결정트리를 이용한 네트워크 공격 탐지패턴의 자동생성 방법

장기영*, 김용민**, 김민수**, 노봉남**
*전남대학교 정보보호 협동과정
**전남대학교 전자 컴퓨터 정보통신 공학부
e-mail:beautyjang@lsrc.jnu.ac.kr

Automatic Generation of Detection Patterns for Network Attack using the Decision Tree

Ki-Young Jang*, Yong-Min Kim**, Min-Soo Kim**, Bong-Nam Noh**
*Interdisciplinary Program of Information Security,
Chonnam National University
**Department of Electronics, Computer and Information
Engeering, Chonnam National University
beautyjang@lsrc.jnu.ac.kr

요 약

오용행위와 비정상행위 그리고 알려지지 않은 공격을 탐지하기 위해 필요한 규칙들을 추출하는 방법이 계속 연구되고 있다. 기존의 네트워크 공격에 대한 침입탐지시스템의 탐지 패턴은 전문가의 수작업에 의해 생성되어 왔고, 수정이 필요할 경우 수작업을 필요로 했다. 그러나 네트워크 공격은 매시간 다양화되고 변형되기 때문에 적절한 대응이 필요하다. 본 논문에서는 이같은 문제를 결정트리를 사용하여 네트워크 패킷 내에서 공격형태를 패턴화하여 자동으로 탐지 패턴을 추출하는 방법을 제안한다.

1. 서론

현재 알려진 공격 기법을 분류하는 방법에는 공격의 대상이 단일 시스템인지 네트워크 자원 또는 네트워크 자체인지에 따라 시스템 공격과 네트워크 공격으로 분류되고, 이 공격을 탐지하는 방법에 따라 오용행위(misuse)와 비정상행위(anomaly)탐지로 나눈다. 최근에는 이에 추가하여 알려지지 않은 공격까지 탐지하려는 연구가 진행중이다. 알려지지 않은 공격에 대한 연구에는 데이터마이닝 기법, 면역시스템 분석 기법, 유전자 알고리즘등을 이용한다[1,2].

최근 공유폴더(135, 139, 445번 포트)에 대한 스캔, HTTP(80번 포트), 트로이 목마 등의 네트워크 공격이 증가추세에 있다[3]. 네트워크 공격에 대한 탐지는 네트워크 공격에 대한 패턴을 생성하여 탐지하는데, 이러한 패턴의 생성과 수정은 전문가의 분석에 의해 이루어져왔다.

본 논문에서는 네트워크 공격을 탐지하기 위한 규칙을 자동으로 생성하는 방법으로 데이터마이닝의 분류 기법 중 결정트리(Decision Tree) 알고리즘을 사용하여 대량의 네트워크 패킷을 분류하고, 분류된 각 결정트리의 노드들의 집합에서 네트워크 패킷을 정상과 공격으로 분류하는 규칙을 추출하는 방법을 제안한다.

2. 관련 연구

시스템에 침입하는 행위는 단일 호스트 및 다중 호스트에 의한 침입과 네트워크에 의한 침입행위에 따른 탐지의 방법이 필요하다. 각 공격은 그에 적합한 탐지의 방법이 필요한데, 네트워크 공격의 경우 네트워크 행위에 대한 정확한 모델링이 어렵고, 공격에 따른 항목들간의 연관 관계를 명확히 구분하기 힘들기 때문에 탐지에 어려움이 있다[4]. 이에 따라 정상행위 모델링의 방법으로 사용자의 정상행위 패턴을 생성하거나 사용자별, 사용자간의 행위를 프로

파일링하여 패턴을 추출하는 방법을 사용한다[5]. 따라서 대부분 생성된 패턴은 특정조건에만 한정적이고 필요에 따라 전문가의 분석에 의해 새로 생성되는 수밖에 없다.

2.1 네트워크 패킷에서 척도(measure)의 선택

침입 탐지 패턴을 생성하는데 가장 중요한 것은 네트워크 공격 패킷에서 어떤 형태로 특성(features)을 추출하느냐 하는 것이다. 네트워크 공격을 탐지할 수 있는 특징있는 척도를 선택하는데 있어 몇 가지 방법이 연구되었다. 플로리다 대학은 척도선정에 관한 연구에서 이더넷의 각 필드, 즉 IP, TCP, UDP, ICMP 프로토콜의 33개 필드값의 특징적인 값들을 추출하고 유사도를 비교하였으나 DARPA 99년 로그 분석에서 탐지율이 50%정도에 그치고 있다[6]. 또다른 유형의 특징을 추출하는 방법은 패킷들의 연관성을 고려한 것이다. 이 방법은 SVM 기반 IDS를 통해 정상행위, PROBE, DOS, U2SE, R2L 공격에서 41개의 특징을 추출한다. 몇 가지의 추가적인 규칙을 적용하여 41개의 특징 중 각 공격에 적당한 특징을 갖는 항목을 선정하였다. 41개의 특징은 공격 특성에 따라 표 1과 같이 분류된다[7,8].

표 1. 공격 형태에 따른 특징의 분류

공 격	선택 특징
Normal	Duration, Service, Source bytes, Destination bytes, Hot indicators, File creations, Count, REG error rate, Same service-REG error rate, Same service rate, Destination-Host-Service-Count, Destination-Host-Same source-port rate, Destination-Host-Service source SYN error rate
Probe	Service, Source bytes, Count, Same service rate, Destination-Host Count, Destination-Host-Same service Count
DoS	Duration, Source bytes, Destination bytes, Count, Same service rate, Connections with SYN errors, Connections-Same service-SYN errors, Destination-Host-Same source-port rate, Destination-Host-Same-Service error rate
U2SE	Source bytes, Destination bytes, Destination-Host Count, Destination-Host-Service Count
R2L	Service, Source bytes, Destination bytes, Destination-Host-Count, Destination-Host-Service

2.2 네트워크 침입탐지에서 결정트리

결정트리는 네트워크 패킷과 같은 크고 성장하는 데이터를 빠른 시간에 분류하기에 적합하다. 결정트리는 크게 노드와 잎, 그리고 노드와 노드, 노드와 잎을 연결하는 줄기로 구성된다. 패킷탐지에서 각각의 노드는 패킷을 정상과 공격으로 구분하는 역할을 하는 규칙(rule)으로 구성되고 잎은 최종 탐지의 결과를 나타내고, 하위 노드는 상위노드의 속성을 이어받는다[9].

3. 네트워크 공격 탐지를 위한 자동 패턴 추출

3.1 자동 패턴 추출을 위한 결정트리의 구성

결정트리를 사용하여 탐지 패턴을 자동으로 추출하기 위해서는 트리의 각 노드를 구성할 적절한 규칙이 필요하다. 본 논문에서는 [8]에서 제시된 41개의 특징을 사용하여 트리를 구성한다. 각각의 노드는 하나의 규칙으로 설계되어 훈련 데이터(training data)로부터 패턴을 추출한다. 이때 트리의 노드를 구성할 특징은 그림 1과 같이 공격에 따라 적합하게 구성한다.

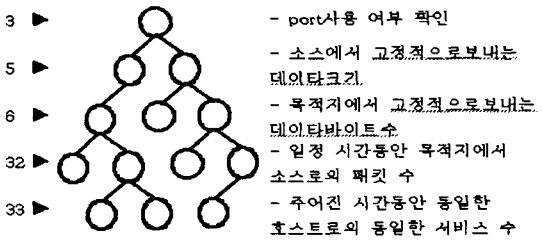

그림 1. R2L 공격에 적용된 결정트리

각 노드에서 추출할 공격 패턴은 척도의 특성에 따라 연속형 범주를 갖을때는 범주형 패턴을, 이산형 범주를 갖을때는 하나 혹은 여러개의 값을 패턴의 형태로 갖는다.

3.2 탐지 패턴 추출 시스템 설계

네트워크 공격 탐지패턴 생성을 위해 몇 개의 단위 모듈을 그림 2와 같이 생성한다. 먼저 기본적인 패턴 생성을 위한 훈련단계를 거치는데 훈련은 DARPA 99년도 2주 데이터의 R2L 공격을 대상으로 한다. 세션과 패킷 분석 단계에서 패킷을 각 필드별로 분류하고, 노드별 트리생성 단계에서는 본 논문에서 제시한 결정트리를 이용하여 훈련을 통한 탐지 패턴을 추출한다. 여기에서 추출된 데이터를 대상으로 연속적인 데이터인지 비연속적인 데이터인지에 따라 생성된 패턴도 범위형태를 갖을 것인지 특정한 하나의 값 혹은 여러 개의 값을 패턴으로 갖을지 결

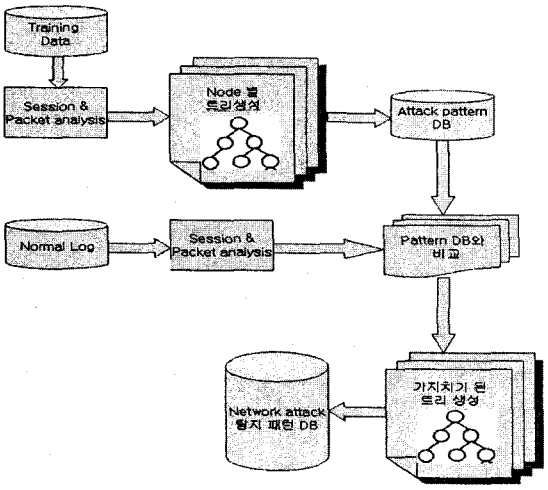

그림 2. 탐지 패턴 추출을 위한 설계

정된다.

이렇게 분석된 가지에 대한 특징은 하나의 공격 패턴으로 저장된다. 정상 로그를 통한 분석과정에서는 공격 패킷의 트리에서 오탐율을 높이는 역할을 하는 정상행위에 해당하는 패턴을 제거하기 위해 정상 행위를 훈련시킨다. 앞서 생성된 정상적인 패킷의 특징과 공격 패턴으로 저장된 패킷과 비교하여 공격패킷에서 정상 패킷의 특징을 제거한다. 오탐율를 높이는 가지를 제거하고난 최종적인 트리의 노드별 특징을 하나의 공격에 대한 규칙으로 정의한다.

표 3. 패턴 추출 알고리즘

```
Input : x(x1, x2, x3, .. ) // network attack packet
Output : generated patterns
begin
  while there is network attack packet do
    Analysis network packet using the Decision Tree
  Insert detection patterns for network attacks into Database
  while there is normal packets do
    Analysis normal packets using the Decision Tree

  if normal pattern is a detection patterns for network attacks then
    Remove the patten
  else
    Insert automatic generated detection patterns into Database
end
```

3.3 탐지 방법

공격 탐지를 위한 방법은 훈련 단계와 유사하다. 입력된 네트워크 패킷을 접속 형태에 따라 세션 단위로 블록화하고 블록화된 세션을 결정트리를 통해 분석한다. 노드별로 분류된 패킷은 탐지패턴 DB에 입력된 패턴과 비교하여 이진 분리와 가중치 함수를 통해 공격과 정상으로 나눈다. 이때 사용되는 가중치식은 (1)과 같다.

$$A_{attack} = \sum_{i=1}^{depth} N_i \qquad (1)$$

A_{attack} : 공격에 따른 가중치의 합
depth : 결정트리의 깊이
N : 각 노드에 따른 가중치

각 노드가 하나의 규칙으로 구성되어 노드를 거쳐갈 때 규칙에 일치하는지를 확인하고 일치하였을 때 가중치를 더하여 공격 패킷을 구분한다.

3.4 실험 및 결과

본 논문에서의 실험 데이터는 DARPA의 1999년 네트워크 데이터를 tcpdump로 패킷 캡쳐한 로그를 사용하였다. 패킷 로그 중 공격 패턴 추출 및 테스트용으로 사용한 공격은 ftpwrite 공격을 사용하였다. Ftpwrite를 사용하여 추출한 공격 패턴은 그림 4와 같다.

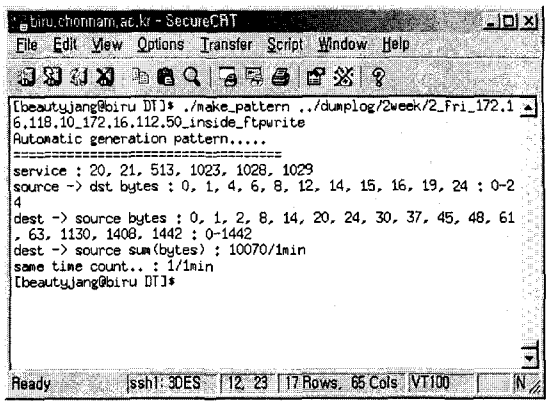

그림 4. ftpwrite에서 추출한 공격패턴

그림에서 보는 바와 같이 R2L 공격을 기반으로 서비스 구분, 호스트에서 목적지로, 목적지에서 호스트로 보내는 데이터의 크기, 단위 시간당 목적지에서 호스트로 보내는 패킷의 총량, 그리고 단위 시간 동안 목적지에서 호스트로의 서비스 연결 카운트를 검사하여 패턴화하였다.

그림 5는 앞서 추출된 공격 패턴을 바탕으로 DARPA 99년 2주와 4주 데이터를 대상으로 실험하였다. 탐지패턴을 기반으로 네트워크 공격 패킷을 탐지 하였을 경우 ftpwrite 공격에 대한 탐지가 모두 이루어졌다. 또한 이와 비슷한 형태를 보이는

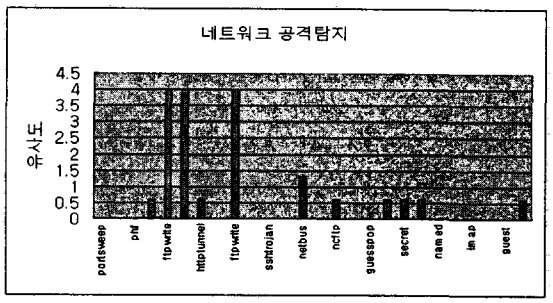

그림 5. 2주와 4주 각 세션별 공격 탐지

netbus, httptunnel과 같은 여러 형태의 공격들도 패턴화된 규칙에 의해 가중치가 부여되어 탐지되었다.

4. 결론

기존의 네트워크 공격에 대한 침입탐지시스템의 탐지 패턴은 전문가의 수작업에 의해 생성되어 왔고, 수정 역시 수작업을 필요로 했다. 그러나 네트워크 공격이 매시간 다양화되고 변형되기 때문에 적절한 대응이 필요하다. 이러한 의미에서 네트워크 공격에 대한 탐지 패턴을 자동으로 생성하는 것은 반드시 필요하다. 본 논문에서 ftpwrite 공격에 대해 실험한 결과 ftpwrite 뿐만 아니라 유사한 형태의 공격의 탐지에도 효과적이였다. 실험에서는 R2L 공격에 대해서만 적용하였지만, 41개의 특징을 모두 적용하여 다른 형태의 공격에서도 패턴 추출이 가능하다.

향후 연구로는 패턴의 정형화에 대한 연구와, 현재 오용행위 및 비정상행위탐지만 적용한 패턴 자동 추출에 대한 연구가 알려지지 않은 공격에 대한 분야까지 적용할 수 있을 것으로 본다.

참고문헌

[1] 이종성, 채수환, "컴퓨터 면역 시스템을 기반으로 한 지능형 침입탐지시스템," 한국정보처리학회 논문지, 1999년 12월.

[2] J. Bala, J. Huang, H. Vafaie, K. DeJong and H. Wechsler, "Hybrid Learning Using Genetic Algorithms and Decision Tree for Pattern Classfiacation," IJCAI conference, Montreal, August pp.19-25, 1995

[3] 한국 정보보호 진흥원 *해킹바이러스 통계 및 분석 월보*, 2003년 7월

[4] 오상현, 이원석, "패킷간 연관 관계를 이용한 네트워크 비정상행위 탐지," 정보보호학회 논문지, 2002년 10월

[5] 윤정혁, "사용자 명령어 분석을 통한 비정상 행위 판정에 관한 연구," 정보보호학회논문지, 2000년 12월

[6] M. Mahoney and P. Chan "PHAD:Packet Header Anomaly Detection for Identifying Hostile Network Traffic," Florida Institute for Technology Technical Report CS-2001-04

[7] S. Mukkamala, A. Sung and G. Janoski "Intrusion Detection using Neural Networks and Support Vector Machines," Proceeding of IEEE International Joint Conference on Neural Networks, p.1702-1707. 2002

[8] http://www.cs.ucsd.edu/users/elkan/clresults.html KDD-CUP-99 Contest

[9] S. Chris, P. Lyn and M. Sara "An Application of Machine Learning to Network Intrusion Detection," 15th Annual Computer Security Applications Conference, December, 1999