(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0117542
(43) 공개일자 2009년11월12일

(51) Int. Cl.
H04L 12/26 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2008-0043643
(22) 출원일자 2008년05월09일
심사청구일자 2008년05월09일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
김명섭
충청남도 연기군 조치원읍 신흥리 푸르지오1차 107-401
박준상
전라남도 무안군 현경면 수양리 783
(74) 대리인
송경근

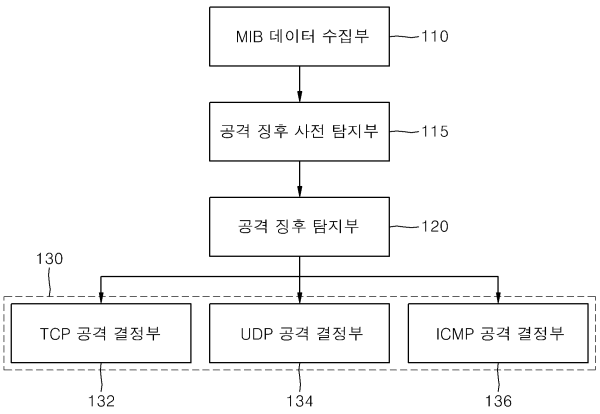
전체 청구항 수 : 총 17 항

(54) SNMP 기반의 트래픽 공격 탐지 장치 및 방법

(57) 요 약

SNMP 기반의 트래픽 공격 탐지 장치 및 방법이 개시된다. MIB 데이터 수집부는 네트워크 단말장치로부터 일정한 주기로 SNMP의 MIB 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집한다. 공격 징후 탐지부는 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정한다. 공격 유형 결정부는 공격성 트래픽으로 결정된 네트워크 트래픽에 대하여 MIB 데이터 값에 의해 파악된 프로토콜별 객체 값의 변화에 따라 트래픽 폭주 공격의 종류를 결정한다. 본 발명에 따르면, 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 선택하여 수집하고, MIB 데이터 값에 기초하여 정상 트래픽과 공격성 트래픽을 구분함으로써, 폴링(polling)에 의한 시스템의 부하를 줄이고 정확하게 트래픽 폭주 공격을 탐지할 수 있다. 또한 MIB 데이터의 갱신 주기를 예측하여 그에 따라 MIB 데이터를 수집함으로써, 트래픽 폭주 공격의 탐지 시간을 줄일 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	KRF-2007-331-D00387
부처명	한국학술진흥재단
연구사업명	신진교수연구지원
연구과제명	인터넷 트래픽 응용레벨 분석 방법에 관한 연구
주관기관	고려대학교 산학협력단
연구기간	2007년08월01일~2008년07월31일

특허청구의 범위

청구항 1

네트워크 단말장치로부터 일정한 주기로 간이 망관리 프로토콜(simple network management protocol : SNMP)의 관리 정보 베이스(management information base : MIB) 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집하는 MIB 데이터 수집부;

상기 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 상기 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 징후 탐지부; 및

공격성 트래픽으로 결정된 상기 네트워크 트래픽에 대하여 상기 MIB 데이터 값에 의해 파악된 프로토콜별 객체값(object identifier : OID)의 변화에 따라 상기 트래픽 폭주 공격의 종류를 결정하는 공격 유형 결정부;를 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 2

제 1항에 있어서,

상기 MIB 데이터 수집부는 상기 수집된 MIB 데이터 값에 의해 파악되는 옥텟의 총 수신 개수(ifInOctets)가 변화되는 시간 간격을 기초로 예측한 상기 MIB 데이터의 갱신 주기에 따라 상기 MIB 데이터를 수집하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 3

제 2항에 있어서,

상기 MIB 데이터의 갱신 주기는 다음의 수학식에 의해 예측되는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치:

$$U_{n+1}=\frac{1}{2}U_n+\frac{1}{2}A_{n-1}\text{-}1$$

여기서, U_{n+1}은 n+1번째 갱신 주기, U_n은 n번째 갱신 시점에서 예측한 n+1번째 갱신 시점까지의 갱신 주기, 그리고 A_{n-1}은 최초 갱신 시점부터 n번째 갱신 시점까지의 갱신 주기에 대한 지수 평균이다.

청구항 4

제 1항에 있어서,

상기 공격 징후 탐지부는 상기 MIB 데이터 값에 의해 파악된 수신된 데이터그램에 대한 응답률이 사전에 설정된 기준 응답률보다 작은 경우 또는 파기된 송신 데이터그램 수(ipOutDiscards)가 증가한 경우에 상기 네트워크 트래픽을 공격성 트래픽으로 결정하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 5

제 1항 또는 제 4항에 있어서,

단위 시간당 수신 데이터의 양이 사전에 설정된 기준값보다 크면 상기 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 징후 사전 탐지부를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 6

제 1항에 있어서,

상기 공격 유형 결정부는,

상기 MIB 데이터 값에 의해 파악된 접속 실패 횟수(tcpAttamptFail) 또는 RST 플래그를 포함한 송신 세그먼트 수(tcpOutRsts)가 변경된 경우에는 상기 트래픽 폭주 공격을 TCP-SYN Flooding 공격으로 결정하는 TCP 공격 결정부를 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 7

제 6항에 있어서,

상기 공격 유형 결정부는,

상기 MIB 데이터 값에 의해 파악된 에러가 된 수신 데이터그램 수(udpInErrs)가 증가한 경우, 또는 도달 불능의 송신 수(icmpOutdestUnreachs) 및 ICMP 메세지의 전체 송신 수(icmpOutMsgs)의 증가량이 일치하고 도달 불능의 수신 수(icmpIndestUnreachs)가 0인 경우에는 상기 트래픽 폭주 공격을 UDP Flooding 공격으로 결정하는 UDP 공격 결정부를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 8

제 6항 또는 제 7항에 있어서,

상기 공격 유형 결정부는,

상기 MIB 데이터 값에 의해 파악된 ICMP 메세지의 전체 수신 수(icmpInMsgs) 또는 ICMP 반향 요청 수(icmpInEchos)가 증가한 경우, 또는 도달 불능의 수신 수(icmpInDestUnreachs), 도달 불능의 송신 수(icmpOutDestUnreachs), ICMP 반향 응답 메세지 수(icmpInEchoReps) 및 파기된 송신 데이터그램 수가 증가한 경우에는 상기 트래픽 폭주 공격을 ICMP Flooding 공격으로 결정하는 ICMP 공격 결정부를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 장치.

청구항 9

네트워크 단말장치로부터 일정한 주기로 간이 망관리 프로토콜(simple network management protocol : SNMP)의 관리 정보 베이스(management information base : MIB) 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집하는 MIB 데이터 수집 단계;

상기 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 상기 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 징후 탐지 단계; 및

공격성 트래픽으로 결정된 상기 네트워크 트래픽에 대하여 상기 MIB 데이터 값에 의해 파악된 프로토콜별 객체값(object identifier : OID)의 변화에 따라 상기 트래픽 폭주 공격의 종류를 결정하는 공격 유형 결정 단계;를 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 10

제 9항에 있어서,

상기 MIB 데이터 수집 단계에서, 상기 수집된 MIB 데이터 값에 의해 파악되는 옥텟의 총 수신 개수(ifInOctets)가 변화되는 시간 간격을 기초로 예측한 상기 MIB 데이터의 갱신 주기에 따라 상기 MIB 데이터를 수집하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 11

제 10항에 있어서,

상기 MIB 데이터의 갱신 주기는 다음의 수학식에 의해 예측되는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법:

$$U_{n+1}=\frac{1}{2}U_n+\frac{1}{2}A_{n-1}-1$$

여기서, U_{n+1}은 n+1번째 갱신 주기, U_n은 n번째 갱신 시점에서 예측한 n+1번째 갱신 시점까지의 갱신 주기, 그리고 A_{n-1}은 최초 갱신 시점부터 n번째 갱신 시점까지의 갱신 주기에 대한 지수 평균이다.

청구항 12

제 9항에 있어서,

상기 공격 징후 탐지 단계에서, 상기 MIB 데이터 값에 의해 파악된 수신된 데이터그램에 대한 응답률이 사전에 설정된 기준 응답률보다 작은 경우, 또는 파기된 송신 데이터그램 수(ipOutDiscards)가 증가한 경우에 상기 네트워크 트래픽을 공격성 트래픽으로 결정하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 13

제 9항 또는 제 12항에 있어서,

단위 시간당 수신 데이터의 양이 사전에 설정된 기준값보다 크면 상기 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 징후 사전 탐지 단계를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 14

제 9항에 있어서,

상기 공격 유형 결정 단계는,

상기 MIB 데이터 값에 의해 파악된 접속 실패 횟수(tcpAttamptFail) 또는 RST 플래그를 포함한 송신 세그먼트 수(tcpOutRsts)가 변경된 경우에는 상기 트래픽 폭주 공격을 TCP-SYN Flooding 공격으로 결정하는 TCP 공격 결정 단계를 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 15

제 14항에 있어서,

상기 공격 유형 결정 단계는,

상기 MIB 데이터 값에 의해 파악된 에러가 된 수신 데이터그램 수(udpInErrs)가 증가한 경우, 또는 도달 불능의 송신 수(icmpOutdestUnreachs) 및 ICMP 메세지의 전체 송신 수(icmpOutMsgs)의 증가량이 일치하고 도달 불능의 수신 수(icmpIndestUnreachs)가 0인 경우에는 상기 트래픽 폭주 공격을 UDP Flooding 공격으로 결정하는 UDP 공격 결정 단계를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 16

제 14항 또는 제 15항에 있어서,

상기 공격 유형 결정 단계는,

상기 MIB 데이터 값에 의해 파악된 ICMP 메세지의 전체 수신 수(icmpInMsgs) 또는 ICMP 반향 요청 수(icmpInEchos)가 증가한 경우, 또는 도달 불능의 수신 수(icmpInDestUnreachs), 도달 불능의 송신 수(icmpOutDestUnreachs), ICMP 반향 응답 메세지 수(icmpInEchoReps) 및 파기된 송신 데이터그램 수가 증가한 경우에는 상기 트래픽 폭주 공격을 ICMP Flooding 공격으로 결정하는 ICMP 공격 결정 단계를 더 포함하는 것을 특징으로 하는 SNMP 기반의 트래픽 공격 탐지 방법.

청구항 17

제 8항 내지 제 13항 중 어느 한 항에 기재된 SNMP 기반의 트래픽 공격 탐지 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 SNMP 기반의 트래픽 공격 탐지 장치 및 방법에 관한 것으로, 보다 상세하게는, SNMP의 MIB 데이터를 이용하여 네트워크 단말장치에 대한 트래픽 폭주 공격을 탐지할 수 있는 장치 및 방법에 관한 것이다.

배 경 기 술

<2> 최근 급속도로 발전한 인터넷 기술로 인하여 사용자들은 네트워크를 통한 다양하고 빠른 서비스를 제공받을 수

있게 되었다. 이와 같이 네트워크를 기반으로 하는 서비스에 대한 의존도가 증가하면서 안전한 네트워크 및 서비스의 제공을 위해 유해 트래픽 탐지 및 차단에 대한 중요성이 증대되었다.

<3> 서비스 거부(denial of service : DoS) 공격으로 대표되는 유해 트래픽인 트래픽 폭주 공격은 네트워크 대역폭, 프로세스 처리 능력 또는 기타 시스템 자원을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격 형태이다. DoS 공격은 한 사용자가 시스템의 리소스를 독점하거나 파괴하여 다른 사용자들에게 올바른 서비스를 제공하지 못하게 하는 것을 말한다. 이러한 DoS 공격은 루트 권한의 획득 또는 시스템이나 사용자 데이터의 파괴 및 변조와 같이 시스템에 치명적인 문제를 일으키지는 않으나, 네트워크나 시스템 서비스에 마비를 일으켜 시스템의 정상적인 수행에 문제를 일으킨다. 또한 DoS 공격을 보다 효과적이며 강력하게 하기 위한 방법인 분산 서비스 거부(Distributed DoS : DDoS) 공격은 수많은 DoS 공격이 한 사람의 공격자에 의해 동시에 일어나게 하는 공격 형태이다. DDoS 공격에서는 공격자가 네트워크로 연결되어 있는 많은 수의 호스트들의 패킷을 범람시킬 수 있는 DoS 공격용 프로그램을 분산 설치하여 이들이 서로 통합된 형태로 공격 대상 시스템에 대해 성능 저하 및 시스템 마비를 일으킨다. 이러한 DoS/DDoS 공격은 공격의 유형을 알 수 없고, 공격시 사용되는 명령들이 암호화되어 있어 공격의 근원지를 추적하는 것도 불가능하다.

<4> DoS/DDoS 공격을 탐지하기 위하여 사용되었던 기존의 방법 중 하나인 패킷 기반의 탐지 시스템은 라우터나 호스트에서 패킷을 검사하고 일정한 시간 간격으로 카운팅하여 특정 포트에서 평균치에 비해 많은 카운팅이 발생하면 이를 위험 신호로 판단하는 방법이다. 이러한 패킷 분석 기반의 트래픽 폭주 공격 탐지 시스템은 고가의 고성능 시스템을 요구하기 때문에 소규모의 네트워크에서 사용하기에는 부적합하며, 시스템의 설치 및 운영의 확장성이 부족하다.

<5> 트래픽 폭주 공격을 탐지하기 위한 다른 방법으로 사용되는 간이 망관리 프로토콜(simple network management protocol : SNMP) 기반의 탐지 방법에서는 트래픽 추이와 프로토콜별 비율 및 공격에 특정한 반응을 보이는 관리 정보 베이스(management information base : MIB)를 이용하여 공격을 탐지한다. 이러한 탐지 방법은 MIB 데이터의 정확한 갱신 주기를 고려하지 않으므로 탐지가 이루어지는 시점의 MIB 데이터의 값을 정확하게 수집하지 못하여 탐지의 정확성이 떨어지는 문제점을 가진다. 또한 사용자나 시스템의 용도가 바뀌게 되면 기준값을 재설정해야하며, 다양해진 공격 방법과 견고해진 공격 도구에 적절히 대응할 수 없다는 문제점도 있다.

발명의 내용

해결 하고자하는 과제

<6> 본 발명이 이루고자 하는 기술적 과제는, 탐지 시간 및 시스템의 부하를 줄이고, 트래픽 폭주 공격을 정확하게 탐지할 수 있는 SNMP 기반의 트래픽 공격 탐지 장치 및 방법을 제공하는 데 있다.

<7> 본 발명이 이루고자 하는 다른 기술적 과제는, 탐지 시간 및 시스템의 부하를 줄이고, 트래픽 폭주 공격을 정확하게 탐지할 수 있는 SNMP 기반의 트래픽 공격 탐지 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.

과제 해결수단

<8> 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치는, 네트워크 단말장치로부터 일정한 주기로 간이 망관리 프로토콜(simple network management protocol : SNMP)의 관리 정보 베이스(management information base : MIB) 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집하는 MIB 데이터 수집부; 상기 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 상기 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 징후 탐지부; 및 공격성 트래픽으로 결정된 상기 네트워크 트래픽에 대하여 상기 MIB 데이터 값에 의해 파악된 프로토콜별 객체 값(object identifier : OID)의 변화에 따라 상기 트래픽 폭주 공격의 종류를 결정하는 공격 유형 결정부;를 구비한다.

<9> 상기의 다른 기술적 과제를 달성하기 위한, 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 방법은, 네트워크 단말장치로부터 일정한 주기로 간이 망관리 프로토콜(simple network management protocol : SNMP)의 관리 정보 베이스(management information base : MIB) 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집하는 MIB 데이터 수집 단계; 상기 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 상기 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정하는 공격 탐지 단계; 및 공격성 트래픽으로 결정된 상기 네트워크 트래픽에 대하여 상기 MIB 데이터 값에 의해

파악된 프로토콜별 객체 값(object identifier : OID)의 변화에 따라 상기 트래픽 폭주 공격의 종류를 결정하는 공격 유형 결정 단계;를 갖는다.

효 과

<10> 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치 및 방법에 의하면, 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 선택하여 수집하고, MIB 데이터 값에 기초하여 정상 트래픽과 공격성 트래픽을 구분함으로써, 폴링(polling)에 의한 시스템의 부하를 줄이고 정확하게 트래픽 폭주 공격을 탐지할 수 있다. 또한 MIB 데이터의 갱신 주기를 예측하여 그에 따라 MIB 데이터를 수집함으로써, 트래픽 폭주 공격의 탐지 시간을 줄일 수 있다.

발명의 실시를 위한 구체적인 내용

<11> 이하에서 첨부된 도면들을 참조하여 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치 및 방법의 바람직한 실시예에 대해 상세하게 설명한다.

<12> 도 1은 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치에 대한 바람직한 실시예의 구성을 도시한 블록도이다.

<13> 도 1을 참조하면, 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치는, MIB 데이터 수집부(110), 공격 징후 탐지부(120) 및 공격 유형 결정부(130)를 구비하며, 공격 징후 사전 탐지부(115)를 더 구비할 수 있다.

<14> MIB 데이터 수집부(110)는 네트워크 단말장치로부터 일정한 주기로 간이 망관리 프로토콜(simple network management protocol : SNMP)의 관리 정보 베이스(management information base : MIB) 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집한다.

<15> SNMP는 네트워크 관리를 위해 사용되는 프로토콜로서, 네트워크 시스템에 접속되는 기기 또는 서비스의 가동 상황, 시스템 성능, 네트워크 트래픽, 시스템 로그에 기록되는 특정 메시지 또는 시스템 로그의 급격한 증가 및 감소를 감시한다. SNMP는 관리 대상이 되는 시스템에 설치되어 필요한 정보를 수집하는 에이전트(agent)와 에이전트가 설치된 시스템에 관리를 위해 필요한 정보를 요청하는 관리자(manager)로 구성된다. SNMP 관리자와 에이전트는 관리자가 에이전트에 감시 대상 시스템의 정보를 요구하고 에이전트가 정보를 취득하여 응답하는 기능, 관리자가 감시 대상 시스템을 요구하고 에이전트가 이를 실행하여 응답하는 기능, 그리고 에이전트가 관리자에게 감시 대상 시스템의 상태 변화를 통지하는 기능을 수행한다. SNMP 에이전트는 네트워크에 연결된 모든 노드에 기본적으로 설치되어 있고, 네트워크 관리를 위한 표준화된 정보를 제공하기 때문에 특별한 설치가 없이도 탐지를 위한 데이터 수집이 가능하다. 따라서 패킷 분석 기반의 탐지 시스템에 비하여 탐지 시스템의 설치 및 운영을 위해 고가의 고성능 시스템이 요구되지 않기 때문에 확장성이 뛰어나다.

<16> 이때 에이전트가 감시 대상 시스템의 정보를 취득하는 과정은 MIB 데이터를 참조하여 이루어진다. MIB는 SNMP를 이용하여 관리될 객체의 분류된 정보를 말하며, 관리되어야 할 객체는 시스템 정보, 네트워크 사용량, 네트워크 인터페이스 정보 등이다. MIB들은 관리가 용이하도록 트리(tree) 구조를 가지며, 각각 객체 ID(OID)라는 식별자가 할당되어 있다. OID는 [1.3.6.1.2.1.1.6]과 같이 계층적으로 표현되고, 관리자는 에이전트에 대하여 OID를 지정하여 감시 대상 시스템의 정보 취득이나 설정 변경을 요구하게 된다. 그러나 모든 시스템이 고유의 MIB를 가지고 있는 것은 아니며, 감시 대상 시스템이 모두 다른 MIB를 구현한다면 SNMP 관리자는 취득하는 MIB 데이터의 OID를 모르기 때문에 모든 대상 시스템의 MIB 파일을 참조해야 한다. 이러한 문제를 해결하기 위해 TCP/IP에 의한 네트워크 시스템에 접속되는 기기가 구현해야 하는 MIB가 표준 MIB로서 RFC에 정의되어 있다. 현재 정의되어 있는 가장 표준적인 MIB는 'MIB-Ⅱ'이고, 관리 대상 객체가 11개의 그룹으로 분류되어 있다.

<17> MIB 데이터 수집부(110)는 이와 같은 OID를 이용하여 감시 대상인 네트워크 단말장치로부터 트래픽 폭주 공격의 탐지에 필요한 MIB 데이터를 수집할 수 있다. 수집되는 MIB 데이터는 트래픽 폭주 공격에 의해 그 값이 변화되는 데이터이며, 이러한 MIB 데이터들은 각각의 트래픽 폭주 공격에 대한 전수 조사를 통해 선정된다. 즉, 일정 기간 동안 모든 MIB 데이터를 정상 트래픽이 발생할 때의 값과 공격성 트래픽이 발생할 때의 값으로 구분하여 조사한 후, 각각의 트래픽 폭주 공격에 대해 그 값이 변화하는 MIB 데이터를 선정한다. 11개의 그룹으로 나누어진 MIB 데이터들 중 본 발명에 따른 트래픽 공격 탐지 장치의 실시에 사용되는 MIB 데이터들이 다음의 표 1에 기재되어 있다.

표 1

<18>

MIB 그룹	사용되는 MIB 데이터
interface	interface.ifTable.ifEntry.ifInOctets interface.ifTable.ifEntry.ifInUcastPkts
IP	ip.ipInReceives ip.ipInDelivers ip.ipOutRequests ip.ipOutDiscards
TCP	tcp.tcpAttamptFails tcp.tcpOutRsts
UDP	udp.udpInErrs
ICMP	icmp.icmpIndestUnreachs icmp.icmpOutdestUnreachs icmp.icmpInMsgs icmp.icmpOutMsgs icmp.icmpInEchos icmp.icmpOuEchoReps

<19> 트래픽 공격 탐지를 위해 필요한 MIB 데이터가 선정되면, MIB 데이터 수집부(110)는 일정한 주기로 이러한 MIB 데이터를 네트워크 단말장치로부터 수집한다. MIB 데이터의 수집은 일정한 시간 간격(예를 들면, 1분 간격)마다 이루어질 수 있다. 그러나, 보다 효율적인 트래픽 공격 탐지를 위해 MIB 데이터의 수집 주기를 상황에 따라 조절할 수 있다.

<20> 도 2는 트래픽 폭주 공격에 대한 interface 그룹에 속하는 MIB 데이터인 ifInOctets 값의 변화를 1초 단위로 나타낸 그래프이다. ifInOctets는 인터페이스를 통한 옥텟의 총 수신 개수를 나타내는 값이다. 도 2를 참조하면, 4초의 시점에 트래픽 폭주 공격이 발생하여 ifInOctets 값이 증가하였고, 최초의 트래픽 공격 탐지는 트래픽 폭주 공격이 발생한 후 14초 뒤인 18초 시점에 이루어졌다. 이때는 다음의 MIB 데이터 갱신 시점 이전에 탐지가 이루어지므로 정상 트래픽으로 판단되고, 다음의 탐지 시점에서 비로소 공격성 트래픽으로 판단된다. 따라서 MIB 데이터 수집이 1분마다 이루어진다면 트래픽 폭주 공격이 발생하고 74초가 지난 후에 공격이 탐지되는 경우가 발생하게 된다.

<21> 위에서 검토한 바와 같이 MIB 데이터 값은 연속적으로 증가하는 것이 아니고 특정한 시간 간격으로 갱신된다. 따라서 이러한 MIB 데이터의 갱신 주기에 맞추어 MIB 데이터의 수집 주기를 설정하면 트래픽 폭주 공격의 탐지 시간을 향상시킬 수 있다. 다만 MIB 데이터의 갱신 주기는 SNMP 에이전트와 MIB 데이터의 종류에 따라 각각 다르게 나타나므로 각각의 MIB 데이터에 따라서 탐지 시간 간격을 유연하게 조절할 수 있도록 해야 한다. 가장 정확한 방법은 1초 간격으로 MIB 데이터를 수집하여 갱신 주기를 알아내는 것이지만, 이는 시스템에 부하를 일으키며 공격 탐지를 위한 트래픽이 증가하게 되는 결과를 가져오므로 이러한 결과를 방지하면서 효율적으로 MIB 데이터의 갱신 주기를 알아낼 수 있는 방법을 사용한다.

<22> 도 3은 MIB 데이터의 갱신 주기를 예측하여 탐지 시점을 결정하기 위한 알고리즘의 코드를 나타낸 도면이고, 도 4는 MIB 데이터의 갱신 주기를 예측하여 탐지 시점을 결정하는 일 예를 시간의 흐름에 따라 도시한 도면이다.

<23> 도 3에서 S_n은 n+1번째 갱신 주기에서 MIB 데이터의 수집을 중지하는 시간, A_n은 최초 갱신 시점부터 n+1번째 갱신 시점까지의 갱신 주기에 대한 지수 평균, t_{old}는 갱신 주기의 시작점, t_{new}는 갱신 주기의 종료 시점, 그리고 U_{n+1}은 n+1번째 갱신 주기를 나타낸다.

<24> 도 4를 참조하면, MIB 데이터 수집부(110)는 초기화 과정에서 먼저 1초 간격으로 MIB 데이터를 수집하여 MIB 데이터 값에 변화가 생기는지 탐지한다. 초기화 과정에서 최초로 MIB 데이터의 갱신이 일어나는 시점을 t_1, 두 번째로 MIB 데이터의 갱신이 일어나는 시점을 t_2라 하면, MIB 데이터의 갱신 주기는 t_2-t_1과 같이 산출된다. 이러한 초기화 과정을 두 번 이상 반복 실시하여 얻어진 MIB 데이터의 갱신 주기 중에서 가장 작은 값이 갱신 주기의 최소값(U_{min})이 되고, 다음의 갱신 주기를 예측하는 과정에서 A_0로 사용된다. 그리고 마지막으로 실시한 초기

화 과정의 t_2는 도 3의 코드에서 t_{old}, 즉 다음 갱신 주기의 시작점이 된다.

<25> t_{old}로부터 탐지 시점 결정 알고리즘이 시작되며, t_{old}는 탐지 시점 결정 알고리즘의 첫 번째 갱신 시점인 동시에 첫 번째 갱신 주기의 시작점이다. 첫 번째 갱신 주기인 U_1을 구하기 위한 과정을 검토하면, 먼저 이전에 계산된 갱신 주기를 바탕으로 S_0의 시간 동안 MIB 데이터의 수집을 중지한다. S_0는 도 3에서와 같이 $S_0=A_0-1=U_{min}-1$의 식에 의해 산출된다. 또한 갱신 주기의 종료 시점은 $t_{new}=t_{old}+S_0$로 추정된다.

<26> 갱신 주기의 정확한 종료 시점을 구하기 위해 MIB 데이터 수집부(110)는 t_{new}부터 1초 간격으로 MIB 데이터를 수집하여 정확한 탐지 시점을 결정한다. 갱신 주기의 시작점인 t_{old}에서의 MIB 데이터 값과 MIB 데이터 수집이 이루어지는 현재 시점인 t_{new}에서의 MIB 데이터 값이 동일하면 갱신이 일어나지 않은 것이므로 1초 뒤에 다시 MIB 데이터를 수집한다. MIB 데이터의 갱신이 일어나기 전까지 갱신 주기의 종료 시점은 1초 간격으로 새로운 t_{new} 값으로 바뀌게 된다. 이때 MIB 데이터 갱신 여부를 결정하기 위해 사용되는 MIB 데이터는 interface 그룹의 ifInOctets 값이다. 다른 그룹에 속하는 MIB 데이터 값은 트래픽 폭주 공격이 발생하는 경우에만 값이 변화하므로 MIB 데이터의 갱신 시점을 찾기 어렵지만, inInOctets 값은 항상 변화하기 때문에 갱신 주기의 탐지에 사용될 수 있다.

<27> t_{old}에서의 MIB 데이터 값과 t_{new}에서의 MIB 데이터 값이 동일하지 않으면 MIB 데이터의 갱신이 일어난 것이다. 따라서 t_{new}는 정확한 MIB 데이터 갱신 주기의 종료 시점이 되고, 첫 번째 갱신 주기인 U_1은 $U_1=t_{new}-t_{old}$의 식에 의해 산출된다. 두 번째 갱신 주기에서 MIB 데이터의 수집을 중지하는 시간인 S_1을 구하기 위해서는 A_1의 값을 구해야 한다. A_1은 U_{min}을 구하기 위해 MIB 데이터를 수집했던 초기화 과정에서의 최초 갱신 시점부터 탐지 시점 결정 알고리즘의 첫 번째 갱신 주기의 종료 시점, 즉 탐지 시점 결정 알고리즘의 두 번째 갱신 시점까지의 갱신 주기에 대한 지수 평균이다. 이 값은 다음의 수학식 1에 의하여 구할 수 있다.

수학식 1

<28> $$A_1=\alpha\times U_1+(1-\alpha)\times A_0$$

<29> 여기서, A_1은 최초 갱신 시점부터 탐지 시점 결정 알고리즘의 두 번째 갱신 시점까지의 갱신 주기에 대한 지수 평균, α는 지수 평균을 구하는 데 사용되는 상수로서 1/2의 값을 가지며, U_1은 탐지 시점 결정 알고리즘의 첫 번째 갱신 주기, 그리고 A_0는 갱신 주기에 대한 지수 평균의 초기값으로, 초기화 과정에서 산출한 갱신 주기의 최소값인 U_{min}이 A_0로 사용된다.

<30> 첫 번째 갱신 주기 U_1 및 첫 번째 갱신 주기까지의 지수평균인 A_1을 구하면 동일한 방법으로 두 번째 갱신 주기인 U_2도 구할 수 있다. 이를 일반화시키면 MIB 데이터의 갱신 주기는 다음의 수학식 2에 의하여 산출된다. 이와 같이 일정 시간동안 MIB 데이터의 수집을 중지하고 최소의 횟수로 MIB 데이터를 수집하여 트래픽 폭주 공격을 탐지함으로써, 시스템의 부하를 줄이면서 공격 탐지의 효율성과 정확성을 높일 수 있다.

수학식 2

<31> $$U_{n+1}=\frac{1}{2}U_n+\frac{1}{2}A_{n-1}-1$$

<32> 여기서, U_{n+1}은 n+1번째 갱신 주기, U_n은 n번째 갱신 시점에서 예측한 n+1번째 갱신 시점까지의 갱신 주기, 그리고 A_{n-1}은 최초 갱신 시점부터 n번째 갱신 시점까지의 갱신 주기에 대한 지수 평균이다.

<33> MIB 데이터 수집부(110)에 의해 결정된 탐지 시점에서 트래픽 폭주 공격의 탐지에 필요한 MIB 데이터가 수집되면 이를 이용하여 트래픽 폭주 공격의 발생 가능성을 탐지한다.

<34> 공격 징후 사전 탐지부(115)는 단위 시간당 수신 데이터의 양이 사전에 설정된 기준값보다 크면 네트워크 트래픽을 공격성 트래픽으로 결정한다. 이는 트래픽 폭주 공격이 발생할 때 네트워크 단말장치로 전송되는 데이터의

양이 정상 트래픽의 경우보다 많아지는 점을 이용한 것이다. 트래픽 폭주 공격이 발생하면 BPS(bits per second)나 PPS(packets per second) 값이 일정한 기준값 이상으로 유지되는데, 이러한 기준값은 한 대의 공격 시스템에 의해 발생되는 최소 BPS 및 PPS 값을 포함하며 상위 계층 전달률과 응답률의 신뢰성을 보장하는 수준에서 결정된다. 따라서 BPS와 PPS 값에 대한 기준값을 각각 1Mbps 및 20pps로 결정하여 기준값 이상의 BPS나 PPS 값이 유지되면 트래픽 폭주 공격이 발생한 것으로 판단할 수 있다. 공격 징후 사전 탐지부(115)에 의해 트래픽 폭주 공격의 가능성이 존재하는 네트워크 트래픽인 공격성 트래픽과 정상 트래픽을 분류하여 이후에 공격 징후 탐지부(120)에서 분석할 네트워크 트래픽의 수를 줄일 수 있다. 따라서 시스템의 부하를 증가시키지 않으면서 효율적으로 트래픽 폭주 공격을 탐지할 수 있게 된다. 공격 징후 사전 탐지부(115)에 의해 네트워크 트래픽이 공격성 트래픽인지 여부를 판단하는 알고리즘에 대한 코드가 도 5에 도시되어 있다.

<35> 공격 징후 탐지부(120)는 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 사전에 설정된 기준 전달률보다 작으면 네트워크 단말장치의 네트워크 트래픽을 트래픽 폭주 공격의 징후를 보이는 공격성 트래픽으로 결정한다.

<36> 트래픽 공격의 탐지가 이루어질 때마다 트래픽 폭주 공격의 유형을 정확하게 판단하려면 정상 트래픽에 대하여도 탐지가 이루어지므로 탐지 시간을 많이 소비하게 되고 시스템의 부하를 증가시킨다. 따라서 먼저 트래픽 폭주 공격의 가능성 유무에 따라 정상 트래픽과 공격성 트래픽을 구분하여 정상 트래픽으로 판단된 네트워크 트래픽에 대하여는 트래픽 폭주 공격을 판단하는 과정을 생략함으로써, 탐지를 위한 소비 트래픽 및 시스템의 부하를 감소시킬 수 있다.

<37> 네트워크 단말장치의 네트워크 트래픽이 공격성 트래픽인지 여부를 판단하는 과정에서는 MIB 데이터 값에 의해 파악되는 데이터그램의 상위 계층 전달률(DeliverRatio)을 이용할 수 있다. 상위 계층 전달률은 인터페이스를 통해 받은 데이터그램이 상위 계층에 전달되는 정도를 나타낸 값으로, 최근 1분 동안의 수신 데이터그램 총 수(ipInReceives)의 변화량에 대한 정상적으로 수신된 데이터그램 수(ipInDelivers)의 변화량의 비로 나타낸다. 정상 트래픽의 경우 상위 계층 전달률은 0.8 이상으로 높지만, 트래픽 폭주 공격이 발생하면 버퍼 공간의 부족과 오류에 의하여 상위 계층 전달률이 0.3 이하로 낮아진다. 따라서 공격 징후 탐지부(120)는 현재 탐지 시점에서 산출한 상위 계층 전달률이 기준 전달률보다 낮으면 트래픽 폭주 공격의 발생 가능성이 있는 것으로 판단하여 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정한다. 기준 전달률은 0.3에서 0.8 사이의 값을 가질 수 있으며, 0.8로 설정되는 것이 바람직하다. 도 6은 트래픽 폭주 공격 중의 하나인 TCP-SYN flooding 공격에 대한 상위 계층 전달률의 변화를 시간의 흐름에 따라 나타낸 그래프이다. 도 6을 참조하면, 트래픽 폭주 공격이 발생하지 않을 때의 상위 계층 전달률은 0.8 이상의 값을 보이며, 트래픽 폭주 공격이 발생하면 상위 계층 전달률이 0.3보다 낮아지는 것을 확인할 수 있다.

<38> 정상 트래픽과 공격성 트래픽을 구분하기 위해서 상위 계층 전달률 외에 수신된 데이터그램에 대한 응답률(ResponseRatio), 또는 파기된 송신 데이터그램 수(ipOutDiscards)를 사용할 수 있다.

<39> 응답률은 최근 1분 동안의 수신 데이터그램 총 수(ipInReceives)의 변화량에 대한 송신 데이터그램 총 수(ipOutRequest)의 변화량의 비로 나타낸다. 정상 트래픽의 경우 응답률은 0.5 이상이지만 트래픽 폭주 공격이 발생하면 0.4 이하로 감소하게 된다. 공격 징후 탐지부(120)는 기준 응답률을 0.4로 설정하여 응답률이 기준 응답률보다 낮으면 네트워크 트래픽을 공격성 트래픽으로 결정할 수 있다.

<40> 트래픽 폭주 공격은 오류가 없는 대량의 패킷을 전송하기 때문에 거의 대부분의 패킷이 정상적으로 수신되지만 버퍼 공간이 부족하므로 수신된 패킷은 폐기된다. 이때 ipOutDiscards 값이 증가하게 되며, 공격 징후 탐지부(120)는 현재 탐지 시점에서 ipOutDiscards 값이 증가한 것으로 판단되면 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정한다.

<41> 도 7은 공격 징후 탐지부(120)가 네트워크 단말장치의 네트워크 트래픽이 공격성 트래픽인지 여부를 판단하는 알고리즘에 대한 코드를 나타낸 도면이다. 도 7에서 weight는 공격성 트래픽 여부를 판단하는 데 사용되는 데이터 값들에 의해 공격성 트래픽의 가능성이 보일 때마다 값이 증가하여 최종적으로 공격성 트래픽으로 결정하는 데 사용된다. Th(DeliverRatio)와 Th(ResponseRatio)는 각각 기준 전달률과 기준 응답률을 나타낸다.

<42> 네트워크 트래픽에 대하여 공격성 트래픽인지 여부에 대한 판단이 끝나면, 공격 유형 결정부(130)는 트래픽 폭주 공격의 징후를 보이는 공격성 트래픽으로 결정된 네트워크 트래픽에 대하여 MIB 데이터 값에 의해 파악된 프로토콜별 객체 값(object identifier : OID)의 변화에 따라 트래픽 폭주 공격의 유무 및 종류를 결정한다. 이를 위해 공격 유형 결정부(130)는 TCP 공격 결정부(132)를 포함할 수 있으며, UDP 공격 결정부(134) 또는 ICMP 공

격 결정부(136)를 선택적으로 구비할 수 있다. 위에 언급한 바와 같이 정상 트래픽으로 판단된 네트워크 트래픽에 대하여는 트래픽 폭주 공격의 종류를 결정하는 과정을 생략한다.

<43> 트래픽 폭주 공격에는 TCP-SYN flooding 공격, UDP flooding 공격 및 ICMP flooding 공격이 있다. 이들은 모두 네트워크 대역폭, 프로세스 처리 능력, 기타 시스템 자원을 고갈시킴으로써 정상적인 서비스를 할 수 없도록 하는 공격 형태이다. 공격 유형 결정부(130)는 각각의 트래픽 폭주 공격에 의해 데이터 값이 변화하는 MIB 데이터를 분석하여 공격의 유형을 결정한다.

<44> TCP 공격 결정부(132)는 MIB 데이터 값에 의해 파악된 접속 실패 횟수(tcpAttamptFail) 또는 RST 플래그를 포함한 송신 세그먼트 수(tcpOutRsts)가 변경된 경우에는 트래픽 폭주 공격을 TCP-SYN flooding 공격으로 결정한다.

<45> TCP-SYN flooding 공격은 소스 ip를 조작해서 서버를 다운시켜 수신 거부 상태로 만드는 공격 형태이다. 클라이언트가 서버에 접속을 요청하는 SYN 패킷을 전송하면 서버가 클라이언트에게 요청을 수락한다는 SYN 패킷과 ACK 패킷을 전송한다. 이때 서버는 대기 상태가 되어 일정 시간 후에 클라이언트로부터 ACK 패킷이 전송되지 않으면 연결을 초기화하는데, 초기화하기 전까지 메모리 공간인 백로그큐(backlog queue)에 SYN 패킷을 저장한다. TCP-SYN flooding 공격에 의해 위조된 요구가 계속 전송되어 백로그큐가 포화 상태로 되면 서버는 더 이상의 연결을 받아들일 수 없는 서비스 거부 상태로 들어간다. 이때 연결이 실패되므로 tcpAttamptFail 값이 증가하며, 연결할 수 없는 경우 RST 패킷을 전송하기 때문에 tcpOutRsts 값도 증가하게 되는 것이다.

<46> 도 8은 TCP 공격 결정부(132)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 TCP-SYN flooding 공격인지 여부가 결정되는 알고리즘의 코드를 나타낸 도면이다. Diff()는 이전 탐지 시점에 대한 데이터 값의 변화량을 나타낸다.

<47> UDP 공격 결정부(134)는 MIB 데이터 값에 의해 파악된 에러가 된 수신 데이터그램 수(udpInErrs)가 증가한 경우, 또는 도달 불능의 송신 수(icmpOutdestUnreachs) 및 ICMP 메세지의 전체 송신 수(icmpOutMsgs)의 증가량이 일치하고 도달 불능의 수신 수(icmpInDstUnreachs)가 0인 경우에는 트래픽 폭주 공격을 UDP Flooding 공격으로 결정한다.

<48> UDP flooding 공격은 UDP 프로토콜을 이용하여 클라이언트가 서버에 가상의 데이터를 연속적으로 보냄으로써, 서버에 부하를 발생시켜 정상적인 서비스를 할 수 없도록 만드는 공격이다. 망사업자에서 수용할 수 있는 용량을 초과하여 IDC 센터 및 웹서버까지 사용자의 접속 요청이 들어올 수 없는 상태가 된다. 따라서 공격받은 네트워크 단말장치는 대량의 패킷을 전송받기 때문에 버퍼 공간의 부족과 체크섬의 오류에 의하여 udpInErrs 값이 증가하며, 상위 프로토콜에 전달되지 않거나 포트가 닫혀있는 등의 오류가 발생하면 오류보고 메시지를 전달하고 전송받기 때문에 icmpOutDestUnreachs 값과 icmpOutMsgs 값이 같은 변화량을 보이며 증가하게 된다. 또한 icmpInDestUnreachs 값은 0으로 나타난다. 도 9에는 UDP 공격 결정부(134)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 UDP flooding 공격인지 여부가 결정되는 알고리즘의 코드가 나타나 있다.

<49> ICMP 공격 결정부(136)는 MIB 데이터 값에 의해 파악된 ICMP 메세지의 전체 수신 수(icmpInMsgs) 또는 ICMP 반향 요청 수(icmpInEchos)가 증가한 경우, 또는 도달 불능의 수신 수(icmpInDestUnreachs), 도달 불능의 송신 수(icmpOutDestUnreachs), ICMP 반향 응답 메세지 수(icmpInEchosReps) 및 파기된 송신 데이터그램 수가 증가한 경우에는 트래픽 폭주 공격을 ICMP Flooding 공격으로 결정한다.

<50> ICMP flooding 공격은 공격 대상의 IP로 서버에 접속해서 서버를 통해 대량의 ICMP 패킷을 직접 전송하여 공격 대상을 다운시키는 공격 방식이다. ICMP flooding 공격이 발생하면 ICMP 반향 요청(echo request)이 증가하여 icmpMsgs 또는 icmpInEchos 값이 증가한다. 또한 상위 프로토콜에 전달되지 않거나 포트가 닫혀있는 등의 오류가 발생하면 오류보고 메시지를 전달하고 전송받기 때문에 icmpInDstUnreachs 및icmpOutDestUnreachs 값이 증가하고, ICMP 반향 요청에 대한 응답으로 icmpOutEchoReps 값이 증가하며, 버퍼 공간의 부족으로 수신된 모든 패킷데 대해 응답이 이루어지지 않고 폐기되는 패킷이 발생하므로 ipOutDiscards 값이 증가하게 된다. 도 10은 ICMP 공격 결정부(136)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 ICMP flooding 공격인지 여부가 결정되는 알고리즘의 코드를 나타낸 도면이다. icmpInDestUnreachs, icmpOutDestUnreachs, icmpOutEchoReps 및 ipOutDiscards 값이 모두 증가하는 경우에만 ICMP flooding 공격으로 결정되는 것을 확인할 수 있다.

<51> 도 11은 TCP-SYN flooding 공격에 의한 MIB 데이터 값의 변화를 시간의 흐름에 따라 나타낸 그래프이다. 도 11을 참조하면, TCP-SYN flooding 공격이 발생한 경우 ipOutDiscards, tcpAttamptFail 및 tcpOutRsts의 값이 급격히 증가한다. 따라서 ipOutDiscards 값의 증가로 공격성 트래픽으로 결정하고, tcpAttamptFail 및 tcpOurRsts 값의 증가로 TCP-SYN flooding 공격임을 결정할 수 있다. 반면 udpInErrs, icmpInDestUnreachs 및

icmpOutMsgs 값은 트래픽 폭주 공격의 발생에 영향을 받지 않으므로 UDP flooding 공격이나 ICMP flooding 공격으로 잘못 판단되지 않는다.

<52> 도 12는 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 방법의 바람직한 실시예의 수행과정을 도시한 흐름도이다.

<53> 도 12를 참조하면, MIB 데이터 수집부(110)는 네트워크 단말장치로부터 일정한 주기로 SNMP의 MIB 데이터 중 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이터를 수집한다(S1210). 이때 수집 대상이 되는 MIB 데이터는 표 1에 나타난 바와 같다. 또한 MIB 데이터 수집부(110)는 수집된 MIB 데이터 값에 의해 파악되는 ifInOctets 값이 변화되는 시간 간격을 기초로 예측한 MIB 데이터의 갱신 주기에 따라 MIB 데이터를 수집할 수 있다. MIB 데이터의 갱신 주기는 수학식 2를 사용하여 예측할 수 있다.

<54> 다음으로 공격 징후 사전 탐지부(115)는 단위 시간당 수신 데이터의 양을 이용하여 정상 트래픽과 공격성 트래픽을 분류하고(S1215), 공격 징후 탐지부(120)는 MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률이 기준 전달률보다 작으면 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정한다(S1220). 기준 전달률은 실험에 의해 결정되며, 0.8의 값을 갖도록 설정할 수 있다. 공격 징후 탐지부(120)는 상위 계층 전달률 이외에도 수신된 데이터그램에 대한 응답률(ResponsRatio), 또는 파기된 송신 데이터그램 수(ipOutDiscards)를 분석하여 공격성 트래픽인지 여부를 결정할 수 있다. 이때 기준 응답률은 0.4로 설정할 수 있으며 ipOutDiscards값이 증가하면 공격성 트래픽으로 결정할 수 있다. 공격 징후 탐지부(120)에 의해 네트워크 단말장치의 네트워크 트래픽이 공격성 트래픽으로 결정되었는지 여부가 판단되고(S1230), 정상 트래픽으로 결정된 경우에는 공격 유형 결정 단계가 생략되며 다음 탐지 시점에서 다시 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 방법에 의해 트래픽 공격이 탐지된다.

<55> 마지막으로 공격 유형 결정부(130)는 공격성 트래픽으로 결정된 네트워크 트래픽에 대하여 MIB 데이터 값에 의해 파악된 프로토콜별 객체 값의 변화에 따라 트래픽 폭주 공격의 종류를 결정한다. TCP 공격 결정부(132)는 MIB 데이터 값에 의해 파악된 접속 실패 횟수(tcpAttamptFail) 또는 RST 플래그를 포함한 송신 세그먼트 수(tcpOutRsts)가 변경된 경우에는 트래픽 폭주 공격을 TCP-SYN Flooding 공격으로 결정한다(S1240). UDP 공격 결정부(134)는 MIB 데이터 값에 의해 파악된 에러가 된 수신 데이터그램 수(udpInErrs)가 증가한 경우, 또는 도달 불능의 송신 수(icmpOutdestUnreachs) 및 ICMP 메세지의 전체 송신 수(icmpOutMsgs)의 증가량이 일치하고 도달 불능의 수신 수(icmpIndestUnreachs)가 0인 경우에는 트래픽 폭주 공격을 UDP Flooding 공격으로 결정한다(S1250). 또한 ICMP 공격 결정부(136)는 MIB 데이터 값에 의해 파악된 ICMP 메세지의 전체 수신 수(icmpInMsgs) 또는 ICMP 반향 요청 수(icmpInEchos)가 증가한 경우, 또는 도달 불능의 수신 수(icmpInDestUnreachs), 도달 불능의 송신 수(icmpOutDestUnreachs), ICMP 반향 응답 메세지 수(icmpInEchoReps) 및 파기된 송신 데이터그램 수가 증가한 경우에는 트래픽 폭주 공격을 ICMP Flooding 공격으로 결정한다(S1260).

<56> 표 2에는 1분마다 트래픽 폭주 공격을 탐지하는 경우와 MIB 데이터의 갱신 주기를 예측하여 탐지 시점을 결정하는 경우 트래픽 공격 탐지에 걸리는 시간을 비교하여 나타내었다.

표 2

<57>

평가 항목		1분마다 탐지	탐지 시점 결정
트래픽 공격 탐지 시간(초)	최대	74	14
	평균	38	10.5
	최소	3	4

<58> 1분마다 트래픽 폭주 공격을 탐지하는 경우에 비해 갱신 주기의 예측에 의해 탐지 시점을 결정하는 경우 트래픽 공격이 탐지되는 시점까지 걸리는 최소 시간은 1초가 증가하였으나, 최대 시간은 60초가 향상되었고, 평균적으로 걸리는 시간은 27.5초 향상되었다.

<59> 또한 표 3에는 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치 및 방법을 실시할 경우 시스템의 부하 및 탐지 트래픽의 양을 나타내었다.

표 3

<60>

평가 항목		본 발명	
CPU 사용(Pentium D 3.40GHz)		< 0.1%	
메모리 사용(512MB)		< 0.4%	
네트워크 부하	입력	156bps	0.2bps
	출력	131bps	0.2bps

<61> 본 발명의 실시에 의하여 시스템의 부하와 탐지 트래픽은 종래 사용된 트래픽 탐지 장치 및 방법에 비하여 증가하였다. 그러나 표 3을 참조하면, 이러한 증가량이 시스템에 영향을 미치지 않는 수준임을 확인할 수 있다. 따라서 본 발명에 의하면 시스템에 영향을 미치지 않으면서 효율적으로 트래픽 폭주 공격을 탐지할 수 있다.

<62> 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치 및 방법의 성능을 평가하기 위하여 MIB 데이터의 갱신 주기가 평균 15초인 시스템을 대상으로 10일 동안 무작위로 TCP-SYN, UDP 및 ICMP flooding 공격을 실시하였다. 이때 특정시간에 세 가지의 트래픽 폭주 공격 중 한 가지만 발생하도록 설정하였다. 10일 동안 TCP-SYN flooding 공격이 794회, UDP flooding 공격이 832회, 그리고 ICMP flooding 공격이 802회로 총 2428회의 공격이 발생하였다. MIB 데이터의 갱신 횟수는 트래픽 공격 탐지 횟수와 동일하며, MIB 데이터의 갱신 시점에서 발생한 공격 횟수는 TCP-SYN flooding 공격이 2526회, UDP flooding 공격이 2769회, 그리고 ICMP flooding 공격이 2613회이고 정상 트래픽의 발생 횟수는 49732회였다.

<63> 공격 징후 탐지부(120)는 49732회의 정상 트래픽 발생 중에서 48441회를 정상 트래픽으로 분류하여 97.51%의 정상 트래픽에 대하여 공격 유형 결정 과정이 생략됨으로써 시스템의 부하를 줄일 수 있었다. 또한 9199회를 공격성 트래픽으로 판단하여 공격 판단률 100%의 결과를 나타내었다. 공격 유형 결정부(130)는 TCP-SYN, UDP 및 ICMP flooding 공격의 유형을 모두 정확하게 분류하였고, 이러한 트래픽 폭주 공격은 공격이 발생한 후 1~2회의 탐지로 모두 탐지되었다. 오탐지가 발생한 경우는 공격시작시점과 탐지시점의 시간차가 3초 이내인 경우였다.

<64> 이러한 실험 결과를 바탕으로 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치 및 방법에 의해 트래픽 폭주 공격의 탐지 시간이 향상되고, 공격을 신속하고 정확하게 탐지할 수 있으며, 트래픽 공격 탐지의 효율성도 향상되었다는 것을 확인할 수 있다.

<65> 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<66> 이상에서 본 발명의 바람직한 실시예에 대해 도시하고 설명하였으나, 본 발명은 상술한 특정의 바람직한 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

도면의 간단한 설명

<67> 도 1은 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 장치에 대한 바람직한 실시예의 구성을 도시한 블록도,

<68> 도 2는 트래픽 폭주 공격에 대한 interface 그룹에 속하는 MIB 데이터인 inInOctets 값의 변화를 1초 단위로 나타낸 그래프,

<69> 도 3은 MIB 데이터의 갱신 주기를 예측하여 탐지 주기를 결정하기 위한 알고리즘의 코드를 나타낸 도면,

<70> 도 4는 MIB 데이터의 갱신 주기를 예측하여 탐지 주기를 결정하는 일 예를 시간의 흐름에 따라 도시한 도면,

<71> 도 5는 공격 징후 사전 탐지부(115)가 네트워크 트래픽이 공격성 트래픽인지 여부를 판단하는 알고리즘에 대한 코드를 나타낸 도면,

<72> 도 6은 트래픽 폭주 공격 중의 하나인 TCP-SYN flooding 공격에 대한 상위 계층 전달률의 변화를 시간의 흐름에

따라 나타낸 그래프,

<73> 도 7은 공격 징후 탐지부(120)가 네트워크 단말장치의 네트워크 트래픽이 공격성 트래픽인지 여부를 판단하는 알고리즘에 대한 코드를 나타낸 도면,

<74> 도 8은 TCP 공격 결정부(132)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 TCP-SYN flooding 공격인지 여부가 결정되는 알고리즘의 코드를 나타낸 도면,

<75> 도 9는 UDP 공격 결정부(134)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 UDP flooding 공격인지 여부가 결정되는 알고리즘의 코드를 나타낸 도면,

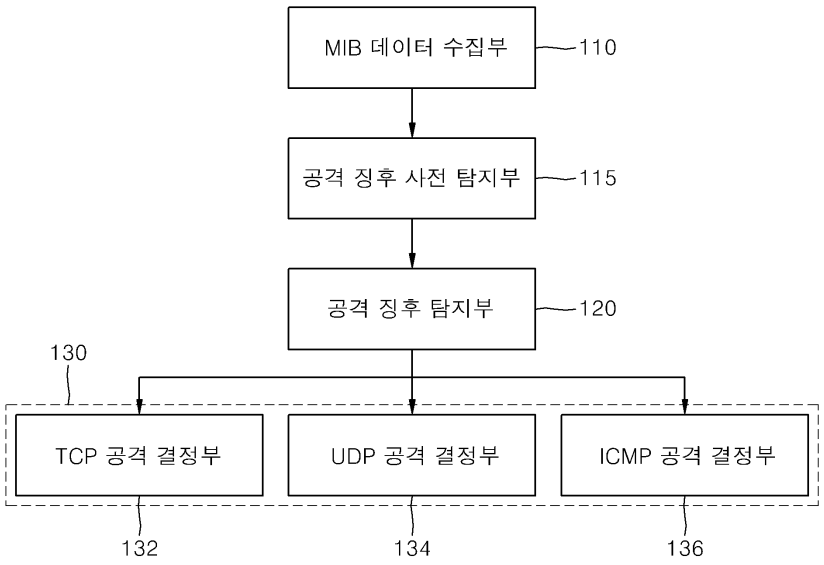
<76> 도 10은 ICMP 공격 결정부(136)에 의해 네트워크 트래픽에 대한 트래픽 폭주 공격이 ICMP flooding 공격인지 여부가 결정되는 알고리즘의 코드를 나타낸 도면,

<77> 도 11은 TCP-SYN flooding 공격에 의한 MIB 데이터 값의 변화를 시간의 흐름에 따라 나타낸 그래프, 그리고,

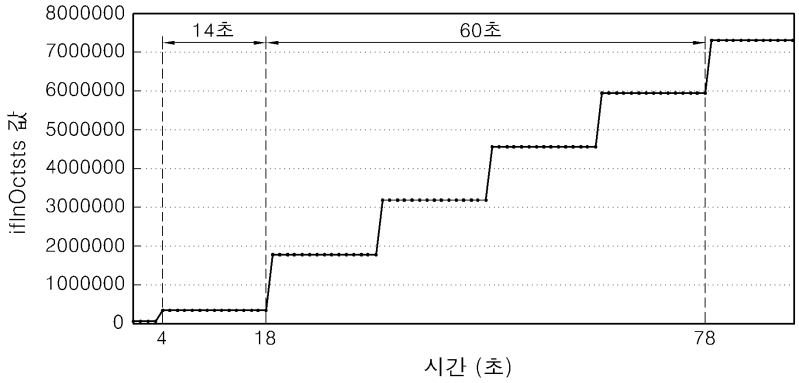
<78> 도 12는 본 발명에 따른 SNMP 기반의 트래픽 공격 탐지 방법의 바람직한 실시예의 수행과정을 도시한 흐름도이다.

도면

도면1



도면2

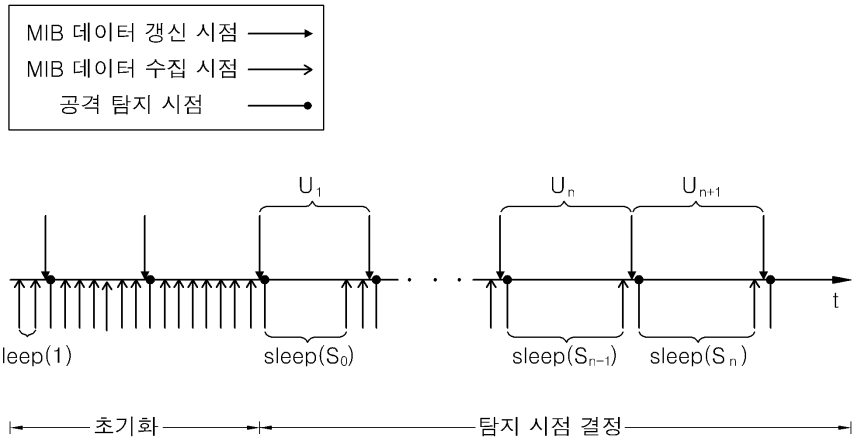


도면3

```
void MIB-Update_Detection(t_old, A_n) {
        S_n = A_n - 1;
        sleep (S_n);  t_new = t_old + S_n;

        while ( Mib(t_new, ifInOctets) == Mib(t_old, ifInOctets) )
        {
        sleep(1);
        t_new = t_new + 1;
        }
        U_n+1 = t_new - t_old;
        A_n+1 = α * U_n+1 + (1-α) * A_n;
        t_old = t_new;
}
```

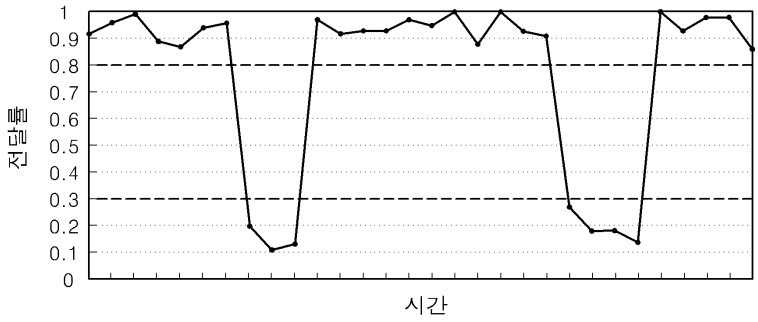
도면4



도면5

```
Boolean Pre_Symptom_analysis( … ) {
        if( bps < Th(bps) && pps < Th(PPS)) return FALSE;
}
```

도면6



도면7

```
Boolean Symptom_analysis( … ) {
        int weight = 0;

        if( DeliverRatio(t) < Th(DeliverRatio) )  weight++;
        if( ResponseRatio(t) < Th(ResponseRatio) )  weight++;
        if( Diff(t, ipOutDiscards) > O) )  weight++;
        if(weight > =1) return TRUE;
        return FALSE;
}
```

도면8

```
Boolean TCP-SYN_Flooding_analysis( … )
{

        if( Diff(t, tcpAttamptFail) > 0 ||
        Diff(t, tcpOutRsts > 0) )
        return TRUE;
        return FALSE;
}
```

도면9

```
Boolean UDP_Flooding_analysis( … )
{
      int weight = 0;
      if( Diff(t, udpInErrs ) > 0) weight ++;
      if( Diff(t, icmpOutDestUnreachs)==diff(t,icmpOutMsgs) &&
          Diff(t,icmpOutDestUnreachs) > 0 &&
          Diff(t, icmpOutMsgs) > 0 &&
          Diff(t, icmpInDestUnreachs) == 0) weight++;

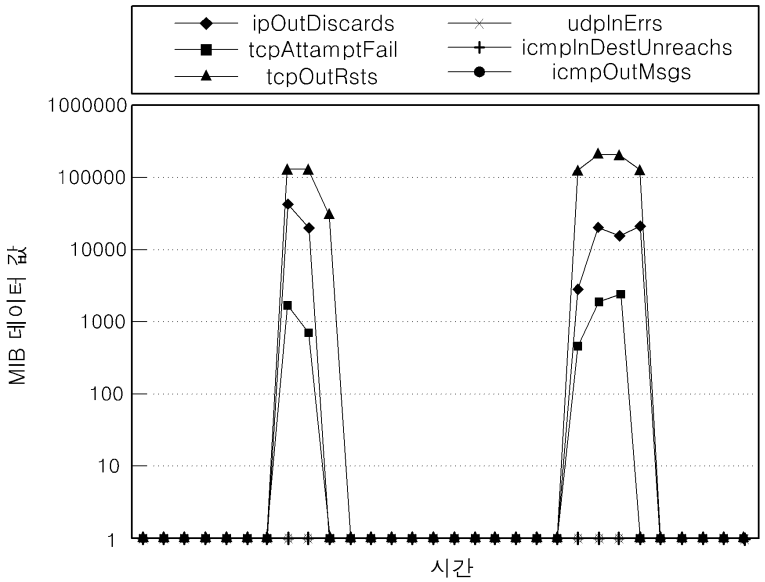
      if(weight > =1) return TRUE;
         return FALSE;
}
```

도면10

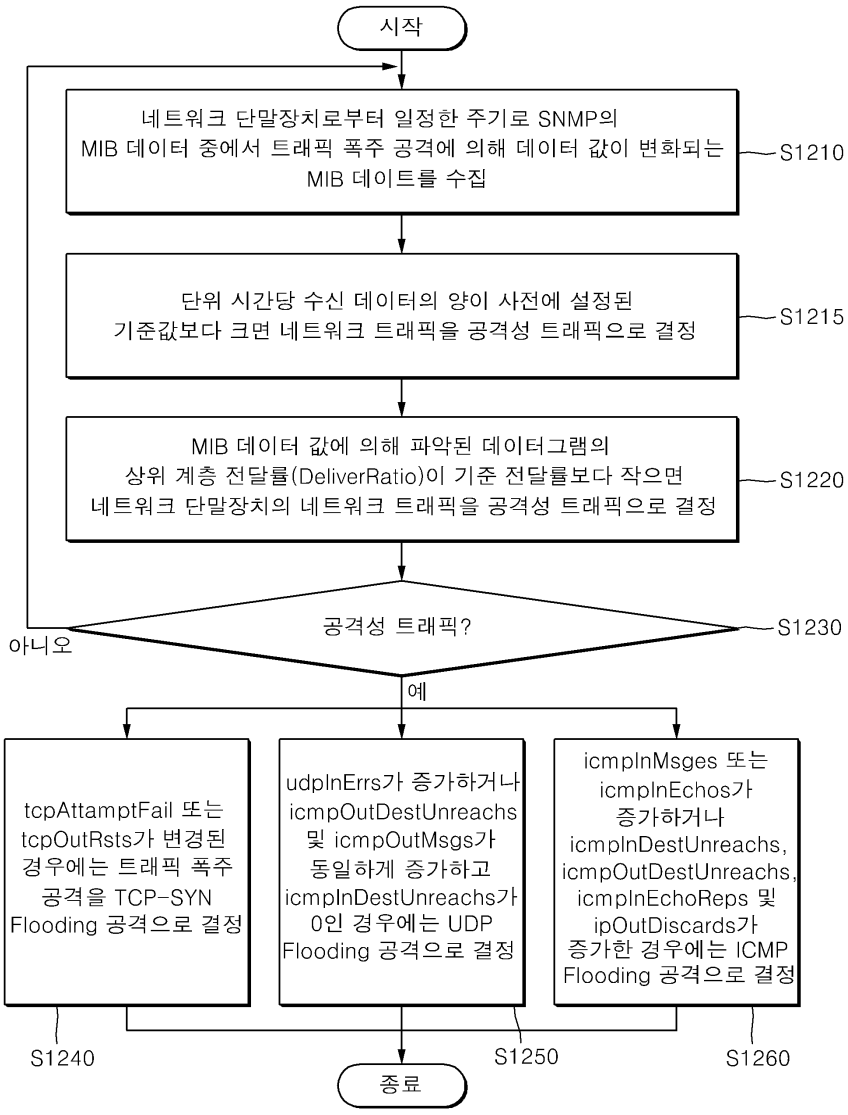
```
Boolean ICMP_Flooding_analysis( … )
{
      int weight = 0;
      if( Diff(t, icmpInMsges) > 0)||
          Diff(t, icmpInEchos) > 0) weight++;
      if( Diff(t, icmpInDestUnreachs) > 0  &&
          Diff(t, icmpOutDestUnreachs) > 0 &&
          Diff(t, icmpOutEchoReps) > 0 &&
          Diff(t, ipOutDiscards) > 0) ) weight++;

      if(weight > =1) return TRUE;
         return FALSE;
}
```

도면11



도면12


시작
네트워크 단말장치로부터 일정한 주기로 SNMP의 MIB 데이터 중에서 트래픽 폭주 공격에 의해 데이터 값이 변화되는 MIB 데이트를 수집
S1210
단위 시간당 수신 데이터의 양이 사전에 설정된 기준값보다 크면 네트워크 트래픽을 공격성 트래픽으로 결정
S1215
MIB 데이터 값에 의해 파악된 데이터그램의 상위 계층 전달률(DeliverRatio)이 기준 전달률보다 작으면 네트워크 단말장치의 네트워크 트래픽을 공격성 트래픽으로 결정
S1220
공격성 트래픽?
S1230
아니오
예
tcpAttamptFail 또는 tcpOutRsts가 변경된 경우에는 트래픽 폭주 공격을 TCP-SYN Flooding 공격으로 결정
S1240
udpInErrs가 증가하거나 icmpOutDestUnreachs 및 icmpOutMsgs가 동일하게 증가하고 icmpInDestUnreachs가 0인 경우에는 UDP Flooding 공격으로 결정
S1250
icmpInMsges 또는 icmpInEchos가 증가하거나 icmpInDestUnreachs, icmpOutDestUnreachs, icmpInEchoReps 및 ipOutDiscards가 증가한 경우에는 ICMP Flooding 공격으로 결정
S1260
종료