DOI: 10.3745/KIPSTC.2008.15-C.5.351

SVM을 이용한 SNMP MIB에서의 트래픽 폭주 공격 탐지

유 재 학[†] · 박 준 상[††] · 이 한 성[†††] · 김 명 섭[††††] · 박 대 희[†††††]

요 약

DoS/DDoS로 대표되는 트래픽 폭주 공격은 대상 시스템뿐만 아니라 네트워크 대역폭 및 프로세서 처리능력, 시스템 자원 등을 고갈시킴으로써 네트워크에 심각한 장애를 유발하기 때문에, 신속한 트래픽 폭주 공격의 탐지는 안정적인 서비스의 제공 및 시스템의 운영에 필수요건이다. 전통적인 패킷 수집을 통한 DoS/DDoS의 탐지방법은 공격에 대한 상세한 분석은 가능하나 설치의 확장성 부족, 고가의 고성능 분석시스템의 요구, 신속한 탐지를 보장하지 못하는 문제점을 갖고 있다. 본 논문에서는 MIB 정보 갱신 시점 단위로 수집된 SNMP MIB 객체 정보를 바탕으로 Support Vector Data Description(SVDD)을 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(FNR), 공격유형별 분류율 수치 등을 확인함으로써 제안된 시스템의 성능을 검증하였다.

키워드 : 침입탐지, SNMP, MIB, DoS/DDoS, Support Vector Machine

Traffic Flooding Attack Detection on SNMP MIB Using SVM

Jaehak Yu[†] · Jun-Sang Park[††] · Hansung Lee[†††] · Myung-Sup Kim[††††] · Daihee Park[†††††]

ABSTRACT

Recently, as network flooding attacks such as DoS/DDoS and Internet Worm have posed devastating threats to network services, rapid detection and proper response mechanisms are the major concern for secure and reliable network services. However, most of the current Intrusion Detection Systems(IDSs) focus on detail analysis of packet data, which results in late detection and a high system burden to cope with high-speed network environment. In this paper we propose a lightweight and fast detection mechanism for traffic flooding attacks. Firstly, we use SNMP MIB statistical data gathered from SNMP agents, instead of raw packet data from network links. Secondly, we use a machine learning approach based on a Support Vector Machine(SVM) for attack classification. Using MIB and SVM, we achieved fast detection with high accuracy, the minimization of the system burden, and extendibility for system deployment. The proposed mechanism is constructed in a hierarchical structure, which first distinguishes attack traffic from normal traffic and then determines the type of attacks in detail. Using MIB data sets collected from real experiments involving a DDoS attack, we validate the possibility of our approaches. It is shown that network attacks are detected with high efficiency, and classified with low false alarms.

Keywords : Intrusion Detection, SNMP, MIB, DoS/DDoS, Support Vector Machine

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 컴퓨터의 시스템은 물론 네트워크의 자원을 고갈시킴으로써, 정상적인 서비스를 수행하지 못하게 하는 공격으로 업무에 막대한 피해를 준다. 안전한 네트워크 운영과 관리를 위하여, 이러한 악의적 접근이나 침입 등을 신속하게 탐지하고 대처할 수 있는 보안 기술이 학계의 최근 중요한 이슈 중 하나이다[1-5].

침입탐지 방법론은 침입에 대한 탐지 전략에 따라 크게 오용 탐지(misuse detection) 모델과 비정상 탐지(anomaly

※ 이 논문은 산업자원부 및 한국산업기술평가원의 성장동력 기술개발사업 및 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원(KRF-2007-331-D00387)을 받아 수행된 연구임
† 준 회 원 : 고려대학교 전산학과 박사과정
†† 준 회 원 : 고려대학교 컴퓨터정보학과 석사과정
††† 정 회 원 : 고려대학교 전산학과 강사
†††† 정 회 원 : 고려대학교 컴퓨터정보학과 조교수(교신저자)
††††† 정 회 원 : 고려대학교 컴퓨터정보학과 교수
논문접수 : 2008년 4월 1일
수 정 일 : 2008년 5월 30일
심사완료 : 2008년 6월 13일

detection) 모델로 나누어진다[6]. 오용 탐지모델은 이미 발견된 공격유형에 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. 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[7-8]. 그러나 이러한 새로운 방법론 역시 전통적인 네트워크의 패킷 정보를 이용하고 있음을 알 수 있다.

기존에 연구된 트래픽 폭주 공격 탐지에서의 전통적인 패킷 수집 방법론[1-3]은 공격에 대한 상세한 분석은 가능하지만 고가의 고성능 분석시스템이 요구될 뿐만 아니라 설치 및 운영상의 확장성이 부족하다는 단점을 가지고 있다. 따라서 이를 보완하기 위한 방법으로 최근 SNMP에서의 MIB 정보를 이용한 침입탐지 방법론[3-5]이 주목을 받고 있다. SNMP MIB 데이터를 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[2-4]. 이는 대부분의 네트워크 기반 시스템들이 기본적으로 SNMP agent를 탑재하고 있기 때문이다. 따라서 SNMP MIB 정보를 이용한 트래픽 폭주 공격의 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.

최근의 연구동향 중, 기계학습 기법과 SNMP MIB 정보를 이용한 매우 흥미로운 몇 개의 침입탐지 시스템이 발표되었다: Li 등[3]은 SNMP MIB-II 데이터를 probability density function으로 변환한 후, backpropagation 기반의 인공신경망을 이용하여 침입 여부를 결정하는 시스템을 제안하였다. Puttini 등[9]은 SNMP MIB 데이터를 Bayesian 분류기에 적용하여 Mobile Adhoc NETworks (MANET)에서의 비정상 트래픽을 탐지하였다. 또한, Ramah 등[10]은 Shyu 등[11]이 제안한 Principle Component Analysis(PCA) 기반의 비정상 탐지 알고리즘을 이용한 탐지시스템을 제안하였다. 이러한 연구들은 모두 침입의 탐지에만 주력하였을 뿐, 공격 종류들의 분류문제까지는 고려하지 않았다. 더욱이, backpropagation과 Bayesian과 같은 기계학습 기법들이 선택적으로 사용되었으나, SVM기반의 기법들은 적용되지 않았음을 알 수 있다. 결과적으로 좋은 성질들을 많이 지니고 있는 SNMP MIB 데이터의 이용과 패턴분석을 위한 자동화 알고리즘의 역사적 진화과정 중, 가장 강력하다고 이미 검증된 SVM을 이용하여 트래픽 폭주공격을 탐지하고 공격유형별 분류를 수행하는 시스템을 설계하는 시도는 현 시점에서 매우 의미가 크다고 할 수 있다.

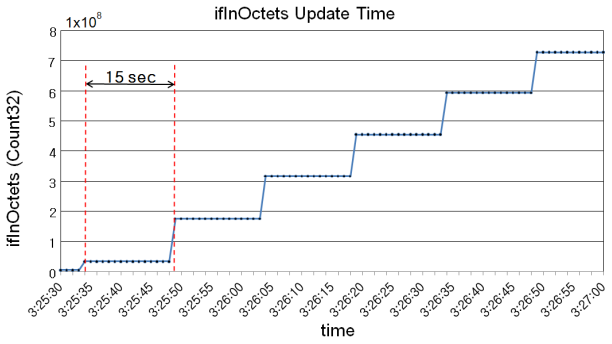
본 논문에서는 패턴 분류 등의 문제에서 매우 우수한 성능을 보이는 SVM을 기반으로 SNMP MIB 정보를 이용하여 보다 가볍고 신속하게 트래픽 폭주공격을 탐지하고 공격유형별 분류를 수행하는 시스템을 제안한다. 본 시스템은 단일 클래스 SVM(One-class SVM)을 기반으로 정상트래픽과 공격트래픽을 빠르게 탐지하는 계층과 탐지된 공격트래픽을 다중 클래스 SVM(Multi-class SVM)을 기반으로 DDoS의 대표적 공격유형인 TCP-SYN flooding, UDP flooding, ICMP flooding으로 분류하는 계층으로 구성된다. 공격유형별 분류는 공격이 발생한 프로토콜에 대해서만 서비스를 제한하고 관리함으로써 보다 안정적인 네트워크의 환경과 원활한 자원관리를 지원할 수 있다. 본 시스템은 SNMP의 MIB을 이용함으로 기존의 패킷 수집 방법론들의 단점인 고가의 고성능 분석시스템의 요구와 설치의 확장성 문제점들을 보완하는 견지에서 다음의 평가 기준들을 모두 만족 한다: 1) 실시간 침입탐지 및 서비스의 안전성 보장; 2) 쉬운 확장성 및 MIB 정보를 이용한 저비용 탐지; 3) 공격유형 시스템의 효율적인 대처 보장; 4) 시스템에서 학습되지 않은 새로운 공격유형의 탐지.

본 논문의 구성은 다음과 같다. 2장에서는 SNMP관련 몇 가지 고려사항을 기술하며, 3장에서는 본 논문에서 제안하는 SNMP-SVM 기반의 계층적 트래픽 폭주 공격 탐지 시스템에 대해 기술한다. 4장에서는 실험결과 및 성능 분석을 기술하며, 마지막으로 5장에서는 결론 및 향후 연구과제에 대해 논한다.

2. SNMP 관련 고려사항

SNMP는 네트워크 및 시스템의 관리를 위한 표준화된 다양한 정보를 제공하지만 SNMP를 이용한 효율적인 트래픽 폭주 공격의 탐지를 위해서는 SNMP의 구조적인 특징으로 인하여 다음의 3 가지 요소를 고려해야한다: 1) 트래픽의 특징을 반영하는 MIB 정보의 선정; 2) MIB 정보의 수집 및 분석 시점의 결정; 3) 수집된 MIB 기반의 탐지 알고리즘.

첫째, MIB 정보의 선정은 우선 다양한 시스템에 적용할 수 있도록 표준화된 MIB 정보에서 선정을 해야 하며, 다양한 시스템의 정상 트래픽 발생 상황과 트래픽 폭주 공격 시 트래픽 상황을 구분할 수 있도록 폭넓은 MIB 정보를 포함해야 한다. 또한, 수집 및 분석 시스템 그리고 네트워크의 부



(그림 1) *ifInOctets*의 갱신 주기

하를 최소화 할 수 있도록 필수적인 MIB 정보만을 수집해야한다.

둘째, 트래픽 폭주 공격이 분산화 되고 고속화됨에 따라 빠른 탐지는 탐지 시스템의 필수요건이 되었다. 반면에 빠른 탐지를 위해 MIB 정보의 수집 및 분석 주기를 단축하게 되면 시스템 및 네트워크의 부하가 증가하게 되므로 적절한 탐지 시점의 결정은 탐지 시스템의 성능을 좌우하는 매우 중요한 요소이다.

(그림 1)은 특정 시스템에서 mib-2 interface 그룹의 *ifInOctets* 값을 매 1초단위로 보여 주고 있다. 그림에서 보듯이 MIB 값은 특정한 주기를 기준으로 갱신됨을 알 수 있다. 그러나 기존의 탐지 시스템[12, 13]들은 1분 또는 그 이상의 주기로 동작하는 Timer를 기준으로 수행하기 때문에 MIB의 갱신 주기가 반영되지 않아 탐지 시간의 지연이 발생한다. MIB의 갱신 주기를 기준으로 탐지 시스템이 동작한다면 탐지의 정확성과 탐지 시간을 향상시킬 것으로 기대된다. 그러나 짧은 탐지 주기는 탐지를 위한 소비 트래픽과 시스템 부하를 증가시키기 때문에 이를 고려한 효율적인 탐지 시점 결정 알고리즘이 요구된다.

셋째, 전통적인 SNMP MIB 기반의 DDoS 탐지 방법은 프로토콜별 추이분석, 일주 트래픽 추이분석, 그리고 객체 정보간의 상관관계를 이용하는 방법 등이 있다 [3-5]. 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 매우 유동적이고 변화가 심한 네트워크에서의 트래픽 예측이 어렵다는 단점이 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. 그러나 기준이 되는 추이 트래픽 설정이 어렵다는 문제점을 가지고 있다. 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 어렵다.

최근의 트래픽 폭주 공격 방법들이 날로 다양해지고 견고해짐으로 전통적인 SNMP MIB 기반의 트래픽 폭주 공격 탐지 방법들은 실제 시스템에 적용하기에는 현실적으로 많은 문제점이 있다. 현존하는 MIB 기반의 DDoS 탐지 시스템들은 대부분 테스트에 사용된 당시의 DoS 공격툴의 기능과 특성에 의존적으로 개발된 시스템으로 새로운 공격유형이나 끊임없이 발전하는 공격툴에 유연하게 대처하기 어렵다. 즉 새로운 공격 형태나 툴이 발견되면 그때마다 새롭게 알고리즘 전체를 수정해야만 하는 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.

3. 트래픽 폭주 공격 탐지 시스템

본 장에서는 2장에서 논의한 SNMP 기반의 트래픽 폭주 공격 탐지에서 고려해야할 사항들의 해결 방안을 상세하게 기술함으로써 본 논문에서 제시하는 SNMP-SVM 기반의 트래픽 폭주공격 탐지 시스템을 설명한다.

3.1 MIB 정보의 선정

본 논문에서는 RFC1213[14]에서 정의한 mib-2 그룹의 MIB 객체들 중, 실제 트래픽 폭주 공격에 반응하는 MIB 객체들만을 선정하였다. 즉, MIB 객체의 선정을 위하여 트래픽 폭주 공격의 대표적 공격 툴인 Stacheldraht[15]를 이용하여 TCP-SYN Flooding 공격, UDP Flooding 공격, ICMP Flooding 공격 등을 타깃 시스템에 실시하였으며, mib-2 그룹의 모든 MIB 객체들의 전수 조사를 실시하였다. 본 논문의 실험에서 사용된 MIB 객체들을 <표 1>에 정리하였다.

〈표 1〉 탐지 시스템에서 사용된 MIB 객체들

mib-2 Group	SNMP MIB objects
interface	interface.ifTable.ifEntry.***ifInOctets*** interface.ifTable.ifEntry.***ifInUcastPkts***
ip	ip.***ipInReceives*** ip.***ipInDelivers*** ip.***ipOutDiscards***
tcp	tcp.***tcpAttemptFails*** tcp.***tcpOutRsts***
udp	udp.***udpInErrors***
icmp	icmp.***icmpInDestUnreachs*** icmp.***icmpOutDestUnreachs*** icmp.***icmpOutEchoReps*** icmp.***icmpOutMsgs***

3.2 MIB 정보의 수집 및 탐지 시점의 결정

SNMP agent는 MIB 정보가 갱신된 시점으로부터 다음 갱신 시점까지는 동일한 MIB 값을 제공하기 때문에 MIB 정보 갱신 시점 직후에 MIB 정보를 수집하는 것이 보다 빠른 탐지를 위해 효과적이다. 따라서 본 논문에서는 아래와 같은 방법을 이용하여 MIB 정보의 갱신 시점을 탐지하고 MIB 정보를 수집하였다.

갱신주기의 탐지를 위해 mib-2 interface 그룹의 *ifInOctets* MIB값을 1초 단위로 확인한다. 갱신 시점의 확인을 위해 매 초 SNMP 메시지 발생에 따른 트래픽의 부하를 줄이기 위하여 본 논문에서는 식 (1)에서와 같이 현재까지의 갱신주기 $\{U_0, U_1, ..., U_{n-1}\}$와 갱신 주기의 지수 평균을 이용하여 다음의 갱신 시점을 예측 (P_n)하고 이로부터 sleep 시간 (S_n)을 결정하여 sleep함으로써 소비 트래픽과 관리 시스템의 부하 증가 문제를 해결하였다. 여기서, 상수 α 값은 0.5를 사용하였다.

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

MIB의 갱신 주기는 SNMP Agent와 시스템에 따라 다르고, 같은 시스템이라 하더라도 시간에 따라 변할 수 있기 때문에 각 갱신 주기에 대한 유동성을 고려한 지수평균(exponential average)값을 적용하여 보다 효율적으로 탐지 시점을 결정할 수 있다. U_n은 실제 측정된 *ifInOctets* MIB 정보의 갱신 주기이며, 최초 갱신 주기 U_0는 시스템 적용 전 일정시간 동안 매초 SNMP 메시지를 발생하여 측정한 갱신 주기들의 최소값으로 결정된다. 탐지 시점의 결정을 위한 알고리즘에서 사용된 기호들을 <표 2>에 정리하였다.

〈표 2〉 탐지 시간 향상 방법에서 사용된 기호

U_n	n 번째 *ifInOctets* 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)

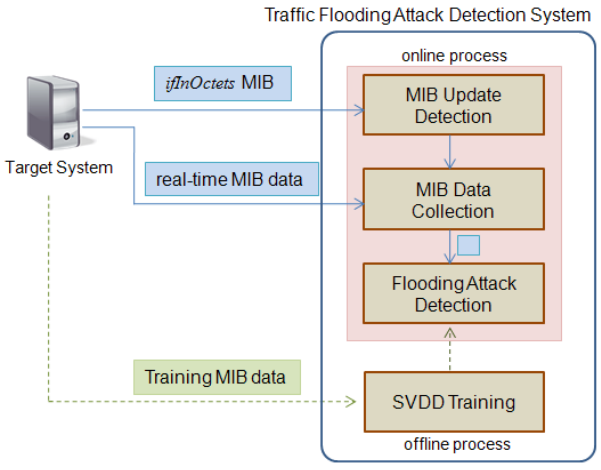
3.3 단일 클래스 SVM 기반의 공격 탐지

통계적 학습이론(statistical learning theory)에 기반을 둔 SVM은 주어진 문제를 항상 전역적 최적해가 보장되는 convex quadratic problem으로 변환하여 해를 구하기 때문에 패턴인식 분야에서 매우 우수한 성능을 보여주고 있다[7]. 그러나 이진 분류기라는 SVM의 기능적 한계점으로 인하여, 주어진 문제가 현재 우리가 다루고자 하는 공격유형의 분류와 같이 다중 분류 문제에는 SVM을 직접적으로 적용할 수가 없다. 따라서 여러 개의 이진 분류기인 SVM을 유기적으로 결합하여 다중 클래스 SVM을 설계하는 것이 일반적인 연구 방법론이다[7-8]. 그러나 SVM을 이용하여 다중 클래스 SVM을 설계할 경우, 각 SVM은 관측되지 않은 영역을 포함하여 결정 경계면을 생성함으로써 새로운 데이터에 대하여 오분류(misclassification)할 가능성이 높다. 그러므로 해당 클래스만을 독립적으로 표현하는 단일 클래스 분류기로서 결정 경계면을 선택하는 것이 다중 클래스 SVM의 설계 시 보다 유리하다. 따라서 본 논문에서는 단일 클래스 SVM의 대표적인 알고리즘인 SVDD를 기반으로 설계된 본 연구실의 다중 클래스 SVM[7, 16]을 일부 변형하여 공격유형을 분류하는 시스템으로 사용한다.

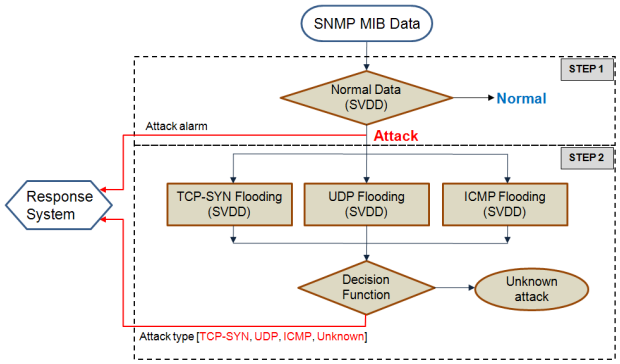
3.4 트래픽 폭주 공격 탐지 시스템

본 논문에서 제안하는 트래픽 폭주 공격 탐지 시스템은 총 4개의 모듈로 구성된다. 즉, 1개의 오프라인 처리 모듈인 SVDD Training 모듈과 3개의 온라인 처리 모듈인 MIB Update Detection, MIB Data Collection, Flooding Attack Detection 모듈로 구성된다(그림 2 참조). 1) SVDD Training 모듈에서는 다양한 트래픽 공격을 임의로 발생시켜 수집된 MIB 정보를 바탕으로 SVDD 기반의 학습을 실시한다. 2) MIB Update Detection 모듈은 *ifInOctets* MIB을 수집하여 탐지 시스템의 동작 시점을 결정하고 MIB Data Collection 모듈을 실행 시킨다. 3) MIB Data Collection 모듈은 MIB 정보를 타깃 시스템으로부터 수집한다. MIB 정보의 수집을 위해 SNMP의 GetRequest 메시지를 사용하고, 하나의 메시지에 12개의 MIB 정보를 모두 포함시킴으로써 트래픽 사용량을 최소화한다. 4) 수집된 정보는 Flooding Attack Detection 모듈로 전달되어 공격유무와 공격유형을 판단한다.

Flooding Attack Detection 모듈은 SVDD Training 모듈에서 성능이 검증된 SVDD들로 구성된 계층적 구조의 폭주 공격 탐지 모듈로써 공격의 탐지뿐만 아니라 공격의 유형까지 판단한다(그림 3 참조). 제안된 Flooding Attack Detection 모듈의 각 계층별 기능은 다음과 같다.



(그림 2) 트래픽 폭주 공격 탐지 시스템의 전체 구조도



(그림 3) SVDD 기반 탐지 모듈의 계층적 탐지 절차

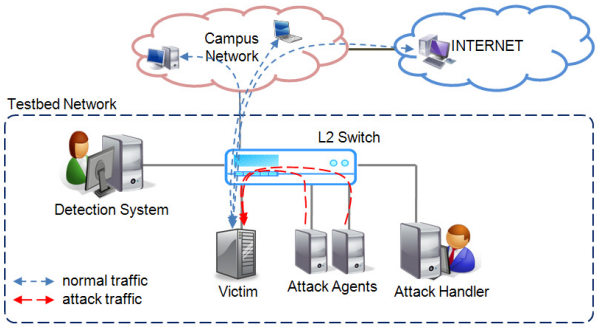
첫 번째 계층은 네트워크의 트래픽 정보 중 정상트래픽만으로 학습된 SVDD로써 정상트래픽과 공격트래픽에 대한 실시간 탐지를 보장하며 점증적 갱신도 가능하다. 또한 학습 시 정상트래픽만을 요구함으로 학습을 위한 별도의 공격트래픽을 준비할 필요가 없으며, 학습 속도 또한 다른 SVM에 비해 상대적으로 빠르다. 학습된 단일 클래스 SVM은 비정상 탐지 모델로써 시스템에서 학습되지 않은 새로운 공격(novel attack)을 탐지하며, 공격트래픽이 탐지되면 공격 대응 시스템(Attack Response System)에 침입 사실을 실시간으로 보고한다.

두 번째 계층은 다중 클래스 SVM 구조로써 트래픽 폭주 공격으로 판단된 공격트래픽을 대표적 공격유형인 TCP-SYN flooding, UDP flooding, ICMP flooding으로 각각 분류하고 침입 대응 시스템에 공격유형에 대한 추가적인 정보를 제공한다. 또한, 공격유형별로 분류되지 못한 공격트래픽과 시스템에서 학습되지 않은 새로운 공격유형을 별도의 클래스로 분류함으로써 실제 시스템의 유지 및 안전성을 보장한다. 프로토콜별 공격유형을 분류함으로써 전체 네트워크 시스템의 중지가 아닌 공격이 발생한 프로토콜에 대해서만 서비스의 제한 및 관리가 가능하기 때문에 안정적인 네트워크의 환경 유지와 시스템의 자원관리 및 서비스를 보장할 수 있다.

4. 실험 및 결과 분석

4.1 실험 환경

본 논문에서 제시한 탐지 방법론의 평가를 위하여 (그림 4)와 같이 실험 환경을 구축하였다: 트래픽 폭주 공격 실험을 위하여 하나의 L2 스위치 장비에 타깃 시스템 (Victim)을 연결하고, 분산 DoS 공격 환경을 만들기 위하여 2대의 Attack Agent와 1대의 Attack Handler를 L2 스위치 장비에 연결하였다. 또한 타깃 시스템으로부터 MIB 정보의 수집 및 탐지를 위하여 1대의 탐지 시스템을 L2 스위치에 연결하였다. L2 스위치는 학내 네트워크를 통하여 인터넷과 연결되어 있기에 타깃 시스템에서는 다양한 인터넷 트래픽이 생성



(그림 4) 실험 환경 구성도

된다. 실제 타깃 시스템에 Apache Web Server, VNC Server, FTP Server, SSH Server, Samba Server 등의 다양한 서버를 운영함으로써 다양한 종류의 정상 트래픽을 발생하였다. 본 실험에서 사용된 시스템은 모두 Linux Fedora 7 또는 8이며, 타깃 시스템의 SNMP Agent는 Net-SNMP v5.4.1이 사용되었다.

4.2 실험 내용 및 결과

본 실험에서 사용한 트래픽 폭주 공격의 대표적 공격 툴인 Stacheldraht[15]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 Linux상에서 동작하는 Net-SNMP agent의 SNMP MIB 정보 갱신 주기인 15초 단위로 표 1에서와 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.

첫 번째 실험은 정상 트래픽과 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)을 성능지표로 사용했으며 실험결과는 표 3에 정리하였다. 여기서 조정상수 C는 0.1, 커널 함수인 가우시안 함수의 상수 σ 값은 0.02로 고정하였다.

$$\text{침입탐지율} = \frac{\sum_{i=1}^{n} T_i}{\sum_{i=1}^{n} I_i} \quad (2)$$

$$FPR = \frac{\sum_{i=1}^{n} P_i}{\sum_{i=1}^{n} N_i} \quad (3)$$

$$FNR = \frac{\sum_{i=1}^{n} F_i}{\sum_{i=1}^{n} I_i} \quad (4)$$

위 식에서 I는 공격 트래픽, T는 공격 트래픽을 정확히 공격으로 분류한 트래픽, N은 정상트래픽, P는 정상트래픽을 공격으로 분류한 트래픽, F는 공격트래픽을 정상으로 판단한 트래픽을 의미한다.

<표 3>의 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. 본 실험의 결과에 의하면, σ 값이 0.02일 때 모두 만족스러운 침입 탐지율과 안전한 FNR(0.67)을 보여줌을 확인할 수 있었다.

두 번째 실험은 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 실험결과는 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.

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

〈표 3〉 트래픽 폭주 공격 탐지의 성능 측정 표

항목 / σ	침입 탐지율	FPR	FNR
0.02	99.33	2.5	0.67

〈표 4〉 트래픽 폭주 공격유형별 분류 정확도

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

위 식에서 I는 해당 클래스의 공격트래픽 총 개수, T는 해당 클래스의 공격트래픽을 정확히 해당 클래스의 공격으로 분류한 개수를 의미한다.

<표 4>의 3가지 공격유형별로 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.

5. 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 위한 SNMP MIB 객체의 선정과 적용에 관한 연구가 요구된다. 또한, 탐지 시스템에 의해 탐지된 공격을 침입방지 시스템의 정책 수립과 연동하는 방안도 요구된다.

참 고 문 헌

[1] M. Kim, H. Kang, S. Hong, Seung-Hwa Chung, and J. 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] E. Duarte and Jr., A. L. Santos, “Network fault management based on SNMP agent groups”, Proc. of ICDCSW 2001, pp.51-56, 2001.

[3] J. Li and C. Manikopoulos, “Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters”, Information Assurance Workshop, IEEE, pp.53-59, 2003.

[4] 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.

[5] J. B. D. Cabrera, L. Lewis, X. Qin, C. Gutierrez, W. Lee, and R. K. Mehra, "Proactive intrusion detection and SNMP-based security management: new experiments and validation", IFIP/IEEE Eighth International Symposium on Integrated Network Management, pp.93-96, 2003.

[6] S. Noel, D. Wijesekera, and C. 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.

[7] H. Lee, J. Song, and D. Park, "Intrusion detection system based on multi-class SVM", RSFDGrC 2005, LNAI, Vol. 3642, pp.511-519, 2005.

[8] 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.

[9] R. Puttini, M. Hanashiro, F. Miziara, R. Sousa, L. García-Villalba, and C. Barenco, "On the anomaly intrusion-detection in mobile adhoc network environments", Proc. of PWC 2006, LNCS 4217, pp.182-193, 2006.

[10] K. Ramah, H. Ayari, and F. Kamoun, "Traffic anomaly detection and characterization in the Tunisian national university network", Proc. of Networking 2006, LNCS 3979, pp.136-147, 2006.

[11] M. Shyu, S. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," Proc. of the IEEE Foundations and New Directions of Data Mining Workshop, pp.172-179, Melbourne, Florida, USA, 2003.

[12] D. Yoo, and C. Oh, "Traffic gathering and analysis algorithm for attack detection", KoCon 2004 Spring Integrated Conference, Vol. 4, pp.33-43, 2004.

[13] 박준상, 조현승, 김명섭, "SNMP MIB의 상관 관계를 이용한 트래픽 폭주 공격 탐지", 통신 학회 추계종합학술발표회, 서울대학교, 서울, Nov. 17, pp.13-16, 2007.

[14] IETF RFC 1213, "Management Information Base for Network Management of TCP/Ip-Based Internets: MIB-II", http://www.rfc-editor.org/rfc/rfc1213.txt.

[15] "Distributed Denial of Service (DDoS) Attacks/tools", http://staff.washington.edu/dittrich/misc/ddos/.

[16] 이한성, 송지영, 김은영, 이철호, 박대희, "다 중클래스 SVM기반의 침입탐지 시스템," 퍼지 및 지능시스템학회 논문지, 제 15권, 제 3 호, pp.282-288, 2005.

유 재 학

e-mail : dbzzang@korea.ac.kr
2001년 건국대학교 전산과학과(학사)
2003년 고려대학교 전산학과(석사)
2003년~현 재 고려대학교 전산학과 박사과정
관심분야 : 데이터마이닝, 기계학습, 홈네트워크, 침입탐지

박 준 상

e-mail : runtoyou@korea.ac.kr
2008년 고려대학교 컴퓨터정보학과(학사)
2008년~현 재 고려대학교 컴퓨터정보학과 석사과정
관심분야 : 네트워크 관리 및 보안, 트래픽 모니터링 및 분석

이 한 성

e-mail : mohan@korea.ac.lr
1996년 고려대학교 전산학과(학사)
1996년~1999년 (주)대우엔지니어링 근무
2002년 고려대학교 전산학과(석사)
2008년 고려대학교 전산학과(박사)
2008년~현 재 고려대학교 전산학과 강사
관심분야 : 멀티미디어마이닝, 기계학습, 인공지능, 지능 데이터베이스, 침입탐지

김 명 섭

e-mail : tmskim@korea.ac.kr
1998년 포항공과대학교 전자계산학과 (학사)
1998년~2000년 포항공과대학교 컴퓨터 공학과(석사)
2000년~2004년 포항공과대학교 컴퓨터 공학과(박사)
2004년~2006년 Post-Doc., Dept. of ECE, Univ. of Toronto, Canada.
2006년~현 재 고려대학교 컴퓨터정보학과 조교수
관심분야 : 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 멀티미디어 네트워크

박 대 희

e-mail : dhpark@korea.ac.kr

1982년 고려대학교 수학과(학사)

1984년 고려대학교 수학과(석사)

1989년 플로리다 주립대학 전산학과(석사)

1992년 플로리다 주립대학 전산학과(박사)

1993년~현 재 고려대학교 컴퓨터정보학과 교수

관심분야 : 지능 데이터베이스, 데이터마이닝, 인공지능, 퍼지이론