유전자알고리즘을 적용한 침입탐지시스템

양지홍[0] 김명준 한명묵
경원대학교 전자계산 대학원
{wlghd[0], guybey77}@web.kyungwon.ac.kr, {mmhan}@kyungwon.ac.kr

Using Genetic Algorithms for Intrusion Detection Systems

Ji-Hong Yang[0] Myung-Jun Kim Myung-Mook Han
Dept. of Computer Science, Kyungwon University

요 약

침입탐지 시스템은 정밀성과 적응성, 그리고 확장성을 필요로 한다. 이와 같은 조건을 포함하면서 복잡한 Network 환경에서 중요하고 기밀성이 유지되어야 할 리소스를 보호하기 위해, 우리는 더욱 구조적이며 지능적인 IDS(Intrusion Detection Systems) 개발의 필요성이 요구 되고 있다. 본 연구는 데이터 마이닝(Data mining)을 통해 입 패턴, 즉 침입 규칙(Rules)을 생성한다. 데이터 마이닝기법중 분류(Classification)에 초점을 맞추어 분석과 실험을 하였으며, 사용된 데이터는 KDD데이터이다. 이 데이터를 중심으로 침입 규칙을 생성하였다. 규칙생성에는 유전자알고리즘(Genetic Algorithms:GAs)을 적용하였다. 즉, 오용탐지(Misuse Detection) 기법을 실험하였으며, 생성된 규칙은 침입데이터를 대표하는 규칙으로 비정상 사용자와 정상 사용자를 분류하게 된다. 규칙은 "Time Based Traffic Model", "Host Based Traffic Model", "Content Model" 이 세가지 모듈에서 각각 상이한 침입 규칙을 생성하게 된다.

본 시스템에서 도출된 침입 규칙은 430M Test data set에서 테스트한 결과 평균 약94.3%의 성능 평가 결과를 얻어 만족할 만한 성과를 보였다.

1. 서 론

침입탐지 시스템은 정밀성과 적응성, 그리고 확장성을 필요로 한다. 이와 같은 조건을 포함하면서 복잡한 Network 환경에서 중요하고 기밀성이 유지되어야 할 리소스를 보호하기 위해, 우리는 더욱 구조적이며 지능적인 IDS개발의 필요성이 요구되고 있다. 본 연구는 데이터 마이닝을 통해 침입 패턴, 즉 침입 규칙(Rules)을생성한다.[1]

Data Mining기법에 크게 주요한 3가지로 Classification, Link analysis, Sequence analysis가 있는데 본 연구에서는 분류에 초점을 맞추어 분석과 실험을 하였으며, 사용된 데이터는 KDD[2]데이터이다. 이 데이터를 중심으로 침입 패턴을 생성하였다. 즉, 오용탐지(Misuse Detection) 기법을 실험하였으며, 생성된 규칙은 침입데이터를 대표하는 규칙로 비정상 사용자와 정상 사용자를 분류하게 된다. 침입탐지는 비정상행위 탐지(Anomaly Detection)와 오용탐지로 나누어 볼 수 있는데, 비정상행위 탐지는 시스템 사용자의 정상적인 행위에 기초한 것이고, 오용탐지는 비정상적인 행위에 기초한 탐지 기법이다.

규칙은 "Time Based Traffic Model", "Host Based Traffic Model", "Content Model" 이 세가지 모듈에서 각각 상이한 침입 규칙을 생성하게 된다.
본 시스템에서 도출된 침입 규칙은 약 700MB의 Test Datas에서 테스트한 결과 평균 약 94.3%의 성능 평가 결과를 얻어 만족할 만한 성과를 보였다.

본 논문의 구성은, 2장에서는 데이터 마이닝 기법에 핵심적으로 사용된 유전자 알고리즘에 관해 기술하였으며, 3장은 침입 탐지 기술, 4장에서는 실험에 사용된 데이터에 대한 분석과 실험 환경 및 제안 시스템에 대한 내용과 함께 실험 결과를 기술하고, 마지막으로 5장에서 결과를 분석하며 성능을 평가한 후 향후 연구 방향에 대하여 논한다.

2. 유전자알고리즘(Genetic Algorithms)

GAs는 유전적 계승과 다윈적 생존 경쟁이라는 자연현상을 모델링한 확률적인 탐색방법으로, 유전검색이 불가능할 정도로 큰 후보해 공간을 갖는 최적화문제에 적용할 수 있다.[3]

대부분의 데이터 마이닝 시스템은 전통적인 기계학습(Machine Learning) 알고리즘의 변형을 사용해 왔다. 기계학습에서 유전자 알고리즘의 기법을 이용한 것을 GA기계학습 또는 GBML(Genetic Based Machine Learning)이라고 한다.

3. 침입탐지 시스템(Intrusion Detection Systems)

현재 사용되어지고있는 침입 탐지를 위한 접근 방법에는 두가지가 있다. 첫 번째 접근방법은 동적인 시스템 사용자의 행위를 and/or의 형태로 특성화 시킨 정상적인 패턴(보통은 통계적인 방법을 사용하여, 사용자 행위들간의 관계)을 정의하여, 그 정의된 것으로 비정상적인 사용자를 탐지하는 방법이다.[4] 이것을 비정상행위 탐지(anomaly detection)라 한다.

두 번째 접근방법은 오용 탐지(misuse detection) 방법이다. 이것은 이미 알려진 공격방법(또는 침입 패턴, 비정상적인 사용자들의 행위, 일정한 프로토콜의 수행 등등)을 정형화하여 비정상적인 사용자들을 탐지한다.

4. 시스템의 구현 및 실험

유전자 알고리즘을 사용한 분류 시스템(classifier system)으로 대표되는 시스템에는 Holland의 Michigan 접근방법과 Smith의 LS-1 시스템으로 대표되는 Pittsburgh 접근방법이 있다. 이중에서 Pittsburgh 접근방법을 사용한 시스템을 통하여 인증되지 않은 사용자들(그것이 외부든 내부든)로부터의 침입에 어떠한 컴퓨터 네트워크를 보호하는 침입탐지 시스템을 개발하는데 그 목적이 있다.

4.1 실험 및 분석

4.1.1 KDD DATA 분석

Training Data sets은 24개의 Training Attack Types을 포함하고 있으며, Test data에는 14개의 유형(types)을 더 포함하고 있다.

4.1.2 속성 분석 및 선택

"same host" 와 "same service" features 모두 connection records의 time-based traffic features 라고 부른다.[2]

호스트(또는 ports)를 스캔하는 slow probing attacks은 매우 오랜 시간을 필요로 한다(2초이상). features는 time window 대신 동일한 호스트에 100개의 connection windows를 사용하여 구성되었다. 이것은 "host-based traffic features"라 불리는 것들의 집합을 산출해 낸다.[2]

packets의 구조화되지 않은 데이터 부분들을 자동적으로 탐색하는 것에 대한 유용한 알고리즘은 이미 잘 알려진 연구 분야이다. Stolfo et al.은 데이터 일부에서 로그인을 시도했을 때 실패한 횟수와 같은 행위를 한 의심이 가는 사용자를 찾는 features를 추가하는 기법(또는 지식 분야)를 사용하였다. 그들 features를 "content " features라 한다.[2]

4.2 제안 시스템

본 시스템에서는 41개 각각의 features Value의 개수와 범위를 전처리기를 통하여 산출해 냈으며, features를 각각의 Value Type에 따라 features를 정의하였다.

표 7. Features 정의 예

protocol_type	icmp	100
	tcp	010
	udp	001

또한 적합함수(Fitness function) 에서는 각 generation에서 모든 염색체들은 그들의 적합도에 의해 평가되고, 새로운 개체 집단은 좀더 좋은 염색체들로 구성이 된다. 여기에, 연산자들은 새로운 개체 집단에 적용되고, 다시 반복된다. 이러한 모델링을 기본으로 삼아 본 실험에서는 전체 Training Data에 맞게 예측된 데이터 개수로 나눈 것을 적합함수로 표현하였다.

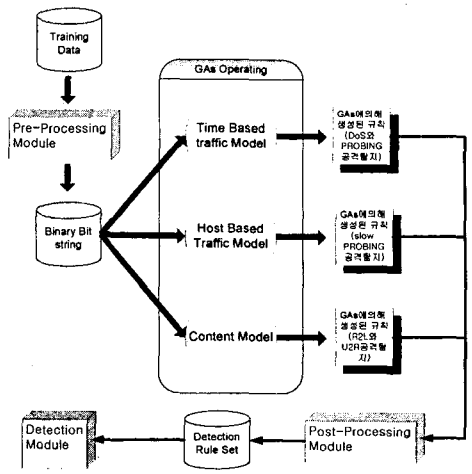

그림 2. 유전자 알고리즘을 이용한 침입 규칙 생성기

GAs연산부분은 3부분으로 나누어지고 각 내부 루틴은 각각 데이터 타입이 틀리게 된다. 처음 랜덤으로 2진 population을 생성하고 그 data와 함께 규칙을 선택하기 위해 임의의 침입규칙들을 training data로 입력시킨다. 그렇게 각 모듈별로 입력이 있은 후 연산에 의해 생성된 최적 해가 나오게 되고 GAs를 통하여 새로운 rule을 만들게 된다.

4.2.1 탐지 모델

위에 제시된 Features의 구성을 통해 다음의 3가지 탐지 모델을 구성하였다.[1]

- ▶ Time based traffic model
  : 9개의 Intrinsic features와 9개의 Time based traffic features로 구성된다. Dos와 PROBING 공격들을 탐지하는데 사용되는 규칙을 생성한다.
- ▶ host based traffic model
  :9개의 Intrinsic features와 10개의 host based traffic features로 구성된다. slow PROBING 공격들을 탐지하는 규칙을 생성한다.
- ▶ content model
  : 9개의 Intrinsic features와 13개의 content features로 구성된다. R2L과 U2R 공격들을 탐지하는 규칙을 생성한다.

위 모델들은 MIT Lincon Lab.에서 제공된 KDD 데이터의 10%(75M)로 트레이닝 시켰으며, 494,021개 레코드로 구성되어있다.

4.3 실험 결과

본 실험에서 사용된 주요 파라미터(Parameters)는 다음과 같다. 먼저 교배율(corssover rate)은 0.6~0.8, 돌연변이율(Mutation rate)은 0.4~0.08의 범위에서 실험하였으며, 게놈은 2진수로 표현하였다.

계산된 결과는 유전자 연산에 사용된 게놈을 선택하기 위한 선택 전략에 사용된다. 스케일링 전략(Scaling Sheme)으로는 선형 스케일링을 사용하였으며, 교배 연

산자로는 2점 교배(2 Point Corssover) 연산자를, 돌연변이 연산자는 교환 돌연변이 연산자를 사용하였다. 비교 연산자는 "비트 비교" 연산자를 종료 연산자는 "세대수렴에 의한 종료"연산자를 사용하였다. 선택 전략으로는 가장 많이 사용되고 있는 룰렛휠선택(Roulette Wheel Selection)을 적용하였다. 집단의 크기는 각각의 트레이닝 데이터와 같게 하여 실험을 하였다.

3가지 탐지 모델들은 각각의 침입유형을 특성화하는 분류 모델들이다. 이들로서 생성된 규칙의 예는 다음과 같다.

표 8. Time based traffic model의 규칙

duration = 011010010110 0~99 ☐ 100~199 ☑ 200~299 ☑ 300~399 ☐ 400~499 ☑ 500~599 ☐ 600~699 ☐ 700~799 ☑ 800~899 ☐ 900~999 ☑ 1000~9999 ☑ 10000~ ☐	duration 속성의 속성값이 "☑"있는 값을 가질때 침입임.
⋮	⋮
dst_host_srv_rerror_rate = 0000010111 0.00~0.10 ☐ 0.11~0.20 ☐ 0.21~0.30 ☑ 0.31~0.40 ☐ 0.41~0.50 ☐ 0.51~0.60 ☐ 0.61~0.70 ☑ 0.71~0.80 ☐ 0.81~0.90 ☐ 0.91~1.00 ☑	dst_host_srv_rerror_rate 속성의 속성값이 "☑"있는 값을 가질때 침입임.

위 41개의 속성들은 "∨(OR)"로 연결되어 있으며,각각의 속성값들은 "∧(AND)"로 연결되어 해석되어진다. 따라서 각각의 "∨"의 개수에 따라 여러 경우의 수가 발생되어, 다양한 규칙이 생성되어 진다.

생성된 규칙들은 테스트 데이터(Test Datas)에서 평가되었으며, 3가지 탐지 모델의 Performance를 평가한다. 사용된 트레이닝 데이터는 침입과 정상이 표시된 데이터를 사용하였으며, 표시되지 않은 데이터로 테스트 되었다. 테스트 데이터는 38개의 공격 유형이 포함 되어 있으며, 이중 14개는 학습되지 않은 공격 유형으로써 본 3개의 모델에서는 이것을 "새로운 공격유형"으로 분류하게 된다. 이것은 지속적인 진화 연산을 통해 생성된 규칙들이 정체되지 않고 새로운 개체(공격 유형)를 통해 새로운 규칙으로 진화를 수행해 간다.

생성된 바이너리(binary) 형태의 규칙은 후처리기(Post-process)를 통해 Raw 데이터 형태로 변환되어 분류자(classifier)에 전달되어 탐지를 수행하게 된다.

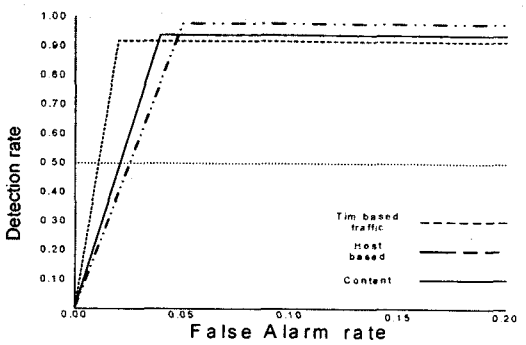

그림 5. 3가지모델의 탐지율 및 오탐지율

그림 5는 본 연구에서 생성된 침입 규칙의 성능(Performance)을 보여 준다. Time based traffic Model은 92%, Host based Model은 97%, Content Model은 94%의 탐지율을, 각각 0.02, 0.03, 0.05의 오탐율을 산출해 냈다.

5. 결론 및 향후 연구 방향

본 연구는 유전자 알고리즘을 IDS에 적용하여 오용 탐지 기법을 처음으로 제안하고 구현한 점에서 의미가 있다. 규칙 생성의 지속적인 업데이트가 힘든 오용탐지 기법에 지속적으로 성장하며 변화해가는 규칙을 자동적으로 생성하는 시스템으로서, 생성된 규칙은 각각의 모델들이 평균 약 94.3%의 탐지율을 보였다.

향후 보완될 점 및 지속적인 연구 방향으로는, 우선 정확한 KDD 컨테스트의 환경하에 실험을 하여 다른 연구들과의 정확한 성능 비교가 이루어져야 하며, 데이터 마이닝의 주요 3분야중 Classification만 실험하였는데, 생성된 3가지의 침입 규칙을 결합하여 다중 분류(Meta-Classification)에 적합하도록 연구하여 성능평가를 해야 할 것이다. 또한 데이터 마이닝의 주요 2분야인 Link analysis와 Sequence analysis를 연구하여 시스템에 추가하여 더욱 정확하고 신뢰있는 침입규칙을 생성하는 것이다. 아울러 비정상행위 탐지에 쓰일 정상적인 사용자의 규칙 생성에 관해 연구할 것이다.

참고문헌

[1]Wenke Lee, Salvatore J. Stolfo, Data Mining Approaches for Intrusion Detection, This research is supported in part by grants from DARPA(F30602-96-1-0311).

[2]Charles Elkan, Results of the KDD'99 Classifier Learning Contest, September 1999.

[3]ZBIGNIEW MICHALEWICZ, "유전자 알고리즘", 11장. 1996.

[4]Terran D. Lane, Machine Learning Techniques For The Computer Security Domain Of Anomaly Detection, A thesis Submitted to the Faculty of Purdue University. August 2000.