Alpha-cut과 Beta-pick를 이용한 시그너쳐 기반 침입탐지 시스템과 기계학습 기반 침입탐지 시스템의 결합

원 일 용[†] · 송 두 헌[††] · 이 창 훈[†††]

요 약

시그너쳐 기반 침입탐지 기술은 과탐지(false positive)가 많고 새로운 공격이나 변형된 유형의 공격을 감지하기 어렵다. 우리는 앞선 논문[1]을 통해 시그너쳐 기반 침입 탐지 시스템과 기계학습 기반 침입 탐지 시스템을 Alpha-cut 방법을 이용하여 결합한 모델을 제시 하였다. 본 논문은 Alpha-cut의 후속연구로 기존 모델에서 감지하지 못하는 미탐지(false negative)를 줄이기 위한 Beta-pick 방법을 제안한다. Alpha-cut은 시그너쳐 기반 침입탐지 시스템의 공격 탐지결과에 대한 정확성을 높이는 방법인 반면에, Beta-pick은 공격을 정상으로 판단하는 경우를 줄이는 방법이다. Alpha-cut과 Beta-pick을 위해 사용된 기계학습 알고리즘은 XIBL(Extended Instance based Learner)이며, C4.5를 적용했을 때와 차이점을 결과로서 제시한다. 제안한 방법의 효과를 설명하기 위해 시그너쳐 기반 침입탐지 시스템의 탐지결과에 Alpha-cut과 Beta-pick을 적용하여 오경보(false alarm)가 감소함을 보였다.

키워드 : 미탐지, 과탐지, 결합모델, 침입탐지 시스템

A Combination of Signature-based IDS and Machine Learning-based IDS using Alpha-cut and Beta pick

Ill Young Weon[†] · Doo Heon Song[††] · Chang Hoon Lee[†††]

ABSTRACT

Signature-based Intrusion Detection has many false positive and many difficulties to detect new and changed attacks. Alpha-cut is introduced which reduces false positive with a combination of signature-based IDS and machine learning-based IDS in prior paper [1]. This research is a study of a succession of Alpha-cut, and we introduce Beta-pick in which attacks can be detected but cannot be detected in single signature-based detection. Alpha-cut is a way of increasing detection accuracy for the signature based IDS, Beta-pick is a way which decreases the case of treating attack as normality. For Alpha-cut and Beta-pick we use XIBL as a learning algorithm and also show the difference of result of C4.5. To describe the value of proposed method we apply Alpha-cut and Beta-pick to signature-based IDS and show the decrease of false alarms.

Key Words : False Negative, False Positive, Combined Model, Intrusion Detection System

1. 서 론

네트워크 침입탐지 분야에서 시그너쳐 기반 침입탐지 기법은 현재 대부분의 상용 시스템의 핵심 부분을 이루고 있다. 그러나 나날이 증가하는 다양한 공격 유형에 대처하기에는 많은 어려움이 있다. 이러한 어려움 중 가장 큰 문제는 새롭거나 변형된 공격 시그너쳐의 갱신 문제인데 전문가의 높은 비용이 요구 된다. 이에 비해 기계학습 기반 침입 탐지 시스템 기법은 사람의 간섭이 거의 없다는 장점을 가지고 있지만, 그 성능이 시그너쳐 기반 침입 탐지 기법에 비하여 낮은 편이다. 그러나 시그너쳐 기반 침입 탐지 기법이 감지하지 못하는 새로운 공격이나, 변형된 공격을 인식할 수 있다는 구조적 특징 때문에 연구가 진행 되어 왔다[2, 3, 6, 14]. 따라서 이러한 두 시스템은 상호 보완적인 관계에 있다. 그러므로 두 기법의 결합은 각각의 단독기법 사용에 비해 침입탐지의 성능을 향상 시킬 수 있다.

현재 두 기법 결합의 주된 연구 방향은 시그너쳐 기반 침입 탐지 기법을 주로 하여 정보를 처리하기 전이나 후에 통계적 기법이나 기계학습 기반 침입 탐지 기법을 이용하여 정

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행됨.
† 준 회 원 : 건국대학교 컴퓨터공학과 박사과정
†† 정 회 원 : 용인송담대학 컴퓨터정보과 교수
††† 종신회원 : 건국대학교 컴퓨터공학과 교수
논문접수 : 2004년 11월 25일, 심사완료 : 2005년 5월 6일

보 처리를 시행 하여 주된 기법에 도움을 주는 것이다. 이것은 시그너쳐 기반 침입탐지 기법이 침입탐지 분야에서 그 성능을 충분히 검증 받아 왔고, 기계학습 기반 기법에 비해 상대적으로 높은 탐지율을 보이기 때문이다. 이러한 기존의 연구들의 주된 목적은 두 기법의 결합을 통하여 시그너쳐 기반 기법의 과탐지(false positive)를 줄이는 것이다[1, 4, 5, 15].

우리는 이미 앞선 논문[1]에서 시그너쳐 탐지 기법을 주로 하고 기계학습 탐지 기법을 보조적으로 사용하는 결합모델을 제안 하였다. 여기에서 Alpha-cut을 이용하여 오경보 중 과탐지를 줄일 수 있음을 보였다. 그러나 침입탐지 영역에서 오경보는 과탐지만 있는 것이 아니라 미탐지(false negative)도 존재 한다. 본 논문은 과탐지를 줄이는 기존의 연구를 확장한 것으로, 시그너쳐 기반 침입 탐지 기법 단독으로 탐지하지 못하는 공격을 탐지할 수 있는 방법(Beta-pick)을 추가로 제시 하였다. 또 Alpha-cut과 Beta-pick의 유용성 검토 실험과는 별도로 위의 두 개념을 모두 적용한 시스템의 성능을 알아보는 실험을 실시하고 그 결과를 분석 하였다. 실험을 위하여 우리는 DARPA 1998, 1999년 Data Set을 이용 하였다[10, 13].

Alpha-cut과 Beta-pick의 개념에서 핵심은 기계학습 알고리즘인데, 우리는 이미 다른 논문[3]에서 이러한 기계학습 기반 침입탐지 시스템의 학습 알고리즘을 위해, IBL을 확장한 XIBL(Extended Instance-based Learner)을 제시 하였다[7, 11, 12]. 본 논문에서 우리는 기계학습의 주된 알고리즘으로 XIBL을 사용하였고, 비교를 위한 알고리즘으로는 C4.5를 사용 하였다[8]. 실험을 위한 시그너쳐 기반 침입탐지 시스템으로 Snort를 사용 하였으며, 기계학습 기반 침입탐지 시스템은 자체적으로 구현하여 사용 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 제안된 결합 모델을 요약 설명하고 특히 Beta-pick를 제시하여 그 타당성을 검토 하였다. 3장에서는 Alpha-cut과 Beta-pick를 모두 적용한 통합 침입 탐지 시스템의 성능평가에 대하여 상세하게 다루었다. 마지막 4장에서는 본 논문의 결론 및 향후 과제를 논의 하였다.

2. 결합 모델

2.1 XIBL

우리가 학습 알고리즘으로 사용하는 XIBL은 원본 IBL을 기반으로 아래와 같이 3가지 특징에 중점을 두고 확장 하였다[3].

첫째, 인스턴스(instance) 사이의 거리 계산에서 심볼형 자료의 경우 IBL은 그 결과가 0 또는 1로 표시되기 때문에, 실수형 속성(attribute)이 정규화에 의해 0과 1 사이의 값을 갖는 것에 비해 실질적 가중치가 높다. 이러한 것을 반영하기 위해 XIBL에서는 이산형 데이터의 거리를 0과 1 사이의 연속 값으로 나타낼 수 있는 Value Difference Metric(VDM)[16]을 적용 하였다.

둘째, IBL은 잡음(noise)에 민감한데 이 문제를 해결 하기 위해 수학적 통계에 근거를 두고 있는 Leave-one-out[17] 잡음 필터를 적용 하였다.

셋째, 속성 가중치 값을 지정하는 방법에서 IB4가 채택한 학습 중의 reward-penalty 부여법 대신 통계적으로 검증된 backward stepwise regression에 의한 속성 가치 판단 기법을 적용하였다.

XIBL의 자세한 구현이나 성능 실험은 본 논문의 범위를 벗어 나므로 여기서는 언급하지 않지만 자세한 내용은 이미 발표된 논문[3, 1]들에 언급 하였다.

XIBL의 학습 지식을 위해 1998년 1주에서 7주 사이의 각 요일마다 해당 공격들에 해당하는 패킷들을 해당 세션(session) 별로 불리하고, 동일한 패킷 개수 비율로 정상 패킷들을 분리해 낸다. 이렇게 하여 정상 과 비정상 비율이 동일한 실험용 전체 data를 구성 하고, 이 자료를 30 대 70 비율로 나눈다. 이때, 각각의 분리 자료 내부의 정상 및 비정상의 비율은 50 대 50으로 동일하다. 전체 자료 중 30% 자료는 XIBL의 특성 및 성능을 측정하기 위한 용도이고, 나머지 70%는 XIBL의 학습을 위해 사용 하였다. 즉 Beta-pick의 유용성 검증을 위해서는 논문[1]의 실험과 동일한 자료를 사용 하였다.

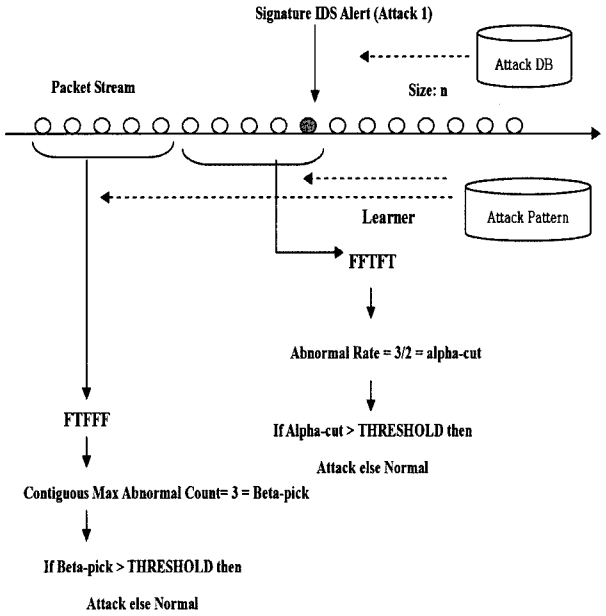
2.2 결합 모델

시그너쳐기반 침입탐지 시스템은 네트워크에서 발생한 패킷을 각각의 프로토콜 스펙에 따라 순차적으로 처리 하면서 각 단계에 해당하는 공격 시그너쳐들을 비교하여 일치하면 경보를 울린다[9]. 이에 비해 기계학습 기반 침입탐지 시스템은 네트워크에서 발생한 각 패킷마다 한 개의 이벤트로 만들고, 이렇게 만들어진 이벤트들을 이용하여 정상 및 비정상 패턴을 학습하게 된다. 탐지 시는 이렇게 학습된 기존 지식을 이용하여 각 패킷마다 정상 또는 비정상으로 분류 하게 된다[1].

시그너쳐기반 침입탐지 시스템의 침입 경보가 발생 했을 때, 발생한 공격의 종류에 따라 n개의 패킷을 역추적 한다. 이렇게 추적된 패킷들에 대하여 기계학습 기반 침입탐지 시스템이 분류한 값(정상 또는 비정상)을 각각 조사하여, 전체 n개 중 비정상으로 분류한 것의 비율을 계산 한다. 이 비정상 비율을 우리는 Alpha-cut이라고 정의 하였다. 여기서 n의 값은 알려진 공격에 대해서 전문가에 의해 공격 데이터베이스(attack DB)에 기록되며, 알려지지 않은 공격은 알려진 공격의 평균값을 사용 한다. Alpha-cut의 주된 목적은 시그너쳐 기반 침입탐지 시스템의 과탐지를 줄이는 것이다. Alpha-cut의 유용성 및 자세한 내용은 이미 논문[1]에 기술 하였다.

시그너쳐기반 침입탐지 시스템이 정상이라고 판단하고 기계학습 기반 침입탐지 시스템 쪽이 비정상으로 분류한 연속 패킷의 갯수를 Beta-pick로 정의 한다. 즉 Beta-pick가 30이란 시그너쳐 기반 침입탐지가 정상이라고 판단한 패킷들에서 기계학습 기반 침입탐지 시스템이 비정상이라고 분류한 패킷의 연속된 개수 중 그 최대값이 30개란 의미 이다. 물론 시그너쳐기반 침입탐지 시스템은 비정상 이라는 경보는 발생 시키지 않는다. 따라서 우리는 시그너쳐 기반 침입탐지 시스템이 공격 경보를 발생시키는 않을 때를 정상 경보 시점으로

본다. 즉 Alpha-cut을 측정하지 않은 모든 패킷들에 대하여 Beta-pick를 적용 시킨다. 이러한 Beta-pick의 주된 목적은 시그너쳐 기반 침입탐지가 감지하지 못한 공격들을 기계학습 기반 시스템이 추가로 감지하게 하는 것이다. 즉 Beta-pick은 Alpha-cut과는 다르게 미탐지를 줄이는 것이 주된 목적이다. (그림 1)은 이러한 Alpha-cut 및 Beta-pick의 개념을 보여 준다.



(그림 1) 결합 모델

2.3 Beta-pick 유용성 분석

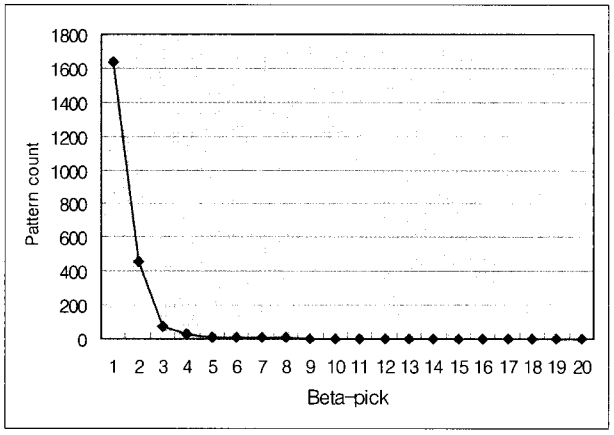
<표 1>은 1998년 공격 자료에서 Snort가 감지하지 못한 공격에 대한 Beta-pick 값을 측정한 결과이다. <표 1>에서 ID는 실험의 편의를 위해 공격에 부여한 고유번호이며, Attack_Name 항목은 공격 이름이다. <표 1>에 의하면 대부분의 공격들은 일정 값 이상의 Beta-pick가 존재함을 알 수 있다. 즉 Beta-pick를 측정하여 일정 값 이상이면 공격이라고 판단 한다면, Snort가 감지하지 못한 공격도 감지하는 것이 가능하다는 것을 의미한다. 특히 동일한 공격에 대하여 Beta-pick의 값이 다르게 나타나는 것은 공격의 지속 시간이 다르거나, 공격의 사이에 포함되어 있는 정상 패킷의 개수가 네트워크의 상태에 따라 달라 졌기 때문이다.

Snort가 정상이라고 판단한 것에는 원래 그 데이터가 비정상인 경우와 정상인 경우로 나누어 진다. 따라서 이러한 Beta-pick값이 의미를 가지기 위해서는 결합된 모델에서 Snort가 감지 하지 못하는 공격들에 대한 Beta-pick와 동시에 정상적인 패킷들의 Beta-pick 사이에 구별되는 패턴이 존재 해야 한다.

(그림 2)는 우리가 실험에 사용한 1998년 정상 자료들에 대한 Beta-pick분포를 표시한 것이다. Beta-pick가 5 이고 패턴 카운트(count)가 13이란 의미는 1998년 정상 자료 전체에서 Beta-pick를 측정했을 때 연속 5회 비정정상 이라고 분류된 경우가 모두 13회 존재 한다는 의미 이다.

<표 1> 1998년 자료 중 Snort가 감지하지 못한 공격에 대한 Beta-pick 분포

ID	Attack_Name	Beta-pick
5	Dict	90
12	Eject	364
16	Ffb	65
20	Ffb	17
24	Format	117
28	Guest	3
37	Loadmodule	88
44	Neptune	138
45	Neptune	160
46	Neptune	119
51	Perlmagic	49
59	Portsweep	216
71	Rootkit	228
72	Rootkit	200
76	Spy	1
...	...	...



(그림 2) 1998년 정상 자료에 대한 Beta-pick분포

<표 1>과 (그림 2)를 비교해 보면 1998년 DARPA Data Set에서는 미탐지를 줄이면서 과탐지를 크게 증가 시키지 않는 적절한 Beta-pick의 임계값이 존재함을 알 수 있다. 즉 <표 1>과 (그림 2)를 고려해 적절한 기준의 Beta-pick값을 적용하면 Snort가 감지하지 못하는 공격을 결합 시스템이 감지하는 것이 가능하다. 그러나 Beta-pick를 적용하면 Snort가 단독으로 감지하지 못한 모든 공격을 결합 시스템에서 감지하는 것이 가능 하다는 뜻은 아니다. 공격이 작은 수의 패킷들로 구성되어 있는 유형에서는 Beta-pick가 아무런 의미를 갖지 못한다.

3. 결합 모델의 통합 성능 실험

본 실험의 목적은 침입탐지 분야에서 결합 모델이 시그너쳐 기반 단독 모델에 비해 유리함을 보이는 것이다.

3.1 환경 및 경보 발생

실험 Data를 위하여 우리는 DARPA Data Set 중 1998년과 1999년 자료를 사용 하였다. 1998년 자료는 기계학습 기반 침입탐지엔진의 학습 지식을 생성하기 위한 용도로 사용 하였고, 1999년 자료는 성능을 측정하기 위해 사용 하였다. 1998년 자료에서는 [1]에서 설명한 방법으로 자료를 생성하고 이렇게 생성된 모든 자료를 기계학습 침입탐지 시스템의 초기 학습자료(training) 생성을 위해 사용 하였다. 1999년 자료는 테스트자료(testing)로 사용 하였는데, 크게 공격 자료와 정상 자료로 구분하여 추출 하였다. 공격 자료의 경우 무작위로 85개의 서로 다른 공격 유형을 선정하고 137회(총 127,405개의 패킷으로 구성)의 공격자료를 추출 하였으며, 정상 자료는 1주 월요일(총 1,369,134개의 패킷으로 구성) 자료를 모두 사용 하였다[10]. <표 2>은 우리가 사용한 비정상 자료의 목록 일부이다.

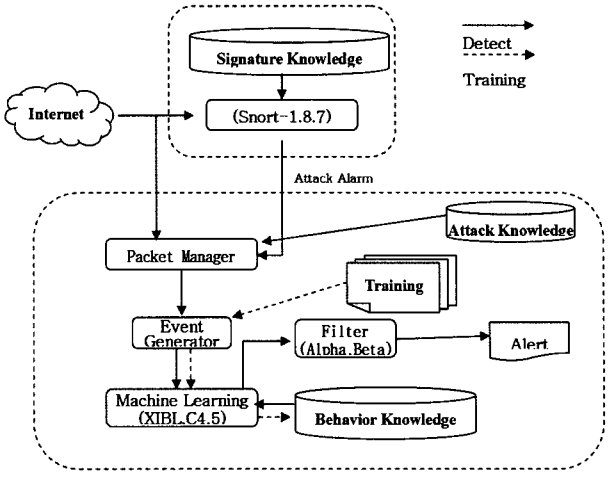
〈표 2〉 1999년에서 추출한 공격 유형

공격유형	공격명
Denial of Service Attacks	arppoison (New in 1999 test) dosnuke (New in 1999 test) selfping (New in 1999 test) ...
User to Root Attacks	anypw (New in 1999 test) casesen (New in 1999 test) ntfsdos (New in 1999 test) ...
...	...

기계학습 기반 침입탐지 시스템이 네트워크의 상태를 모델링 하기 위해 우리는 네트워크 패킷 하나당 학습자료(event) 하나를 생성하는 방법을 사용 하였다. 한 개의 이벤트를 구성하는 속성 집합은 TCP/IP 패킷의 헤더에서 추출 하였으며, 여기에 관련된 내용은[1, 3]에 자세하게 기술 하였다.

실험을 위한 시스템 구성은 다음과 같다. 시그너쳐 기반의 침입탐지 시스템은 Snort(1.8.7)을 사용하였고 환경은 [9]에서 배포하는 기본 환경 설정을 사용하였다. 기계학습 기반 침입탐지 시스템은 자체 구현하여 사용하였다. 기계학습 기반 침입탐지 시스템에서 사용하는 학습 알고리즘은 IBL을 확장한 XIBL을 사용하였고, 학습 알고리즘의 비교 실험을 위해 C4.5를 사용하였다[7, 8, 11, 12]. (그림 3)은 이러한 시스템 구성을 보여 준다.

(그림 3)에서 Attack Knowledge는 각각의 알려진 공격 타입을 구성하는 패킷들의 평균 개수가 저장되어 있다. 등록되지 않은 공격유형에 대해서는 기존 등록된 공격의 평균 패킷 개수를 사용한다. Packet Manger는 Snort의 경보를 기준으로 원시 패킷을 구분하는 기능을 수행 하며, 이 정보를 이용하여 Event Generator는 학습 및 판단에 필요한 자료를 생성한다. 기존의 정상 및 비정상 사례 자료를 이용하여 학습엔진에서 관련 지식(behavior knowledge)을 자동으로 구성 한다. 결합 모델에서 Alpha-cut과 Beta-pick를 적용하여 최종 경보를 발생하는 과정을 <표 3>에 의사코드로 기술하였다.



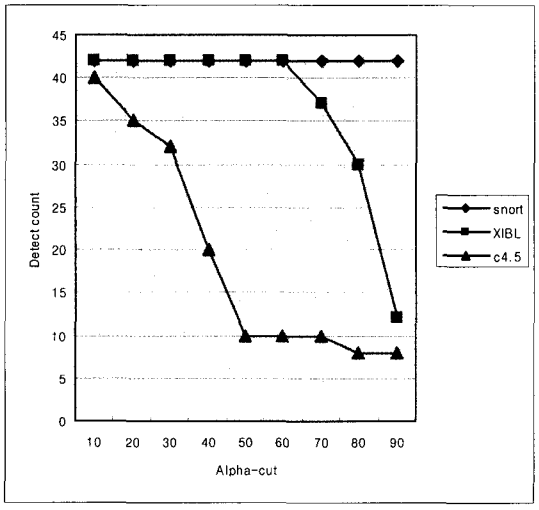
(그림 3) 결합 시스템

〈표 3〉 결합 시스템의 경보 발생

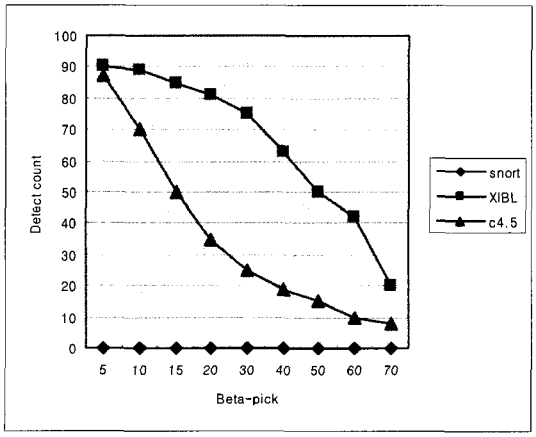
```
Key:
 AC:  Alpha-cut value
 BP:  Beta-pick value
 K:  number of packets of attack
 AK: average number of packet of known type attack
      (for unknown type attack)
 LA: learning algorithm
DECISION RULE()
IF  SNORT triggers an alarm on input packet x THEN
  IF  the type of attack is known THEN
       trace back to K packets
       examine K packets by LA
   ELSE
       trace back to AK packets
       examine AK packets by LA
  ENDIF
  get  AC
  IF  AC >= Alpha-threshold  THEN
       send alarm
  ELSE
       pass that packet x
  ENDIF
ELSE
 examine BP with the same source IP
 IF  BP >= Beta-threshold THEN
     send alarm
 ENDIF
ENDIF
```

3.2 실험 결과 및 분석

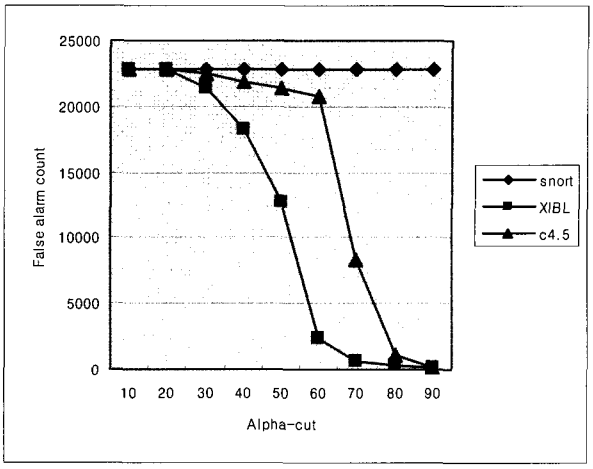
실험에 대한 결과는 공격 자료와 정상 자료에 대한 Alpha-cut과 Beta-pick로 나누어 측정 하였다. Alpha-cut은 10 에서 90까지 10의 간격으로 측정 하였으며, Beta-pick는 5, 10, 15, 20, 30, 50, 60, 70으로 측정 하였다. 공격 자료에서는 시스템이 탐지한 공격 횟수를 측정 하였는데, 동일한 공격에 대한 2회 이상의 경보는 모두 1회의 탐지로 기록 하였다. 이와는 다르게 정상 자료에서 발생한 경보는 모두 오경보이므로 경보의 횟수를 중심으로 결과를 측정 하였다. (그림 4)는 137회의 공격에 대하여 Snort가 공격 이라고 감지한 공격 자료에 대한 결합 시스템에서 Alpha-cut을 적용한 경우의 공격 탐지 횟수를 기록한 것이다. (그림 5)는 Snort가 감지하지 못한 공격에 대한 Beta-pick를 적용한 결합 시스템의 공격 탐지 횟수를 기록한 것이다. (그림 6)은 정상 자료에서 Snort가 발생시킨 오경보들에 대한 Alpha-cut을 적용시켜 경보의 량을 줄인 결과를 기록한 것이다. Beta-pick의 적용은 정상 자료에서 Snort에서는 발생하지 않는 오경보가 추가로 발생 하게 되는데 (그림 7)은 이것을 기록한 것이다.



(그림 4) Snort가 탐지한 공격에 대한 Alpha-cut 적용

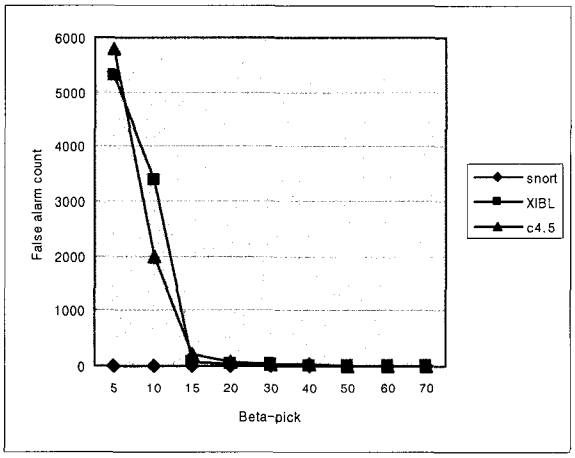


(그림 5) Snort가 탐지하지 못한 공격에 대한 Beta-pick 적용



(그림 6) 정상자료에서 Snort의 false alarm 대한 Alpha-cut 적용

결합시스템에 적절한 Alpha-cut의 임계값을 설정하기 위해서는 (그림 4)와 (그림 6)을 동시에 고려해야 하는데, (그림 4)에서는 최대한 Snort의 탐지 횟수를 유지 하며 (그림 6)에서는 최대한 오경보 횟수를 줄이는 것이 적절 하다. 적절한 Beta-pick의 임계값을 설정하기 위해서는 (그림 5)와 (그림 7)을 동시에 고려해야 하는데, (그림 5)에서는 탐지 횟수를 최대한 높이며 (그림 7)에서는 오경보 횟수를 최대한 줄여야 한다.



(그림 7) 정상자료에서 Beta-pick 적용으로 발생한 오경보

<표 4>는 위의 결과에서 Alpha-cut의 임계값을 50, Beta-pick의 임계값은 20으로 설정 하였을 경우에 대한 통합적 해석의 한 예이다. 이 임계값들은 [1]과 앞 장의 실험 결과에서 보편적인 운용 환경에서 적절 하다고 판단되어 선택 하였다. 137회의 공격 시도에 대하여 Snort단독 시스템은 42회를 탐지 하였다. 특히 <표 4>에서 동일한 공격에 대한 다중 경보는 모두 1회의 탐지로 기록 하였다. 결합 시스템의 경우 Snort가 탐지한 공격들에 대하여 Alpha-cut을 적용한 경우 XIBL은 100% 탐지 했으며, C4.5의 경우는 10회만 탐지 하여 Snort 단독에 비해 23.8% 정도의 탐지 율을 나타내었다.

〈표 4〉 성능 실험 통합 해석 예

Original Data	Single System	Combined System		
	Snort	Algorithm / Filter	XIBL	C4.5
Abnormal (137times try)	Abnormal (42 times detect)	Alpha-cut	Abnormal (42times detect)	Abnormal (10 times detect)
			Normal	Normal
	Normal (95 times miss)	Beta-pick	Abnormal (81 times detect)	Abnormal (35 times detect)
			Normal	Normal
Normal	*Abnormal (22,787 alarm)*	Alpha-cut	*Abnormal (12,791 alarm)*	*Abnormal (21,403 alarm)*
			Normal	Normal
	Normal	Beta-pick	*Abnormal (43 alarm)*	*Abnormal (53 alarm)*
			Normal	Normal

Snort가 탐지 하지 못한 95회에 대하여 Beta-pick를 적용한 XIBL은 81회의 탐지를 보여 주었으며, C4.5는 35회의 탐지를 보여 주었다. 실험용 정상 자료들에 대하여 Snort는 22,787회의 오경보를 발생 시켰는데, 이 오경보에 Alpha-cut을 적용한 XIBL은 12,791회로 오경보의 량이 Snort에 비해 43.8%나 줄어 들었다. 그러나 Snort가 발생 시키지 않은 오경보가 Beta-pick를 적용한 XIBL에는 발생하는데 그 회수는 43회로 상대적으로 경미하였다. C4.5의 경우 Snort가 발생시킨 22,787회의 오경보에 Alpha-cut 을 적용한 경우 21,403회로 약 6%의 오경보양을 줄일 수 있었다. 또 Beta-pick를 적용하면 Snort에서는 발생하지 않는 오경보가 53회 발생 하였다. 특히 Beta-pick로 잘 탐지되는 것은 DOS 및 Probing 유형의 공격 들이고, R2L이나 U2R 유형의 공격들은 잘 탐지하지 못하였다.

실험결과에서 C4.5의 성능이 XIBL에 비해 저조한 이유는 다음과 같다. C4.5는 다량의 데이터를 아주 짧은 시간 안에 비교적 정확한 규칙으로 생성하는 곳에는 적합하다. 그러나 학습 중에 주어진 자료가 달라지면 매번 다른 트리(tree)를 형성하는데, 때로는 주어진 자료에 따라 매우 다른 형태의 트리가 형성되기도 한다. 침입탐지 환경은 기본적으로 실시간적이라는 점에서는 C4.5와 부합하지만 자료의 역동성(dynamic)이라는 점에서 C4.5가 침입탐지 분야에서는 매우 제한적으로 사용되어 왔다. 즉, 변화의 여지가 작은 규칙 군집의 검색 효율화에서는 성능이 우수하지만 패킷 정보를 직접 다루는 경우에는 부적합하다고 할 수 있기 때문이다[8]. 이에 비해 XIBL은 학습 시간이 많이 소모 되지만, 동적인 데이터 환경에서도 안정된 지식을 생성할 수 있는 특징 때문에 탐지율이 상대적으로 높은 것으로 추정 된다.

<표 4>의 결과를 오경보의 양이라는 관점에서 보면 Snort 단독과 비교해 결합모델의 경우 약 56.7% 수준으로 오경보의 양이 감소함을 알 수 있다. 경보의 질이라는 관점에서 보면 결합모델의 경보에는 Snort가 탐지하는 대부분의 공격이 포함되어 있으며, Snort가 탐지하지 못하는 공격도 상당량 포함되어 있다. 다만 여기에는 필연적으로 Snort에는 존재하지 않는 새로운 오경보 발생이라는 희생이 요구 된다.

현재 대부분의 침입탐지 관리자들이 가장 어려움을 호소하는 점은 과도한 오경보의 양인데, 이러한 관점에서 보면 제안된 결합모델은 유사한 탐지 율을 유지 하면서 오경보의 양을 상당 수준으로 줄인 수 있다는 점에서 그 의미가 크다고 할 수 있다. 또 시그너쳐 기반 침입탐지 시스템 단독으로 감지하지 못하는 공격들을 결합 시스템에서 감지 할 수 있다는 것도 중요한 의미를 갖는다.

본 논문에서 제안한 시스템의 부하에 대한 정량적인 고려는 하지 않았지만, 시그너쳐 단독 시스템에 비해 Alpha-cut과 Beta-pick를 적용한 시스템이 가지는 정성적인 부하를 고려하면 다음과 같다. 기계학습 기반 침입탐지 시스템은 시그너쳐 기반 탐지 시스템과는 별도의 독립된 시스템 형태이다. 즉 학습을 통한 지식을 생성 한 후 각각의 패킷에 대하여 정상 및 비정상 여부를 판단한다. 이러한 기계학습 기반 시스템은 학습 시에 많은 부하를 요구 하지만 탐지 시에는 만들어진 지식을 이용하여 판단 하므로 지식을 생성한 알고리즘에 따라 다르지만 대체로 부하가 거의 없다고 할 수 있다. Alpha-cut과 Beta-pick를 적용한 시스템은 기계학습 기반 시스템의 경보를 이용하여 시그너쳐 기반 시스템의 경보가 없는 동안에는 Beta-pick를 측정하고, 시그너쳐 기반 시스템의 경보가 발생하면 Beta-pick의 측정을 멈추고, Alpha-cut을 측정하게 된다. 따라서 시그너쳐 기반 단독 시스템에 비해 제안된 시스템은 기계학습 시스템 쪽의 학습부하와 탐지시의 탐지 부하에 Alpha-cut 및 Beta-pick의 계산 부하의 합이라 할 수 있다.

4. 결 론

우리는 본 논문에서 시그너쳐 기반 침입탐지 기법과 기계학습 기반 침입탐지 기법의 결합 모델을 [1]에서 확장하여 제시 하였다. 제안된 결합모델 침입탐지 시스템은 시그너쳐 기반 침입탐지와 동시에 기계학습 기반 침입탐지 시스템 쪽에서 자체적인 분류를 실시한다. 기계학습 기반 침입탐지 시스템은 시그너쳐 기반 침입탐지 시스템의 침입 경보에 대한 정확성을 보정하고, 시그너쳐 기반 침입탐지 시스템이 탐지하지 못하는 침입 유형도 탐지 할 수 있는 구조를 가지고 있다. 결합 모델의 유용성 증명은 DARPA Data Set을 이용한 실험으로 보였다. 실험 결과는 단독 모델보다 결합모델이 경보의 양과 질이라는 관점에서 여러 가지 장점이 있음을 알 수 있다.

결합모델 침입탐지 시스템의 최종 목표는 성능 향상 이라고 할 수 있는데, 본 논문에서 성능 향상의 의미를 단순한 탐지율의 절대적 수치의 증가만을 의미 하지는 않았다. 실험 환경과 조건에 따라 탐지 율은 얼마든지 달라 질 수 있으므로, 우리가 제안한 두 시스템의 결합 방법은 의미가 있으며 실

필드에서도 적용될 수 있다는 것을 보이는 것이 본 논문의 중요한 목적이다. 침입탐지 영역에서 오경보는 과탐지, 미탐지가 존재 하는데, 이것은 동시에 true negative, true positive와는 각각 대칭적인 구조를 가지고 있다. 어떤 요인으로 한쪽의 과탐지 가 줄어들면 true negative에도 영향을 끼치게 된다. 또 미탐지를 줄이면 true positive도 영향을 받게 된다. 따라서 성능 향상의 가장 이상적인 방향은 최소의 진성 경보를 희생 하면서 최대의 오경보를 줄이는 것이다. 다만 이러한 기준 값은 시스템을 운용하는 관리자의 환경에 의존적이라고 할 수 있다. 따라서 우리의 입장은 결합 모델 시스템의 특성을 결정짓는 변수들의 특징에 대하여 각각 설명 하고 그 임계값의 선택은 관리자의 선택으로 남긴다.

시그너쳐 기반 침입탐지와 기계학습 기반 침입탐지 기법을 결합 하는 방법으로는 각각의 알고리즘 장점을 조합하여 새로운 알고리즘을 만들어 사용하는 적극적 결합과, 이와는 반대로 한쪽의 처리 결과를 다른 한쪽에서 다시 처리하는 소극적 결합이 있다. 구현이라는 면에서는 후자가 쉽고 효율적이라고 할 수 있으나, 이러한 방법의 결합은 궁극적으로 성능 향상에 그 한계를 가지고 있다고 할 수 있다. 따라서 전자의 생각처럼 두 탐지 기술의 장점을 적극적으로 수용하는 새로운 침입탐지 알고리즘에 대한 연구가 필요 하다.

참 고 문 헌

[1] 원일용, 송두헌, 이창훈, "Misuse IDS의 성능 향상을 위한 패킷 단위 기계학습 알고리즘의 결합 모형", 정보처리학회논문지C, 제11-C권, pp.301-308, 2004.

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

[3] I. Won, D. Song, C. Lee, C. Heo, Y. Jang, "A Machine Learning approach toward an environment-free network anomaly IDS-A primer report", In Proc. of 5th International Conference on Advanced Communication, 2001.

[4] K. Julisch, "Mining alarm clusters to improve alarm handling efficiency", In 17th Annual Computer Security Application Conference (ACSAC), pp.12-21, 2000.

[5] K. Julisch, "Mining Intrusion Detection Alarms for Actionable Knowledge", In 8th ACM International Conference on Knowledge Discovery and Data Mining, 2002.

[6] I. Won, D. Song, C. Lee, "The Architecture of Network Intrusion Detection Systems", Communication of the Korean Institute of Communication Sciences, 19(8), pp.41-51, 2002.

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

[8] Kruegel, C.& Toth, T., "Using decision trees to improve signature-based detection", In 6th Symposium on Recent Advances in Intrusion Detection(RAID), Lecture Note in Computer Science, Springer Verlag, USA, September, 2003.

[9] SNORT : http://www.snort.org.

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

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

[12] Cost, Scott and Salzberg and Steven Salzberg, "A Weighted Nearest Neighbor Algorithm for Learning with symbolic Features", In Journal of Machine Learning, Vol.10, pp.57-78,1993.

[13] 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.

[14] Manganaris, S., Christensen, M., Zerkle, D. & Hermiz, K., "A Data Mining Analysis of RTID Alarms", In 2nd Workshop on Recent Advances in Intrusion Detection (RAID99), 1999.

[15] Patton, S., Yurcik, W., & Doss, D., "An Achilles' Heel in Signature-based IDS : Squealing False Positives in SNORT", Lecture Notes in Computer Science, Springer Verlag, USA, 2003.

[16] C. Stanfill and D. Waltz, "Toward memory-based reasoning", Communications of the ACM, 1986.

[17] S. Cost, and S. Salzberg, "A Weighted Nearest Neighbor Algorithm for Learning with Symbolic Features", In Journal of Machine Learning, Vol.10, pp.57-78, 1993.

원 일 용

e-mail : clcc@konkuk.ac.kr

1997년 경원대학교 전자계산학과

2000년 건국대학교 컴퓨터공학과(석사)

2000년~현재 건국대학교 컴퓨터 공학과 박사과정

관심분야 : 지능시스템, 복잡성의 과학, 네트워크 보안 등

송 두 헌

e-mail : mypham@naver.com

1981년 서울대학교 계산통계학과

1983년 한국과학기술원 전산학과(석사)

1994년 캘리포니아대학교 전산학과 박사 수료

1983년~1986년 KIST 연구원

1997년~현재 용인송담대학 컴퓨터정보과 교수

관심분야 : 기계학습, 데이터마이닝, 데이터베이스, 보안 등

이 창 훈

e-mail : chlee@konkuk.ac.kr

1980년 연세대학교 수학과 졸업

1977년 한국과학기술원 전산학과(석사)

1993년 한국과학기술원 전산학과(박사)

1996년~2000년 건국대학교 서울캠퍼스 정보통신원 원장

2000년~2002년 건국대학교 정보통신대학원 원장

2001년~2002년 건국대학교 정보통신대학 학장

1980년~현재 건국대학교 컴퓨터공학과 교수

관심분야 : 지능시스템, 운영체제, 보안, 전자상거래 등