네트워크 패킷의 그룹화를 이용한 Anomaly 침입탐지 시스템

유상현*, 원일용*, 송두헌**, 이창훈*
*건국대학교 컴퓨터공학과
**용인송담대학 컴퓨터게임정보과
e-mail: simonyoo@konkuk.ac.kr

An Anomaly Intrusion Detection System Using Grouping of Network Packets

Sang Hyun Yoo*, Ill-Young Weon*, Doo Heon Song**, Chan-Hoon Lee*
* Department of Computer Engineering, Konkuk University
** Department of Computer Game & Information, Young-in SongDam College

요 약

기계학습 방법을 이용한 네트워크 기반 침입탐지 시스템은 어떤 학습알고리즘을 사용하여 구현되었느냐에 따라 그 결과가 매우 달라진다. 학습을 위한 전처리를 많이 하면 비례하여 성능이 개선되지만, 실제 사용의 유용성면에서는 성능이 떨어지게 된다. 따라서 최소한의 전처리를 하여 침입탐지의 탐지율을 보장하는 방법이 필요 하다. 본 논문에서는 네트워크기반 침입탐지 문제를 기계학습을 이용하여 해결하는 방법을 제안 하였다. 제안된 모델은 탐지 속도와 각종 공격들의 패킷 분포를 고려하여 관련된 그룹으로 분류하고, 이것을 학습하는 시스템이다. 실험을 통하여 제안된 모델의 유용성을 검증 하였다.

1. 서론

침입탐지 시스템에서 가장 먼저 수집되는 데이터는 네트워크에서 발생하는 패킷이다. 이렇게 수집되어진 패킷들은 각기 다른 성향을 나타낸다. 패킷들 중에서 몇몇의 패킷들은 그룹으로 묶여서 비정상적인 행동을 하는데, 이러한 비정상적인 행동을 침입탐지 시스템에서는 공격이라고 명명한다. 기계학습 방법을 이용하여 공격에 대한 패턴을 자동으로 생성하고 감지하는 방법에 대하여 많은 시도가 있었다. 이러한 연구는 DARPA에서 지원하는 프로젝트에서 공식적인 그 출발을 볼 수 있으며, 여기에는 다양한 방법들이 제안 되었다[1,4,5,6].

이렇게 제안된 기존의 방법들은 실제로 사용되기 위해서는 몇 가지 문제점이 있었다. 첫째로, 침입 탐지율은 높지만, 과도한 데이터의 전처리로 인해 시간이 너무나 많은 시간이 소유 된다는 것이다. 둘째로, 기존의 방법들 중에서 성능이 높았던 학습 방법은 주로 감독학습 방법인데, 학습시간이 많이 소모가 된다는 데에는 문제가 없지만, 탐지 시에 판단 시간이 많이 소모 된다는 것이 문제이다. 이러한 이유는 공격패턴을 만들기 위해 대용량의 데이터를 사용하기 때문이다. 따라서 기계학습의 효과를 유지하면서 탐지경보 발생 시간을 최소화하는 새로운 접근법이 요구 되고 있다.

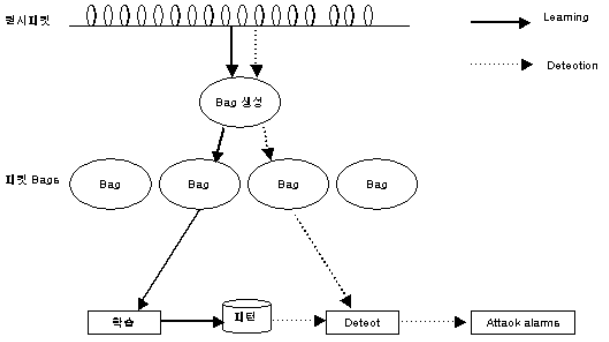
기존의 전처리 방법들은 네트워크와 보안이라는 도메인의 고려 없이 전통적이고 일반적인 방법을 사용하였는데, 우리는 이 논문에서 기존의 방법과는 다르게 도메인의 특성을 최대한 분석하여 빠르고 효과적인 전처리 방법을 제안 하였다. 이러한 전처리 방법의 핵심은 정상 및 비정상 패킷이 뒤 섞여 있는 패킷의 흐름을 고려하여 관련 있는 패킷을 그룹화 하는 것이다. 이렇게 생성된 그룹을 신경망을 이용하여 학습하고, 학습된 데이터를 이용 침입율을 분석 및 실험한 모델을 제안한다. 이 논문의 구성은 다음과 같다. 2장에서 제안된 모델의 이론에 대하여 설명하였다. 3장에서는 실험과 그 결과에 대하여 분석 하였다. 4장에서는 결론 및 향후과제에 대하여 언급 하였다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성・지원사업의 연구결과로 수행되었음

2. Bag 단위 접근

2.1 Bag 모델

네트워크에서 패킷의 연속 흐름에는 정상과 비정상 패킷이 서로 뒤 섞여있다. 이렇게 정상과 비정상이 섞여 있기 때문에 패킷을 순차적으로 단순하게 학습 하는 것은 학습율 면에서 좋지 않다고 알려져 있다[5,8]. 특히 한 개의 공격을 구성하는 패킷들을 개별적으로 보면 정상인 경우가 대다수 섞여 있으므로 패킷을 개별단위로 다루어서는 효과가 떨어짐을 알 수 있다. 이에 우리는 이러한 공격이라는 분야의 특성을 활용할 수 있게 하기 위하여 패킷을 각 목적지 주소(IP)별로 패킷을 분리하고, 서로 관련되는 패킷 그룹(group)으로 —이후 Bag으로 명명함, 나누어 학습을 하고 학습된 데이터의 패턴을 비교, 분석하여 침입을 찾는 방법을 제안 하였다. [그림 1]은 이러한 모델을 개념적으로 보여 준다.



[그림 1] Bag을 통한 탐지 모델

2.2 Bag 생성

아래 <표 1>는 Bag생성의 알고리즘을 기술한 것이다. 알고리즘의 특징은 목적지 IP별로 먼저 패킷의 흐름을 분류 하고 의심스러운 패킷은 의심스러운 것들로 묶고, 정상인 패킷은 정상적인 것으로 묶어서 다루는 것에 기반 하고 있다. 이러한 데이터 모델링은 한 개의 공격을 구성하는 흐름에는 정상 및 비정상이 뒤 섞여 있다는 점을 반영한 것이며, 한 개의 패킷에 대한 경보 보다는 여러 개의 패킷에 대하여 대표 경보를 발생 시킨다는 점에서, 기존의 기계학습법에 비해 좀더 자연스러우며 관리자가 다루어야 할 정보의 크기를 많이 줄일 수 있다는 장점이 있다.

<표 1> Bag 생성 과정

Bag Generation
1. XIBL을 이용하여 학습지식을 생성.
2. 각각의 Bag을 만들 인스턴스들에 대하여
2.1 만약 목적지 IP가 동일한 완성되지 않은 Bag이 없으면 새로운 Bag을 시작 하고 2로 감.
2.2 Bag의 크기가 특정 크기 이상이 아니라면 해당 Bag에 인스턴스 추가하고 2로 감.
2.3 새로운 인스턴스와 Bag의 시간 차이가 기준값 이상 이면 해당 Bag을 종료하고 새로운 Bag을 생성 2로 감.
2.3 새로운 인스턴스의 시간차가 Bag의 시간차 평균의 K배 이상이 아니면 해당 Bag을 종료하고 새로운 Bag을 생성하고 2로 감.
2.4 새로운 인스턴스의 클래스 값을 예측함.
2.5 새로운 인스턴스의 추가가 기존의 Bag의 위험도를 증가 시키지 않으면 새로운 인스턴스를 해당 Bag에 포함 시키고, 새로운 인스턴스를 포함하는 새로운 Bag을 시작 2로 감.
2.6 위험도가 특정 값 이상 이면 해당Bag에 인스턴스를 추가하고 Bag을 종료하고 2로 감.
2.7 Bag에 새로운 인스턴스 추가 없이 종료하고 새로운 인스턴스를 포함하는 새로운 Bag을 시작하고 2로 감.

Bag의 적당한 크기 선정을 위해서 우리는 새로운 패킷이 기존 Bag에 첨가 되었을 때 위험도가 특정 값 이상 증가하면 새로운 Bag을 생성하고, 위험도가 특정 값 이하로 감소하면 정상인 데이터 흐름이 시작된다고 판단하여 Bag을 종료 하였다. 특히 새로운 패킷의 발생 시간이 해당 Bag의 마지막 패킷의 발생 시간과 비교하여 특정 시간 이상 이면 Bag을 종료 하도록 하였다. 이러한 Bag생성과 패킷의 성향 분류를 위해 우리는 기계학습법의 하나인 XIBL을 사용하였다[2,3].

2.3 신경망을 이용한 Bag 학습

생성된 Bag의 학습을 위하여 우리가 사용한 것은 신경망의 오류 역전파 알고리즘(BP)을 사용하였다. BP는 지도학습의 일종으로 가장 보편적으로 쓰이는 학습 알고리즘이다. 일반적인 개념은 입력 데이터가 여러 개의 은닉층을 통과하여 출력층으로 출력이 되면, 그 값을 목표 출력 값과의 오차가 최소가 되는 가중치 값들을 구한 후, 각 노드에 대한 가중치 값의 변화가 없을 때가지 역방향 즉 출력층, 은닉층의 순서로 가중치를 갱신하여 학습 하는 방식이다. 우리가 사용한 가중치 계산식은 아래(1) 와 같다.

$$\delta_{pk} = (d_{pk} - O_{pk}) f_k^{'}(net_{pk})$$
$$E = E + E_p, \quad (E_p = \sum_{k=1}^{M-1} \delta_{pk}^2) \quad (1)$$

본 논문에서 구현한 신경망의 구조를 위하여 우리는 우선 학습할 모든 Bag의 인스턴스의 크기를 조사하고 가장 큰 값을 기준으로 입력 노드를 결정 한

다[10]. Bag의 인스턴스의 크기가 최댓값 미만인 것들은 모두 0 으로 입력 값을 계산 하였다. 출력은 하나로 계산하였고 은닉층을 3개로 주는 신경망 구조를 구현하였다. 또한 시스템을 테스트하기 위하여 Bag의 데이터 중 30%를 테스트에 사용하였고, 나머지 70%는 학습 하는 과정으로 구현하였다.

3. 실험

3.1 실험 Data

우리가 본 논문에서 실험용으로 사용한 데이터는 DARPA에서 제공하는 1998년 데이터 중 Sample 용 데이터이다[6]. 이 자료는 특정 네트워크 환경에서 특별한 시나리오에 의해 만들어진 데이터 들이다. 이때 많은 공격들이 행하여지는데, 이렇게 발생되는 모든 패킷들을 tcpdump 형태로 만들어 제공된 데이터들이다. 또한 언제 어디서 어디로 어떠한 공격이 행하여 졌는지에 대한 추가 정보가 별도의 로그 파일(리스트파일)로 제공된다. Sample용 데이터는 14600개가량의 패킷으로 구성되어 있으며 여기에는 5 종류의 서로 다른 공격이 20회 포함되어 있다.

패킷의 가장 기본이 되는 자료는 IP이다. IP의 데이터는 다시 다양한 계층으로 분화 되는데, TCP, UDP, ARP 등이 그 대표적인 예이다[9]. 우리는 IP와 TCP 레벨의 범위에서 학습 자료를 추출 하였는데, 그 이유 중에 하나는 UDP와 ARP에 비해 대다수의 공격들이 TCP를 기반으로 하고 있기 때문이고, 또 다른 이유는 TCP의 콘텐츠에서 데이터를 추출하면 각종 프로토콜별로 세분화 할 수 있기 때문이다. 그러나 TCP의 콘텐츠에서 자료를 추출할 경우 그 정보가 방대해 지기 때문에, IP와 TCP 헤더 레벨에서 데이터를 추출하였다. 이러한 헤더를 구성하는 요소 중 정상 및 비정상의 판단의 기준이 되는 필드를 선택하기 위해 우리는 기계학습 분야의 필드 선택 알고리즘의 하나인 Mutual Information(MI)[7]을 이용하였다. 아래 수식 (2)은 MI값을 계산하기 위해 우리가 사용한 수식 이다. 이산형에 대해서는 아래 식을 바로 적용하였고, 수치형 필드에 대해서는 통계적인 분석을 시행하고 이산형으로 자료를 변형한 후 아래 식을 적용 하였다.

$$I(X,Y) = \sum_{x,y} p(x,y) \times \log_2 \frac{p(x,y)}{f(x)g(y)} \quad (2)$$

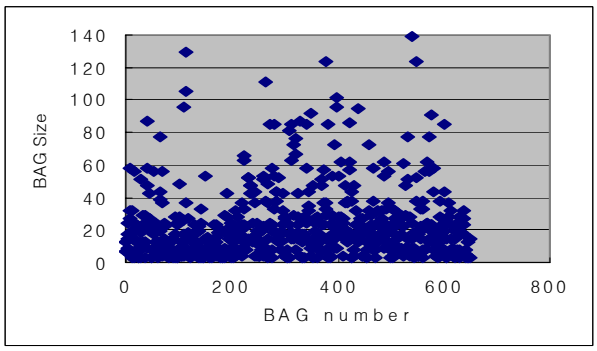
이렇게 선택된 필드는 모두 8개 이며, <표 2>는 해당 항목을 보여 준다. MI값이 1에 가까울수록 해당 필드는 정상 및 비정상을 판단하는 기준으로 의미가 높다는 뜻이다.

<표 2> MI값

Field	MI	Selection
Total length	0.0	
Service type	0.0035	Accepted
Time to live	0.0838	Accepted
Protocol	0.0	
Source IP	0.0865	Accepted
Destination IP	0.1535	Accepted
Source port	0.3253	Accepted
Destination port	0.1270	Accepted

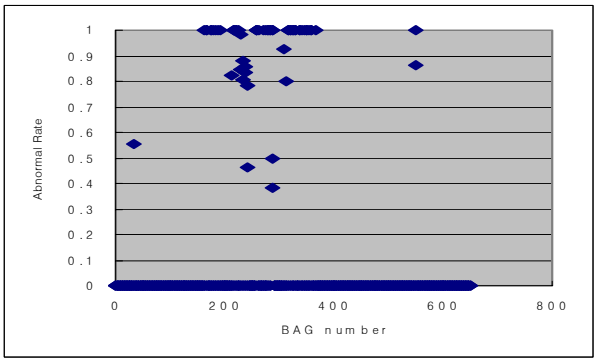
3.2 Bag 생성 분석

생성된 Bag의 평가를 위해 우리는 Bag의 개수와 한 Bag을 구성하는 정상 및 비정상 비율을 비교하였다. 한 개의 Bag을 구성하는 인스턴스의 개수가 너무 작거나 크면 의미가 없을 것이다. [그림 2]는 생성된 Bag의 인스턴스 개수의 분포로 대략 20 에서 60 개의 인스턴스들로 한 개의 Bag이 이루어진 것을 볼 수 있다.



[그림 2] Bag의 크기 분포

또한 정상 및 비정상의 비율이 0 이나 100%에 근접해야 데이터의 구분도가 높은 것이며, 50%에 근접하면 정상 또는 비정상으로 분류하는 변별력이 의미가 없어진다. [그림 3]은 생성된 Bag에서 Bag을 구성하는 인스턴스들의 비정상 비율로 0 이나 1에 수렴하여 한 개의 Bag에는 비슷한 특성을 갖는 패킷들이 모이는 것을 알 수 있다.



[

그림 3] Bag의 비정상 비율분포

3.3 탐지율 분석

신경망에서 제일 중요한 것은 학습 횟수와 학습율이다. 그래서 우리는 만 번의 학습을 시도 하였고, 학습율은 0.5를 주었다. 전체 오차의 한계는 0.5를 주고 실험 하였다. 본 논문에서 구현한 신경망에서의 중요한 요인 중에 하나는 비정상 비율을 0.1에서 1 사이로 변화를 주고 침입탐지를 측정했다는 것이다. 비정상 비율이란 한 개의 Bag에 클래스가 어느 정도의 비정상 공격을 가지고 있는지를 비율로 나타낸 것이다. 아래 <표 3>은 비정상 비율에 대한 여러 가지 공격성향을 탐지한 결과이다.

<표 3> 비정상 비율에 따른 공격성향(개)

	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
TN	0	0	0	0	0	0	0	0	0	0
FN	18	18	18	17	16	16	16	16	14	13
FP	0	0	0	0	0	0	0	0	0	0
TP	177	177	177	177	177	178	178	178	180	181
*Acc	90.7%	90.7%	90.7%	91.2%	91.2%	91.7%	91.7%	91.7%	92.7%	93.2%

*Acc(Accuracy)

비정상 비율에 따른 총 공격성향 개수는 195개이고, 그 중 비정상 비율을 0.1로 하고 측정한 결과 공격을 정상으로 판단한 FN(False Negative)의 경우가 18개임을 볼 수 있다. 이에 반해서 0.9로 테스트 할 경우 FN이 현저하게 떨어진 14개인 것을 볼 수 있다. 또한 정상을 정상이라고 판단한 TP(True Positive)의 개수는 늘어났다. 이런 한 결과는 정확도가 굉장히 높아짐을 볼 수 있는데 처음에 90.7%에서 93.2%까지의 정확도가 높아졌다. 비정상 비율이 높아질수록 신경망의 성능이 최적이 되었다.

4. 결론 및 향후 과제

우리는 이 논문에서 네트워크기반 침입탐지 문제를 기계학습을 이용하여 해결하는 방법을 제안 하였다. 제안된 모델은 데이터의 전처리 속도를 고려하였고, 실제 패킷흐름에서 공격의 패킷 분포를 관련된 그룹으로 분류 하였다. 이렇게 생성된 그룹을 신경망으로 학습하고 탐지했다. 또한 실험을 통하여 제안된 모델의 유용성을 확인 하였는데, 기존의 여러 기계학습 기법에 비해 정확도는 떨어지지만 실제 사용이라는 면에서는 구조상의 빠른 전처리로 인해 의미를 갖는다고 할 수 있다.

앞으로의 과제는 좀더 나은 신경망 알고리즘을 구현하는 것이고 또한 XIBL로 Bag을 구성하는 것이 아닌 신경망을 이용한 Bag생성의 연구와 다른 학습 데이터와 다른 기계학습 알고리즘을 이용하여 실험하는 연구가 계속되어야 할 것 이다.

참고문헌

[1] W. LEE. "A Data Mining Framework for constructing Features and Models for Intrusion Detection Systems", Ph.D. Dissertation, Columbia University, 1999

[2] Aha.D & Kibler.D Noise-tolerant instance-based learning algorithms. Proceedings of the Eleventh International Joint Conference on Artificial Intelligence pp.794-799, 1989.

[3] Stanfill.C & Waltz.D Toward memory-based reasoning. Communications of the ACM, 1986

[4] Lippman.R et. Al. Evaluation intrusion detection systems: The 1998 DARPA Off-line intrusion detection evaluation, Proc. Of DARPA Information Survivability Conference and Exposition, pp 12-26, 2000

[5] Won.I Song.D Lee.C Heo.Y & Jang.J A Machine Learning approach toward an environment-free network anomaly IDS A primer report, In Proc. of 5th International Conference on Advanced Communication Technology, 2003.

[6] DARPA data set: www.ll.mit.edu/IST/ideval

[7] MI:http://en.wikipedia.org/wiki/Mutual_information

[8] Song.D, I.Cang Lee, The Utility of Packet level decision in Misuse Intrusion Detection System: An analysis of DARPA dataset toward a hybrid behavior based IDS. The 3rd Asia Pacific International Symposium on Information Technology ,Jan. 13-14 2004, Istanbul, Turkey

[9] Behrouz.A, Forouzan TCP/IP Protocol Suite. MaGRAW-HILL,2000

[10] Jan Ramon and Luc de Raedt. Multi instance neural networks. In Proceedings of the International Conference on Machine Learning 2000 Workshop on Attribute-Value and Relational Learning, 2000.