



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0001786
(43) 공개일자 2010년01월06일

(51) Int. Cl.

H04L 12/24 (2006.01) G06F 15/00 (2006.01)
G06F 21/00 (2006.01) H04L 12/26 (2006.01)

(21) 출원번호 10-2008-0061837

(22) 출원일자 2008년06월27일

심사청구일자 2008년06월27일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

박대회

서울특별시 강남구 도곡동 타워팰리스 A-1601

정용화

대전 유성구 지족동 877 열매마을아파트 505동 402호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 19 항

(54) 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지방법, 그 장치 및 이를 기록한 기록 매체

(57) 요약

서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용한 트래픽 폭주 공격 탐지 방법, 그 장치 및 이를 기록한 기록 매체가 개시된다.

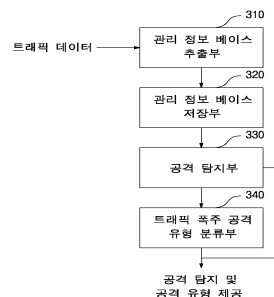
본 발명에 따른 서포트 벡터 데이터 명세를 트래픽 폭주 공격 탐지 방법은,

관리 정보 베이스의 집합 중에서 트래픽 폭주 공격률을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격률의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출하는 단계; 상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집하는 단계; 서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하는 단계; 트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류하는 단계를 포함한다.

본 발명에 의하면, 일반적인 대규모 네트워크 환경에서 적은 비용과 적은 노력으로 침입 탐지 시스템을 구축할 수 있고, 고사양의 패킷 기반 탐지 시스템을 설치하기 힘든 규모로 운영되는 오피스 네트워크나 홈 네트워크에서의 침입탐지에 적용할 수 있고, 실시간 침입탐지 및 시스템에서 학습되지 않은 새로운 공격 유형을 탐지할 수 있으며, 공격 유형별 트래픽 분류를 수행할 수 있어 더욱 안전한 시스템 운영과 서비스 지원을 보장할 수 있는 효과가 있다.

그리고, 본 발명은 전통적인 트래픽 정보 추출에 비해 그 비용이 적게 소비되는 SNMP MIB에서의 경량적 트래픽 정보와 이미 패턴분류 및 함수근사 등의 문제에서 그 성능이 검증된 SVM의 계층적 구조를 띄고 있으므로, 본 발명은 전통적인 DDoS에서의 고성능 분석시스템 및 확장성의 문제를 해결함과 동시에 MIB의 최소 갱신주기인 시간 단위로 트래픽 정보를 수집함으로써 전통적인 DDoS 탐지에서의 실시간 침입의 탐지가 어렵다는 문제점을 극복하였고, 단일클래스 SVM을 이용한 DDoS의 공격유형을 세분화하여 분류한 최초의 시도으로써 그 의미가 크다고 볼 수 있다.

대표도 - 도3



(72) 발명자

김명섭

충청남도 연기군 조치원읍 신흥리 푸르지오1차
107-401

유재학

충북 옥천군 옥천읍 죽향리 옥향아파트 103동 803
호

특허청구의 범위

청구항 1

관리 정보 베이스의 집합 중에서 트래픽 폭주 공격률을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격률의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출하는 단계;

상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집하는 단계;

서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하는 단계;

트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류하는 단계를 포함하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 2

제 1 항에 있어서,

상기 트래픽 폭주 공격의 유형을 분류하는 단계는

상기 트래픽 폭주 공격이 상기 서포트 벡터 데이터 명세에 정의되지 않은 트래픽 폭주 공격에 해당하는 경우, 상기 트래픽 폭주 공격의 별도의 클래스를 생성하는 단계를 더 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 3

제 1 항에 있어서,

상기 관리 정보 베이스는

MIB-2 그룹의 관리 정보 베이스인 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 4

제 1 항에 있어서,

상기 트래픽 폭주 공격률의 트래픽 폭주 공격은

TCP-SYN 플러딩(flooding) 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격을 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 5

제 1 항에 있어서,

상기 관리 정보 베이스의 다음의 갱신 주기는

상기 관리 정보 베이스의 실제 측정 갱신 주기가 U^n 이고, 상기 관리 정보 베이스의 n-1 번째 갱신 주기의 지수 평균 값이 P^{n-1} 이며, 상기 관리 정보 베이스의 n 번째 슬립시간이 S^n 이며, 미리 설정된 시스템 파라미터가 α 일 때, 상기 관리 정보 베이스의 다음의 갱신 주기 P^n 은 하기의 식 1에 의해 결정되는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

$$P_n = \alpha \times P_{n-1} + (1 - \alpha) \times U_{n-1}$$

$$S_n = P_n - 1 \quad (1)$$

청구항 6

제 5 항에 있어서,

상기 관리 정보 베이스의 실제 측정된 갱신 주기 중 최초의 실제 측정 갱신 주기 U_0 는

사용자에 의해 미리 일정 시간 동안 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정된 상기 관리 정보 베이스의 실제 측정 갱신 주기의 최소값으로 결정되는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 7

제 1 항에 있어서,

상기 트래픽 폭주 공격 여부의 탐지를 수행하는 단계는

정상 트래픽 만으로 학습된 단일 클래스의 서포트 벡터 머신에 의해 상기 트래픽 폭주 공격 여부를 탐지하는 단계인 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 8

제 1 항에 있어서,

상기 트래픽 폭주 공격의 유형을 분류하는 단계는

상기 트래픽 폭주 공격을 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격의 유형으로 분류하는 단계를 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법.

청구항 9

제 1 항 내지 제 8 항 중 어느 한 항의 방법을 컴퓨터에서 수행시킬 수 있는 프로그램으로 기록된 기록 매체.

청구항 10

관리 정보 베이스의 집합 중에서 트래픽 폭주 공격률을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격률의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출하는 관리 정보 베이스 추출부;

상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집하는 관리 정보 베이스 저장부;

서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하는 공격 탐지부;

트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류하는 트래픽 폭주 공격 유형 분류부를 포함하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 11

제 10 항에 있어서,

상기 트래픽 폭주 공격 유형 분류부는

상기 트래픽 폭주 공격이 상기 서포트 벡터 데이터 명세에 정의되지 않은 트래픽 폭주 공격에 해당하는 경우, 상기 트래픽 폭주 공격의 별도의 클래스를 생성하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트

래픽 폭주 공격 탐지 장치.

청구항 12

제 10 항에 있어서,

상기 관리 정보 베이스는

MIB-2 그룹의 관리 정보 베이스인 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 13

제 10 항에 있어서,

상기 트래픽 폭주 공격탐의 트래픽 폭주 공격은

TCP-SYN 플러딩(flooding) 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격을 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 14

제 10 항에 있어서,

상기 관리 정보 베이스의 다음의 갱신 주기는

상기 관리 정보 베이스의 실제 측정 갱신 주기가 U_n 이고, 상기 관리 정보 베이스의 n-1 번째 갱신 주기의 지수 평균 값이 P_{n-1} 이며, 상기 관리 정보 베이스의 n 번째 슬립시간이 S_n 이며, 미리 설정된 시스템 파라미터가 α 일 때, 상기 관리 정보 베이스의 다음의 갱신 주기 P_n 은 하기의 식 2에 의해 결정되는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

$$P_n = \alpha \times P_{n-1} + (1 - \alpha) \times U_{n-1}$$

$$S_n = P_n - 1 \quad (2)$$

청구항 15

제 14 항에 있어서,

상기 관리 정보 베이스의 실제 측정된 갱신 주기 중 최초의 실제 측정 갱신 주기 U_{0n} 은

사용자에 의해 미리 일정 시간 동안 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정된 상기 관리 정보 베이스의 실제 측정 갱신 주기의 최소값으로 결정되는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 16

제 10 항에 있어서,

상기 공격 탐지부는

정상 트래픽 만으로 학습된 단일 클래스의 서포트 벡터 머신에 의해 상기 트래픽 폭주 공격 여부를 탐지하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 17

제 10 항에 있어서,

상기 트래픽 폭주 공격 유형 분류부는

상기 트래픽 폭주 공격을 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격의 유형으로 분류하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 18

제 10 항에 있어서,

상기 공격 탐지부로부터 전송된 트래픽 폭주 공격 탐지 메시지 및 상기 트래픽 폭주 공격 유형 분류부로부터 전송된 트래픽 폭주 공격의 유형에 따라 상기 트래픽 폭주 공격에 대한 방어 기작을 수행하는 방어 기작 수행부를 더 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

청구항 19

제 18 항에 있어서,

상기 방어 기작 수행부와 연결되고, 상기 방어 기작 수행부의 방어 기작을 저장하여 방어 기작 알고리즘을 업데이트하는 전략 설정부를 더 포함하는 것을 특징으로 하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치.

명세서

발명의 상세한 설명

기술분야

<1> 본 발명은 망에 대한 침입 탐지에 관한 것으로서, 특히 네트워크에서의 트래픽 폭주 공격에 대하여 공격 패턴을 분석하고, 또한 빠르고 신속한 침입탐지를 구현할 수 있는 서포트 벡터 데이터 명세(Support Vector Data Description: SVDD)를 이용한 트래픽 폭주 공격 탐지 방법, 그 장치 및 이를 기록한 기록 매체를 제공하는 것이다.

배경기술

- <2> 최근개방형 통신 환경 및 인터넷의 급속한 보급에 따라, 더욱 빠르고 편리하게 정보 획득 및 처리가 가능하게 되었다. 이와 같이 네트워크 기반 서비스의 의존도가 증가하면서 사용자는 인터넷으로부터 필요한 정보를 빠르게 획득할 수 있으며, 자신의 정보르 인터넷을 통해 홍보하는 수단으로까지 이용하고 있다.
- <3> 그러나, 이러한 긍정적인 특면과 함께 최근 정상적인 서비스를 방해하는 유해 트래픽이나 웜 등을 통한 네트워크의 피해사례가 보고되고 있고, 아울러, 개인, 기업은 물론 국가의 중요한 정보가 불법으로 유출되어 잘못 이용되는 사례가 급증하고 있다. 실제로 1990년도를 기점으로 하여 바이러스나 고의적인 의도로 망에 접근하여 비정상적인 트래픽을 발생시켜 망을 마비시킬 정도의 피해를 입히는 사례들이 늘어나고 있다.
- <4> 이러한 해킹 등의 불법행위를 방지하고 중요한 정보 자산을 보호하기 위한 보안 시스템의 설치가 근래 들어 중요하게 인식되고 있다.
- <5> 이에 대하여, 방 보호에 관한 연구 역시 이에 대응하기 위해 활발한 연구들이 진행되고 있으나, 아직 지능적으로 대응하여 이런 상황을 조기에 예방할 수 있는 방안은 존재하지 않는 실정이다. 대신 실시간적인 망 감시를 통하여 비정상적인 트래픽 발생 징후를 파악하여 이를 대처하는 방법들을 주로 이용하고 있다.
- <6> 대표적인 유해 트래픽인 트래픽 폭주 공격은 대상이 되는 컴퓨터 시스템은 물론 네트워크의 자원을 고갈시킴으로써 정상적인 서비스를 수행하지 못하는 공격으로 업무에 막대한 피해를 준다.
- <7> 안전한 네트워크 운영과 관리를 위하여 이러한 악의적 접근이나 침입 등을 신속하게 탐지하고 대처할 수 있는 보안 기술이 최근 중요한 이슈이다.
- <8> 보안 시스템의 가장 대표적인 장치로 방화벽(fire-wall)을 들 수 있으며, 이는 두 IP간에 흐르는 패킷을 미리 정해놓은 규칙에 따라 차단하거나 보내주는 패킷 필터 프로그램으로서 불법적인 트래픽을 제어하는 역할을 한다. 하지만, 방화벽은 접속/차단 규칙에 의해 이미 공개된 불법적인 트래픽에 대해서는 효과적인 차단이 가능하지만, 접속/차단 규칙 자체가 노출되어 해킹 되면 불법적인 트래픽이라도 인지할 수 없는 단점을 갖고 있다. 이에 대한 보완책으로 불법행위를 미연에 탐지하여 사전에 경보하는 사전 경보 기능 및 초기 대응 기능을 구비

한 침입 탐지 장치(Intrusion Detection System)가 새로운 대안으로 제시되고 있다.

- <9> 침입 탐지 장치의 기본 기능은 네트워크에서 비인가자의 불법적인 정보 자원의 사용 및 변조, 파괴 행위를 탐지하는 것이다. 침입 탐지 장치는 그 특성상 네트워크 트래픽을 캡처하기 때문에 모든 패킷을 분석한 기록 리포트를 제공할 수 있다. 즉, 침입 탐지 장치는 이메일 및 웹메일 등의 자료를 캡처하여 사전에 키워드에 의해 불법적인 자료를 차단시키며, 누가 어떤 자료에 대해 해킹을 했는가에 대한 기록을 제공하여 사후 불법 행위자를 찾는 데에 중요 자료로 활용될 수 있다.
- <10> 침입 탐지 장치는 탐지 방법에 따라, 오용 탐지(Signature Detection or Misuse Detection) 모델과 비정상 탐지(Anomaly Detection) 모델로 나뉘어진다.
- <11> 오용 탐지 모델은 이미 발견된 공격 유형에 대한 면밀한 분석을 통하여 규칙 베이스화하고, 이를 기반으로 탐지를 수행하는 방법으로, 새로운 공격유형이 발견될 시에는 수동으로 규칙 베이스를 갱신해야만 새로운 공격에 대처할 수 있다는 문제점을 가지고 있다.
- <12> 반면에, 비정상 탐지 모델은 미리 정의된 정상 행동에 대한 프로파일로부터 크게 벗어나는 데이터를 비정상 행동으로 판단하여 공격을 탐지하는 방법으로, 새로운 공격유형을 탐지할 수 있다는 점에서는 실용적이나, 탐지된 공격유형에 대한 추가적인 세부 정보를 알 수 없기 때문에, 침입에 따른 적절한 대처를 할 수 없다는 한계를 지니고 있다.
- <13> 최근의 기술 문헌을 보면, 보다 지능적인 침입탐지 모델의 설계를 위하여 데이터마이닝 및 기계 학습 기법을 침입탐지시스템에 적용하려는 시도가 활발히 진행중이다.
- <14> 이러한 기술 동향 중 특히 패턴 분류(pattern classification) 및 함수 근사(function approximation) 등의 문제에서 매우 우수한 성능을 보이는 서포트 벡터 머신(Support Vector Machine:SVM)을 침입 탐지에 적용하려는 시도가 주목을 받고 있다. 그러나, 이러한 새로운 방법론 역시 전통적인 네트워크의 패킷 정보를 이용하고 있음을 알 수 있다.
- <15> 서포트 벡터 머신은 통계 분류와 회귀 분석을 쓰는 지도 학습 방법을 가리키는 말이다. 이는 커널 트릭을 써서 비선형 분류 문제에 선형 분류의 테크닉을 적용하며, 현재 알려져 있는 많은 수법 중에서 가장 인식 성능이 뛰어난 학습 모델의 하나이다.
- <16> 서포트 벡터 머신이 뛰어난 인식 성능을 발휘할 수 있는 이유는, 미학습 데이터에 대해서 높은 식별 성능을 얻기 위한 공리가 있는 것이다. 서포트 벡터 머신은, 선형 문턱 소자를 이용하고, 2 클래스의 패턴 식별기를 구성하는 수법이다. 훈련 샘플로부터 「마진 최대화」라고 하는 기준으로 선형 문턱 소자의 파라미터를 학습한다. 1960년대에 Vapnik등이 고안 한 Optimal Separating Hyperplane를 기반으로 하고 있어, 1990년대가 되어 커널 학습법과 조합한 비선형 분류 수법으로 확장되었다.
- <17> 그러나, 이러한 새로운 방법론 역시 전통적인 네트워크의 패킷 정보를 이용하고 있음을 알 수 있다.
- <18> 이와 같이, 기존에 연구된 트래픽 폭주 공격 탐지에서의 전통적인 패킷 수집 방법론은 공격에 대한 상세한 분석은 가능하지만, 고가의 고성능 분석시스템이 요구될 뿐만 아니라, 설치 운영상의 확장성이 부족하다는 단점을 가지고 있다.
- <19> 따라서, 이를 보완하기 위한 방법으로 최근 단순 네트워크 관리 프로토콜(Simple Network Management Protocol:SNMP)에서의 관리 정보 베이스(Management Information Base:MIB) 정보를 이용한 침입 탐지 방법론이 주목을 받고 있다.
- <20> 이와 같이, 단순 네트워크 관리 프로토콜은 네트워크를 관리하기 위한 프로토콜이다. 단순 네트워크 관리 프로토콜은 관리할 대상인 관리 객체를 정하고, 효율적으로 관리하기 위하여 관리 객체를 분류하여야 하는데, 이것이 바로 관리 정보 베이스이다.
- <21> 관리 정보 베이스는 관리되어야 할 자원 객체의 분류된 정보를 말한다. 관리되어야 할 객체는 시스템 정보, 네트워크 사용량, 네트워크 인터페이스 정보 등이 된다.
- <22> 단순 네트워크 관리 프로토콜에서의 관리 정보 베이스를 이용한 트래픽 폭주 공격 탐지는 관리 정보 베이스의 데이터 수집을 위한 시스템 및 네트워크 리소스(Resource)의 사용이 적고, 계층과 프로토콜을 기준으로 표준화된 네트워크 성능 데이터를 제공 받을 수 있기 때문에 패킷 기반의 탐지 방법에 비하여 보다 빠르고 효과적인 탐지와 분류가 가능하다.

- <23> 이는 대부분의 네트워크 기반 시스템들이 단순 네트워크 관리 프로토콜 에이전트(SNMP agent)를 탑재하고 있기 때문이다. 따라서, 단순 네트워크 관리 프로토콜의 관리 정보 베이스의 정보를 이용한 트래픽 폭주 공격의 탐지는 고사양의 패킷 기반 탐지 시스템을 설치하기 힘든 소규모로 운영되는 오피스 네트워크나 홈 네트워크에서의 침입탐지 시스템으로 적합하다.
- <24> 또한, 대규모의 네트워크에서도 적은 비용과 노력으로 탐지 시스템을 구축하는 대안이 될 수 있다.
- <25> 최근의 기술 동향 중에서 기계 학습 기법과 단순 네트워크 관리 프로토콜 관리 정보 베이스를 이용한 침입 탐지 시스템이 개발되었다.
- <26> LI 등은 BNMP MIB-II 데이터를 확률 밀도 함수(Probability Density Function:PDF)로 변환한 후, 역전파(backpropagation) 기반의 인공신경망을 이용하여 침입 여부를 결정하는 시스템을 제안하였다.
- <27> Puttini 등은 SNMP MIB 데이터를 베이시안(Bayesian) 분류기에 적용하여 모바일 애드혹 네트워크(Moble Adhoc NETwork:MANET)에서의 비정상 트래픽을 탐지하였다.
- <28> 또한, Ramah 등은 Shyu 등이 제안한 PCA 기반의 비정상 탐지 알고리즘을 이용한 탐지 시스템을 제안하였다.
- <29> 그러나, 이러한 연구 등은 모두 외부의 침입에 대하여 침입 탐지에만 주력하였을 뿐, 공격 유형의 분류 문제까지는 고려하지 않았고, 역전파(backpropagation)와 베이시안(baysian)과 같은 기계학습 기법들이 선택적으로 사용되었으나, 서포트 벡터 머신(Support Vector Machine) 기반의 기법들은 적용되지 않았음을 알 수 있다.
- <30> 이와 같이, 종래의 MIB 기반의 공격 탐지 시스템들은 대부분 테스트에 사용된 당시의 DoS 공격툴의 기능과 특성에 의존적으로 개발된 시스템으로 새로운 공격유형이나 끊임없이 발전하는 공격툴에 유연하기 어렵고, 새로운 공격 형태나 툴이 발견되면 그때마다 새롭게 알고리즘 전체를 수정해야 하므로, 실시간 침입 탐지, 시스템에서 학습되지 않은 새로운 공격 유형의 탐지, 및 공격 유형별 트래픽 분류등이 보장되지 않아 안전한 시스템 운영과 서비스가 어렵다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

- <31> 따라서, 본 발명이 해결하고자 하는 첫 번째 과제는 패턴 분류 등의 문제에서 가장 우수한 성능을 가지는 서포트 벡터 머신(Support Vector Machine:SVM)을 기반으로 단순 네트워크 관리 프로토콜(Simple Network Management Protocol:SNMP)에서의 관리 정보 베이스(Management Information Base:MIB) 정보를 이용하여 실시간적인 공격 트래픽 탐지와 새로운 공격 유형을 탐지할 수 있는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법을 제공하는 것이다.
- <32> 본 발명이 해결하고자 하는 두 번째 과제는 상기 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법을 수행할 수 있는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치를 제공하는 것이다.
- <33> 본 발명이 해결하고자 하는 세 번째 과제는 상기 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법을 컴퓨터에서 수행시킬 수 있도록 프로그램으로 기록된 기록 매체를 제공하는 것이다.

과제 해결수단

- <34> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,
- <35> 관리 정보 베이스의 집합 중에서 트래픽 폭주 공격툴을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격툴의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출하는 단계; 상기 추출된 관리 정보 베이스의 기측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집하는 단계; 서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하는 단계; 트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류하는 단계를 포함하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법을 제공한다.
- <36> 한편, 상기 트래픽 폭주 공격의 유형을 분류하는 단계는 상기 트래픽 폭주 공격이 상기 서포트 벡터 데이터 명세에 정의되지 않은 트래픽 폭주 공격에 해당하는 경우, 상기 트래픽 폭주 공격의 별도의 클래스를 생성하는 단

계를 더 포함하는 것을 특징으로 한다.

<37> 또한, 상기 관리 정보 베이스는 MIB-2 그룹의 관리 정보 베이스일 수 있다.

<38> 아울러, 상기 트래픽 폭주 공격트의 트래픽 폭주 공격은 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격을 포함할 수 있다.

<39> 그리고, 상기 관리 정보 베이스의 다음의 갱신 주기는 상기 관리 정보 베이스의 실제 측정 갱신 주기가 U_{n-1} 이고, 상기 관리 정보 베이스의 n-1 번째 갱신 주기의 지수 평균 값이 P_{n-1} 이며, 상기 관리 정보 베이스의 n 번째 슬립시간이 S_n 이며, 미리 설정된 시스템 파라미터가 α 일 때, 상기 관리 정보 베이스의 다음의 갱신 주기

$$P_n = \alpha \times P_{n-1} + (1 - \alpha) \times U_{n-1}$$

P_n 은 수학적 $S_n = P_{n-1}$ 에 의해 결정될 수 있다.

<40> 한편, 상기 관리 정보 베이스의 실제 측정된 갱신 주기 중 최초의 실제 측정 갱신 주기 U_0 는 사용자에게 의해 미리 일정 시간 동안 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정된 상기 관리 정보 베이스의 실제 측정 갱신 주기의 최소값으로 결정될 수 있다.

<41> 또한, 상기 트래픽 폭주 공격 여부의 탐지를 수행하는 단계는 정상 트래픽 만으로 학습된 단일 클래스의 서포트 벡터 머신에 의해 상기 트래픽 폭주 공격 여부를 탐지하는 단계일 수 있다.

<42> 그리고, 상기 트래픽 폭주 공격의 유형을 분류하는 단계는 상기 트래픽 폭주 공격을 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격의 유형으로 분류하는 단계를 포함할 수 있다.

<43> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<44> 관리 정보 베이스의 집합 중에서 트래픽 폭주 공격트를 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격트의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출하는 관리 정보 베이스 추출부; 상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집하는 관리 정보 베이스 저장부; 서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하는 공격 탐지부; 트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류하는 트래픽 폭주 공격 유형 분류부를 포함하는 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치를 제공한다.

<45> 여기서, 상기 트래픽 폭주 공격 유형 분류부는 상기 트래픽 폭주 공격이 상기 서포트 벡터 데이터 명세에 정의되지 않은 트래픽 폭주 공격에 해당하는 경우, 상기 트래픽 폭주 공격의 별도의 클래스를 생성하는 것을 특징으로 한다.

<46> 아울러, 상기 관리 정보 베이스는 MIB-2 그룹의 관리 정보 베이스일 수 있다.

<47> 한편, 상기 트래픽 폭주 공격트의 트래픽 폭주 공격은 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격을 포함할 수 있다.

<48> 그리고, 상기 관리 정보 베이스의 다음의 갱신 주기는 상기 관리 정보 베이스의 실제 측정 갱신 주기가 U_{n-1} 이고, 상기 관리 정보 베이스의 n-1 번째 갱신 주기의 지수 평균 값이 P_{n-1} 이며, 상기 관리 정보 베이스의 n 번째 슬립시간이 S_n 이며, 미리 설정된 시스템 파라미터가 α 일 때, 상기 관리 정보 베이스의 다음의 갱신 주기

$$P_n = \alpha \times P_{n-1} + (1 - \alpha) \times U_{n-1}$$

P_n 은 수학적 $S_n = P_n - 1$ 에 의해 결정될 수 있다.

- <49> 그리고, 상기 관리 정보 베이스의 실제 측정된 갱신 주기 중 최초의 실제 측정 갱신 주기 U_0 는 사용자에게 의해 미리 일정 시간 동안 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정된 상기 관리 정보 베이스의 실제 측정 갱신 주기의 최소값으로 결정될 수 있다.
- <50> 한편, 상기 공격 탐지부는 정상 트래픽 만으로 학습된 단일 클래스의 서포트 벡터 머신에 의해 상기 트래픽 폭주 공격 여부를 탐지하는 것을 특징으로 한다.
- <51> 또한, 상기 트래픽 폭주 공격 유형 분류부는 상기 트래픽 폭주 공격을 TCP-SYN flooding 공격, UDP 플러딩 공격 및 ICMP 플러딩 공격의 유형으로 분류할 수 있다.
- <52> 그리고, 상기 장치는 상기 공격 탐지부로부터 전송된 트래픽 폭주 공격 탐지 메시지 및 상기 트래픽 폭주 공격 유형 분류부로부터 전송된 트래픽 폭주 공격의 유형에 따라 상기 트래픽 폭주 공격에 대한 방어 기작을 수행하는 방어 기작 수행부를 더 포함할 수 있다.
- <53> 아울러, 상기 장치는 상기 방어 기작 수행부와 연결되고, 상기 방어 기작 수행부의 방어 기작을 저장하여 방어 기작 알고리즘을 업데이트하는 전략 설정부를 더 포함할 수 있다.
- <54> 상기 세 번째 과제를 해결하기 위하여 본 발명은,
- <55> 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 기록매체를 제공한다.

효 과

- <56> 본 발명에 의하면, 일반적인 대규모 네트워크 환경에서 적은 비용과 적은 노력으로 침입 탐지 시스템을 구축할 수 있고, 고사양의 패킷 기반 탐지 시스템을 설치하기 힘든 규모로 운영되는 오피스 네트워크나 홈 네트워크에서의 침입탐지에 적용할 수 있고, 실시간 침입탐지 및 시스템에서 학습되지 않은 새로운 공격 유형을 탐지할 수 있으며, 공격 유형별 트래픽 분류를 수행할 수 있어 더욱 안전한 시스템 운영과 서비스 지원을 보장할 수 있는 효과가 있다.
- <57> 그리고, 본 발명은 전통적인 트래픽 정보 추출에 비해 그 비용이 적게 소비되는 SNMP MIB에서의 경량적 트래픽 정보와 이미 패턴분류 및 함수근사 등의 문제에서 그 성능이 검증된 SVM의 계층적 구조를 띄고 있으므로, 본 발명은 전통적인 DDoS에서의 고성능 분석시스템 및 확장성의 문제를 해결함과 동시에 MIB의 최소 갱신주기인 시간 단위로 트래픽 정보를 수집함으로써 전통적인 DDoS 탐지에서의 실시간 침입의 탐지가 어렵다는 문제점을 극복하였고, 단일클래스 SVM을 이용한 DDoS의 공격유형을 세분화하여 분류한 최초의 시도으로써 그 의미가 크다고 볼 수 있다.

발명의 실시를 위한 구체적인 내용

- <58> 실제로 패턴 분류에 있어서 결과적으로 좋은 성질을 가지고 있는 SNMP MIB 데이터의 이용과 패턴 분석을 위한 자동화 알고리즘의 역사적 진화과정 중 가장 강력하다고 이미 검증된 서포트 벡터 머신을 이용하여 트래픽 폭주 공격을 탐지하고, 공격 유형별 분류를 수행하는 시스템을 설계하는 시도는 아주 중요하다.
- <59> 이와 관련하여, 본 발명은 기존의 서비스 거부(Denial of Service:DoS) 공격을 보다 다양하고 견고하게 발전시킨 분산 서비스 거부(Distributed Denial of Service:DDoS) 공격에 대한 공격 유형별 탐지를 수행하는 새로운 침입 탐지 모델을 제공한다.
- <60> 본 발명은 서비스 거부/분산 서비스 거부로 대표되는 트래픽 폭주 공격을 단순 네트워크 관리 프로토콜에서의 관리 정보 베이스의 객체 정보를 기반으로 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 트래픽 폭주 공격을 실시간으로 탐지함과 동시에 공격 유형별로 트래픽 폭주 공격을 탐지하고, 이를 공격 유형별로 분류하는 시스템을 제공한다.
- <61> 이를 위하여, 먼저 네트워크 망의 트래픽 정보 중에서 정상 트래픽만으로 학습된 단일 클래스의 서포트 벡터 머

신(Support Vector Machine:SVM)으로 정상 트래픽과 공격 트래픽에 대한 경량적인 실시간 트래픽 폭주 공격 탐지를 보장하고, 점진적인 갱신이 가능하다.

- <62> 또한 본 발명은 정상 트래픽만으로 학습하므로 학습 속도 또한 매우 빠르고, 시스템에서 학습되지 않은 새로운 공격(novel attack)을 탐지할 뿐만 아니라, 공격 트래픽이 탐지되면 침입 대응 시스템에 침입 사실과 시스템의 상태 보고를 실시간으로 보고한다.
- <63> 이에 따라, 다중 클래스의 서포트 벡터 머신 구조로써 트래픽 폭주 공격으로 판단된 공격 트래픽을 분산 서비스 거부(Distributed Denial of Service:DDoS)의 대표적 공격 유형별로 분류하고, 침입 대응 시스템에 공격 유형에 대한 추가적인 정보를 제공하며, 시스템에서 학습되지 않은 새로운 공격 유형을 별도의 클래스로 분류함으로써 실제 시스템의 자원 관리 및 안전성을 보장할 수 있다.
- <64> 따라서, 본 발명은 네트워크 환경에서의 트래픽 폭주 공격을 탐지하는 모델로써 네트워크 대역폭 및 프로세서 처리 능력, 원활한 시스템 자원 관리와 안전성 확보에 기여할 수 있는 모델을 제공한다.
- <65> 특히, 트래픽 폭주 공격의 대표적 유형인 TCP SYN flooding, UDP flooding, ICMP flooding의 프로토콜별 분류 탐지를 수행함으로써 보다 유연한 네트워크 시스템 자원관리와 안전성을 보장할 수 있다.
- <66> 본 발명은 단순 네트워크 관리 프로토콜(Simple Network Management Protocol:SNMP)에서의 관리 정보 베이스(Management Information Base:MIB) 정보를 이용함으로써, 기존의 패킷 수집 방법론들의 단점인 고가의 고성능 분석 시스템의 요구와 설치의 확장성 문제점을 보완하는 건지에서 1) 실시간 침입 탐지 및 서비스의 안전성 보장, 2) 쉬운 확장성 및 관리 정보 베이스 정보를 이용한 저비용 탐지, 3) 공격 유형 시스템의 효율적인 대처 보장, 4) 시스템에서 학습되지 않은 새로운 공격유형의 탐지를 모두 만족한다.
- <67> 단순 네트워크 관리 프로토콜은 네트워크 및 시스템의 관리를 위한 표준화된 다양한 정보를 제공하지만, 단순 네트워크 관리 프로토콜을 이용한 효율적인 트래픽 폭주 공격의 탐지를 위해서는 단순 네트워크 관리 프로토콜의 구조적인 특징으로 인하여 아래와 같은 3가지의 요소를 모두 고려해야 한다.
- <68> 첫 번째는 트래픽의 특징을 반영하는 관리 정보 베이스 정보의 선정이다.
- <69> 이는 우선 다양한 시스템에 적용할 수 있도록 표준화된 관리 정보 베이스 정보에서 선정해야 하고, 다양한 시스템의 정상 트래픽 발생 상황과 트래픽 폭주 공격시 트래픽 상황을 구분할 수 있도록 폭넓은 관리 정보 베이스 정보를 포함할 수 있다.
- <70> 그리고, 수집 시스템, 분석 시스템, 그리고 네트워크의 부하를 최소화 할 수 있는 필수적인 관리 정보 베이스 정보만을 수집하여야 한다.
- <71> 두 번째는 신속한 탐지이다.
- <72> 즉, 트래픽 폭주 공격이 분산화되고 고속화됨에 따라 빠른 탐지는 탐지 시스템의 필수 요건이 되었다. 반면에 빠른 탐지를 위하여 관리 정보 베이스의 정보의 수집 및 분석 주기를 단축하게 되면, 시스템 및 네트워크의 부하가 증가하게 되므로, 적절한 탐지 시점의 결정은 탐지 시스템의 성능을 결정하는 매우 중요한 요소이다.
- <73> 도 1은 특정의 시스템에서 MIB-2 인터페이스 그룹의 옥텟(Octets) 값을 매 1초 단위로 도시하고 있다.
- <74> 도 1에서 볼 수 있는 바와 같이, 관리 정보 베이스 값은 특정한 주기(15초)를 기준으로 갱신되고 있다. 그러나, 기존의 탐지 시스템은 1분 또는 그 이상의 주기로 동작하는 타이머를 기준으로 관리 정보 베이스 값의 갱신을 수행하기 때문에, 관리 정보 베이스의 갱신 주기가 제때에 반영되지 않아 트래픽 탐지 시간의 지연이 발생한다.
- <75> 관리 정보 베이스의 갱신 주기를 기준으로 트래픽 탐지 시스템이 동작한다면 탐지의 정확성과 탐지 속도를 향상시킬 수 있다.
- <76> 그러나, 짧은 탐지 주기는 탐지를 위한 소비 트래픽과 시스템 부하를 증가시키기 때문에 이를 고려한 효율적인 탐지 시점 알고리즘이 요구된다.
- <77> 세 번째는 단순 네트워크 관리 프로토콜에서의 관리 정보 베이스 기반의 분산 서비스 거부 탐지 방법이 고려되어야 한다.
- <78> 전통적인 단순 네트워크 관리 프로토콜에서의 관리 정보 베이스 기반의 분산 서비스 거부 탐지 방법은 프로토콜별 추이 분석, 일주 트래픽 추이 분석, 그리고 객체 정보 간의 상관관계를 이용하는 방법이 있다.

- <79> 프로토콜별 추이분석은 시스템에서 발생하는 트래픽 정보를 수집하여 하루 동안 시간대 별로 프로토콜 분포를 예측하여 기준값을 생성하고, 현재 발생하는 트래픽의 프로토콜 분포와 비교하여 공격 트래픽을 탐지하는 방법이나, 이는 매우 유동적이고 변화가 심한 네트워크에서는 트래픽 예측을 정확하게 수행할 수 없다는 문제점이 있다.
- <80> 일주 트래픽 추이분석은 일분 또는 수십분 단위로 관리 정보 베이스의 정보를 일정 기간 동안 수집한 후 모든 트래픽을 수용할 수 있는 기준 트래픽 추이 데이터를 설정하는 방법이다.
- <81> 그러나, 이는 기준이 되는 추이 트래픽 설정이 어렵다는 문제점이 있다.
- <82> 마지막으로, 관리 정보 베이스 객체 정보간의 상관관계를 이용하여 공격 트래픽을 탐지하는 방법이다.
- <83> 이는 비교적 정확한 공격 트래픽 탐지에는 도움이 되지만, 객체 정보 간의 상관관계를 정의해야 할 뿐만 아니라, 별도로 연산하고 처리하기 위한 시간과 처리된 결과값을 저장하고 관리하기 위한 추가적인 리소스를 요구하기 때문에 시스템의 안전성을 보장하기 위한 실시간 탐지가 어렵다.
- <84> 최근의 트래픽 폭주 공격 방법들이 날로 다양해지고 견고해짐으로 전통적인 단순 네트워크 관리 프로토콜의 관리 정보 베이스 기반의 트래픽 폭주 공격 탐지 방법들은 실제 시스템에 적용하기에는 현실적으로 많은 문제점이 있다.
- <85> 현존하는 관리 정보 베이스 기반의 분산 서비스 거부 탐지 시스템은 대부분 테스트에 사용된 당시의 서비스 거부 공격들의 성능과 특성에 의존적으로 개발된 시스템으로 새로운 공격 유형이나, 끊임없이 발전하는 공격들에 유연하게 대처하기가 어렵다.
- <86> 즉, 새로운 공격 형태나 톨이 발견되면 그때마다 새롭게 알고리즘 전체를 수정해야만 하는 단점을 가지고 있다.
- <87> 결과적으로 실시간 침입탐지와 시스템에서 학습되지 않은 새로운 공격 유형의 탐지 및 공격 유형별 트래픽 분류 등의 기능이 보장되는 보다 안전한 시스템 운영과 서비스가 가능한 새로운 대안이 요구되는 것이다.
- <88> 이하, 본 발명의 바람직한 실시예를 첨부도면에 의거하여 상세히 설명하기로 한다.
- <89> 그러나, 다음에 예시하는 본 발명의 실시예는 여러 가지 다른 형태로 변형할 수 있으며, 본 발명의 범위가 다음에 상술하는 실시예에 한정되는 것은 아니다. 본 발명의 실시예는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위하여 제공된다.
- <90> 도 2는 본 발명의 일 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법의 흐름도이다.
- <91> 도 2를 참조하면 우선, 관리 정보 베이스의 집합 중에서 트래픽 폭주 공격들을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격들의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출한다(S210).
- <92> 이에 본 발명에서는 RFC1213에서 정의한 MIB-2 그룹의 MIB 객체들 중에서, 실제 트래픽 폭주 공격에 반응하는 MIB 객체들만을 선정한다.
- <93> 즉, MIB 객체의 산정을 위하여 트래픽 폭주 공격의 대표적인 공격들에 해당하는 Stacheldraht를 이용하여 TCP-SYN flooding 공격, UDP 플러딩 공격, ICMP 플러딩 공격 등을 타겟 시스템에 실시하였으며, MIB-2 그룹의 모든 MIB 객체들의 전수 조사를 실시한다.
- <94> 본 발명에 적용되는 MIB 객체들을 정리하면, 하기의 표 1과 같다.

표 1

mib-2 Group	SNMP MIB objects
interface	interface.ifTable.ifEntry. <i>ifInOctets</i> interface.ifTable.ifEntry. <i>ifInUcastPkts</i>
ip	ip. <i>ipInReceives</i> ip. <i>ipInDelivers</i> ip. <i>ipOutDiscards</i>
tcp	tcp. <i>tcpAttemptFails</i> tcp. <i>tcpOutRsts</i>
udp	udp. <i>udpInErrors</i>
icmp	icmp. <i>icmpInDestUnreaches</i> icmp. <i>icmpOutDestUnreaches</i> icmp. <i>icmpOutEchoReps</i> icmp. <i>icmpOutMsgs</i>

<95>

<96>

그 다음, 상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집한다(S220).

<97>

단순 네트워크 관리 프로토콜 에이전트는 관리 정보 베이스 정보가 갱신된 시점으로부터 다음 갱신 시점까지는 동일한 관리 정보 베이스 값을 제공하기 때문에, 관리 정보 베이스 정보 갱신 시점 직후에 관리 정보 베이스의 정보를 수집하는 것이 보다 빠른 탐지를 위해 효과적이다.

<98>

따라서, 본 발명에서는 아래와 같이 관리 정보 베이스의 정보의 갱신 시점을 결정하여 관리 정보 베이스의 정보를 수집한다.

<99>

우선, 갱신 주기의 탐지를 위하여 MIB-2 인터페이스 그룹의 *ifInOctets* MIB 값을 특정 시간 단위로 확인한다.

<100>

바람직하게는 상기 관리 정보 베이스의 정보의 갱신 시점은 1초 단위로 설정될 수 있다.

<101>

갱신 시점의 확인을 위해 매 초 단순 네트워크 관리 프로토콜의 메시지 발생에 따른 트래픽의 부하를 줄이기 위하여 본 발명에서는 하기의 수학적 식 1과 같이 갱신 주기 P_n 과 슬립 시간 S_n 을 결정한다.

수학적 식 1

$$P_n = \alpha \times P_{n-1} + (1 - \alpha) \times U_{n-1}$$

<102>

$$S_n = P_n - 1$$

<103>

상기 수학적 식 1에서 볼 수 있는 바와 같이, 현재까지의 갱신 주기 $\{U_0, U_1, U_2, \dots, U_{n-1}\}$ 와 갱신 주기의 지수 평균을 이용하여 다음의 예측 갱신 주기 P_n 를 구하고, 이로부터 슬립 시간 S_n 을 결정하여 슬립함으로써 소비 트래픽과 관리 시스템의 부하 증가 문제를 해결할 수 있다. 여기서 상수 α 는 미리 설정된 시스템 파라미터 일 때, 상수 α 값은 0.5로 설정할 수 있다.

<104>

관리 정보 베이스의 갱신 주기는 단순 네트워크 관리 프로토콜 에이전트와 시스템에 따라 다르고, 같은 시스템이라고 할 지라도 시간에 따라 변할 수 있기 때문에 각 갱신 주기에 대한 유동성을 고려한 지수 평균(exponential average) 값을 적용하여 보다 효율적으로 트래픽 탐지 시점을 결정할 수 있다.

<105> 상기 수식 1에서 U^n 은 실제 측정된 *iflnOctets* MIB 정보의 갱신 주기이며, 최초 갱신 주기인 U_0 는 시스템의 적용 전의 일정 시간 동안 매초 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정한 갱신 주기들의 최소값으로 결정된다.

<106> 트래픽 탐지 시점의 결정을 위한 알고리즘에서 사용된 기호를 다시 정리하면, 하기의 표 2와 같다.

표 2

U_n	n 번째 <i>iflnOctets</i> MIB의 갱신 주기
P_n	n 번째 갱신 주기의 지수 평균 값(예측한 값)
S_n	n 번째 sleep 시간(1초 단위)
α	= 1/2(상수)

<107>

<108> 그 다음, 서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행한다(S230).

<109> 본 발명에 의하면, 서포트 벡터 데이터 명세 트레이닝을 통하여 트래픽 폭주 공격 발생에 대하여 공격의 탐지만 아니라, 공격의 유형까지 판단한다.

<110> 여기서, 본 발명에 따른 트래픽 폭주 공격에 대한 트래픽 폭주 공격 탐지는 아래와 같이 수행된다.

<111> 네트워크의 트래픽 정보 중에서 정상트래픽만으로 학습된 서포트 벡터 데이터 명세로 정상트래픽과 공격트래픽에 대한 실시간 탐지를 보장하며, 점증적인 갱신도 가능하다.

<112> 또한, 학습시에 정상 트래픽만을 요구함으로써 학습을 위한 별도의 공격 트래픽을 준비할 필요가 없으며, 학습 속도 또한 다른 서포트 벡터 머신에 비해 상대적으로 빠르다.

<113> 학습된 단일 클래스의 서포트 벡터 머신은 비정상 탐지 모델로 시스템에서 학습되지 않은 새로운 공격을 탐지하면, 공격 트래픽이 탐지되면, 공격 대응 시스템에 침입 사실을 실시간으로 보고한다.

<114> 또한, 본 발명에 따른 탐지된 트래픽 폭주 공격에 대한 트래픽 공격의 유형 분류는 아래와 같이 수행된다.

<115> 다중 클래스의 서포트 벡터 머신의 구조로 트래픽 폭주 공격으로 판단된 공격 트래픽을 대표적인 공격유형인 TCP-SYN flooding, UDP flooding, ICMP flooding으로 각각 분류하고, 침입 대응 시스템에 공격 유형에 대한 추가적인 정보를 제공한다.

<116> 또한, 공격 유형별로 분류되지 못한 공격 트래픽과 시스템에서 학습되지 않은 새로운 공격 유형을 별도의 클래스로 분류함으로써 실제 시스템의 유지 및 안정성을 보장한다.

<117> 프로토콜별 공격 유형을 분류함으로써, 전체 네트워크 시스템의 중지가 아닌 공격이 발생한 프로토콜에 대해서만 서비스의 제한 및 관리가 가능하기 때문에 안정적인 네트워크의 환경 유지와 시스템의 자원 관리 및 서비스를 보장할 수 있다.

<118> 마지막으로, 전술한 바와 같이, 트래픽 폭주 공격이 발생한 경우, 상기 서포트 벡터 데이터 명세를 기반으로 상기 트래픽 폭주 공격의 유형을 분류한다(S240).

<119> 한편, 상기 단계(S230)를 상술하기 위하여 우선, 단일 클래스 서포트 벡터 머신 기반의 공격 탐지에 대하여 상술하기로 한다.

<120> 통계적 학습 이론(Statistical learning theory)에 기반을 둔 서포트 벡터 머신(Support Vector Machine:SVM)은 주어진 문제를 항상 전역적 최적해가 보장되는 볼록 이차 방정식 문제(convex quadratic problem)로 변환하여 해를 구하기 때문에 패턴 인식 분야에서 매우 우수한 성능을 보인다.

<121> 그러나, 서포트 벡터 머신은 이진 분류기라는 기능적인 한계점으로 인하여 다중 분류 문제에는 서포트 벡터 머신을 직접적으로 적용할 수 없다.

<122> 따라서, 서포트 벡터 머신을 이용하여 다중 클래스 서포트 벡터 머신을 설계할 경우, 각 서포트 벡터 머신은 관측되지 않은 영역을 포함하여 결정 경계면을 생성함으로써, 새로운 데이터에 대하여 오분류(misclassification)

n)할 가능성이 높다.

<123> 그러므로, 해당 클래스만을 독립적으로 표현하는 단일 클래스 분류기로 결정 경계면을 선택하는 것이 더 유리하다.

<124> 따라서, 본 발명에서는 단일 클래스 서포트 벡터 머신의 대표적인 알고리즘인 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 기반으로 다중 클래스 서포트 벡터 머신을 수정하여 공격유형을 분류할 수 있는 시스템을 제공한다.

<125> d 차원 입력 공간 상에 존재하는 K 개의 데이터의 집합 $D_k = \{x_i^k \in R^d \mid i=1, \dots, N_k\}; k=1, \dots, K$ 이 주어졌을 경우, 각각의 클래스를 분류하기 위한 분류기는 각 클래스의 학습 데이터를 포함하면서 체적을 최소화하는 구체(Sphere)를 구하는 문제로 정의되며, 하기의 수학적 2에 의해 수식화된다.

수학적 2

$$\min L_0(R_k^2, a_k, \xi_k) = R_k^2 + C \sum_{i=1}^{N_k} \xi_i^k$$

$$s.t. \|x_i^k - a_k\|^2 \leq R_k^2 + \xi_i^k, \xi_i^k \geq 0, \forall i.$$

<126>

<127> 상기 수학적 2에서 a_k 는 k 번째 클래스를 표현하는 구체의 중심을 의미하고, R_k^2 은 구체 반경의 제곱을 의미하며, ξ_i^k 는 k 번째 클래스에 속한 i 번째 학습 데이터 x_i^k 가 구체에서 벗어나는 정도를 나타내는 벌점 항을 의미한다. 또한 C 는 상대적 중요성을 조정하는 트레이드 오프 상수(trade off constant)를 의미한다.

<128> 따라서, 수학적 2에 관한 쌍대 문제를 구하기 위하여 라그랑제 함수(Lagrange function) L 을 도입한다. 이를 수식으로 표현하면 하기의 수학적 3과 같다.

수학적 3

$$\begin{aligned} L(R_k^2, a_k, \xi_k, \alpha_k, \eta_k) \\ = R_k^2 + C \sum_{i=1}^{N_k} \xi_i^k \\ + \sum_{i=1}^{N_k} \alpha_i^k [(x_i^k - a_k)^T (x_i^k - a_k) - R_k^2 - \xi_i^k] \\ - \sum_{i=1}^{N_k} \eta_i^k \xi_i^k \\ \text{where, } \alpha_i^k \geq 0, \eta_i^k \geq 0, \forall i. \end{aligned}$$

<129>

<130> 상기 수학적 3에서 변수 R_k^2, a_k, ξ_k 에 대해서는 최소값을 가져야 하고, 변수 α_k, η_k 에 대해서는 최대값을 가져야 하므로, 아래의 수학적 4의 조건식을 만족하여야 한다.

수학식 4

$$\frac{\partial L}{\partial R_k^2} = 0: \sum_{i=1}^{N_k} a_i^k = 1.$$

$$\frac{\partial L}{\partial \xi_i^k} = 0: C - \alpha_i^k - \eta_i^k = 0 \therefore \alpha_i^k \in [0, C], \forall i.$$

$$\frac{\partial L}{\partial a_k} = 0: a_k = \sum_{i=1}^{N_k} \alpha_i^k x_i^k$$

<131>

<132> 상기 수학식 4를 라그랑제 함수 L 에 대입하면 하기의 수학식 5에 따라 쌍대 문제를 얻게 된다.

수학식 5

$$\min_{\alpha_k} \sum_{i=1}^{N_k} \sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k \langle x_i^k, x_j^k \rangle - \sum_{i=1}^{N_k} \alpha_i^k \langle x_i^k, x_i^k \rangle$$

$$s.t. \sum_{i=1}^{N_k} \alpha_i^k = 1, \alpha_i^k \in [0, C], \forall i$$

<133>

<134> 입력 공간에서 정의되는 구체는 매우 간단한 형태의 영역만을 나타낼 수 있다. 이러한 한계를 극복하기 위하여 커널 함수(kernel function) k 를 통하여 정의되는 고차원의 특징 공간(feature space) F 위에서 정의되는 구체를 사용하는 방법으로 확장될 수 있다.

<135> 각각의 클래스는 각각의 특징 공간에서 자신의 경계를 보다 정확하게 표현할 수 있으므로, 시스템의 학습은 각각의 클래스들이 매핑되는 특징 공간의 독립성을 고려하여 하기의 수학식 6에 따른 컨벡스 쿼드라틱 문제(convex quadratic problem)의 해답을 얻음으로써 이루어진다.

수학식 6

$$\min_{\alpha_k} \sum_{i=1}^{N_k} \sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k) - \sum_{i=1}^{N_k} \alpha_i^k k_k(x_i^k, x_i^k)$$

$$s.t. \sum_{i=1}^{N_k} \alpha_i^k = 1, \alpha_i^k \in [0, C], \forall i$$

<136>

<137> 특히 가우시안 커널을 사용할 경우, $k(x, x) = 1$ 이 성립하므로, 상기 수학식 6은 하기의 수학식 7과 같이 단순화할 수 있다.

수학식 7

$$\min_{\alpha_k} \sum_{i=1}^{N_k} \sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k)$$

$$s.t. \sum_{i=1}^{N_k} \alpha_i^k = 1, \alpha_i^k \in [0, C], \forall i.$$

<138>

<139> 한편, 학습 종료 후, 적용 과정에서 각각의 클래스의 결정함수는 하기의 수학식 8과 같이 정의된다.

수학식 8

$$f_k(x) = R_k^2 - \left[1 - 2 \sum_{i=1}^{N_k} \alpha_i^k k_k(x_i^k, x) + \sum_{i=1}^{N_k} \sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k) \right] \geq 0$$

<140>

<141> 상기 수학식 8을 기반으로 살펴보면, 서로 다른 특징 공간상에서 정의되는 단일 서포트 벡터 머신의 출력인 $f_k(x)$ 값은 각 클래스의 특징 공간 상의 경계로부터 해당 클래스 데이터와의 절대 거리를 의미함으로, 서로 다른 특징 공간상의 절대 거리를 비교하여 소속 클래스를 결정하는 것은 바람직하지 않다.

<142> 따라서, 특징 공간상의 절대 거리 $f_k(x)$ 를 특징 공간 상에서 정의되는 구형체의 반경 R_k 로 나눔으로써 상대적 거리 $\hat{f}_k(x) = f_k(x)/R_k$ 를 계산하고, 상대 거리가 가장 큰 클래스를 입력 데이터 x 의 소속 클래스로 결정한다.

수학식 9

Class of $x \equiv \arg \max_{k=1, \dots, K} \hat{f}_k(x)$

$$\equiv \arg \max_k \left[\left\{ R_k^2 - \left(1 - 2 \sum_{i=1}^{M_k} \alpha_i^k k_k(x_i^k, x) + \sum_{i=1}^{M_k} \sum_{j=1}^{M_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k) \right) \right\} / R_k \right]$$

<144> 도 3은 본 발명의 일 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치의 블록도를 도시한 것이다.

<145> 도 3을 참조하면, 본 발명의 일 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치는 관리 정보 베이스 추출부(310), 관리 정보 베이스 저장부(320), 공격 탐지부(330), 및 트래픽 폭주 공격 유형 분류부(340)로 구성될 수 있다.

<146> 우선, 관리 정보 베이스 추출부(310)는 관리 정보 베이스의 집합 중에서 트래픽 폭주 공격들을 적용하여 전수 조사를 수행하고, 상기 트래픽 폭주 공격들의 트래픽 폭주 공격에 반응하는 관리 정보 베이스를 추출한다.

<147> 즉, 관리 정보 베이스 추출부(310)는 RFC1213에서 정의한 MIB-2 그룹의 MIB 객체들 중에서, 실제 트래픽 폭주 공격에 반응하는 MIB 객체들만을 산정한다.

<148> 즉, MIB 객체의 산정을 위하여 트래픽 폭주 공격의 대표적인 공격들에 해당하는 Stacheldraht를 이용하여 TCP-SYN flooding 공격, UDP 플러딩 공격, ICMP 플러딩 공격 등을 타겟 시스템에 실시하고, MIB-2 그룹의 모든 MIB 객체들의 전수 조사를 실시한다. 본 발명에 적용되는 MIB 객체들을 정리하면, 상기의 표 1과 같다.

<149> 그리고, 관리 정보 베이스 저장부(320)는 상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집한다.

<150> 또한, 상기 추출된 관리 정보 베이스의 기 측정된 정보의 갱신 주기를 이용하여 상기 관리 정보 베이스의 다음의 갱신 주기를 예측하며, 상기 예측된 관리 정보 베이스의 갱신 주기에 상기 관리 정보 베이스의 정보를 수집한다.

<151> 단순 네트워크 관리 프로토콜 에이전트는 관리 정보 베이스 정보가 갱신된 시점으로부터 다음 갱신 시점까지는 동일한 관리 정보 베이스 값을 제공하기 때문에, 관리 정보 베이스 정보 갱신 시점 직후에 관리 정보 베이스의 정보를 수집하는 것이 보다 빠른 탐지를 위해 효과적이다.

<152> 따라서, 본 발명에서는 전술한 바와 같이 관리 정보 베이스의 정보의 갱신 시점을 결정하여 관리 정보 베이스의 정보를 수집한다.

<153> 우선, 갱신 주기의 탐지를 위하여 MIB-2 인터페이스 그룹의 *ifInOctets* MIB 값을 특정 시간 단위로 확인한다.

<154> 갱신 시점의 확인을 위해 매 초 단순 네트워크 관리 프로토콜의 메시지 발생에 따른 트래픽의 부하를 줄이기 위하여 본 발명에서는 상기의 수학식 1과 같이 갱신 주기 P_n 과 슬립 시간 S_n 을 결정한다.

<155> 상기 수학식 1에서 볼 수 있는 바와 같이, 현재까지의 갱신 주기 $\{U_0, U_1, U_2, \dots, U_{n-1}\}$ 와 갱신 주

기의 지수 평균을 이용하여 다음의 예측 갱신 주기 P^n 를 구하고, 이로부터 슬립 시간 S^n 을 결정하여 슬립함으로써 소비 트래픽과 관리 시스템의 부하 증가 문제를 해결할 수 있다. 여기서 상수 α 는 미리 설정된 시스템 파라미터로, 시스템 파라미터의 상수 α 값은 0.5로 설정할 수 있다.

- <156> 관리 정보 베이스의 갱신 주기는 단순 네트워크 관리 프로토콜 에이전트와 시스템에 따라 다르고, 같은 시스템이라고 할지라도 시간에 따라 변할 수 있기 때문에 각 갱신 주기에 대한 유동성을 고려한 지수 평균(exponential average) 값을 적용하여 보다 효율적으로 트래픽 탐지 시점을 결정할 수 있다.
- <157> 상기 수학적 식 1에서 U^n 은 실제 측정된 *iflnOctets* MIB 정보의 갱신 주기이며, 최초 갱신 주기인 U_0 는 시스템의 적용 전의 일정 시간 동안 매초 단순 네트워크 관리 프로토콜 메시지를 발생함으로써 측정한 갱신 주기들의 최소값으로 결정된다.
- <158> 공격 탐지부(330)는 서포트 벡터 머신(Support Vector Machine:SVM)의 서포트 벡터 데이터 명세(Support Vector Data Description:SVDD)를 이용하여 상기 수집된 관리 정보 베이스의 정보를 분석함으로써 트래픽 폭주 공격 여부의 탐지를 수행하고, 트래픽 폭주 공격 유형 분류부(340)는 상기 공격 탐지부(330)에서 탐지된 공격의 공격 유형을 분류한다.
- <159> 본 발명에 의하면, 서포트 벡터 데이터 명세 트레이닝을 통하여 트래픽 폭주 공격 발생에 대하여 공격의 탐지만 아니라, 공격의 유형까지 판단한다.
- <160> 여기서, 본 발명에 따른 트래픽 폭주 공격에 대한 트래픽 폭주 공격 탐지는 아래와 같이 수행된다.
- <161> 네트워크의 트래픽 정보 중에서 정상트래픽만으로 학습된 서포트 벡터 데이터 명세로 정상트래픽과 공격트래픽에 대한 실시간 탐지를 보장하며, 점증적인 갱신도 가능하다.
- <162> 또한, 학습시에 정상 트래픽만을 요구함으로써 학습을 위한 별도의 공격 트래픽을 준비할 필요가 없으며, 학습 속도 또한 다른 서포트 벡터 머신에 비해 상대적으로 빠르다.
- <163> 학습된 단일 클래스의 서포트 벡터 머신은 비정상 탐지 모델로 시스템에서 학습되지 않은 새로운 공격을 탐지하면, 공격 트래픽이 탐지되면, 공격 대응 시스템에 침입 사실을 실시간으로 보고한다.
- <164> 또한, 본 발명에 따른 탐지된 트래픽 폭주 공격에 대한 트래픽 공격의 유형 분류는 아래와 같이 수행된다.
- <165> 다중 클래스의 서포트 벡터 머신의 구조로 트래픽 폭주 공격으로 판단된 공격 트래픽을 대표적인 공격유형인 TCP-SYN flooding, UDP flooding, ICMP flooding으로 각각 분류하고, 침입 대응 시스템에 공격 유형에 대한 추가적인 정보를 제공한다.
- <166> 또한, 공격 유형별로 분류되지 못한 공격 트래픽과 시스템에서 학습되지 않은 새로운 공격 유형을 별도의 클래스로 분류함으로써 실제 시스템의 유지 및 안정성을 보장한다.
- <167> 한편, 본 발명의 다른 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치는 도 4와 같다.
- <168> 즉, 1개의 오프라인 처리부인 서포트 벡터 데이터 명세 트레이닝부(미도시)를 추가적으로 구성하여 트래픽 공격 탐지를 위하여 서포트 벡터 데이터 명세를 트레이닝하고, 3개의 온라인 처리부인 관리 정보 베이스 추출부(410), 관리 정보 베이스 저장부(420), 공격 탐지부(430)를 구성할 수 있다.
- <169> 우선, 관리 정보 베이스 추출부(410)는 다양한 트래픽 공격을 임의로 발생시켜 수집된 관리 정보 베이스의 정보를 바탕으로 서포트 벡터 데이터 명세 기반의 학습을 실시한다.
- <170> 그리고, 관리 정보 베이스 저장부(420)는 *iflnOctets* MIB를 수집하여 트래픽 폭주 공격 탐지 장치의 동작 시점을 결정한다.
- <171> 여기서, 관리 정보 베이스의 정보의 수집을 위하여 단순 네트워크 관리 프로토콜의 GetRequest 메시지를 사용하고, 하나의 메시지에 12개의 관리 정보 베이스의 정보를 모두 포함시킴으로써 트래픽 사용량을 최소화한다.
- <172> 한편, 수집된 정보는 공격 탐지부(430)로 전달됨으로써, 트래픽 폭주 공격의 유무를 판단할 수 있고, 더 나아가

공격 유형 분류부(440)에서 공격 유형을 판단할 수 있다.

- <173> 여기서, 공격 탐지부(430)는 네트워크의 트래픽 정보 중에서 정상트래픽만으로 학습된 서포트 벡터 데이터 명세로 정상트래픽과 공격트래픽에 대한 실시간 탐지를 보장하며, 점증적인 갱신도 가능하다.
- <174> 또한, 학습시에 정상 트래픽만을 요구함으로써 학습을 위한 별도의 공격 트래픽을 준비할 필요가 없으며, 학습 속도 또한 다른 서포트 벡터 머신에 비해 상대적으로 빠르다.
- <175> 학습된 단일 클래스의 서포트 벡터 머신은 비정상 탐지 모델로 시스템에서 학습되지 않은 새로운 공격을 탐지함으로써 공격 트래픽이 탐지되면, 방어 기작 수행부(450)에 침입 사실을 실시간으로 보고한다.
- <176> 트래픽 폭주 공격 유형 분류부(440)는 다중 클래스의 서포트 벡터 머신의 구조로 트래픽 폭주 공격으로 판단된 공격 트래픽을 대표적인 공격유형인 TCP-SYN flooding(441), UDP flooding(442), ICMP flooding(443)으로 각각 분류하고, 방어 기작 수행부(450)에 공격 유형에 대한 추가적인 정보를 제공한다.
- <177> 또한, 공격 유형별로 분류되지 못한 공격 트래픽과 시스템에서 학습되지 않은 새로운 공격 유형을 별도의 새로운 클래스(449)로 분류함으로써 실제 시스템의 유지 및 안정성을 보장한다.
- <178> 더욱이, 전략 설정부(460)에서는 상기 방어 기작 수행부(450)과 연결되어 상기 방어 기작 수행부(450)의 방어 기작을 저장하여 방어 기작 알고리즘을 업데이트한다.
- <179> 이와 같이, 프로토콜별 공격 유형을 분류함으로써, 전체 네트워크 시스템의 중지가 아닌 공격이 발생한 프로토콜에 대해서만 서비스의 제한 및 관리가 가능하기 때문에 안정적인 네트워크의 환경 유지와 시스템의 자원 관리 및 서비스를 보장할 수 있다.
- <180> 본 발명에서 제시한 트래픽 폭주 공격의 탐지의 성능 평가를 위하여 도 5와 같이 실험 환경을 구축하였다.
- <181> 트래픽 폭주 공격 실험을 위하여 하나의 L2 스위치 장비에 타겟 시스템(Victim)을 연결하고, 분산 서비스 거부 공격 환경을 만들기 위하여 2대의 공격 에이전트(Attack agent)와 1대의 공격 핸들러(Attack handler)를 L2 스위치 장비에 연결하였다.
- <182> 또한, 타겟 시스템으로부터 관리 정보 베이스의 정보의 수집 및 탐지를 위하여 1대의 탐지 시스템을 L2 스위치에 연결하였다.
- <183> L2 스위치는 학내 네트워크를 통하여 인터넷과 연결되어 있기 때문에 타겟 시스템에서는 다양한 인터넷 트래픽이 생성된다.
- <184> 실제로, 타겟 시스템에 아파치 웹 서버(Apache Web Server), VNC 서버, FTP 서버, SSH 서버, 썸바 서버(Samba Server) 등의 다양한 서버를 운영함으로써, 다양한 종류의 정상 트래픽을 발생하였다.
- <185> 본 실시예에서 사용된 시스템은 모두 리눅스 페도라(Linux Fedora) 7 또는 8이며, 타겟 시스템의 단순 네트워크 관리 에이전트는 Net-SNMP v5.4.1이 사용되었다.
- <186> 본 실시예에서 사용한 트래픽 폭주 공격의 대표적 공격 툴인 Stacheldraht는 다른 트래픽 폭주 공격 툴인 Trinoo, TFN, TFN2K에 비하여 공격방법 및 형태가 더욱 발전되고 견고해진 툴로써, 트래픽 폭주 공격 시 반응을 보였던 MIB 정보인 tcpInErrs와 udpNoPorts에 대하여 반응을 보이지 않았다.
- <187> 이는 Stacheldraht가 트래픽 폭주 공격의 대상이 되는 클라이언트의 포트를 미리 스캔한 후 공격트래픽에 사용 가능한 포트번호로 할당하고, TCP 세그먼트의 체크 합(check sum) 값을 정상적인 값으로 위장하기 때문이다.
- <188> 본 실시예에서는 실험 결과의 정확도 및 실시간 탐지 성능 분석을 위하여 리눅스 상에서 동작하는 Net-SNMP 에이전트의 SNMP MIB 정보 갱신 주기인 15초 단위로 상기의 표 3에서와 같이 Interface, ip, tcp, udp, icmp 그룹에서 선정된 12개의 MIB 객체 정보를 수집하였다. 본 실시예에서 사용한 데이터는 정상트래픽 1,000개와 공격 트래픽별 TCP-SYN flooding, UDP flooding, ICMP flooding을 각각 200개씩 생성하여 실험하였다.
- <189> 첫 번째 실시예는 정상 트래픽과 공격트래픽을 신속하게 탐지하는 것으로 정상트래픽 600개만으로 SVDD를 학습하였고, 테스트를 위하여 정상트래픽은 400개, 공격트래픽은 유형별로 50개씩 랜덤하게 추출하여 테스트하였다. 성능 측정을 위하여 침입 탐지율(Detection Rate), False Positive Rate(FPR) 및 False Negative Rate(FNR)을 성능지표로 사용했으며 그 결과는 하기의 표3과 같다. 여기서 조정상수 C는 0.1, 커널 함수인 가우시안 함수의 상수 값은 0.02로 고정하였다.

한편, 침입 탐지율은 하기의 수학식 10에, 폴스 포지티브 비율인 FPR은 하기의 수학식 11에, 폴스 네가티브 비율인 FNR은 하기의 수학식 12와 같이 연산되어 진다.

수학식 10

$$\text{침입 탐지율} = \frac{\sum_{i=1}^n T_i}{\sum_{i=1}^n I_i}$$

수학식 11

$$FPR = \frac{\sum_{i=1}^n P_i}{\sum_{i=1}^n N_i}$$

수학식 12

$$FNR = \frac{\sum_{i=1}^n F_i}{\sum_{i=1}^n I_i}$$

상기 수학식 10, 수학식 11, 수학식 12에서 I 는 공격 트래픽, T 는 공격 트래픽을 정확히 공격으로 분류한 트래픽, N 은 정상 트래픽, P 는 정상트래픽을 공격으로 분류한 트래픽, F 는 공격 트래픽을 정상으로 판단한 트래픽을 의미한다.

표 3

항목 σ	침입 탐지율	FPR	FNR
0.02	99.33	2.5	0.67

표 3의 성능 평가를 위한 항목 중 FPR은 정상트래픽을 공격트래픽으로 오 판정한 비율을 나타내며 이는 시스템에 큰 영향을 미치지 않지만, FNR은 공격트래픽을 정상트래픽으로 판단하는 비율로써 보안상 커다란 문제점을 야기하는 매우 중요한 지표이다. 첫 번째 실시예의 결과에 의하면, σ 값이 0.02일 때 모두 만족스러운 침입 탐지율과 안전한 FNR(0.67)을 보여줌을 확인할 수 있었다.

두 번째 실시예는 트래픽 폭주 공격의 대표적 공격유형인 TCP-SYN flooding, UDP flooding, ICMP flooding으로 분류하는 실험으로써 공격유형별로 랜덤하게 150개씩 각각의 SVDD로 학습하였으며, 학습에 참여하지 않은 공격유형별 트래픽 50개로 테스트 하였다. 이때 150개의 공격트래픽 중 TCP-SYN flooding 공격트래픽 1개가 정상트래픽으로 분류되어 실제 분류 테스트에 참여한 공격트래픽은 총 149개이다. 성능 측정을 위하여 분류 정확도(Classification Accuracy)를 성능지표로 사용했으며 그 결과는 표 4에 정리하였다. 여기서 조정상수 C는 0.1,

커널 함수인 가우시안 함수의 상수 σ 값은 TCP는 0.4, UDP는 0.3, ICMP는 0.1로 각각 고정하였다.

한편, 여기서, 상기 분류 정확도는 하기의 수학식 13로 표현된다.

수학식 13

$$\text{분류정확도} = \frac{\sum_{i=1}^n T_i}{\sum_{i=1}^n I_i}$$

상기 수학식 13에서 I 는 해당 클래스의 트래픽 총 갯수, T 는 해당 클래스의 공격 트래픽을 정확히 해당 클래스의 공격으로 분류한 갯수를 의미한다.

표 4

분류정확도 (항목별) σ	TCP-SYN flooding	UDP flooding	ICMP flooding	전체 분류정확도
TCP(0.4) UDP(0.3) ICMP(0.1)	93.88	100.0	98.0	97.32

상기 표 4의 3가지 공격 유형별로 σ 값이 (TCP: 0.4, UDP: 0.3, ICMP: 0.1)일 때 전체 분류 정확도에서 만족스러운 성능을 보이고 있음을 확인하였으며, 정확히 분류하지 못한 TCP SYN flooding 공격트래픽 3개 중 2개는 TCP flooding 클래스로 분류되었으며 1개는 어떤 클래스에도 속하지 않는 공격유형의 클래스로 분류되었다. 또한 정확히 분류하지 못한 ICMP flooding 공격트래픽 1개는 TCP flooding 클래스로 분류됨을 확인할 수 있었다.

본 발명에서는 기존의 패킷 수집을 통한 트래픽 폭주 공격 탐지 시 고성능 분석시스템의 요구 및 실시간 탐지가 어렵다는 단점을 보완하는 차원에서 SVDD를 기반으로 한 계층적 구조의 새로운 침입탐지 시스템을 제안하였다. 제안된 모델은 실시간 처리를 위하여 15초 단위의 SNMP MIB 정보를 이용하여 저비용 및 실시간 탐지, 시스템에서 학습되지 않은 새로운 공격유형의 발견, 쉬운 확장성 및 프로토콜별 분류탐지로 인한 원활한 네트워크 시스템의 자원관리와 안전성 확보에 기여하였다.

한편, 본 발명의 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법은 소프트웨어를 통해 실행될 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다. 그러나, 이와 같은 변형은 본 발명의 기술적 보호범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

도면의 간단한 설명

도 1은 특정의 시스템에서 MIB-2 인터페이스 그룹의 옥텟(Octets) 값을 도시한 그래프이다.

도 2는 본 발명의 일 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 방법의 흐름도이다.

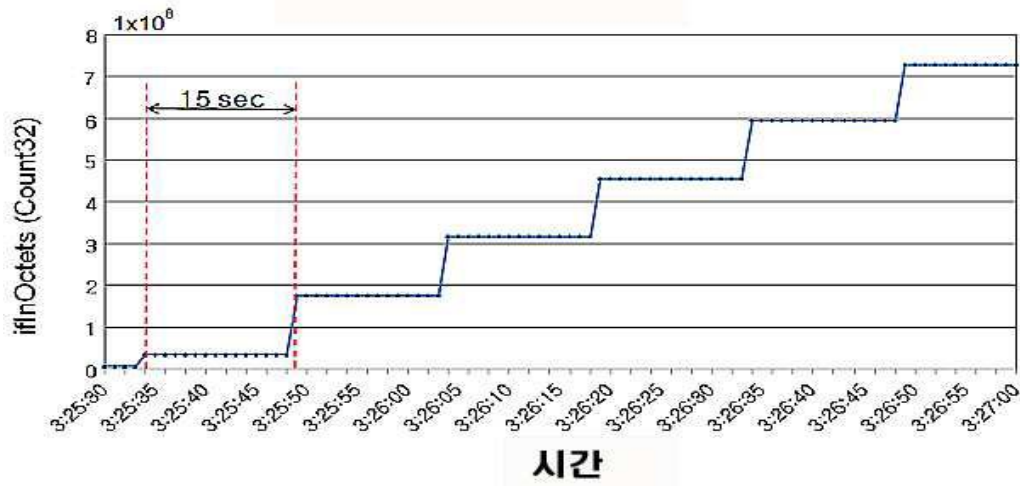
도 3은 본 발명의 일 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치의 블록도를 도시한 것이다.

<210> 도 4는 본 발명의 다른 실시예에 따른 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지 장치의 블록도를 도시한 것이다.

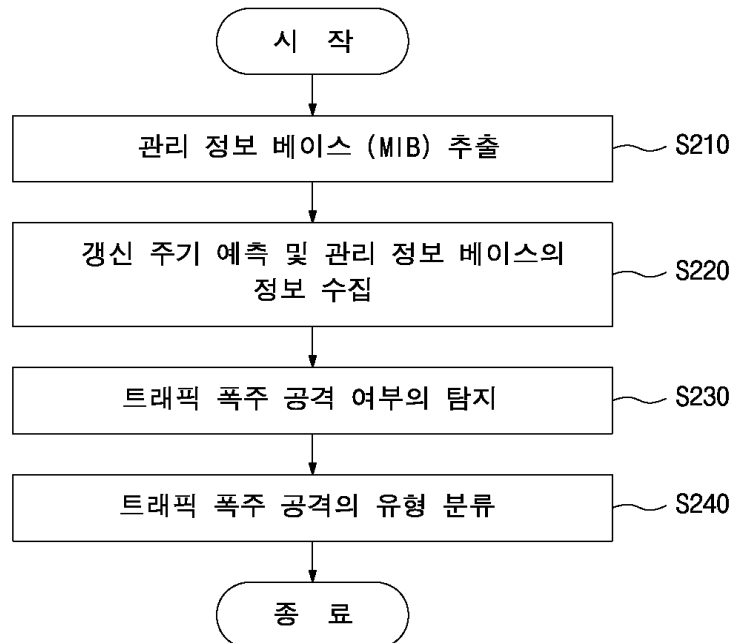
<211> 도 5는 본 발명의 서포트 벡터 데이터 명세를 이용한 트래픽 폭주 공격 탐지의 성능 평가를 위해 구축된 성능평가 시스템을 도시한 것이다.

도면

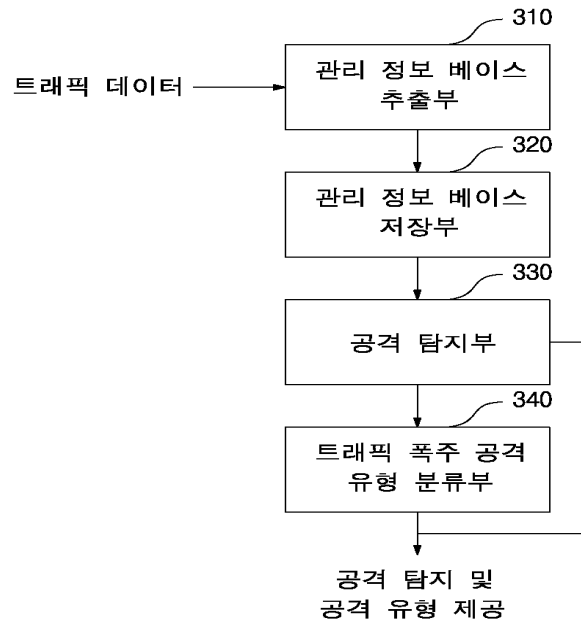
도면1



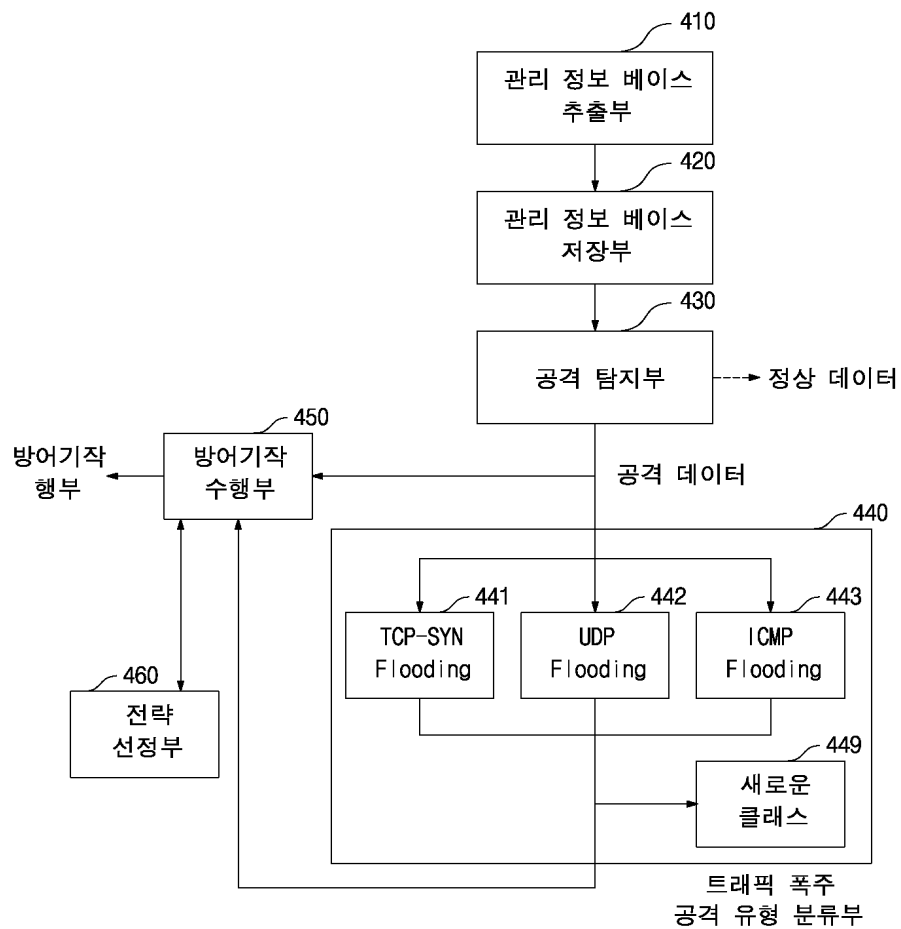
도면2



도면3



도면4



도면5

