하고, 상기 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류하는 수신부, 트레이닝 기간 동안에 정상 모델로부터 생성된 N 그램 테이블을 참고하여, 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 새로운 패턴 검사부를 포함할 수 있다.

[0014] 일실시예에 따른 무선 트래픽의 패턴 분석 장치는 상기 정상 모델에 N 그램 모델을 적용하여 상기 정상 모델에 존재하는 패턴으로부터 상기 N 그램 테이블을 생성하는 N-그램 테이블 생성부를 더 포함할 수 있다.

[0015] 일실시예에 따른 상기 새로운 패턴 검사부는, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 정상일 확률을 계산할 수 있다.

[0016] 일실시예에 따른 상기 새로운 패턴 검사부는, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단할 수 있다.

[0017] 일실시예에 따른 상기 새로운 패턴 검사부는, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단하는 무선 트래픽의 패턴 분석 장치.

[0018] 일실시예에 따른 상기 새로운 패턴 검사부는, 상기 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단할 수 있다.

[0019] 일실시예에 따른 상기 새로운 패턴 검사부는, 상기 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단할 수 있다.

[0020] 일실시예에 따른 무선 트래픽의 패턴 분석 장치는 정상 모델로부터 패턴들을 분류하는 분류부, 상기 분류된 패턴들 중에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 계산하고, 상기 제1 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 계산하며, 전체 프레임 중에서 상기 제1 프레임이 나올 확률을 계산하는 계산부, 및 상기 계산 결과를 고려하여 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단하여 정상 모델에 추가하여 개선시키는 개선부를 포함한다.

[0021] 일실시예에 따른 무선 트래픽의 패턴 분석 방법은 정상 모델에 N 그램 모델을 적용하여 상기 정상 모델에 존재

하는 패턴으로부터 N 그램 테이블을 생성하는 단계, 무선 트래픽을 수신하고, 상기 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류하는 단계, 및 상기 생성된 N 그램 테이블을 참고하여, 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계를 포함할 수 있다.

[0022] 일실시예에 따른 상기 정상 여부를 판단하는 단계는, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 확률을 계산하는 단계를 포함할 수 있다.

[0023] 일실시예에 따른 상기 각 패턴에 대한 확률을 계산하는 단계는, 상기 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단하는 단계를 포함할 수 있다.

[0024] 일실시예에 따른 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는, 상기 분류된 패턴에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단하는 단계를 포함할 수 있다.

[0025] 일실시예에 따른 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는, 상기 분류된 패턴에서, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단하는 단계를 포함할 수 있다.

[0026] 일실시예에 따른 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하는 단계는, 상기 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단하는 단계를 포함할 수 있다.

발명의 효과

[0027] 실시예들에 따르면, 무선 LAN 환경에서 새로운 패턴의 정상 여부를 판단하기 위해 무선 침입 탐지 시스템의 원천 기술로 활용될 수 있다.

[0028] 실시예들에 따르면, 무선 랜 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지할 수 있다.

[0029] 실시예들에 따르면, 정상적인 트래픽임에도 불구하고 비정상적인 트래픽으로 분류될 확률을 줄일 수 있다.

도면의 간단한 설명

[0030] 도 1은 일실시예에 따른 무선 트래픽 패턴 분석 장치를 설명하는 도면이다.

도 2는 일실시예에 따른 무선 트래픽 패턴을 설명하는 도면이다.

도 3은 일실시예에 따른 무선 트래픽 패턴 분석 장치를 설명하는 도면이다.

도 4는 일실시예에 따른 무선 트래픽 패턴 분석 방법을 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0031] 이하에서, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 이러한 실시예들에 의해 권리범위가 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0032] 아래 설명에서 사용되는 용어는, 연관되는 기술 분야에서 일반적이고 보편적인 것으로 선택되었으나, 기술의 발달 및/또는 변화, 관례, 기술자의 선호 등에 따라 다른 용어가 있을 수 있다. 따라서, 아래 설명에서 사용되는 용어는 기술적 사상을 한정하는 것으로 이해되어서는 안 되며, 실시예들을 설명하기 위한 예시적 용어로 이해되어야 한다.

[0033] 또한 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 설명 부분에서 상세한 그 의미를 기재할 것이다. 따라서 아래 설명에서 사용되는 용어는 단순한 용어의 명칭이 아닌 그 용어가 가지는 의미와 명세서 전반에 걸친 내용을 토대로 이해되어야 한다.

[0035] 도 1은 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)를 설명하는 도면이다.

[0036] 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 무선 LAN 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지하기 위해 패턴을 분석하여 확률적으로 해당 패턴이 정상 패턴인지 잠재적인 공격이 가능한 패턴인지 판단할 수 있다.

[0037] 이를 위해, 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 수신부(110) 및 새로운 패턴 검사부 (120)를 포함할 수 있다.

[0038] 먼저, 일실시예에 따른 수신부(110)는 무선 트래픽을 수신하고, 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류할 수 있다. 일실시예에 따른 수신부(110)는 세션 제너레이터(111), 패턴 제너레이터(112), 및 패턴 카운터(113)을 이용해서 캡쳐된 프레임으로부터의 IEEE 802.11의 특징들이 포함된 프레임들을 적어도 하나 이상의 패턴으로 분류할 수 있다.

[0039] 다음으로, 일실시예에 따른 새로운 패턴 검사부 (120)는 트레이닝 기간 동안에 정상 모델로부터 생성된 N 그램 테이블을 참고하여, 적어도 하나 이상의 패턴에 대한 정상 여부를 판단할 수 있다.

[0040] 일실시예에 따른 새로운 패턴 검사부 (120)는 분류된 패턴에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단할 수 있다. 또한, 일실시예에 따른 새로운 패턴 검사부 (120)는 분류된 패턴에서, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단할 수도 있다. 또한, 일실시예에 따른 새로운 패턴 검사부 (120)는 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단할 수 있다. 또한, 일실시예에 따른 새로운 패턴 검사부 (120)는 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단할 수 있다.

[0041] 기존 무선 침입 탐지 시스템은 트레이닝 단계에서 대량의 무선 트래픽을 수집하여 정상 모델을 만들고, 새로운 무선 트래픽이 감지되면 기존에 만들어진 정상 모델과 비교하여 정상모델에 없는 트래픽일 경우 이를 비정상적인 트래픽으로 판단하는 방식이다. 그러나 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 트레이닝 단계 동안 정상 모델과 더불어 정상 무선 트래픽 패턴들의 N-Gram 테이블을 생성하여 이를 바탕으로 새로운 무선 트래픽 패턴이 감지되었을 때 FPR 값을 낮추기 위한 발명이다.

[0042] 이를 위해, 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 정상 모델에 N 그램 모델을 적용하여 정상 모델로부터 N 그램 테이블을 생성하는 N-그램 테이블 생성부(150)를 더 포함할 수 있다.

[0043] 무선 트래픽은 프레임으로 구성되는데, 프레임의 흐름은 일반적으로 패턴을 가지고 있다.

[0044] 무선 트래픽은 이하 도 2를 통해 보다 상세히 설명한다.

[0045] 도 2는 일실시예에 따른 무선 트래픽 패턴을 설명하는 도면이다.

[0046] 도면부호 210에서 사각형 하나는 무선 프레임 하나를 뜻하며, 사각형 안의 내용은 프레임의 타입을 뜻한다. 예를 들면 인증(Auth) 프레임, 인증(Auth) 프레임, 연결요청(AssoReq) 프레임, 연결응답(AssoRes) 프레임, 데이터(Data) 프레임, 데이터(Data) 프레임, 인증해제(DeAuth) 프레임 등으로 흐름을 갖는다.

[0047] 무선 트래픽을 수집하였다고 가정할 때 순차적인 프레임의 패턴 구성은 도면부호 220과 같다.

[0048] 패턴 길이를 4라고 하면, 4개의 프레임을 가지고 하나의 패턴을 만들 수 있다. 따라서 첫 번째 패턴(221)은 [Auth, Auth, AssoReq, AssoRes] 가 되며, 두 번째 패턴은 첫 번째 프레임 바로 다음 프레임부터 시작하여 4개의 프레임으로 두 번째 패턴을 만들 수 있다. 즉 두 번째 패턴(222)은 [Auth, AssoReq, AssoRes, Data] 이다. 같은 방법으로 수집된 마지막 프레임까지 패턴을 구성하면, 총 7개의 패턴이 구성될 수 있다.

[0049] 수신부(110)는 위에서 설명한 방법으로 트레이닝 기간 동안 만들어진 패턴을 모두 모아놓은 것을 정상적인 패턴으로 간주하여 정상 모델(Normal Model)이라고 정의할 수 있다. 또한, 정의된 정상 모델은 데이터베이스(140)에 기록 및 유지될 수 있다.

[0050] 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 정상 모델이 만들어지면 트레이닝 단계를 끝내고, 공격 트래픽 검출부(130)에서 검출 단계를 수행할 수 있다. 이 단계에서는 실시간으로 수집된 트래픽에 대해 구성된 패턴을 정상 모델에 존재하는 패턴들과 비교할 수 있다.

[0051] 일실시예에 따른 무선 트래픽 패턴 분석 장치(100)는 트레이닝 단계에서 만들어진 정상 모델을 바탕으로 생성된 N-그램 테이블을 참조하여 패턴의 정상 여부를 판단하기 때문에, 정상 모델에 존재하지 않는 새로운 패턴이 발견되면 정상일 수도 있는 패턴을 비정상 패턴으로 간주하는 비율을 낮출 수 있다.

[0052] 이러한 정상을 비정상으로 간주하는 비율을 오류양성률(False Positive Rate)이라고 한다. 기존의 오류양성률

(False Positive Rate) 값을 감소시키기 위해 자연어처리 분야(음성인식, 기계 번역 등)에서 사용되는 기법인 N 그램 모델을 활용할 수 있다.

[0053] 다시 도 1을 참고하면, 새로운 패턴 검사부(120)는 N 그램 모델을 활용하여 비정상 패턴을 검출할 수 있다.

[0054] 구체적으로, N 그램은 i번째에 어떠한 사건이 일어날 확률을 이전의 i-1, i-2, … ,i-N+1번째 사건을 바탕으로 조건부 확률 값을 구하는 방법으로서, N=2일 경우 i-1번째 사건을 바탕으로 i번째 사건의 확률을 구하는 것을 뜻하며, N=3일 경우 i-1, i-2 번째 사건을 바탕으로 i번째 사건의 확률을 구하는 것을 뜻한다.

[0055] N 그램 테이블 생성부(150)는 이러한 N 그램 모델을 적용시켜 트레이닝 단계에서 N 그램 테이블을 생성할 수 있다.

[0056] 또한, 새로운 패턴 검사부 (120)는 검출 단계에서 N 그램 테이블을 기반으로 새로운 패턴에 대해 정상일 확률 값을 구할 수 있다. 먼저 N 그램 테이블 생성 과정에 대해 설명하자면, 도 2의 무선 트래픽(210)을 참고할 수 있다.

[0057] N 그램 테이블 생성부(150)는 트레이닝 단계에서 정상 모델이 생성된 후에 정상 모델에 존재하는 패턴을 기반으로 N 그램 테이블을 생성할 수 있다.

[0058] N=2 일 경우에는 이전 프레임 하나만 참고하기 때문에 첫번째 패턴 [Auth, Auth, AssoReq, AssoRes]에 대해 만들어지는 2-그램은 (Auth, Auth), (Auth, AssoReq), (AssoReq, AssoRes) 이다.

[0059] 따라서 첫 번째 패턴에 대해 만들어지는 2-그램 테이블은 [표 1]과 같다.

[0060] [표 1]에서 테이블 안의 숫자는 패턴이 발견된 수를 의미한다.

표 1

[0062]

1st 프레임 \ 2nd 프레임	Auth	AssoReq	AssoRes	Data	DeAuth
Auth	1	1	0	0	0
AssoReq	0	0	1	0	0
AssoRes	0	0	0	0	0
Data	0	0	0	0	0
DeAuth	0	0	0	0	0

[0064] 두번째 패턴의 경우 [Auth, AssoReq, AssoRes, Data]이므로 만들어지는 2-gram은 (Auth, AssoReq), (AssoReq, AssoRes), (AssoRes, Data) 이며, 2-그램 테이블은 [표 2]와 같이 업데이트 된다.

표 2

[0065]

1st 프레임 \ 2nd 프레임	Auth	AssoReq	AssoRes	Data	DeAuth
Auth	1	2	0	0	0
AssoReq	0	0	2	0	0
AssoRes	0	0	0	1	0
Data	0	0	0	0	0
DeAuth	0	0	0	0	0

[0067] 같은 방법으로 모든 패턴에 대해 만들어지는 2-그램 테이블은 [표 3]과 같다.

표 3

[0068]

2nd 프레임 / 1st 프레임	Auth	AssoReq	AssoRes	Data	DeAuth
Auth	1	4	0	0	0
AssoReq	0	0	4	0	0
AssoRes	0	0	0	3	0
Data	0	0	0	3	3
DeAuth	3	0	0	0	0

[0070] 새로운 패턴 검사부(120)는 검출 과정에서 N 그램 테이블을 기반으로 기반으로 새로운 패턴에 대한 확률을 계산할 수 있다.

[0071] 새로운 패턴 검사부(120)는 위에서 설명한 방법대로 N 그램 테이블이 생성되면 검출 단계에서 테이블을 기반으로 새로운 패턴에 대해 정상 패턴일 확률 값을 구한다. 이를 설명하기 위해 [표 4]의 새로운 2-그램 테이블로 예를 들어 설명한다.

표 4

[0072]

2nd 프레임 / 1st 프레임	Auth	AssoReq	AssoRes	Data	DeAuth
Auth	3	4	6	11	2
AssoReq	12	3	1	2	1
AssoRes	1	1	1	5	9
Data	7	0	0	24	3
DeAuth	3	1	4	2	1

[0074] 정상 모델에 존재하지 않는 새로운 패턴 [Data, Data, Data, Deauth]가 관찰되었다고 가정해보면, 새로운 패턴 검사부(120)는 $\mathbb{P}(Data, Data, Data, DeAuth)\,\mathbb{P}(Data, Data, Data, DeAuth)$ 의 확률을 구할 수 있다. 만약, N=2일 경우에는 새로운 패턴 검사부(120)는 이전의 프레임만 고려하여 [수학식 1]과 같이 조건부 확률들을 곱하여 전체 확률을 구할 수 있다.

[0076] [수학식 1]

[0077] $$\mathbb{P}(Data, Data, Data, DeAuth) = \mathbb{P}(Data|Data)\mathbb{P}(Data|Data)\mathbb{P}(Data|DeAuth)$$

[0079] 새로운 패턴 검사부(120)는 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 확률을 계산할 수 있다.

[0081] 크네세르-네이 스무딩(Kneser-Ney Smoothing)은 [수학식 2]와 같다.

[0083] [수학식 2]

[0084] $$P_{KN}(x_i|x_{i-n+1}^{i-1}) = \frac{c(x_{i-n+1}^{i}) - D(c(x_{i-n+1}^{i}))}{\sum_{x_i} c(x_{i-n+1}^{i})} + \lambda(x_{i-n+1}^{i-1}) P_{KN}(x_i|x_{i-n+2}^{i-1})$$

[0086] 따라서 $\mathbb{P}(Data|Data)\,\mathbb{P}(Data|Data)$ 는 [수학식 3]과 같이 계산된다.

[0088] [수학식 3]

[0089] $$P_{KN}(Data|Data) = \frac{c(Data, Data) - D(c(Data, Data))}{\sum_{x_i} c(Data, x_i)} + \lambda(Data) P_{KN}(Data)$$

[0091] [수학식 3]에서 $c(Data, Data)\,c(Data, Data)$ 는 테이블에서 데이터 프레임 다음에 데이터 프레임이 오는 빈도를 뜻하므로, 예시 테이블을 보면 24이다. 또한, $\mathrm{D}(c(Data, Data))\,\mathrm{D}(c(Data, Data))$ 는 $c(Data, Data)\,c(Data, Data)$ 값에 따라 정해지는 디스카운팅(Discounting) 값이며, $\lambda(Data)\lambda(Data)$ 는 상수이다. 또한, $\sum_{x_i} c(Data, x_i) \sum_{x_i} c(Data, x_i)$ 는 Data 프레임 다음에 올 수 있는 모든 프레임들의 빈도수의 합이므로, 34이다. 또한, $P_{KN}(Data)\,P_{KN}(Data)$ 는 전체 프레임 중 Data 프레임이 나올 확률이다.

[0092] $P_{KN}(Data|DeAuth)\,P_{KN}(Data|DeAuth)$ 도 같은 수식을 통해 확률 값을 계산해서 각각의 확률 값을 구한 뒤에 이를 다 곱해서 $\mathbb{P}(Data, Data, Data, DeAuth)\,\mathbb{P}(Data, Data, Data, DeAuth)$ 값을 구할 수 있다.

[0093] 결국, 새로운 패턴 검사부(120)는 구해진 값이 일정 기준치(threshold) 값보다 크면, [Data, Data, Data, DeAuth] 패턴이 정상일 확률이 높다고 판단하여 정상 패턴으로 간주할 수 있다.

[0094] 도 3은 일실시예에 따른 무선 트래픽 패턴 분석 장치(300)를 설명하는 도면이다.

[0095] 일실시예에 따른 무선 트래픽 패턴 분석 장치(300)는 분류부(310), 계산부(320), 및 개선부(330)를 포함할 수 있다.

[0096] 일실시예에 따른 분류부(310)는 정상 모델로부터 패턴들을 분류할 수 있다.

[0097] 일실시예에 따른 계산부(320)는 분류된 패턴들 중에서, 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 계산하고, 상기 제1 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 계산하며, 전체 프레임 중에서 상기 제1 프레임이 나올 확률을 계산할 수 있다.

[0098] 일실시예에 따른 개선부(330)는 계산 결과를 고려하여 패턴의 확률 값이 특정 임계값 이상인 경우 정상 패턴으로 판단하여 정상 모델에 추가하여 정상 모델을 개선시킬 수 있다.

[0099] 결국, 본 발명을 이용하면, 무선 LAN 환경에서 새로운 패턴의 정상 여부를 판단하기 위해 무선 침입 탐지 시스템의 원천 기술로 활용될 수 있다. 또한, 실시예들에 따르면, 무선 랜 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지할 수 있고, 정상적인 트래픽임에도 불구하고 비정상적인 트래픽으로 분류될 확률을 줄일 수 있다.

[0100] 도 4는 일실시예에 따른 무선 트래픽 패턴 분석 방법을 설명하는 도면이다.

[0101] 본 발명은 트레이닝 단계 동안 정상 모델과 더불어 정상 무선 트래픽 패턴들의 N 그램 테이블을 생성하여 이를 바탕으로 새로운 무선 트래픽 패턴이 감지되었을 때 정상 패턴인지 비정상 패턴인지 판단하여 기존보다 오류양성률(False Positive Rate) 값을 낮추기 위한 발명이다.

[0102] 이를 위해, 일실시예에 따른 무선 트래픽 패턴 분석 방법은 정상 모델에 N 그램 모델을 적용하여 정상 모델에 존재하는 패턴으로부터 N 그램 테이블을 생성할 수 있다(단계 401). 일실시예에 따른 무선 트래픽 패턴 분석 방법은 각 패턴에 대한 확률을 계산하기 위해, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대한 확률을 계산할 수 있다.

[0103] 일실시예에 따른 무선 트래픽 패턴 분석 방법은 무선 트래픽을 수신하고, 상기 수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류할 수 있다(단계 402).

[0104] 일실시예에 따른 무선 트래픽 패턴 분석 방법은 생성된 N 그램 테이블을 참고하여, 상기 적어도 하나 이상의 패턴에 대한 정상 여부를 판단할 수 있다(단계 403).

[0105] 예를 들어, 일실시예에 따른 무선 트래픽 패턴 분석 방법은 적어도 하나 이상의 패턴에 대한 정상 여부를 판단하기 위해, 분류된 패턴에서 제1 데이터 프레임 다음에 제2 데이터 프레임이 위치하는 빈도를 고려하여 정상 여부를 판단할 수 있다. 또한, 분류된 패턴에서, 특정 데이터 프레임 다음에 올 수 있는 모든 데이터 프레임들의 빈도수의 합을 고려하여 정상 여부를 판단할 수 있고, 분류된 패턴에서, 전체 프레임 중 특정 데이터 프레임이 나올 확률을 고려하여 정상 여부를 판단할 수 있다. 뿐만 아니라, 적어도 하나 이상의 패턴이 새로운 패턴인 경우, 크네세르-네이 스무딩(Kneser-Ney Smoothing)을 통해 상기 각 패턴에 대해 정상일 확률을 계산한 후, 특정 임계값 이상인 경우 상기 적어도 하나 이상의 패턴을 정상 패턴으로 판단할 수 있다.

[0106] 이러한 과정을 통해, 일실시예에 따른 무선 트래픽 패턴 분석 방법을 이용하면, 무선 LAN 환경에서 새로운 패턴의 정상 여부를 판단하기 위해 무선 침입 탐지 시스템의 원천 기술로 활용될 수 있다. 또한, 실시예들에 따르면, 무선 랜 환경에서 발생할 수 있는 새로운 무선 트래픽 패턴의 정상 여부를 탐지할 수 있고, 정상적인 트래픽임에도 불구하고 비정상적인 트래픽으로 분류될 확률을 줄일 수 있다.

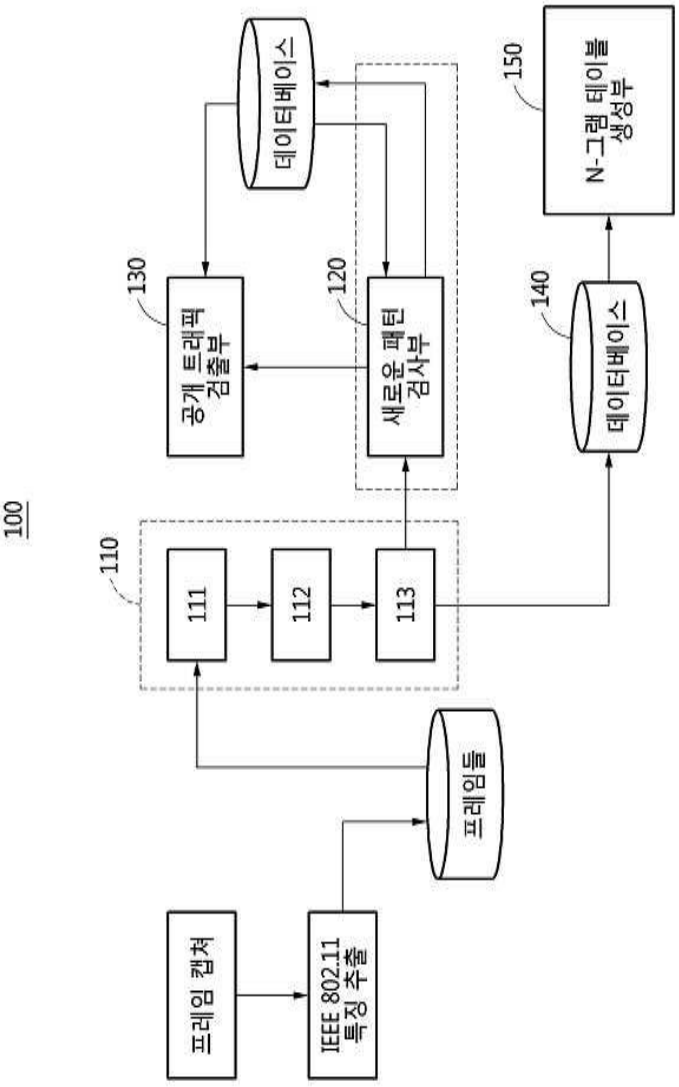
[0108] 본 발명의 일실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0109] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

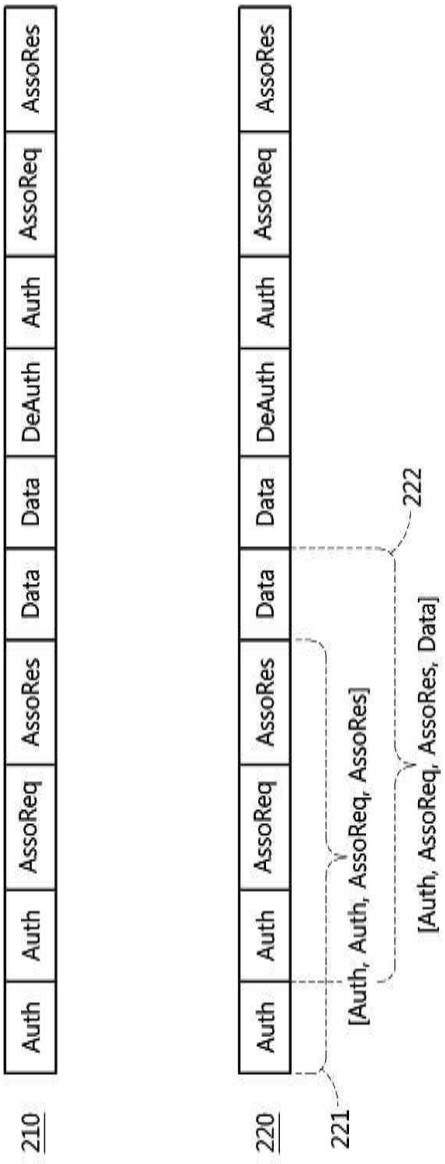
[0110] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

도면

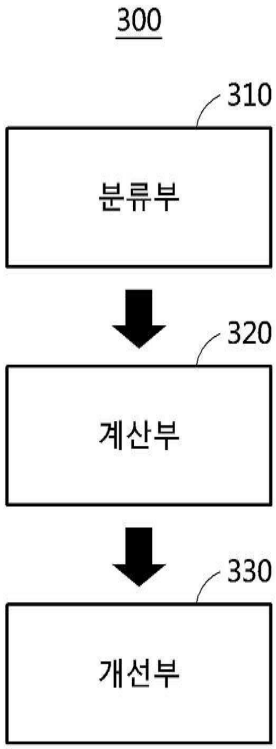
도면1


100
110
111
112
113
120
새로운 패턴 검사부
130
공개 트래픽 검출부
데이터베이스
140
데이터베이스
150
N-그램 테이블 생성부
프레임들
프레임 캡쳐
IEEE 802.11 특징 추출

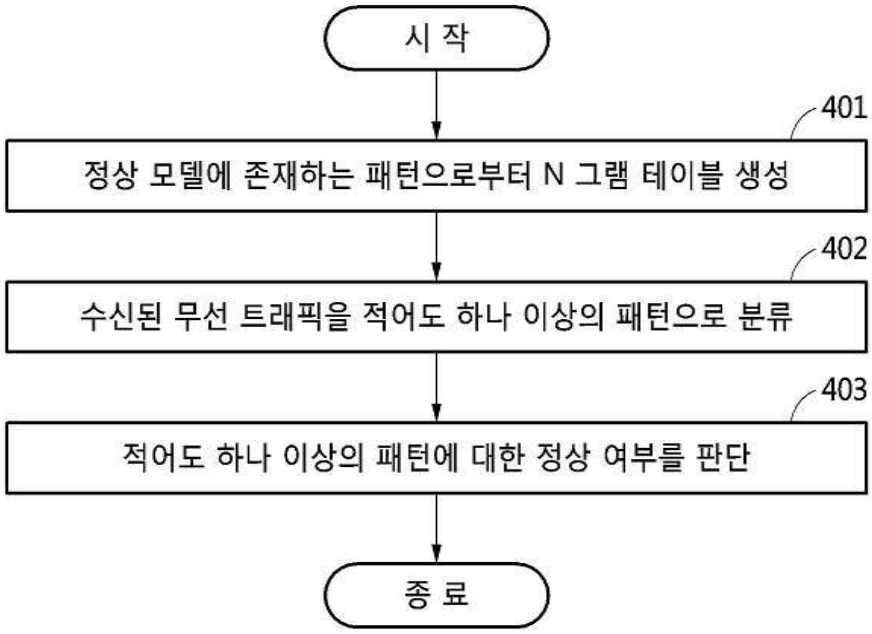
도면2


210
Auth
Auth
AssoReq
AssoRes
Data
DeAuth
Auth
AssoReq
AssoRes
220
Auth
Auth
AssoReq
AssoRes
Data
Data
DeAuth
Auth
AssoReq
AssoRes
221
[Auth, Auth, AssoReq, AssoRes]
222
[Auth, AssoReq, AssoRes, Data]

도면3


300
310
분류부
320
계산부
330
개선부

도면4


시 작
401
정상 모델에 존재하는 패턴으로부터 N 그램 테이블 생성
402
수신된 무선 트래픽을 적어도 하나 이상의 패턴으로 분류
403
적어도 하나 이상의 패턴에 대한 정상 여부를 판단
종 료