(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 11/30 (2006.01)

(45) 공고일자 2007년08월02일
(11) 등록번호 10-0745613
(24) 등록일자 2007년07월27일

(21) 출원번호 10-2006-0025307
(22) 출원일자 2006년03월20일
심사청구일자 2006년03월20일

(65) 공개번호
(43) 공개일자

(73) 특허권자 고려대학교 산학협력단

(72) 발명자 이희조

박현도

(74) 대리인 유미특허법인

(56) 선행기술조사문헌
KR 1020030087583 A
KR 1020030063949 A

심사관 : 김근모

전체 청구항 수 : 총 8 항

(54) 네트워크 감시를 수행하는 장치 및 프로그램이 저장된 기록매체

(57) 요약

네트워크가 웜에 감염되어 있는지를 판단하는 네트워크 감시 장치 및 프로그램이 저장된 기록 매체에 관한 것이다.

네트워크 감시 장치는 네트워크로부터 트래픽을 수집하여 그 특성을 행렬에 나타내고 행렬에서 정상 트래픽 특성을 제거한 후 행렬의 랭크값을 계산한다.

네트워크 감시 장치는 유입 트래픽 및 유출 트래픽에 대해서 랭크값 계산을 통해 네트워크의 상태를 구체적으로 파악할 수 있고, 서브네트워크 별로 트래픽 특성을 행렬에 나타내어 랭크값을 계산함으로써 웜에 감염된 서브네트워크를 용이하게 파악할 수 있다.

대표도

도 1

특허청구의 범위

청구항 1.

네트워크를 감시하는 장치에 있어서,

상기 네트워크로 유입되는 유입 트래픽 및 상기 네트워크로부터 유출되는 유출 트래픽을 수집하는 트래픽 수집부;

제1 시간 영역에서 상기 유입 트래픽의 특성을 제1 유입 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유입 트래픽의 특성을 제2 유입 트래픽 행렬에 나타내는 유입 트래픽 행렬 생성부;

상기 제1 시간 영역에서 상기 유출 트래픽의 특성을 제1 유출 트래픽 행렬에 나타내고 상기 제2 시간 영역에서 상기 유출 트래픽의 특성을 제2 유출 트래픽 행렬에 나타내는 유출 트래픽 행렬 생성부;

상기 제1 유입 트래픽 행렬 및 상기 제2 유입 트래픽 행렬을 XOR하여 정상 유입 트래픽 소거 행렬을 생성하고 상기 제1 유출 트래픽 행렬 및 상기 제2 유출 트래픽 행렬을 XOR하여 정상 유출 트래픽 소거 행렬을 생성하는 정상 트래픽 소거부;

상기 정상 유입 트래픽 소거 행렬의 랭크값인 유입 랭크값 및 상기 정상 유출 트래픽 소거 행렬의 랭크값인 유출 랭크값을 계산하는 랭크값 계산부;

상기 유입 랭크값이 소정의 값보다 크면 상기 네트워크가 웜으로부터 공격받고 있다고 판단하고 상기 유출 랭크값이 소정의 값보다 크면 상기 네트워크가 웜에 감염되어 있다고 판단하는 네트워크 상태 판단부를 포함하는 장치.

청구항 2.

제1항에 있어서,

상기 유입 트래픽 행렬 생성부는 상기 유입 트래픽의 IP(Internet Protocol) 주소를 상기 제1 유입 트래픽 행렬 및 상기 제2 유입 트래픽 행렬에 나타내고,

상기 유출 트래픽 행렬 생성부는 상기 유출 트래픽의 IP(Internet Protocol) 주소를 상기 제1 유출 트래픽 행렬 및 상기 제2 유출 트래픽 행렬에 나타내는 장치.

청구항 3.

제1항 또는 제2항에 있어서,

상기 네트워크 상태 판단부는

상기 유입 랭크값이 제1 값보다 작고 상기 유출 랭크값이 제2 값보다 작으면 상기 네트워크가 안정하다고 판단하고,

상기 유입 랭크값이 제3 값보다 크고 상기 유출 랭크값이 상기 제2 값보다 작으면 상기 네트워크가 웜으로부터 공격받고 있다고 판단하고,

상기 유입 랭크값이 상기 제1 값보다 작고 상기 유출 랭크값이 제4 값보다 크면 상기 네트워크가 웜에 감염되어 있다고 판단하며,

상기 유입 랭크값이 상기 제3 값보다 크고 상기 유출 랭크값이 제4 값보다 크면 상기 네트워크가 웜으로부터 공격받고 있으며 웜에 감염되어 있다고 판단하는 장치.

청구항 4.

네트워크를 감시하는 프로그램이 저장된 기록 매체에 있어서,

네트워크를 감시하는 장치에 있어서,

상기 네트워크로 유입되는 유입 트래픽 및 상기 네트워크로부터 유출되는 유출 트래픽을 수집하는 기능;

제1 시간 영역에서 상기 유입 트래픽의 특성을 제1 유입 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유입 트래픽의 특성을 제2 유입 트래픽 행렬에 나타내는 기능;

상기 제1 시간 영역에서 상기 유출 트래픽의 특성을 제1 유출 트래픽 행렬에 나타내고 상기 제2 시간 영역에서 상기 유출 트래픽의 특성을 제2 유출 트래픽 행렬에 나타내는 기능;

상기 제1 유입 트래픽 행렬 및 상기 제2 유입 트래픽 행렬을 XOR하여 정상 유입 트래픽 소거 행렬을 생성하고 상기 제1 유출 트래픽 행렬 및 상기 제2 유출 트래픽 행렬을 XOR하여 정상 유출 트래픽 소거 행렬을 생성하는 기능;

상기 정상 유입 트래픽 소거 행렬의 랭크값인 유입 랭크값 및 상기 정상 유출 트래픽 소거 행렬의 랭크값인 유출 랭크값을 계산하는 기능;

상기 유입 랭크값이 제1 값보다 크고 상기 유출 랭크값이 제2 값보다 작으면 상기 네트워크가 웜으로부터 공격받고 있다고 판단하는 기능; 및

상기 유입 랭크값이 제3 값보다 작고 상기 유출 랭크값이 제4 값보다 크면 상기 네트워크가 웜에 감염되어 있다고 판단하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 5.

제4항에 있어서,

상기 유입 랭크값이 상기 제3 값보다 작고 상기 유출 랭크값이 상기 제2 값보다 작으면 상기 네트워크가 안정하다고 판단하는 기능; 및

상기 유입 랭크값이 상기 제1 값보다 크고 상기 유출 랭크값이 상기 제4 값보다 크면 상기 네트워크가 웜으로부터 공격받고 있으며 웜에 감염되어 있다고 판단하는 기능을 더 포함하는 프로그램이 저장됨 기록 매체.

청구항 6.

제4항 또는 제5항에 있어서,

상기 유입 트래픽의 특성 및 상기 유출 트래픽의 특성은 IP(Internet Protocol) 주소인 프로그램이 저장된 기록 매체.

청구항 7.

복수의 서브네트워크를 포함하는 네트워크를 감시하는 장치에 있어서,

상기 네트워크의 트래픽을 수집하는 트래픽 수집부;

제1 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제1 시간의 트래픽 행렬들에 나타내고 제2 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제2 시간의 트래픽 행렬들에 나타내는 트래픽 행렬 생성부;

상기 서브네트워크 별로 상기 제1 시간의 트래픽 행렬들 및 상기 제2 시간의 트래픽 행렬들을 XOR하여 복수의 정상 트래픽 소거 행렬을 생성하는 정상 트래픽 소거부;

상기 서브네트워크 별로 상기 복수의 정상 트래픽 소거 행렬의 랭크값을 계산하는 랭크값 계산부; 및

상기 복수의 랭크값 중 소정의 값보다 큰 랭크값이 존재하는 지 검색하여 상기 소정의 값보다 큰 랭크값에 해당하는 서브네트워크가 웜에 감염되어 있거나 웜에 의해 공격받고 있다고 판단하는 감염 서브네트워크 판단부를 포함하는 장치.

청구항 8.

복수의 서브네트워크를 포함하는 네트워크를 감시하는 프로그램이 저장된 기록 매체에 있어서,

상기 네트워크의 트래픽을 수집하는 기능;

제1 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제1 시간의 트래픽 행렬들에 나타내는 기능;

제2 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제2 시간의 트래픽 행렬들에 나타내는 기능;

상기 서브네트워크 별로 상기 제1 시간의 트래픽 행렬들 및 상기 제2 시간의 트래픽 행렬들을 XOR하여 복수의 정상 트래픽 소거 행렬을 생성하는 기능;

상기 서브네트워크 별로 상기 복수의 정상 트래픽 소거 행렬의 랭크값을 계산하는 기능; 및

상기 복수의 랭크값 중 소정의 값보다 큰 랭크값이 존재하는 지 검색하여 상기 소정의 값보다 큰 랭크값에 해당하는 서브네트워크가 웜에 감염되어 있거나 웜에 의해 공격 받고 있다고 판단하는 기능을 포함하는 프로그램이 저장된 기록 매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 감시를 수행하는 장치 및 프로그램이 저장된 기록 매체에 관한 것이다. 특히 본 발명은 네트워크가 웜에 감염되어 있는지를 판단하는 장치 및 프로그램이 저장된 기록 매체에 관한 것이다.

1988년 Morris 웜이 처음으로 출현한 이래로 인터넷에서의 웜에 의한 피해사고는 끊임없이 증가하고 있다. Code Red와 Nimda 웜은 인터넷 상의 수십만 대의 컴퓨터를 감염시켰으며, 공공분야에서부터 개인의 시스템까지 수백만 달러의 피해를 가져다 주었다. 이러한 인터넷 웜은 자기 자신을 복제하여 네트워크 상의 컴퓨터들을 감염시키는 독립된 프로그램이다. 웜은 인터넷 상에 있는 수많은 컴퓨터들을 감염시키기 위하여, 네트워크 조사, 취약점 검사, 자가 복제 등을 자동으로 수행한다. 현재까지 보고된 웜 중 가장 빠른 웜으로 기록되어있는 SQL_Overflow 웜은 10여분 만에 전 세계의 취약한 서버의 90%를 감염시켰으며, 감염된 서버는 매 8.5초마다 2배의 수치로 증가하였다. 이러한 수치로 볼 때 SQL_Overflow 웜은 이전의 Code Red 웜에 감염된 서버가 매 37분마다 2배로 늘어났던 것에 비해 엄청난 속도로 컴퓨터들을 감염시켰다는 것을 쉽게 알 수 있다. 이렇게 빠른 전염 속도로 파급되는 인터넷 웜에 대응하기 위해서는 웜이 네트워크의 컴퓨터들을 감염시키는 초기 단계를 탐지하여 웜의 확산을 예방하는 것이 제일 중요하다.

웜을 탐지하는 기법들 중에는 크게 두 가지로 구분할 수 있다. 트래픽의 임계치를 이용하는 방법과 웜의 행동 양상을 이용하여 탐지하는 방법들이 있다. 트래픽의 임계치를 사용하는 방법들은 정상적인 트래픽과 비 정상적인 트래픽의 구분을 명확하게 할 수 없기 때문에 잘못된 탐지를 하는 비율이 높다. 한편, 신종 웜의 출현 주기가 짧아지고 종류도 다양해짐에 따라서 기존의 웜의 행동 양상을 이용한 웜의 탐지는 네트워크를 보호하는 대에 있어서 더 이상 충분하지 않다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 네트워크가 웜에 감염되어 있는지를 판단하는 장치 및 프로그램이 저장된 기록 매체를 제공하는 것이다.

발명의 구성

본 발명의 한 특징에 따른 네트워크 감시 장치는 트래픽 수집부, 유입 트래픽 행렬 생성부, 유출 트래픽 행렬 생성부, 정상 트래픽 소거부, 랭크값 계산부 및 네트워크 상태 판단부를 포함한다. 이때 트래픽 수집부는 네트워크로 유입되는 유입 트래픽 및 상기 네트워크로부터 유출되는 유출 트래픽을 수집한다. 그리고 유입 트래픽 행렬 생성부는 제1 시간 영역에서 상기 유입 트래픽의 특성을 제1 유입 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유입 트래픽의 특성을 제2 유입 트래픽 행렬에 나타내고, 유출 트래픽 행렬 생성부는 제1 시간 영역에서 상기 유출 트래픽의 특성을 제1 유출 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유출 트래픽의 특성을 제2 유출 트래픽 행렬에 나타낸다. 정상 트래픽 소거부는 상기 제1 유입 트래픽 행렬 및 상기 제2 유입 트래픽 행렬을 XOR하여 정상 유입 트래픽 소거 행렬을 생성하고 상기 제1 유출 트래픽 행렬 및 상기 제2 유출 트래픽 행렬을 XOR하여 정상 유출 트래픽 소거 행렬을 생성하고, 랭크값 계산부는 상기 정상 유입 트래픽 소거 행렬의 랭크값인 유입 랭크값 및 상기 정상 유출 트래픽 소거 행렬의 랭크값인 유출 랭크값을 계산하며, 네트워크 상태 판단부는 상기 유입 랭크값이 소정의 값보다 크면 상기 네트워크가 웜으로부터 공격받고 있다고 판단하고 상기 유출 랭크값이 소정의 값보다 크면 상기 네트워크가 웜에 감염되어 있다고 판단한다.

본 발명의 다른 특징에 따른 네트워크 감시 장치는 복수의 서브네트워크를 포함하는 네트워크를 감시하는 장치로서, 상기 네트워크의 트래픽을 수집하는 트래픽 수집부와, 제1 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제1 시간의 트래픽 행렬들에 나타내고 제2 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제2 시간의 트래픽 행렬들에 나타내는 트래픽 행렬 생성부와, 상기 서브네트워크 별로 상기 제1 시간의 트래픽 행렬들 및 상기 제2 시간의 트래픽 행렬들을 XOR하여 복수의 정상 트래픽 소거 행렬을 생성하는 정상 트래픽 소거부와, 상기 서브네트워크 별로 상기 복수의 정상 트래픽 소거 행렬의 랭크값을 계산하는 랭크값 계산부 및 상기 복수의 랭크값 중 소정의 값보다 큰 랭크값이 존재하는 지 검색하여 상기 소정의 값보다 큰 랭크값에 해당하는 서브네트워크가 웜에 감염되어 있거나 웜에 의해 공격받고 있다고 판단하는 감염 서브네트워크 판단부를 포함한다.

본 발명의 한 특징에 따른 프로그램이 저장된 기록 매체는 네트워크를 감시하는 프로그램이 저장된 기록 매체로서, 상기 네트워크로 유입되는 유입 트래픽 및 상기 네트워크로부터 유출되는 유출 트래픽을 수집하는 기능과, 제1 시간 영역에서 상기 유입 트래픽의 특성을 제1 유입 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유입 트래픽의 특성을 제2 유입 트래픽 행렬에 나타내는 기능과, 제1 시간 영역에서 상기 유출 트래픽의 특성을 제1 유출 트래픽 행렬에 나타내고 제2 시간 영역에서 상기 유출 트래픽의 특성을 제2 유출 트래픽 행렬에 나타내는 기능과, 상기 제1 유입 트래픽 행렬 및 상기 제2 유입 트래픽 행렬을 XOR하여 정상 유입 트래픽 소거 행렬을 생성하고 상기 제1 유출 트래픽 행렬 및 상기 제2 유출 트래픽 행렬을 XOR하여 정상 유출 트래픽 소거 행렬을 생성하는 기능과, 상기 정상 유입 트래픽 소거 행렬의 랭크값인 유입 랭크값 및 상기 정상 유출 트래픽 소거 행렬의 랭크값인 유출 랭크값을 계산하는 기능과, 상기 유입 랭크값이 제1 값보다 크고 상기 유출 랭크값이 제2 값보다 작으면 상기 네트워크가 웜으로부터 공격받고 있다고 판단하는 기능, 및 상기 유입 랭크값이 제3 값보다 작고 상기 유출 랭크값이 제4 값보다 크면 상기 네트워크가 웜에 감염되어 있다고 판단하는 기능을 포함한다.

본 발명의 다른 특징에 따른 프로그램이 저장된 기록 매체는 복수의 서브네트워크를 포함하는 네트워크를 감시하는 프로그램이 저장된 기록 매체로서, 상기 네트워크의 트래픽을 수집하는 기능과, 제1 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제1 시간의 트래픽 행렬들에 나타내는 기능과, 제2 시간 영역에서 상기 트래픽의 IP 주소를 상기 서브네트워크 별로 제2 시간의 트래픽 행렬들에 나타내는 기능과, 상기 서브네트워크 별로 상기 제1 시간의 트래픽 행렬들 및 상기 제2 시간의 트래픽 행렬들을 XOR하여 복수의 정상 트래픽 소거 행렬을 생성하는 기능과, 상기 서브네트워크 별로 상기 복수의 정상 트래픽 소거 행렬의 랭크값을 계산하는 기능, 및 상기 복수의 랭크값 중 소정의 값보다 큰 랭크값이 존재하는 지 검색하여 상기 소정의 값보다 큰 랭크값에 해당하는 서브네트워크가 웜에 감염되어 있거나 웜에 의해 공격받고 있다고 판단하는 기능을 포함한다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

웜은 랜덤하게 IP 주소를 생성하여 감염 대상을 결정한다. 따라서 웜에 감염되어 있거나 웜에 의해 공격받고 있는 네트워크 상에는 랜덤한 IP를 가진 트래픽이 많이 존재하게 된다. 본 발명의 실시예에 따른 웜 탐지 장치는 이와 같은 웜의 특징을 활용한다.

다음은 도 1 내지 도 7를 참고하여 본 발명의 다양한 실시예에 따른 웜 탐지 장치에 대하여 설명한다.

도 1은 본 발명의 제1 실시예에 따른 네트워크 감시 장치(100)를 도시한 블록도이다.

도 1에 도시된 바와 같이 본 발명의 제1 실시예에 따른 네트워크 감시 장치(100)는 제1 네트워크(10)와 연동하며, 트래픽 수집부(110), 트래픽 행렬 생성부(120), 정상 트래픽 소거부(130), 랭크값 계산부(140), 웜 존재 판단부(150)를 포함한다.

트래픽 수집부(110)는 제1 네트워크(10) 상의 트래픽을 수집한다.

트래픽 행렬 생성부(120)는 트래픽 수집부(110)가 수집한 트래픽의 특성을 행렬로 표현한다. 트래픽 행렬 생성부(120)는 트래픽에 포함되어 있는 IP(Internet Protocol) 주소로 행렬을 생성할 수도 있다. IP 주소를 통한 행렬 생성 방법에 대하여 도 2를 참고하여 설명한다.

도 2는 본 발명의 실시예에 따라 IP 주소를 통해 생성한 트래픽 행렬을 도시한 도면이다.

본 발명의 실시를 위해서 반드시 IPv4를 사용할 필요는 없지만, 본 발명의 실시예를 설명하기 위하여 IPv4를 사용하겠다. IPv4에서 IP 주소는 32비트로 구성되고, 보통 8비트씩 나뉘어 표현되는데, 설명의 편의를 위하여 IP 주소의 각 8비트를 IP_1, IP_2, IP_3, IP_4라고 하도록 한다. 이때 IP_1은 IP 주소의 상위 8비트이고, IP_4는 IP 주소의 하위 8비트이다.

트래픽 행렬은 64개의 행과 64개의 열로 되어 있으며, 트래픽 행렬의 각 원소(element)는 1비트의 크기를 갖는다. 트래픽 행렬은 4*4의 크기의 부분 행렬 256개로 표현될 수 있다. 각 부분 행렬의 (1, 1)의 위치는 트래픽 행렬의 (i, j)가 되는데, (i, j)는 다음의 수학식 1에 의해 결정된다.

수학식 1

$$i = (IP_4 / 16) * 4$$

$$j = (IP_4 \bmod 16) * 4$$

여기서 수식 $(IP_4 \bmod 16)$는 IP_4를 16으로 나눈 나머지를 의미한다. 한편, 트래픽 행렬의 (i, j)에 위치하는 부분 행렬을 $M_{i,j}$라고 표시하도록 한다.

부분 행렬($M_{i,j}$)의 k번째 열인 m_k는 다음 수학식 2에 의해 결정된다.

수학식 2

$$m_1 = \text{first 4bit of } IP_3$$

$$m_2 = \text{first 4bit of } IP_3$$

$$m_3 = \text{first 4bit of } IP_4$$

$$m_4 = \text{first 4bit of } IP_4$$

다시 도 1에 대해 설명한다.

트래픽 행렬 생성부(120)는 도 2에 도시된 방법에 따라 트래픽 수집부(110)가 수집하는 t-1초에서 t초 사이의 트래픽을 트래픽 행렬 M(t)에 표시한다. t-1초에서 t초 사이에서 트래픽 행렬의 (i, j)에 위치될 트래픽이 2회 이상 수집된다면, 트래픽 행렬 생성부(120)는 나중에 수집된 트래픽으로 덮어쓰기를 반복한다. 한편 트래픽 행렬 생성부(120)는 t-2초에서 t-1초 사이의 트래픽을 트래픽 행렬 M(t-1)에 표시한다.

정상 트래픽 소거부(130)는 트래픽 행렬 생성부(120)가 생성한 트래픽 행렬에서 정상 트래픽 특성을 소거한다. 정상 트래픽 소거부(130)는 트래픽 행렬 생성부(120)가 생성한 두 개의 행렬인 M(t-1)와 M(t)에 대해 다음 수학식 3에서 보여주는 것과 같이 Exclusive OR(XOR)를 수행하여 M'(t)를 생성함으로써 용이하게 정상 트래픽 특성을 소거할 수 있다.

수학식 3

$$M'(t) = M(t-1) \oplus M(t)$$

정상 트래픽의 IP 주소는 t-2초에서 t-1초 사이에서와 t-1초에서 t초 사이에서 변하지 않을 가능성이 높으므로 트래픽 행렬 생성부(120)가 M(t-1)와 M(t)에 대해 Exclusive OR를 수행하여 M'(t)를 생성하는 경우 M'(t)에서는 정상 트래픽이 대부분 제거된다. 이하에서는 M'(t)를 정상 트래픽 소거 행렬이라 부르도록 한다.

랭크값 계산부(140)는 정상 트래픽 소거 행렬 M'(t)의 랜덤의 정도를 계산하기 위하여 랭크값(rank)을 계산한다.

랜덤한 m*n 이진 행렬의 랭크값은 다음 수학식 4에 따르는 확률을 가지고 r=1, 2, ..., min(m,n)을 갖는다.

수학식 4

$$2^{r<n+m-r>-nm}\prod_{i=0}^{r-1}\frac{(1-2^{i-n})(1-2^{i-m})}{(1-2^{i-r})}$$

수학식 4를 그래프로 표시한 도면이 도 3과 같다.

도 3은 랜덤 행렬의 랭크값의 확률 분포를 도시한 그래프이다.

수학식 4의 결과와 도 3에 의하면 랜덤한 64*64 이진 행렬은 99.999%의 확률로 60 이상의 랭크값을 갖는다.

이와 같은 결과에 따라, 웜 존재 판단부(150)는 정상 트래픽 소거 행렬 M'(t)의 랭크값이 60이상인지 판단한다. 만약 정상 트래픽 소거 행렬 M'(t)의 랭크값이 60 이상이면, 정상 트래픽 소거 행렬 M'(t)은 99.999%의 확률로 랜덤한 이진 행렬이므로 제1 네트워크(10) 상에 웜이 존재할 확률이 매우 높아진다. 따라서 이 경우 웜 존재 판단부(150)는 제1 네트워크(10)상에 웜이 존재한다고 판단할 수 있다.

다음은 도 4를 참고하여 본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)에 대해 설명한다.

도 4는 본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)를 도시한 블록도이다.

도 4에 도시된 바와 같이 본 발명의 제2 실시예에 따른 네트워크 감시 장치(200)는 제2 네트워크(20)과 제3 네트워크(30) 사이에 존재하는 게이트웨이(40)와 연결되어 제3 네트워크(30)의 상태를 감시하며, 트래픽 수집부(210), 트래픽 행렬 생성부(220), 정상 트래픽 소거부(230), 랭크값 계산부(240), 네트워크 상태 판단부(250)를 포함한다. 네트워크 감시 장치(200)는 게이트웨이(40) 대신에 방화벽 등과 연결될 수도 있다.

트래픽 수집부(220)는 유입 트래픽 수집부(211), 유출 트래픽 수집부(212)를 포함한다. 유입 트래픽 수집부(211)는 제2 네트워크(20)에서 제3 네트워크(30)로 유입되는 유입 트래픽을 수집하고, 유출 트래픽 수집부(212)는 제3 네트워크(30)에서 제2 네트워크(20)로 나가는 트래픽인 유출 트래픽을 수집한다.

트래픽 행렬 생성부(220)는 유입 트래픽 행렬 생성부(221), 유출 트래픽 행렬 생성부(222)를 포함한다. 유입 트래픽 행렬 생성부(221)는 t-1초에서 t초 사이의 유입 트래픽으로 유입 트래픽 행렬 $M_I(t)$를 생성하고, t-2초에서 t-1초 사이의 유입 트래픽으로 유입 트래픽 행렬 $M_I(t-1)$를 생성한다. 유출 트래픽 행렬 생성부(222)는 t-1초에서 t초 사이의 유출 트래픽으로 유출 트래픽 행렬 $M_O(t)$를 생성하고, t-2초에서 t-1초 사이의 유출 트래픽으로 유출 트래픽 행렬 $M_O(t-1)$를 생성한다.

정상 트래픽 소거부(230)는 정상 유입 트래픽 소거부(231) 및 정상 유출 트래픽 소거부(232)를 포함한다. 정상 유입 트래픽 소거부(231)는 $M_I(t-1)$와 $M_I(t)$에 대하여 XOR을 수행하여 정상적인 유입 트래픽이 소거된 $M_I'(t)$를 생성하고, 정상 유출 트래픽 소거부(232)는 $M_O(t-1)$와 $M_O(t)$에 대하여 XOR을 수행하여 정상적인 유출 트래픽이 소거된 $M_O'(t)$를 생성한다. 이를 수학식으로 나타내면 수학식 5와 같다.

수학식 5

$$M_I'(t) = M_I(t-1) \oplus M_I(t)$$
$$M_O'(t) = M_O(t-1) \oplus M_O(t)$$

랭크값 계산부(240)는 유입 랭크값 계산부(241) 및 유출 랭크값 계산부(242)를 포함한다. 유입 랭크값 계산부(241)는 $M_I'(t)$의 랭크값인 유입 랭크값(R_I)을 계산하고, 유출 랭크값 계산부(242)는 $M_O'(t)$의 랭크값인 유출 랭크값(R_O)을 계산한다. 이를 수학식으로 나타내면 수학식 6과 같다.

수학식 6

$$R_I = rank(M_I'(t))$$
$$R_O = rank(M_O'(t))$$

네트워크 상태 판단부(250)는 유입 랭크값(R_I) 및 유출 랭크값(R_O)의 값에 따라 네트워크의 상태를 파악한다. 네트워크 상태 판단부(250)는 유입 랭크값(R_I) 및 유출 랭크값(R_O)이 모두 소정의 값(예를 들어, 20)보다 낮은 경우라면, 제3 네트워크(30)가 웜에 영향을 받고 있지 않는다고 판단한다. 또한 네트워크 상태 판단부(250)는 유입 랭크값(R_I)이 소정의 값(예를 들어, 60)보다 크고, 유출 랭크값(R_O)이 20보다 낮으면 제3 네트워크(30)가 웜에 의해 공격을 받고 있다고 판단한다. 그리고 네트워크 상태 판단부(250)는 유입 랭크값(R_I)이 20보다 작고, 유출 랭크값(R_O)이 60보다 크면 제3 네트워크(30)가 웜에 감염되어 있다고 판단한다. 한편, 네트워크 상태 판단부(250)는 유입 랭크값(R_I) 및 유출 랭크값(R_O)이 60보다 크면 제3 네트워크(30)가 웜에 감염되어 있으며 또한 제2 네트워크(20)로부터 웜에 의한 공격을 받고 있다고 판단한다. 네트워크 상태 판단부(250)의 네트워크 상태 판단 기준을 도 5에 도시하였다.

도 5는 본 발명의 실시예에 따른 네트워크 상태 판단 기준을 나타낸다. 도 5에서 $R_{I,min}$과 $R_{O,min}$은 각각 유입 트래픽 및 유출 트래픽에 웜에 의한 트래픽이 섞여 있지 않음을 나타내는 행렬 $M_I'(t)$와 행렬 $M_O'(t)$의 랭크값이고, $R_{I,max}$과 $R_{O,max}$는 각각 유입 트래픽 및 유출 트래픽에 웜에 의한 트래픽이 섞여 있음을 나타내는 행렬 $M_I'(t)$와 행렬 $M_O'(t)$의 랭크값이다.

도 6은 본 발명의 제3 실시예에 따른 네트워크 감시 장치(300)를 도시한 블록도이다.

도 6에 도시된 바와 같이 본 발명의 제3 실시예에 따른 네트워크 감시 장치(300)는 제4 네트워크(50)의 웜의 활동을 감시하며, 트래픽 수집부(310), 트래픽 행렬 생성부(320), 정상 트래픽 소거부(330), 랭크값 계산부(340), 감염 서브네트워크 판단부(350)을 포함한다.

제4 네트워크(50)는 복수의 서브네트워크(subnetwork)(51)를 포함한다. 예를 들어 제4 네트워크(50)는 /16 네트워크일 수 있고, 서브네트워크(51)는 /24 네트워크일 수 있다. 여기서 /16 네트워크는 네트워크의 주소가 32비트의 IP 주소 중 상위 16비트에 의해 결정되는 네트워크이고, /24 네트워크는 네트워크의 주소가 32비트의 IP 주소 중 상위 24비트에 의해 결정되는 네트워크이다. 따라서 /16 네트워크는 2^{16}개의 네트워크 노드를 포함할 수도 있고, 또는 2^8개의 /24 네트워크를 포함할 수 있다. /24 네트워크는 2^8개의 네트워크 노드를 포함할 수 있다.

트래픽 수집부(310)는 제4 네트워크(50) 상의 트래픽을 수집한다.

트래픽 행렬 생성부(320)는 제1 시간(예를 들어 t-2초에서 t-1초 사이의 시간) 및 제2 시간(예를 들어 t-1초에서 t초 사이의 시간)에서 서브네트워크(51) 별로 각각 트래픽 행렬을 생성한다. 제4 네트워크(50)가 /16 네트워크이고 서브네트워크(51)가 /24 네트워크라면 제4 네트워크(50)는 256개의 서브네트워크(51)를 포함하므로, 트래픽 행렬 생성부(320)는 제1 시간에서 256개의 트래픽 행렬을 생성하고, 제2 시간에서 256개의 트래픽 행렬을 생성한다.

정상 트래픽 소거부(330)는 트래킥 행렬 생성부(320)가 생성한 제1 시간에서의 트래픽 행렬 및 제2 시간에서의 트래픽 행렬에 대해 XOR을 수행하여 서브네트워크(51) 별로 정상 트래픽 소거 행렬을 생성한다. 즉, 제4 네트워크(50)가 /16 네트워크이고 서브네트워크(51)가 /24 네트워크인 경우 정상 트래픽 소거부(330)는 256개의 정상 트래픽 소거 행렬을 생성한다.

랭크값 계산부(340)는 서브네트워크(51) 별로 생성된 정상 트래픽 소거 행렬의 랭크값을 계산한다.

감염 서브네트워크 판단부(350)는 랭크값 계산부(340)에서 계산된 복수개의 랭크값 중에서 소정의 값(예를 들어 60)을 초과하는 랭크값이 있는 경우 해당 서브네트워크(51)가 웜에 감염되어 있거나 웜에 의해 공격받고 있다고 판단한다.

도 7은 시간의 경과에 따라 서브네트워크 별로 네트워크의 랭크값의 추이를 나타낸 그래프이다.

도 7에 따르면, 48번째의 서브네트워크가 웜에 감염되어 있음을 알 수 있다.

이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

본 발명에 따르면 네트워크 감시 장치는 유입 트래픽의 특성이 반영된 행렬의 랭크값과 유출 트래픽의 특성이 반영된 행렬의 랭크값을 이용하여 네트워크의 구체적인 상태를 파악할 수 있다. 특히 유입 트래픽의 특성이 반영된 행렬의 랭크값이 정상 범위를 초과하는 경우 네트워크 감시 장치는 네트워크가 웜으로부터 공격받고 있음을 조기에 발견하여 웜에 대해 대응할 수 있따.

또한 본 발명에 따르면 네트워크 감시 장치는 서브네트워크별로 트래픽의 IP 주소가 반영된 행렬의 랭크값을 이용하여 감염된 서브네트워크를 파악할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 제1 실시예에 따른 네트워크 감시 장치를 도시한 블록도이다.

도 2는 본 발명의 실시예에 따라 IP 주소를 통해 생성한 트래픽 행렬을 도시한 도면이다.

도 3은 랜덤 행렬의 랭크값의 확률 분포를 도시한 그래프이다.

도 4는 본 발명의 제2 실시예에 따른 네트워크 감시 장치를 도시한 블록도이다.

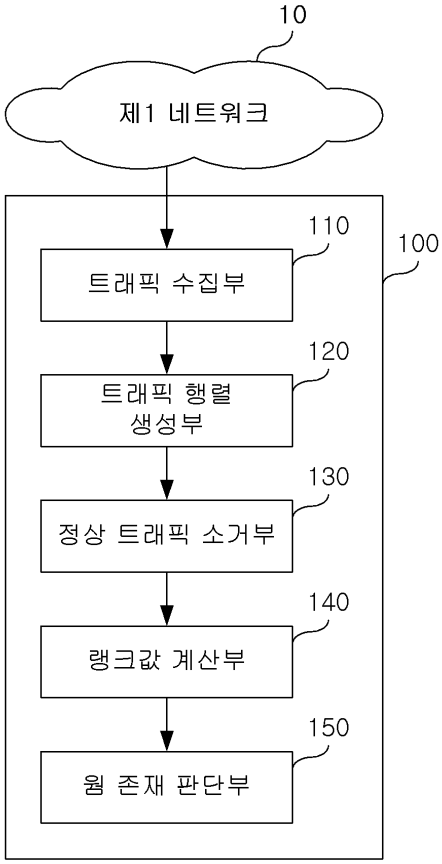
도 5는 본 발명의 실시예에 따른 네트워크 상태 판단 기준을 나타낸다.

도 6은 본 발명의 제3 실시예에 따른 네트워크 감시 장치를 도시한 블록도이다.

도 7은 시간의 경과에 따라 서브네트워크 별로 네트워크의 랭크값의 추이를 나타낸 그래프이다.

도면

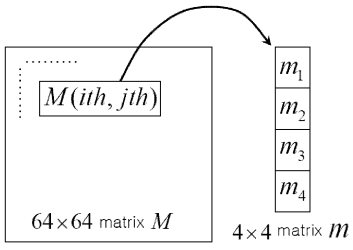
도면1



도면2

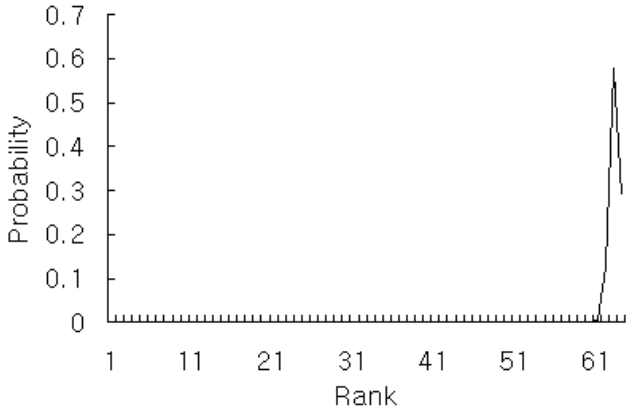
$$IP\ 주소 = IP_1.IP_2.IP_3.IP_4$$

$$i = (IP_4 / 16) \times 4$$
$$j = (IP_4 (\mathrm{mod} 16)) \times 4$$

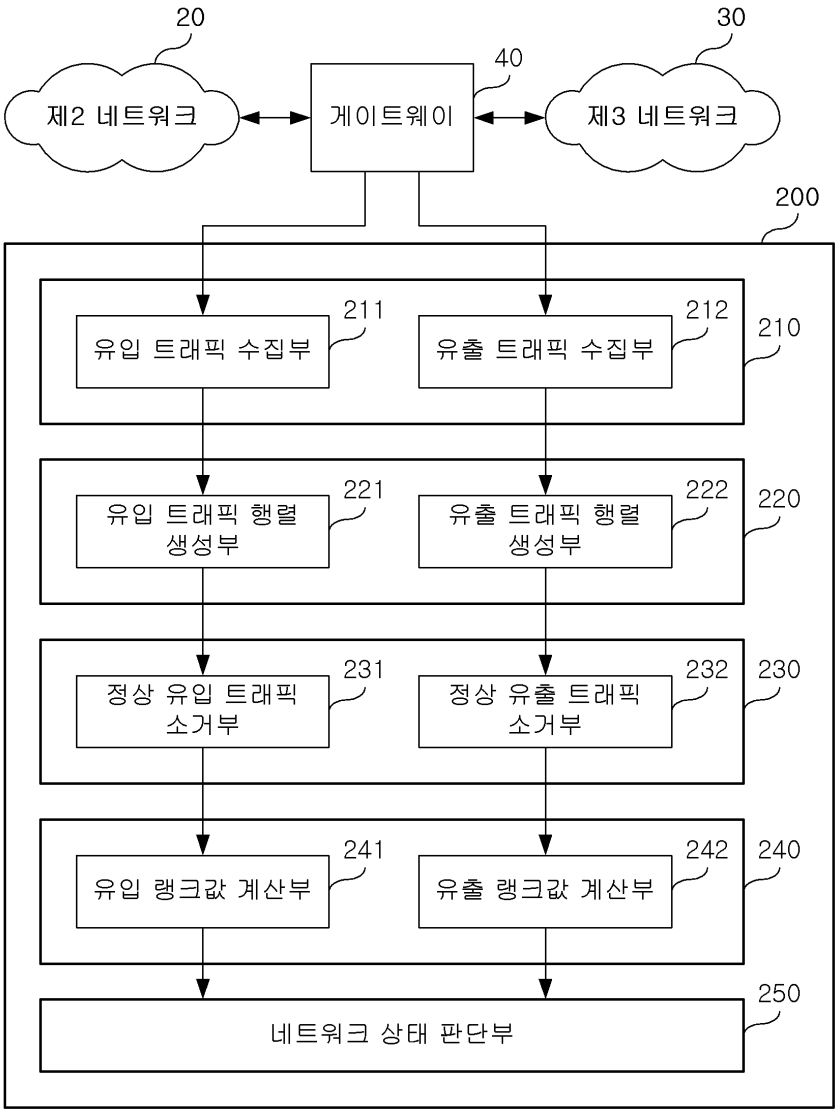


$$m_1 = first\ 4bit\ of\ IP_3$$
$$m_2 = last\ 4bit\ of\ IP_3$$
$$m_3 = first\ 4bit\ of\ IP_4$$
$$m_4 = last\ 4bit\ of\ IP_4$$

도면3


0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Probability
1
11
21
31
41
51
61
Rank

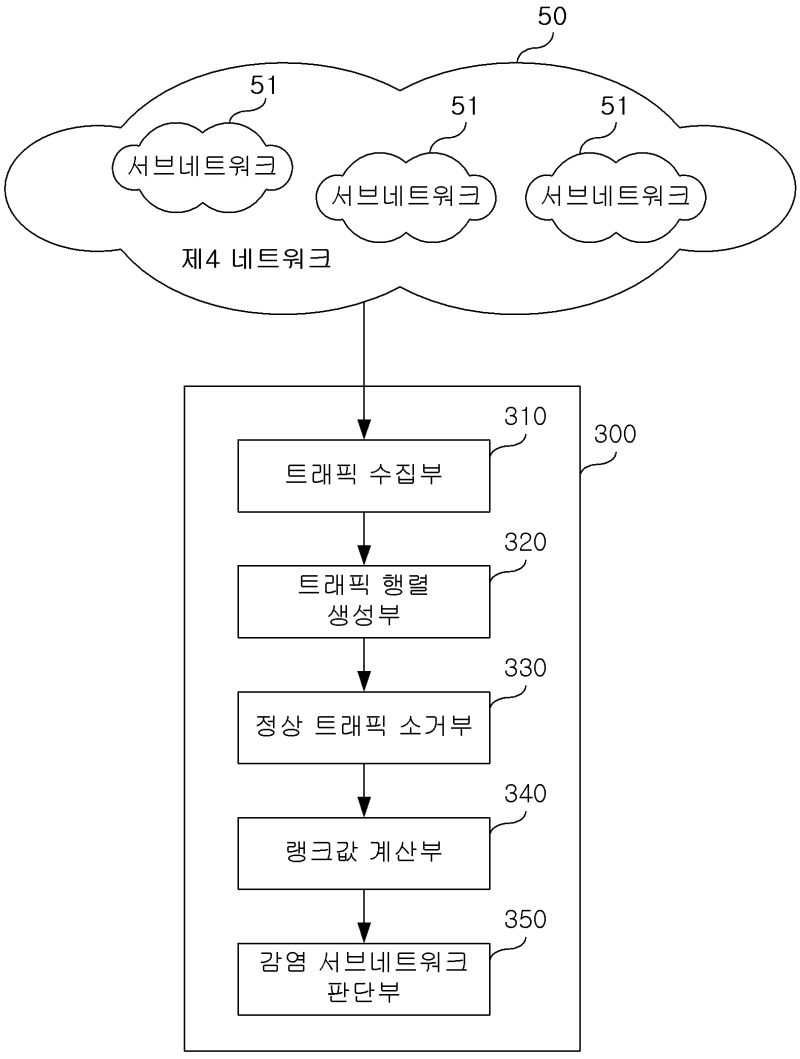
도면4


20
30
40
제2 네트워크
게이트웨이
제3 네트워크
200
211
212
210
유입 트래픽 수집부
유출 트래픽 수집부
221
222
220
유입 트래픽 행렬 생성부
유출 트래픽 행렬 생성부
231
232
230
정상 유입 트래픽 소거부
정상 유출 트래픽 소거부
241
242
240
유입 랭크값 계산부
유출 랭크값 계산부
250
네트워크 상태 판단부

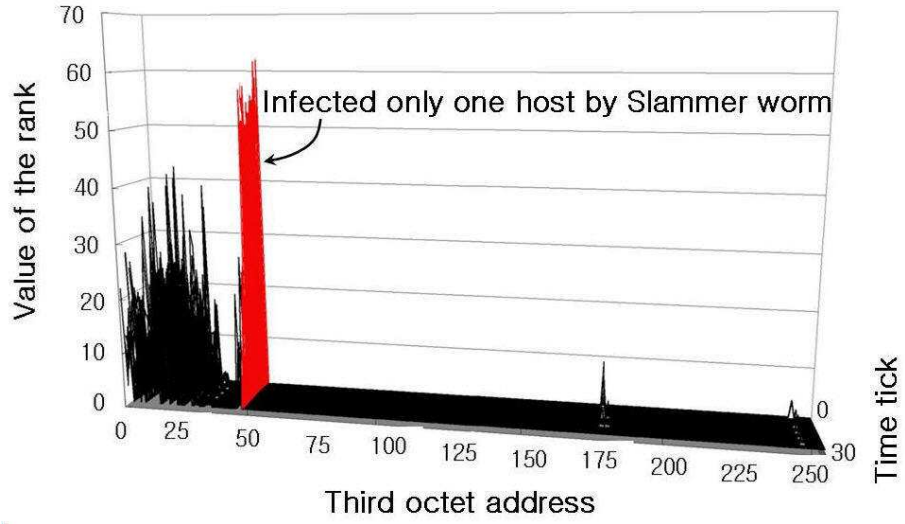
도면5

랭크값	네트워크 상태
$R_I < R_{I,min}$ & $R_O < R_{O,min}$	안정 상태
$R_I > R_{I,max}$ & $R_O < R_{O,min}$	웜에 의한 공격을 받는 상태
$R_I < R_{I,min}$ & $R_O > R_{O,max}$	웜에 감염되어 있는 상태
$R_I > R_{I,max}$ & $R_O > R_{O,max}$	웜에 감염되어 있으며, 웜에 의한 공격을 받는 상태

도면6



도면7


Infected only one host by Slammer worm
Value of the rank
70
60
50
40
30
20
10
0
0
25
50
75
100
125
150
175
200
225
250
Third octet address
0
30
Time tick