# SVDD와 SNMP MIB을 이용한 트래픽 폭주 공격의 탐지

유재학○, 박준상, 이한성, 김명섭, 박대희
고려대학교 컴퓨터정보학과
{dbzzang○, runtoyou, mohan, tmskim, dhpark}@korea.ac.kr

# Detection of Traffic Flooding Attacks using SVDD and SNMP MIB

Jaehak Yu○, Junsang Park, Hansung Lee, Myungsup Kim, Daihee Park
Dept. of Computer & Information Science, Korea University

**요 약**

DoS/DDoS로 대표되는 트래픽 폭주 공격은 대상 시스템뿐만 아니라 네트워크 대역폭, 프로세서 처리능력, 시스템 자원 등에 악영향을 줌으로써 네트워크에 심각한 장애를 유발할 수 있다. 따라서 신속한 트래픽 폭주 공격의 탐지는 안정적인 서비스 제공 및 시스템 운영에 필수요건이다. 전통적인 패킷 수집을 통한 DoS/DDoS의 탐지방법은 공격에 대한 상세한 분석은 가능하나 설치의 확장성 부족, 고가의 고성능 분석시스템의 요구, 신속한 탐지를 보장하지 못한다는 문제점을 갖고 있다. 본 논문에서는 15초 단위의 SNMP MIB 객체 정보를 바탕으로 SVDD(support vector data description)를 이용하여 보다 빠르고 정확한 침입탐지와 쉬운 확장성, 저비용탐지 및 정확한 공격유형별 분류를 가능케 하는 새로운 시스템을 설계 및 구현하였다. 실험을 통하여 만족스러운 침입 탐지율과 안전한 false negative rate, 공격유형별 분류율 수치 등을 확인함으로써 제안된 시스템의 성능을 검증하였다.

## 1. 서 론

최근 네트워크의 발전으로 사용자들은 인터넷으로부터 보다 다양하고 빠른 서비스를 이용할 수 있게 되었다. 이와 같이 네트워크 기반 서비스의 의존도가 증가하면서 사용자는 인터넷으로부터 필요한 정보를 빠르게 획득할 수 있으며, 자신의 정보를 인터넷을 통해 홍보하는 수단으로까지 사용하고 있다. 그러나 이러한 긍정적인 측면과 함께 최근 정상적인 서비스를 방해하는 유해 트래픽이나 웜 등을 통한 네트워크의 피해사례가 보고되고 있다. 대표적인 유해 트래픽인 트래픽 폭주 공격은 대상이 되는 컴퓨터 시스템은 물론 네트워크의 자원을 고갈시킴으로써 정상적인 서비스를 수행하지 못하게 하는 공격으로 업무에 막대한 피해를 준다. 이러한 악의적인 접근이나 침입 등을 신속하게 탐지하고 대처할 수 있는 보안 기술이 학계의 최근 중요한 이슈 중 하나이다[1-3].

침입탐지 방법론은 침입에 대한 탐지 전략에 따라 크게 오용탐지(misuse detection) 모델과 비정상 탐지(anomaly detection) 모델로 나누어진다[4]. 오용 탐지모델은 이미 발견된 공격유형에 대한 면밀한 분석을 통하여 규칙 베이스화 하고 이를 기반으로 탐지를 수행하는 방법으로, 새로운 공격유형이 발견될 시에는 수동으로 규칙 베이스를 갱신해야만 새로운 공격에 대처할 수 있다는 문제점을 가지고 있다. 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 없기에 침입에 따른 적절한 대처를 할 수 없다는 한계점을 피할 수 없다. 최근의 연구문헌 조사에 의하면 보다 지능적인 침입탐지 모델의 설계를 위하여 데이터마이닝 및 기계학습 기법을 침입탐지시스템에 적용하려는 시도가 활발히 진행 중이다. 이러한 연구 동향 중 특히 패턴 분류(pattern classification) 및 함수 근사(function approximation) 등의 문제에서 매우 우수한 성능을 보이는 support vector machine (SVM)을 침입탐지에 적용하려는 연구가 주목을 받고 있다[5-6].

기존에 연구된 트래픽 폭주 공격 탐지에서의 패킷 수집 방법론[1-2]은 공격에 대한 상세한 분석은 가능하지만 고가의 고성능 분석시스템이 요구될 뿐만 아니라 설치 및 운영상의 확장성 문제, 실시간으로 빠른 탐지가 어렵다는 단점 등을 가지고 있다. 따라서 이를 보완하기 위한 방법으로 최근SNMP에서의 MIB 정보를 이용한 침입탐지 방법론[2-3]이 또한 주목을 받고 있다. SNMP MIB 정보를 이용한 트래픽 폭주 공격 탐지는 MIB 데이터 수집을 위한 시스템 및 네트워크 리소스의 사용이 적고, 계층과 프로토콜을 기준으로 표준화된 네트워크 성능 데이터를 제공 받을 수 있기 때문에 패킷 기반 탐지 방법에 비해 보다 빠르고 효과적인 탐지와 분류가 가능하다[2-3]. 이는 대부분의 네트워크 기반 시스템들이 기본적으로SNMP agent를 탑재하고 있기 때문이다. 따라서 SNMP MIB 정보를 이용한 트래픽 폭주 공격 탐지는 고사양의 패킷기반 탐지 시스템을 설치하기 힘든 소규모로 운영되는 오피스 네트워크나 홈네트워크에서의 침입탐지 시스템으로 적합하다. 또한 대규모의 네트워크에서도 적은 비용과 노력으로 탐지 시스템을 구축할 수 있는 대안이 될 수 있다.

전통적인 SNMP MIB 기반의 DDoS 탐지 방법은 프로토콜별 추이분석, 일주 트래픽 추이분석, 그리고 MIB에서의 특정 객체와 객체 정보간의 상관관계를 이용하여 공격트래픽을 탐지한다

* 본 연구는 산업자원부 및 한국산업기술평가원의 성장동력 기술개발사업의 연구결과로 수행되었습니다.

[2-3]. 프로토콜별 추이분석은 시스템에서 발생하는 트래픽 정보를 수집하여 하루 동안 시간대별로 프로토콜 분포를 예측하여 기준 값을 설정하고 현재 발생되는 트래픽의 프로토콜 분포와 비교하여 공격트래픽을 탐지하는 방법이다.그러나 이 방법은 유동적이고 변화가 심한 네트워크에서는 트래픽 예측이 어렵다는 단점을 지니고 있다. 일주 트래픽 추이분석은 일분 또는 수 십분 단위로 MIB 정보를 일정 기간 동안 수집한 후 모든 트래픽을 수용할 수 있는 기준 트래픽 추이 데이터를 설정하는 방법이다. 즉, 하루 동안의 트래픽 흐름을 예측하고 예측된 값과 현재 발생되는 트래픽을 비교하여 공격트래픽과 정상트래픽을 분류하는 방법으로 기준이 되는 추이 트래픽 설정이 어렵다. 마지막으로 MIB 객체 정보간의 상관관계를 이용하여 공격트래픽을 탐지하는 방법은 비교적 정확한 공격트래픽 탐지에는 도움이 되지만 객체 정보간의 상관관계를 정의해야 할 뿐만 아니라 별도로 연산하고 처리하기 위한 시간과 처리된 결과 값을 저장하고 관리하기 위한 추가적인 리소스를 요구하기 때문에 시스템의 안전성을 보장하기 위한 실시간 탐지가 어렵다는 단점을 가지고 있다. 또한, 현존하는 MIB 기반의 DDoS 탐지 시스템들은 대부분 테스트에 사용된 당시의DoS 공격툴의 기능과 특성에 의존적으로 개발된 시스템으로 새로운 공격유형이나 끊임없이 발전하는 공격툴에 유연하게 대처하기 어렵다. 즉 새로운 공격 형태나 툴이 발견되면 그때마다 새롭게 알고리즘 전체를 수정해 나가야하는 단점을 가지고 있다.결과적으로 실시간 침입탐지와 시스템에서 학습되지 않은 새로운 공격유형의 탐지 및 공격유형 별 트래픽 분류 등의 기능이 보장되는 보다 안전한 시스템 운영과 서비스가 가능한 새로운 대안이 요구된다.

본 논문에서는 패턴 분류 등의 문제에서 매우 우수한 성능을 보이는 SVDD를 기반으로 SNMP MIB 정보를 이용하여 보다 신속하고 정확한 DDoS 탐지와 효율적인 시스템 자원관리를 위한 DDoS의 공격유형별 분류를 수행하는 시스템을 제안한다. 본 시스템은 단일 클래스 SVM을 기반으로 정상트래픽과 공격트래픽을 빠르게 탐지하는 계층과 탐지된 공격트래픽을 다중 클래스 SVM(multi-class SVM)을 기반으로 DDoS의 대표적 공격유형인 TCP SYN flooding, UDP flooding, ICMP flooding으로 분류하는 계층으로 구성된다. 공격유형별 분류는 공격이 발생한 프로토콜에 대해서만 서비스를 제한하고 관리함으로써 보다 안정적인 네트워크 환경과 원활한 자원관리를 지원할 수 있다. 본 시스템은 SNMP의 MIB을 이용함으로 기존의 패킷 수집 방법론들의 단점인 고가의 고성능 분석시스템 요구와 설치의 확장성 문제, 실시간으로 빠른 탐지가 어렵다는 문제점들을 보완하는 견지에서 다음의 평가 기준들을 모두 만족한다. 1) 실시간 침입탐지 및 서비스의 안전성 보장 2) 쉬운 확장성 및 MIB 정보를 이용한 저비용 탐지 3) 공격유형별 트래픽 분류로 시스템의 효율적 자원관리 보장 4) 전체 시스템의 피해가 아닌 부분적 서비스 제한 및 관리 5) 시스템에서 학습되지 않은 새로운 공격유형의 탐지

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하는 SVDD 기반의 계층적 트래픽 폭주 공격 탐지 모델을 소개한다. 3장에서는 실험결과 및 성능 분석을 기술하며 마지막으로 4장에서는 결론 및 향후 연구과제에 대해 논한다.

## 2. 트래픽 폭주 공격 탐지 시스템

본 장에서는 우선 DDoS의 침입탐지를 위한 단일 클래스 SVM을 소개하고, 이를 주요 구성요소로 하는 새롭게 제안된 계층적 트래픽 폭주 공격 탐지 모델을 자세히 설명한다.

### 2.1 다중 클래스 SVM

Support vector machine(SVM)은 주어진 문제의 전역적 최적해(global optimum solution)를 보장함으로 패턴 분류 및 함수 근사 등에 적용되어 매우 우수한 성능을 보이고 있다.특히, 침입탐지의 경우 대부분의 데이터는 정상 데이터인 반면 일부의 트래픽만이 공격트래픽으로써 학습에 사용가능한 트래픽의 크기는 차이가 크다. 따라서 이진 분류기인 SVM은 관측되지 않은 영역을 포함하여 결정 경계면을 생성함으로 새로운 학습 데이터에 대해서 오분류(misclassification)를 할 가능성이 높다. 따라서 해당 클래스만을 독립적으로 표현하는 단일 클래스 SVM(one-class SVM)으로 결정 경계면을 결정하는 것이 보다 유리하다. 본 논문에서는 단일 클래스 SVM의 대표적인 알고리즘인 support vector data description(SVDD)[5]를 기반으로 실시간적인 공격트래픽 탐지와 공격 유형들을 분류하는 다중 클래스 SVM을 제안한다.

$d$-차원의 입력공간상에 존재하는 $K$-개의 데이터의 집합 $D_k = \{ x_i^k \in R^d \mid i = 1, \ldots, N_k \};\ k = 1, \ldots, K$ 이 주어졌을 경우, 각각의 클래스를 분류하기 위한 분류기는 각 클래스의 학습 데이터를 포함하면서 체적을 최소화하는 구체(sphere)를 구하는 문제로 정의되며, 다음의 최적화 문제를 통하여 수식화된다.

$$\begin{aligned} &\min L_0(R_k^2, a_k, \xi_k) = R_k^2 + C\sum_{i=1}^{N_k} \xi_i^k \\ &s.t \quad \|x_i^k - a_k\|^2 \le R_k^2 + \xi_i^k, \xi_i^k \ge 0, \forall i. \end{aligned} \tag{1}$$

여기에서, $a_k$는 $k$-번째 클래스를 표현하는 구체의 중심이며, $R_k^2$은 구체의 반경의 제곱, $\xi_i^k$는 $k$-번째의 클래스에 속한 $i$-번째 학습 데이터 $x_i^k$가 구체에서 벗어나는 정도를 나타내는 벌점 항이며, $C$는 상대적 중요성을 조정하는 상수(trade-off constant)이다.

식(1)에 관한 쌍대 문제(dual problem)를 구하기 위하여 라그랑제함수(Lagrange function) $L$을 도입한다.

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

학습 종료 후 적용 과정에서, 각각 클래스의 결정함수는 다음과 같이 정의된다.

$$\begin{aligned} f_k(x) &= R_k^2 - \Big[1 - 2\sum_{i=1}^{N_k} \alpha_i^k k_k(x_i^k, x) \\ &\quad + \sum_{i=1}^{N_k}\sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k)\Big] \ge 0 \end{aligned} \tag{3}$$

서로 다른 특징 공간상에서 정의되는 단일 SVM의 출력 $f_k(x)$값은 각 클래스의 특징 공간상의 경계로부터 해당 테스트 데이터와의 절대 거리를 의미함으로 서로 다른 특징 공간

상의 절대거리를 비교하여 소속 클래스를 결정하는 것은 바람직하지 않다. 따라서 특징 공간상의 절대거리 $f_k(x)$를 특징 공간상에서 정의되는 구형체의 반경 $R_k$로 나눔으로서 상대적 거리 $\hat{f}(x) = f_x(x)/R_k$를 계산하고, 상대거리가 가장 큰 클래스를 입력 데이터 $x$의 소속 클래스로 결정한다

$$\begin{aligned} &\text{Class of } x \equiv \arg \max_{k=1,\ldots,K} \hat{f}_k(x) \\ &\equiv \arg \max_k \Big[ \Big\{ R_k^2 - \Big(1 - 2\sum_{i=1}^{N_k} \alpha_i^k k_k(x_i^k, x) \\ &+ \sum_{i=1}^{N_k}\sum_{j=1}^{N_k} \alpha_i^k \alpha_j^k k_k(x_i^k, x_j^k)\Big)\Big\}/R_k \Big] \end{aligned} \quad (4)$$

### 2.2 SVDD 기반의 트래픽 폭주 공격 탐지 시스템

본 장에서는 실제 네트워크 환경에 적용 가능한SVDD 기반의 트래픽 폭주 공격 탐지와 세분화된 공격유형별 분류에 대하여 설명한다. 본 논문에서 제안된 모델의 각 계층별 기능은 다음과 같다: 첫 번째 계층은 네트워크망의 트래픽 정보 중 정상 트래픽만으로 학습된 단일 클래스 SVM으로서 정상트래픽과 공격트래픽에 대한 경량적 실시간 탐지를 보장한다또한 학습 시 정상트래픽만을 요구함으로 학습을 위한 별도의 공격트래픽을 준비할 필요가 없으며, 학습 속도 또한 매우 빠르다. 학습된 단일 클래스 SVM은 비정상 탐지모델로써 시스템에서 학습되지 않은 새로운 공격(novel attack)을 탐지하며, 공격트래픽이 탐지되면 침입 대응 시스템(intrusion response system)에 침입 사실을 실시간으로 보고한다 두 번째 계층은 다중 클래스 SVM 구조로써 트래픽 폭주 공격으로 판단된 공격트래픽을 DDoS의 대표적 공격유형인 TCP SYN flooding, UDP flooding, ICMP flooding으로 각 각 분류하고 침입 대응 시스템에 공격유형에 대한 추가적인 정보를 제공한다또한, 공격유형별로 분류되지 못한 공격트래픽 혹은그리고 시스템에서 학습되지 않은 새로운 공격유형을 별도의 클래스로 분류함으로써 실제 시스템의 유지 및 안전성을 보장하였다.프로토콜별 공격유형을 분류함으로써 전체 네트워크 시스템의 마비가 아닌 공격이 발생한 프로토콜에 대해서만 서비스의 제한 및 관리가 가능하기 때문에 안정적인 네트워크의 환경 유지시스템 자원관리 및 서비스를 보장할 수 있다. 아래의 그림 1은 본 논문에서 제안하는 SNMP MIB 정보를 이용한 트래픽 폭주 공격 탐지 시스템의 전체적인 구성도를 보여준다.

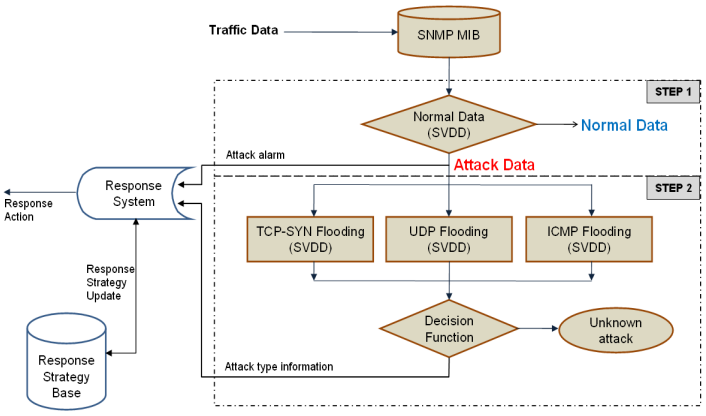


그림 1. SVDD 기반 트래픽 폭주 공격 탐지 시스템의 구조도

## 3. 실험 및 결과 분석

본 논문에서 사용된 MIB 객체들은 모든 SNMP agent에서 공통으로 제공하는 RFC1213[7]에서 정의된 MIB-2 그룹의 MIB 객체들과 실제 공격에서 반응하는 MIB 객체들로 구성되었다. 아래의 [표 1]에서는 본 논문의 실험에서 사용된 MIB 객체들을 정리하였다. 본 실험에서 사용한 트래픽 폭주 공격의 대표적 공격 툴인 Stacheldraht[8]는 다른 트래픽 폭주 공격 툴인 Trinoo, TFN, TFN2K에 비하여 공격방법 및 형태가 더욱 발전되고 견고해진 툴로써, 이전 연구에서 공격 시 반응을 보였던 MIB 정보인 tcpInErrs와 udpNoPorts에 대하여 반응을 보이지 않았다. 이는 Stacheldraht가 트래픽 폭주 공격의 대상이 되는 클라이언트의 포트를 미리 스캔한 후 공격트래픽에 사용 가능한 포트번호로 할당하고 TCP 세그먼트의 체크 합(check sum) 값 등을 정상적인 값으로 위장하기 때문이다.본 실험에서는 실험 결과의 정확도 및 실시간 탐지 성능 분석을 위하여 SNMP MIB 정보의 최소 갱신 주기인 15초 단위로 [표 1]에서와 같이 Interface, IP, TCP, UDP, ICMP 그룹에서 선정된 12개의 MIB 객체 정보를 수집하였다. 실험에서 사용한 데이터는 정상트래픽 1,000개와 공격트래픽별 TCP SYN flooding, UDP flooding, ICMP flooding을 각각 200개씩 생성하여 실험하였다.

[표 1] 탐지 시스템에서 사용된 MIB 객체들

| MIB-2 Group | SNMP MIB objects |
|---|---|
| Interface | interface.ifTable.ifEntry.ifInOctets<br>interface.ifTable.ifEntry.ifInUcastPkts |
| IP | ip.ipInReceives<br>ip.ipInDelivers<br>ip.ipOutDiscards |
| TCP | tcp.tcpAttemptFails<br>tcp.tcpOutRsts |
| UDP | udp.udpInErrors |
| ICMP | icmp.icmpInDestUnreachs<br>icmp.icmpOutDestUnreachs<br>icmp.icmpOutEchoReps<br>icmp.icmpOutMsgs |

첫 번째 실험은 정상트래픽과 공격트래픽을 신속하게 탐지하는 실험으로 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)를 성능지표로 사용했으며 실험결과는 [표 2]에 정리하였다. 여기서 조정상수 C는 0.1, 커널 함수인 가우시안 함수의 상수 $\sigma$ 값은 0.02로 고정하였다.

$$\text{침입 탐지율} = \frac{\sum_{i=1}^{n} T_i}{\sum_{i=1}^{n} I_i} \quad (5)$$

$$FPR = \frac{\sum_{i=1}^{n} P_i}{\sum_{i=1}^{n} N_i} \quad (6)$$

$$FNR = \frac{\sum_{i=1}^{n} F_i}{\sum_{i=1}^{n} I_i} \quad (7)$$

위 식에서 $I$는 공격트래픽, $T$는 공격트래픽을 정확히 공격으로 분류한 트래픽, $N$은 정상트래픽, $P$는 정상트래픽을 공격으로 분류한 트래픽, $F$는 공격트래픽을 정상으로 판단한 트래픽을 의미한다.

[표 2] 트래픽 폭주 공격 탐지의 성능 측정 표

| 항목 / $\sigma$ | 침입 탐지율 | FPR | FNR |
|---|---|---|---|
| 0.02 | 99.33 | 2.5 | 0.67 |

[표 2]의 성능 평가를 위한 항목 중FPR은 정상트래픽을 공격트래픽으로 오 판정한 비율을 나타내며 이는 시스템에 큰 영향을 미치지 않지만, FNR은 공격트래픽을 정상트래픽으로 판단하는 비율로써 보안상 커다란 문제점을 야기하는 매우 중요한 지표이다. 본 실험의 결과에 의하면 $\sigma$ 값이 0.02일 때 모두 만족스러운 침입 탐지율과 안전한 FNR(0.67)을 보여줌을 확인할 수 있었다.

두 번째 실험은 DDoS의 대표적 공격유형인 TCP SYN flooding, UDP flooding, ICMP flooding으로 분류하는 실험으로써 공격유형별로 랜덤하게 150개씩 각각의 SVDD로 학습하였으며, 학습에 참여하지 않은 공격유형별 트래픽50개로 테스트 하였다. 이때 150개의 공격트래픽 중 TCP SYN flooding 공격트래픽 1개가 정상트래픽으로 분류되어 실제 분류 테스트에 참여한 공격트래픽은 총149개이다. 성능 측정을 위하여 분류 정확도(classification accuracy)를 성능지표로 사용했으며 실험결과는 [표 3]에 정리하였다. 여기서 조정상수 C는 0.1, 커널 함수인 가우시안 함수의 상수 $\sigma$ 값은 TCP: 0.4, UDP: 0.3, ICMP: 0.1로 각각 고정하였다.

$$\text{분류정확도} = \frac{\sum_{i=1}^{n} T_i}{\sum_{i=1}^{n} I_i} \quad (8)$$

위 식에서 $I$는 해당 클래스의 공격트래픽 총 개수, $T$는 해당 클래스의 공격트래픽을 정확히 해당 클래스의 공격으로 분류한 개수를 의미한다.

[표 3] 트래픽 폭주 공격유형별 분류 정확도

| 분류정확도(항목별) / $\sigma$ | 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 |

[표 3]의 3가지 공격유형별로 $\sigma$ 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 못한ICMP flooding 공격트래픽 1개는 TCP flooding 클래스로 분류됨을 확인할 수 있었다.

## 4. 결 론

본 논문에서는 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. 만족스러운 침입 탐지율과 안전한 FNR, 공격유형별 분류 수치 등을 실험을 통하여 확인함으로써 제안된 시스템의 성능을 검증하였다.

향후 연구 과제로는 보다 정확하고 빠른 탐지를 위한SNMP MIB 객체의 선정과 적용에 관한 연구가 요구된다.

## 참고 문헌


[1] Myung-Sup Kim, Hun-Jeong Kang, Seong-Cheol Hong, Seung-Hwa Chung, and James W. Hong, "A flow-based method for abnormal network traffic detection", Proc. of NOMS 2004, Seoul, Korea, Apr. 19-23, pp. 559-612, 2004.

[2] Jun Li and C. Manikopoulos, "Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters", Information Assurance Workshop, IEEE, pp. 53~59, 2003.

[3] L. P. Gaspary, R. N. Sanchez, D. W.Antunes, and E. Meneghetti, "A SNMP-based platform for distributed stateful intrusion detection in enterprise networks", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 10, pp. 1973~1982, 2005.

[4] Steven Noel, Duminda Wijesekera, and Charles Youman, "Modern intrusion detection, data mining, and degrees of attack guilt", in Applications of Data Mining in Computer Security, Kluwer Academic Publisher, pp. 1-31, 2002.

[5] Hansung Lee, Jiyoung Song, and Daihee Park, "Intrusion detection system based on multi-class SVM", RSFDGrC 2005, LNAI, Vol. 3642, pp. 511-519, 2005.

[6] T. Ambwani, "Multi class support vector machine implementation to intrusion detection", Proceedings of the International Joint Conference on Neural Networks, Vol. 3, pp. 2300~2305, 2003.

[7] IETF RFC 1213, "Management information base for network management of TCP/IP-based internets: MIB-II", http://www.rfc-editor.org/rfc/rfc1213.txt.

[8] "Distributed denial of service (DDoS) attacks/tools", http://staff.washington.edu/dittrich/misc/ddos/.