제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

데이터 마이닝 기반의 침입유형별 탐지 모델

김상영, 우종우
국민대학교 컴퓨터 학부

e-mail : cwwoo@kookmin.ac.kr

Detection Models for Intrusion Types based on Data Mining

Sangyoung Kim, Chongwoo Woo
School of Computer Science, Kookmin University

요 약

인터넷의 급속한 발전으로 인한 유용성 이면에는, 공공 시스템에 대한 악의적인 침입에 따른 피해가 날로 증가되고 있다. 이에 대비하기위한 침입 탐지 시스템들이 소개되고 있으나, 공격의 형태가 다양하게 변화되고 있기 때문에 침입탐지 시스템도 이에 대비할 수 있도록 지속적인 연구 노력이 필요하다. 최근의 다양한 연구노력 중에는 데이터 마이닝 기법을 이용하여 침입자의 정보를 분석하는 연구가 활발히 진행되고 있다. 본 논문에서는 데이터 마이닝 기법을 사용하여 KDD CUP 99 의 훈련 집합(Training Set)을 기반으로 효과적인 분류를 하기 위한 모델을 제시하였다. 제시된 모델에서는 휴리스틱을 적용하여 효과적으로 필요한 데이터를 생성할 수 있었으며, 또한 각 공격 유형마다 분류자를 두어 보다 정확하고 효율적인 탐지가 가능하도록 하였다.

1. 서 론

인터넷 인구의 급속한 증가는 긍정적인 측면과 함께 시스템 보안 위협이라는 문제점을 야기 하고 있으며, 이에 대응하기 위해 정보 보호 기술이라는 새로운 분야가 등장하게 되었다. 이와 함께 주목을 받고 있는 기술이 바로 침입 탐지 시스템 (Intrusion Detection System: IDS)이다. IDS 는 기본적으로 보안 관련 정보 수집, 수집된 정보의 분석 및 침입 판정, 보고 및 대응 행동등의 기능을 수행하게 된다.

IDS 에서 침입 패턴을 탐지하는 기법에 대한 다양한 연구가 진행되고 있으며, 이에 대한 대표적인 연구들로는 규칙 기반의 NIDES(Next Generation Intrusion Detection Expert System)[1], 비 정상 탐지 기법을 이용한 Hyper View[2], 패트리 넷[3]을 사용한 IDIOT[4]등이 있으며, 이 밖에도 신경망이나 유전자 알고리즘, 데이터 마이닝 등을 이용한 연구들이 진행되고 있다. 이러한 시스템은 침입 모델에 따라 오용 탐지(Misuse Detection)와 비정상 행위 탐지(Anomaly Detection)로 구분 지을 수 있지만, 최근에는 두 가지 탐지를 병행하여 사용함으로써 침입 탐지 기능을 향상 시키려는 시스템들이 늘어가고 있는 추세이다.

이렇게 다양한 IDS 시스템들이 소개 되고 있으나, 인터넷이 발전해 감에 따라 일시에 분석해야 하는 감사 데이터의 양이 방대해져 감으로 인해 여러 가지 알려져 있는 방법론들 중에서 대용량의 데이터에서 유용한 정보를 획득하기 위한 방법인 데이터 마이닝에 대한 적용이 많아 지고 있는 추세이다.

본 논문에서는 KDD CUP 99[5] 훈련 집합(Training Set)에 대해서 데이터 마이닝 기법을 적용하여 공격 유형에 대한 분류 모델을 제시하였다. 이러한 분류 모델은 기존의 모델들이 주어진 데이터에 대해 단순히 마이닝기법을 적용하는 것에 비하여, 본 모델에서는 침입탐지와 관련하여 필수적인 요소들만을 선택할 수 있게 하였고, 또한 침입과 무관하다고 여겨지는 연속형 필드에 대해서도 적용 가능한 방안을 제시 하였다. 이러한 분류모델은 현재 본 연구와 병행하여 진행되고 있는 액티브 네트워크 기반의 멀티에이전트 시스템 연구에서, 침입탐지를 수행하는 감시 에이전트의 부분으로 사용될 예정이다[6].

본 논문의 구성은 IDS 에서의 마이닝 기법들에 대한 간략한 소개와 KDD CUP 99 데이터에 대한 분석을 제 2 장 관련 연구에서 기술하고, 제 3 장에서 본 논문에서 제안하는 시스템의 설계, 그리고 제 4 장에서 결론을 통해 맺는다

2. 관련 연구

2.1 침입 탐지에서의 데이터 마이닝

데이터 마이닝에서의 핵심 요소는 많은 데이터에서 특정한 패턴을 발견하는 것이다. 데이터 마이닝은 다양한 기법을 가지고 적용할 수 있지만, 침입 탐지 분야에 적용할 수 있는 부분은 다음과 같다[7].

- 분류(Classification) : 감사 데이터를 미리 정의된 여러 개의 항목들 중 하나로 맵핑 하는 것이다. 이것은 두 가지 처리 과정을 거치는 데, 먼저 훈련 데이터 집합을 사용하여 모델을 생성하고 다음으로 생성된 모델에 대해서 시험 데이터를 가지고 부류를 분류하여 모델의 정확성을 확인한다.
- 메타-분류(Meta-classification) : 기존에 이미 존재하는 다양한 분류자들을 가지고 귀납적으로 상호 연관성을 학습하는 메커니즘이다. 다양한 분류자에서 수집한 다른 양상을 가진 모델들을 결합하는 역할을 수행한다.
- 연결 분석 (Link Analysis) : 데이터 베이스에서 필드들 사이의 관계를 결정하는 것을 의미하며 연관 규칙을 사용하여 분석을 수행한다.
- 연속성 분석 (sequence Analysis) : 시간을 기반으로 하여 빈번하게 등장하는 감사 이벤트의 순서에 대한 관계를 모델링 하는 방법이다.
- Bagging (Bootstrap aggregating) : 다중 버전의 예측자를 생성하여 집합적인 예측자를 얻는 방법이다. 일반적으로 분류 방법에 부가적으로 사용하여 불안정한 모델을 안정적으로 만들고 정확도를 높이는데 사용한다.
- Boosting : 학습 알고리즘에 대한 정확도를 향상시키기 위한 방법으로서 약한 모델을 견고하게 만드는데 이용된다. 드물게 발생하는 패턴에 대한 분류를 위해 사용되는 알고리즘이다.

2.2 KDD Cup 99

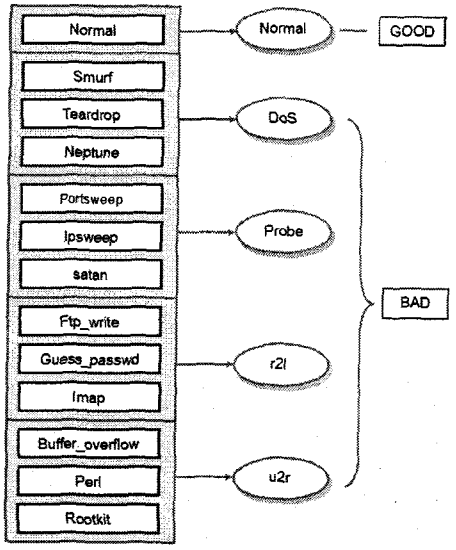
KDD Cup 은 지식 발견과 데이터 마이닝 분야의 발전을 위해 개최되는 국제 대회이다. 여기서는 매년 다른 형태의 데이터들이 제공되며, 데이터 마이닝 규칙의 우수성을 경쟁을 통하여 발전 시켜 나가려는 목적을 가지고 있다. KDD Cup 99 데이터는 1998 년에 DARPA 에서 침입 탐지에 관련된 데이터로 제공된 것이며, 미 공군에서 사용되는 지역 네트워크에서의 TCP/IP dump 데이터로 구성되었다 [8]

이 데이터는 각 TCP/IP 연결에 대해서 41 개의 필드를 가지고 있으며, 크게 4 가지 형태의 공격 유형을 가지며 세부적으로 13 가지의 공격으로 이루어져 있다 [그림 1 참조]. 각 공격 형태는 다음과 같은 것을 의미한다.

- DoS : 분산 서비스 공격 (Denial of Service)
- r2l : 원격에서의 비인가 접근 공격
- u2r : 슈퍼 유저 권한으로의 비인가 접근 공격
- probing : 시스템의 취약점에 대한 감시 또는 스캔 공격

훈련 집합은 743MB 의 용량의 약 5,000,000 개의 레코드로 이루어져 있다. 하드웨어의 제약으로 인해 이 중 10%정도를 훈련 데이터로 사용하며, 이는 75MB 의 용량으로 총 494,021 개의 레코드를 포함한다. 이것은 19.69%의 정상 패턴을 가지고 나머지 레코드에는 특정한 공격의 형태를 명시하는 레이블이 존재한다.

시험집합은 전체 430MB 크기이고, 위와 같은 이유에서 10%인 1.4MB 의 311,029 개의 레코드로 이루어 진다.



[그림 1] 공격 유형의 분류

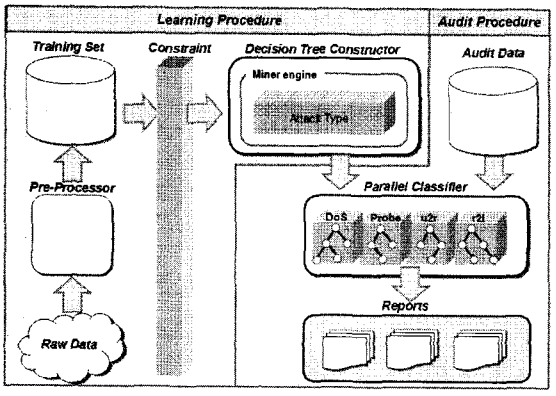
시험 집합에는 특정한 공격의 형태를 명시하는 라벨을 가지고 있지 않으며, 시험 집합의 분류 결과를 기준으로 마이닝 도구의 오 분류도 및 정확성을 판단할 수 있게 된다.

KDD Cup 데이터의 레코드 형태는 네트워크 시스템 로그에서 볼 수 있는 연속형 데이터 (예: duration, src_bytes, dst_bytes 등) 와 이산형 데이터 (예: protocol_type, service, flag 등)를 가지고 있다. 이 데이터는 침입 탐지의 관점에서 일반적인 로그 데이터와 달리

문제점을 가지고 있는데, 정확한 시간 정보가 아닌 duration 을 사용하는 것과 공격 형태의 원인을 파악하는 데 중요한 근원지 주소를 표시 하지 않았다는 것이다.

3. 설계

본 연구에서의 시스템 구조는 다음 [그림 2]와 같이 구성하였다.



[그림 2] 시스템 구조

각 구성 요소에 대해 간단히 살펴 보면, 먼저 학습 과정과 감사 과정으로 나누어 진다.

학습이 이루어 지는 과정은

① KDD Cup 데이터를 전처리 작업 후에 훈련 집합으로 만든다.
② 마이닝을 수행하기 전에 제약들을 적용한다.
③ 결정 트리 생성기에서 마이닝 엔진이 각 공격 유형에 따른 분류자를 생성한다.

감사가 이루어지는 과정은

① 감사 데이터를 가지고 이미 생성된 분류자에 보낸다.
② 분류자는 입력 되는 감사 데이터를 병렬로 받아들여 각 공격 유형 별로 판단하는 작업을 수행한다.
③ 처리된 결과물은 시스템 관리자에게 보고 되어 침입 탐지를 위한 목적으로 사용된다.

3.1 Pre-Processing

데이터 마이닝에서의 훈련 집합에 사용되는 데이터는 대부분 많은 양을 가진 데이터 이기 때문에 신속한 처리를 위해 데이터 베이스에 정형화 된 형태로 저장해야 한다. 일반적인 로그 데이터의 경우 이렇게 데이터 베이스에 데이터를 저장할 때 실제로 훈련 집합으로 사용될 요소를 선택하고 필요 없는 요소들을 제거 해야 하는 데 이러한 작업을 전 처리 작업이라고 한다.

KDD Cup 데이터도 마찬가지로 아스키 코드 형태로 제공이 되며, 데이터 내에 잘못되거나 필요 없는 부분들이 존재하므로 이것을 제거하고 모델링 하기에 적합한 형태로 정형화 시키는 작업을 수행한다.

3.2 Constraint

공격 유형을 모델링 하는 결정 트리를 생성하기 전에 학습 과정에서 포함되는 제약(Constraint)은 각 공격 유형에 적합한 요소들을 선택하는 과정이다. KDD Cup 데이터에는 많은 필드가 포함되어 있으나 모든 필드가 공격을 탐지하는 데 필요한 것은 아니다. 또한, 각 공격 형태에 따라서 필요로 하는 필드가 달라지게 된다.

제약에서는 이러한 요소들을 고려하여 각 분류자에 적합한 필수 요소들만을 선택하여 결정 트리 생성기에 전달하는 작업을 수행 한다. 또한 연속형 데이터에 대한 이산화 문제가 요구 된다. 결정 트리에서의 트리 생성시 예측변수에 해당하는 노드의 기준은 대부분 이산형 변수이기 때문에 연속형 변수를 이산형 변수로 변형 하여야 한다.

제약을 수행하는 방법을 DoS 공격을 예로 들어 설명하면, 먼저 각 유형에 속하는 공격에서 필수적인 필드를 선택한다. 필수적인 필드란 해당 공격 유형을 특징 지을 수 있는 필드를 말한다. 공격 유형에 영향을 주는 필드는 대부분 이산형 필드에 속하므로 이산형 필드인 [protocol type, service, flag, land, logged in, root_shell, su_attempted, Is_hot_login, Is_guest_login] 을 선택하고 추가적으로 연속형 데이터에서 공격에 영향을 미칠 수 있는 [count]를 추가 하였다.

[표 1] DoS 에서의 제약을 적용한 필드

Attack type / Field Name	Smurf	Teardrop	Neptune	Type
Protocol type	icmp	udp	Tcp	Discrete
Service	ecr_i	private	auth,bgp,courier,csnet_ns...	Discrete
Flag	SF	SF	REJ, RSTO, SO	Discrete
Land	0	0	0	Discrete
Logged in	0	0	0	Discrete
Root_shell	0	0	0	Discrete
SU_attempted	0	0	0	Discrete
Is_host_login	0	0	0	Discrete
Is_guest_login	0	0	0	Discrete
Count	2-511	1-200	1-302	Continuous

[표 1]은 이렇게 선택한 필드에 대해 KDD Cup 데이터를 적용한 결과이다. 이렇게 얻어진 필드 정보는 전체 데이터에서 DoS 공격에 대한 결정 트리를 생성하는데 있어서 예측 변수로 사용된다. Count 와 같은 연속 변수의 경우 각 공격에 해당하는 Count 값들의 평균을 경계로 하여 이산화 한다.

3.3 Decision Tree Constructor

결정 트리 생성자는 내부적으로 결정 트리 생성 알고리즘을 가진다. 이와 같은 대표적인 결정 트리 생성 알고리즘으로는 ID3, CART, C4.5 등이 있으며, 최근에는 C4.5 가 가장 많이 사용되고 있다. 제약을 통과하여 전달 되어진 필드와 데이터를 입력으로 받아서 마이닝 엔진에서는 각 공격 유형에 해당 하는 결정 트리를 생성 한다. 마이닝 엔진은 주어진 입력을 트리 생성 알고리즘의 입력에 맞게 주어서 결정 트리를 생성하는 역할을 수행한다. 여기에서는 DoS, Probe, u2r, r2l 에 대한 결정 트리가 생성 된다. 이렇게 생성된 결정 트리는 각 공격 유형에 대한 모델로서 분류자에 구성 요소가 된다.

3.4 Classifier Modeling

훈련 집합에서 최종적인 목표 변수는 침입/정상으로 설정할 수 있다. 그러나, KDD Cup 에서 나타난 공격 형태는 22 가지나 되고 각 공격은 다른 형태의 특징을 가지고 있다. 따라서, 단순히 침입/정상으로의 목표 변수 설정과 단일 분류자에 의한 분류는 정확한 분류를 수행하기 어렵다. 또한 빈도수가 매우 낮은 공격 형태의 경우 해당 공격에 대한 분류자 모델을 형성하기 어렵다는 문제점을 가진다.

이러한 문제를 해결하기 위해서, 각 공격에 대한 분류자 대신에 공격 유형별 분류자를 생성하여 특정 공격 유형을 기반으로 모델을 생성 하였다. 각 공격 유형에 대한 분류자를 모델링 하는 방법은 데이터 마이닝을 이용한 결정 트리 기법을 사용하였다.

3.5 Report

분류자를 통해 생성된 결과는 세 가지로 요약 될 수 있다. 첫째는 침입이 발생했다는 사실, 두 번째는 어떤 유형의 침입이 발생 했는가 하는 것, 세 번째는 해당 되는 침입에 대한 흔적이 어떤 것인가 하는 정보 이다. 이렇게 나온 결과들은 일반적인 IDS 에서 전달하는 침입에 대한 알람 이상의 역할을 담당한다.

해당 되는 결과물은 일반적으로 시스템관리자에게 침입에 대한 정보를 제공할 뿐 아니라, 서론에서 언급하였던 프로젝트를 통해 침입에 대한 능동적인 대응을 위한 수단으로 이용할 수 있다.

4. 결론 및 향후 연구 과제

본 논문은 침입 탐지를 위해서 실제적인 감사 데이터인 KDD Cup 데이터를 가지고 탐지를 위한 분류자의 모델링을 제안하였다. 이러한 실제적인 데이터를 통한 분석은 실 세계의 로그 데이터나 실 시간 감사 데이터에 대해서도 쉽게 적용 될 수 있다. 특히 본 연구의 모델에서는 우선적으로 침입 탐지 영역에 적합한 휴리스틱을 사용 함으로서 필수 적인 필드만으로 데이터를 구성하였다. 또한 각 공격 유형마다 서로 다른 분류자를 생성 함으로서 보다 정확하고 효율적인 탐지를 가능하게 한다.

향후 연구 과제로서, 현재는 많은 필드 데이터에 대해서 임의적인 휴리스틱을 적용하여 필수 필드를 선택하는 방법을 사용하고 있으나, 해당 침입과 관련이 없다고 생각되는 필드가 침입과 연관성을 가질 수도 있기 때문에, 보다 효과적으로 필수 필드를 선택할 수 있는 알고리즘에 관한 연구가 수행되어야 할 것이다.

참고문헌

[1] D. Anderson, T. Frivold, and A. Valdes. "Next-generation intrusion-detection expert system (NIDES)". Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, USA, May, 1995.

[2] H. Debar, M. Becker, and D. Siboni. "A network componet for an intrusion detection system". In Proceedings of the 1992 IEEE Computer society Symposium on Research in Security and Privacy, pp. 240-250, Oakland, CA, USA, May 1992. IEEE, IEEE Computer Society press, Los Alamitos, CA, USA.

[3] W. Reisig, "Petri Nets, An introduction", In W. Brauer, G. Rozenberg, A. Salomaa, eds: EATCS, Monographs on Theoretical Computer Science, Springer Verlag, Berlin, 1985.

[4] M. Crosbie, B. Dole, T. Ellis, I. Krsul, and E. Spafford. "IDIOT-Users Guide", Technical Report TR-96-050, Dept. of Computer Science, Purdue University, West Lafayette, IN, USA, 1996.

[5] R. Ziyyon, "KDD-99 Classifier Learning Contest LLSoft's Results Overview", eds: SIGKDD Explorations, 2000 ACM SIGKDD Volume 1, Issue 2, pp. 67-75, January, 2000.

[6] C. Woo, S. Hwang, J. Choi, and S. Kim, "Multi-agent based Intruder tracing System in the Active network Environment". In Proceedings of the 5th ICACT, pp. 719-723, January, 2003.

[7] W. Lee and S. Stolfo, "Data mining approach for Intrusion detection", In Proceeding of the 7th UESNIX security Symposium, January, 1998.

[8] S. Mukkamala, G. Janowski, A. H. Sung, "Intrusion Detection using Neural Networks and Support Vector Machines", In Proceedings of IEEE IJCNN, pp.1702-1707, May, 2002.