(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04L 12/22

(45) 공고일자 2005년10월11일
(11) 등록번호 10-0520687
(24) 등록일자 2005년10월05일

(21) 출원번호 10-2003-0008826
(22) 출원일자 2003년02월12일

(65) 공개번호 10-2004-0072365
(43) 공개일자 2004년08월18일

(73) 특허권자 박세웅

주식회사 안철수연구소

(72) 발명자 이희조

박세웅

손희정

김효곤

(74) 대리인 남상선

심사관 : 신성길

(54) 네트워크 상태 표시 장치 및 방법

요약

네트워크의 비정상적인 상황을 시각적으로 표시할 수 있도록 한 네트워크 상태 표시 장치 및 방법이 개시되어 있다. 이러한 본 발명의 장치는, 외부 통신망으로부터 수집된 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력하는 네트워크 트래픽 수집부; 네트워크 트래픽의 동향을 감시하기 위하여 상기 네트워크 트래픽 수집부에서 전송되는 커넥션 정보를 분석한 후 현재의 네트워크 상황에 대한 좌표 점 데이터 형태로 표시하는 네트워크 상태 표시부; 및 네트워크 비정상적인 상황에 대응하기 위하여 상기 네트워크 트래픽 상태 표시부의 좌표 점 데이터를 받아 비정상적인 네트워크 상황에 대한 공격 특징을 판정하는 공격 특징 판정부로 이루어지며, 현재 네트워크 상황이 3차원 직교 좌표로 표시되므로 네트워크의 비정상적인 상황 판정이 용이하고, 스캐닝 공격 및 서비스 거부 공격 등을 패킷의 커넥션 정보만을 이용하여 판정되므로 공격 특징에 필요한 판정 처리 시간을 단축시켜 고속 네트워크에 적용이 용이하며, 공격 특징에 대한 탐지의 정확성을 더욱 향상시킬 수 있다.

대표도

도 2

색인어

통신망, 서비스 거부 공격, 트래픽, 네트워크상태, 스캐닝 공격

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 네트워크 상태 표시 장치의 구성을 보인 도이다.

도 2는 도 1의 네트워크 트래픽 상황을 보인 도이다.

도 3은 본 발명에 따른 네트워크 상태 표시 과정을 보인 흐름도이다.

도 4는 도 3의 공격 판정 과정을 보인 흐름도이다.

도 5은 도 4의 호스트 스캐닝 공격을 보인 도이다.

도 6은 도 4의 포트 스캐닝 공격을 보인 도이다.

도 7은 도 4의 특정 목적지 IP주소의 특정 포트의 서비스 거부 공격을 보인 도이다.

도 8는 도 4의 특정 목적지 IP주소의 서비스 거부 공격을 보인 도이다.
〈도면의 주요 부분에 대한 부호의 설명〉

삭제

101 : 네트워크 트래픽 수집부

103 : 상태 정보 수집부

105 : 네트워크 상태 표시부

107 : 공격 특징 판정부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 상태 표시 장치 및 방법에 관한 것으로서, 보다 상세하게는 외부 정보 통신망으로부터 유입되는 초기 연결 요청 패킷 중 헤더의 커넥션 정보를 분석하여 유효성 및 불법성 여부를 분석하고, 내부 네트워크의 비정상적인 상황을 유도하는 트래픽 패턴을 인식시켜 현재 네트워크 상태를 용이하게 인식할 수 있도록 한 네트워크 상태 표시 장치 및 방법에 관한 것이다.

최근에는 블루투스와 같은 네트워크에 필요한 제반 기술 및 응용 분야가 개발되고 있다. 이와 같은 네트워크가 네트워크 분야에서 한 주류를 형성하면서 이질적인 기기들의 집합체인 네트워크를 제어, 관리하기 위한 에이전트가 필요하나, 이러한 에이전트로의 불법적 접근은 기업의 안전을 해칠 수도 있다. 이러한 기업 및 그 밖의 네트워크에서 외부로부터의 안전을 지키기 위해서는 네트워크의 특성에 따라 침입탐지, 침입차단, 역추적, 바이러스 방지 등의 많은 기술을 요구한다.

그러나, 이러한 비정상적인 네트워크 상황 감시 및 제어하는 방법에 있어, 수집된 네트워크 트래픽 정보 중 한 특정 항목에 대한 비율만으로 판단하거나, 여러 항목에 대해 검토를 하더라도 각각의 연관성을 살펴보지 않았다.

하나의 예로, 네트워크 트래픽 상태의 분석을 유입되는 네트워크 패킷의 비율과 방출되는 네트워크 패킷 비율의 차이로 비정상적인 공격 상황을 검출하는 방법이 있으며, 이 경우 스캐닝 공격의 판정을 위해 많은 양의 패킷 정보가 필요한 단점이 있다.

또 다른 예로, 패킷의 소스 주소, 목적지 주소, 목적지 포트 번호 각각의 트래픽 양의 측정을 각각 분석하는 방법이 있으며, 이 방법은 각 결과에 대한 연관성이 이루어지지 않아 정확한 공격의 형태를 판정할 수 없는 문제점이 발생하였다.

발명이 이루고자 하는 기술적 과제

이에, 본 발명은 상기한 문제점을 해결하기 위하여 창출된 것으로서, 본 발명은 네트워크의 트래픽 상태가 소스 주소, 목적지 주소, 및 목적지 포트 번호에 의해 3차원 형태의 시각적으로 표시되므로, 공격의 발생 및 특징을 간단하게 검출할 수 있도록 하는 네트워크 상태 표시 장치 및 방법을 제공하고자 하는데 그 목적이 있다.

상기와 같은 목적을 달성하기 위한 본 발명에 따른 네트워크 상태 표시 장치는,

외부 정보 통신망으로부터 수집된 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력하는 네트워크 트래픽 수집부;

네트워크 트래픽의 동향을 감시하기 위하여 상기 네트워크 트래픽 수집부에서 전송되는 커넥션 정보를 분석하여 현재 네트워크 상황에 대한 좌표 점 데이터 형태로 표시하는 네트워크 상태 표시부; 및

네트워크의 비정상적인 상황에 대응하기 위하여 상기 네트워크 트래픽 상태 표시부의 좌표 점 데이터를 받아 비정상적인 네트워크 상황에 대한 공격 특징을 판정하는 공격 특징 판정부로 이루어지는 것에 특징이 있다.

바람직하게, 상기 좌표 점 데이터는 소스 주소, 목적지 주소, 및 목적지 포트 번호를 포함하는 것에 특징이 있다.

바람직하게, 상기 공격 특징 판정부의 공격 특징은, 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 호스트 스캐닝 공격으로 판정하는 것을 특징으로 한다.

바람직하게, 상기 공격 특징 판정부의 공격 특징은, 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 포트 스캐닝 공격으로 판정하는 것에 특징이 한다.

바람직하게, 상기 공격 특징 판정부의 공격 특징은, 목적지 포트 번호 및 목적지 IP주소가 고정이고 소스 IP 주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 특정 목적지 IP주소의 특정 포트에 대한 서비스 거부 공격으로 판정하는 것에 특징이 있다.

바람직하게, 상기 공격 특징 판정부의 공격 특징은, 목적지 IP 주소가 고정이고 소스 IP 주소 및 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 면으로 표시되면 특정 목적지 IP주소의 서비스 거부 공격인 것으로 판정하는 것에 특징이 있다.

본 발명의 다른 특징은,

링크를 통과하는 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력하는 제1과정;

상기 제1 과정에서 수집된 상기 커넥션 정보를 분석한 후 현재의 네트워크 상황에 대한 좌표 점 데이터 형태로 3차원 직교 좌표에 표시하는 제2과정; 및

비정상적인 네트워크 트래픽 상황에 대응하기 위하여 상기 제2 과정에서 생성된 좌표 점 데이터를 받아 네트워크의 비정상적인 상황 발생 및 공격의 특징을 판정하는 제3 과정을 포함하는 것에 특징이 있다.

바람직하게, 상기 제2 과정의 커넥션 정보는 소스 IP 주소, 목적지 IP 주소 및 목적지 포트 번호인 것을 특징으로 한다.

본 발명에 의하면, 현재 네트워크 트래픽 상황이 3차원 직교 좌표의 시각화로 표시되므로 네트워크의 비정상적인 상황 판정이 용이하고, 스캐닝 공격 및 서비스 거부 공격 등을 패킷의 커넥션 정보 만으로 판정되므로 공격 특징의 판정에 필요한 처리 시간을 단축시켜 고속 네트워크에 적용이 용이하고, 공격 특징에 대한 탐지의 정확성을 더욱 향상시킬 수 있다.

발명의 구성 및 작용

이하, 본 발명의 실시 예를 통해 본 발명을 보다 상세히 설명한다.

도 1은 본 발명에 따른 네트워크 상태 표시 장치의 구성을 보인 도이다. 도 1에 있어서, 본 발명은 네트워크 트래픽 수집부(101), 상태 정보 수집부(103), 네트워크 상태 표시부(105) 및 공격 특징 판정부(107)로 구성된다.

상기 네트워크 트래픽 수집부(101)는 엑세스 네트워크(미도시됨)인 외부 통신망으로부터 수집한 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력한다. 즉, 상기 네트워크 트래픽 수집부(101)는 양방향 통신이 가능한 TCP/IP 통신망의 세션(Session) 중 초기 연결 요청 패킷의 헤더로부터 패킷 수집 시각, 소스 IP 주소, 목적지 IP 주소, 목적지 포트 번호를 추출한 후 커넥션 정보를 출력한다. 상기 커넥션 정보는 소스 IP 주소, 목적지 IP 주소, 목적지 포트 번호를 포함한다.

상기 상태 정보 수집부(103)는 네트워크 초기 연결 요청 패킷 중 커넥션 정보를 분석하고, 분석된 커넥션 정보에 따라 테이블의 정보를 갱신한 후 가공하여 좌표 점 데이터를 출력하고, 상기 네트워크 상태 표시부(105)는 상기 상태 정보 수집부(103)로부터 가공된 좌표 점 데이터를, 즉, 소스 IP주소, 목적지 IP 주소, 및 목적지 포트 번호가 각각의 축으로 설정된 3차원 직교 좌표에 표시한다.

즉, 상기 좌표 점 데이터는 도 2에 도시 된 바와 같이 소정 시간(망 속도에 따라 1초 내지 1분으로 설정) 동안 입력된 커넥션 정보를 받아 가공한 후 3차원 직교 좌표에 한 점으로 표시된다.

여기서, 상기 공격 특징 판정부(107)는 상기 네트워크 상태 표시부(105)의 좌표 점 데이터를 통상적인 이미지 처리를 통해 선과 면으로 인식하는 알고리즘을 이용하여 네트워크 비정상적인 상황에 대한 공격 특징을 판정하도록 구비된다. 여기서, 본 발명의 실시 예에서 상기 공격 특징 판정부(107)의 공격 특징은 이미지 프로세싱을 이용하여 판정되도록 구비되어 있으나, 공격 특징 판정에 대한 정확도를 높이기 위하여 다양한 프로세서를 통해 판정될 수도 있다.

즉, 상기 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변이면 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되고, 이 경우 호스트 스캐닝 공격으로 판정하고, 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변이면 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되고, 이 경우 포트 스캐닝 공격으로 판정한다.

그리고, 목적지 포트 번호 및 목적지 IP주소가 고정이고 소스 IP 주소가 가변이면 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되고, 이 경우 소스 IP 주소 변조(Spoofing)를 사용한 특정 목적지 IP주소의 특정 포트에 대한 서비스 거부 공격으로 판정한다.

그리고, 상기 목적지 IP 주소가 고정이고, 소스 IP 주소 및 목적지 포트 번호가 가변이면 3차원 직교 좌표에 면으로 표시되고, 이 경우 소스 IP 주소 변조를 사용한 특정 목적지 IP주소의 서비스 거부 공격인 것으로 판정한다.

그리고, 이러한 비정상적인 네트워크 상황과 공격 특징은 정상적으로 유도하는 프로그램 룰을 생성하여 비정상적인 상황에 대응한다.

도 3는 본 발명에 따른 네트워크 상태를 표시하기 위한 방법의 전체 흐름도이다.

도 3에 있어서, 링크(미도시됨)를 통과하는 네트워크 초기 연결 요청 패킷을 수집하여 상태 유닛 별로 분류하여(단계 200), 상기 단계(200)에서 수집된 네트워크 초기 연결 요청 패킷의 상태 정보를 수집하여 통계 및 패턴 분석 처리하고, 현재의 트래픽 상황에 대한 커넥션 정보를 추출한다(단계 300). 그 후 소정 시간이 경과되었는 지를 체크하여(단계 400) 소정 시간이 경과되었다고 판정되면(즉, 소정 시간 동안 트래픽 정보가 수집되었다고 판단되면) 트래픽 상황에 대한 커넥션 정보를 좌표 점 데이터로 표시한다(단계 500).

상기 단계(500)를 통해 좌표에 점 데이터로 표시된 후 상기 표시된 좌표 점 데이터를 이용하여 공격 특징을 판정한다(단계 600). 상기 단계(600)에서 판정된 공격 특징에 따라 정책을 채택하여 트래픽의 정상 조건을 보정한다(단계 700).

도 4는 도 3에 도시 된 공격 특징 판정 과정을 설명하기 위한 흐름도이고, 도 5 내지 도 8은 도 4의 공격 특징에 따른 좌표 점 데이터들을 보인 도들이다.

도 4에서, 상기 네트워크 상태 표시부(105)에서 공급된 좌표 점 데이터를 분석하여 상기 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변인 지를 체크하여(단계 601) 도 5에 도시 된 바와 같이, 상기 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변인 경우 호스트 스캐닝 공격으로 판정하고(단계 603), 상기 단계(601)에서 상기 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변이 아니라고 판단되면, 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변인 지를 체크한다(단계 605).

상기 단계(605)에서 도 6에 도시 된 바와 같이, 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변인 경우 포트 스캐닝 공격으로 판정하며(단계 607), 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변이 아니라고 판정되면, 상기 단계(609)로 진행한다.

그리고, 상기 단계(609)는 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변인 지를 체크하고, 여기서, 도 7에 도시된 바와 같이, 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변이라고 판정되면, 특정 목적지 IP주소의 특정 포트의 서비스 거부 공격으로 판정한다(단계 611).

한편, 상기 단계(609)에서 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변이 아니라고 판정되면, 단계(613)로 진행하고, 상기 단계(613)는 상기 목적지 IP 주소가 고정이고 소스 IP 주소 및 목적지 포트 번호가 가변인 지를 체크하며, 여기서, 도 8에 도시 된 바와 같이, 목적지 IP 주소가 고정이고 소스 IP 주소 및 목적지 포트 번호가 가변이면, 특정 목적지 IP주소의 서비스 거부 공격인 것으로 판정한다(단계 615).

그리고, 상기의 과정을 통해 공격 특징의 판정이 완료되면 상기 단계(700)로 진행되어 네트워크의 비정상적 상황에 대응한다.

발명의 효과

이상, 본 발명에 의하면, 현재 네트워크 트래픽 상황이 3차원 직교 좌표로 표시되므로 네트워크의 비정상적인 상황 판정이 용이하고, 스캐닝 공격 및 서비스 거부 공격 등을 패킷의 커넥션 정보만으로 판정되므로 공격 특징의 판정에 필요한 처리 시간을 단축시켜 고속 네트워크에 적용이 용이하며 비정상적인 상황에 대응하는 속도가 빠르고, 공격성 특징에 대한 탐지의 정확도를 더욱 향상시킬 수 있는 효과를 얻을 수 있다.

이와 같이, 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범주에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허 청구범위 뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

(57) 청구의 범위

청구항 1.

외부 통신망으로부터 수집된 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력하는 네트워크 트래픽 수집 수단;

네트워크 트래픽의 동향을 감시하기 위하여 상기 네트워크 트래픽 수집 수단에서 전송되는 커넥션 정보를 분석한 후 현재의 네트워크 상황에 대한 좌표 점 데이터 형태로 표시하는 네트워크 상태 표시 수단; 및

네트워크의 비정상적인 상황에 대응하기 위하여 상기 네트워크 상태 표시부의 좌표 점 데이터를 받아 비정상적인 네트워크 상황에 대한 공격 특징을 판정하는 공격 특징 판정 수단으로 이루어지는 것에 특징으로 하는 네트워크 상태 표시 장치.

청구항 2.

제1항에 있어서, 상기 좌표 점 데이터는 소스 주소, 목적지 주소, 및 목적지 포트 번호를 포함하는 것을 특징으로 하는 네트워크 상태 표시 장치.

청구항 3.

제1항에 있어서, 상기 공격 특징 판정부의 공격 특징은, 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 호스트 스캐닝 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 장치.

청구항 4.

제1항에 있어서, 상기 공격 특징 판정부의 공격 특징은 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 포트 스캐닝 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 장치.

청구항 5.

제1항에 있어서, 상기 공격 특징 판정부의 공격 특징은, 목적지 포트 번호 및 목적지 IP주소가 고정이고 소스 IP 주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 특정 목적지 IP주소의 특정 포트에 대한 서비스 거부 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 장치.

청구항 6.

제1항에 있어서, 상기 공격 감지부의 공격 특징은, 목적지 IP 주소가 고정이고 소스 IP 주소 및 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 면으로 표시되면 특정 목적지 IP주소의 서비스 거부 공격인 것으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 장치.

청구항 7.

링크를 통과하는 네트워크 초기 연결 요청 패킷을 분석하여 커넥션 정보를 출력하는 제1과정;

상기 제1 과정에서 수집된 상기 커넥션 정보를 분석한 후 현재의 네트워크 상황에 대한 좌표 점 데이터 형태로 3차원 직교 좌표에 표시하는 제2과정; 및

네트워크 비정상적인 상황에 대응하기 위하여 상기 제2 과정에서 생성된 좌표 점 데이터를 받아 네트워크의 비정상적인 상황 발생 및 공격의 특징을 판정하는 제3 과정을 포함하는 것을 특징으로 하는 네트워크 상태 표시 방법.

청구항 8.

제7항에 있어서, 상기 제2 과정의 커넥션 정보는 소스 IP 주소, 목적지 IP 주소 및 목적지 포트 번호인 것을 특징으로 하는 네트워크 상태 표시 방법.

청구항 9.

제7항에 있어서, 상기 공격 특징 판정부의 공격 특징은, 소스 IP 주소와 목적지 포트 번호가 고정이고 목적지 IP 주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 면으로 표시되면 호스트 스캐닝 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 방법.

청구항 10.

제7항에 있어서, 상기 공격 특징 판정부의 공격 특징은 소스 IP 주소와 목적지 IP 주소가 고정이고 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 포트 스캐닝 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 방법.

청구항 11.

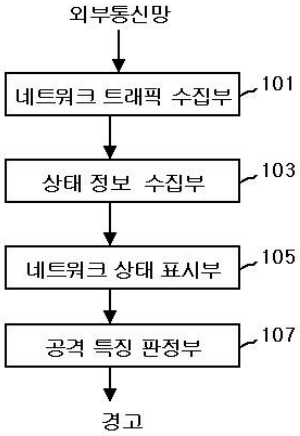
제7항에 있어서, 상기 공격 특징 판정부의 공격 특징은, 목적지 포트 번호 및 목적지 IP주소가 고정이고 소스 IP 주소가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 선으로 표시되면 특정 목적지 IP주소의 특정 포트에 대한 서비스 거부 공격으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 방법.

청구항 12.

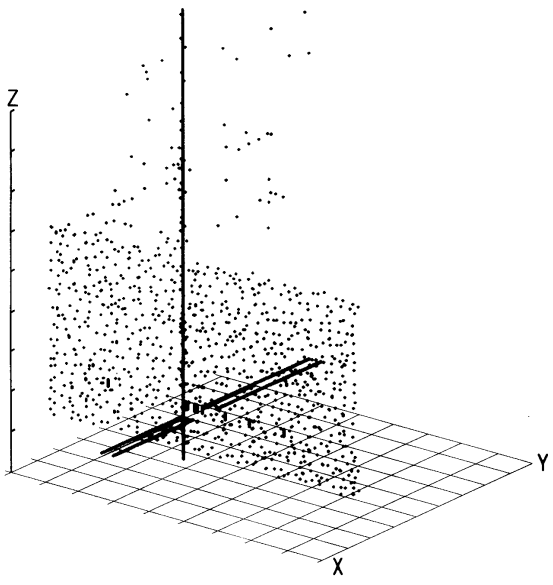
제7항에 있어서, 상기 공격 감지부의 공격 특징은, 목적지 IP 주소가 고정이고 소스 IP 주소 및 목적지 포트 번호가 가변되어 상기 좌표 점 데이터가 3차원 직교 좌표에서 면으로 표시되면 특정 목적지 IP주소의 서비스 거부 공격인 것으로 판정하는 것을 특징으로 하는 네트워크 상태 표시 방법.

도면

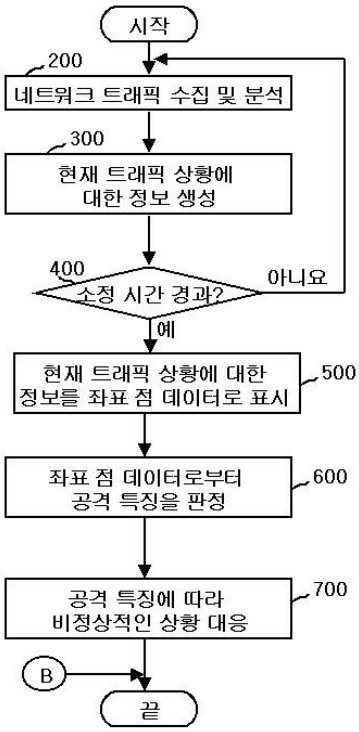
도면1


외부통신망
네트워크 트래픽 수집부
101
상태 정보 수집부
103
네트워크 상태 표시부
105
공격 특징 판정부
107
경고

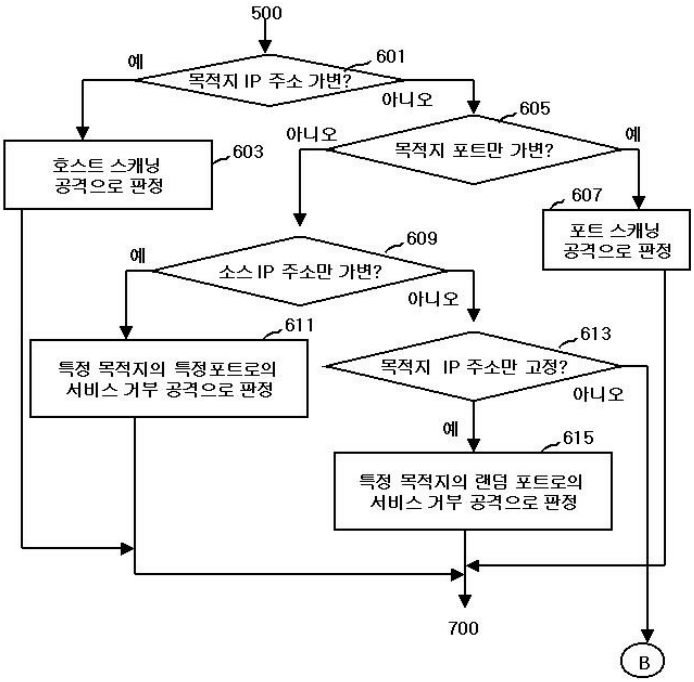
도면2


Z
Y
X

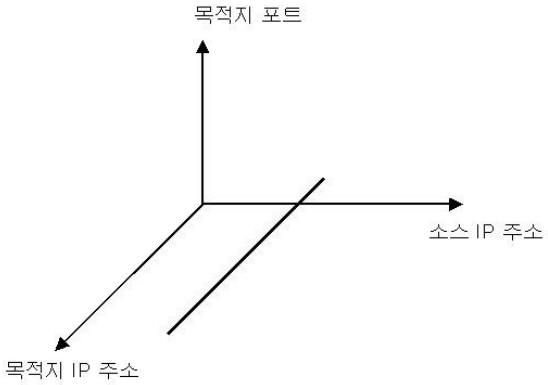
도면3


시작
200
네트워크 트래픽 수집 및 분석
300
현재 트래픽 상황에
대한 정보 생성
400
소정 시간 경과?
아니요
예
현재 트래픽 상황에 대한
정보를 좌표 점 데이터로 표시
500
좌표 점 데이터로부터
공격 특징을 판정
600
공격 특징에 따라
비정상적인 상황 대응
700
B
끝

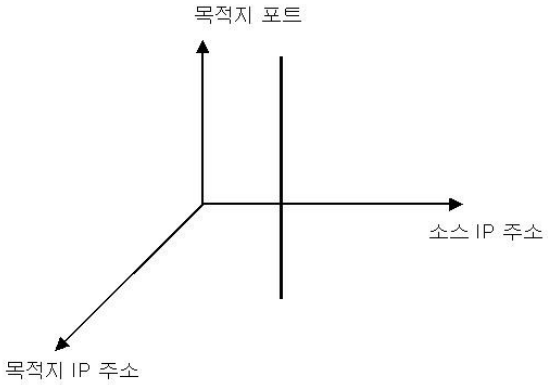
도면4


500
601
목적지 IP 주소 가변?
예
아니오
603
호스트 스캐닝
공격으로 판정
605
목적지 포트만 가변?
아니오
예
607
포트 스캐닝
공격으로 판정
609
소스 IP 주소만 가변?
예
아니오
611
특정 목적지의 특정포트로의
서비스 거부 공격으로 판정
613
목적지 IP 주소만 고정?
아니오
예
615
특정 목적지의 랜덤 포트로의
서비스 거부 공격으로 판정
700
B

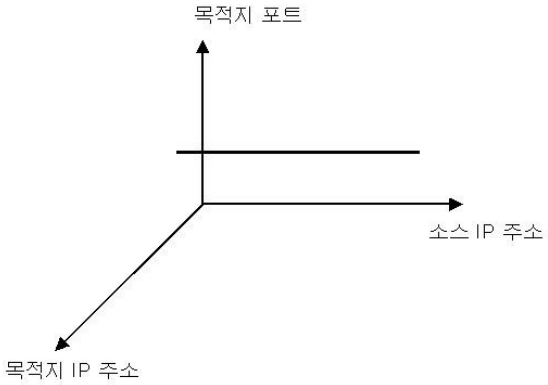
도면5



도면6



도면7



도면8