침입탐지를 위한 최적의 감사기록 축약에 관한 실험적 평가

서 연규, 조 성배
연세대학교 컴퓨터과학과
e-mail:{kitestar,sbcho}@csai.yonsei.ac.kr

Empirical Evaluation on Optimal Audit Data Reduction for Intrusion Detection

Yeon-Gyu Seo and Sung-Bae Cho
Dept. of Computer Science, Yonsei University

요 약

최근 그 심각성이 커지고 있는 해킹피해를 줄이기 위한 한 방법으로 시스템에 침입한 불법적 사용을 탐지하는 연구가 활발히 진행되고 있다. 침입을 탐지하는 방법으로는 오용탐지와 비정상행위 탐지가 있는데 비정상행위 탐지를 위해서는 정보수집의 정확성, 신속성과 함께 다량의 정보들로부터 필요한 정보를 추출하고 축약하는 것이 중요하다. 본 논문에서는 감사기록 도구인 BSM으로부터 정보를 추출하고 자기조직화 신경망을 이용하여 다차원의 정보를 저차원정보로 축약·변환하는 방법에 대한 실험적인 검증을 시도하였다. 또한 BSM에서 얻을 수 있는 데이터의 유용성을 조사하기 위하여 축약된 감사자료에 의한 탐지성능을 살펴보았다. 실험결과, 시스템 호출 및 파일관련 정보의 축약이 탐지성능향상에 크게 기여하는 중요한 척도임을 알 수 있었으며 각 척도마다 탐지성능이 좋은 맵의 크기가 다름을 알 수 있었다. 이러한 축약된 정보는 여러 정상행위 모델링방법에 의해 유용하게 사용될 수 있을 것이다.

1. 서론

침입탐지는 시스템의 불법적인 사용이나 오용, 남용 등에 의한 침입을 탐지해내는 것으로 기본적으로 감사기록, 시스템 테이블, 네트워크 부하기록 등의 자료로부터 사용자의 행위에 대한 정보를 분석하는 작업을 한다[12].

일반적으로 침입탐지 방법은 침입모델에 따라 비정상행위 탐지와 오용 침입탐지의 두 가지로 나눌 수 있다. 두 탐지방법 중에서 오용탐지의 경우는 잘 알려진 침입패턴에 대해서는 높은 탐지 성능을 보이지만 유사한 침입이라도 알려지지 않은 변종패턴일 경우는 탐지할 수 없다는 단점이 있다. 반면, 비정상행위 탐지의 경우 잘 알려진 침입에 대해서 오용탐지 만큼의 높은 성능을 보장하지는 않지만, 알려지지 않은 침입패턴에 대해서도 탐지가 가능하기 때문에 최근 관심이 고조되어 관련분야에서 많은 연구가 이루어지고 있다. 이에 관한 대부분의 연구들은 정상행위에 대한 프로파일을 작성하고 사용자의 행위가 프로파일과 얼마나 유사한가에 따라 침입여부를 결정한다. 정상행위에 대한 프로파일을 생성하는 방법으로는 통계적 기법에서부터 인공지능적인 기법(에이전트, 유전자 알고리즘, 신경망) [3, 4]에 이르기까지 다양한 방법이 시도되고 있다.

본 논문에서는 입력되는 패턴에 따라 자기 조직화하여 유사한 패턴으로 분류해주는 자기조직화 신경망(Self-Organizing Map : SOM)[6]을 이용하여 다양한 감사기록의 정보를 대표값으로 축약함으로써 침입탐지시스템에서 정상행위 모델링을 위한 순서화된 정보로 사용될 수 있도록 한다[10]. 이때, 침입탐지를 위해 추출해야 할 정보의 선정은 탐지성능과 관련되기 때문에 중요하다. 따라서, 탐지를 위한 최적의 척도선정을 위해 각 척도들이 탐지성능에 미치는 영향을 실험적으로 분석하고자 한다.

2절에서는 감사기록의 축약을 위한 전체과정에 대해 설명하고 3절에서는 BSM감사기록의 척도선택에 대해 간단히 살펴본다. 4절에서는 추출된 감사기록의 다차원 정보를

저차원 정보로 변환하는 방법에 대해 설명한다. 5절에서는 실험을 통해 SOM의 맵크기에 따른 척도가 탐지성능에 미치는 영향을 알아보고 마지막으로 결론을 맺는다.

2. 침입탐지 시스템 개요

비정상행위 탐지 시스템은 그림 1과 같이 감사기록으로부터 탐지에 유용한 정보를 추출하고 이를 축약하여 정상행위 프로파일을 생성하는 부분과 저장된 정상행위 프로파일을 이용하여 사용자의 행위에 대한 비정상행위 여부를 판별하는 부분으로 구분된다. 비정상행위 탐지의 성능에 영향을 미치는 요인으로는 탐지에 사용할 유용한 척도의 선정 및 축약과 정상행위의 모델링 및 판별이 고려될 수 있는데, 본 논문에서는 최적의 척도선정 및 축약에 대해서 다룬다.

침입탐지를 위한 감사기록생성을 위해 본 논문에서는 SunOS의 BSM(Basic Security Module)을 이용한다[12]. BSM으로부터 생성된 많은 양의 감사기록에서 불필요한 자료를 제거하고 여과된 자료를 축약하여 모델링 모듈이 침입탐지에 사용할 수 있도록 한다. 이때 생성된 순서적인 정보중에서 중요정보가 제거되거나 잘못된 축약은 탐지율의 저하를 초래하게 되므로 탐지성능에 중요한 영향을 미칠 수 있다[8].

감사기록의 축약과정에서 지금까지 통계적 방법이 주로 사용되어왔으나[5], 수학적으로 모델링이 가능하지 않은 경우에는 사용될 수 없다. 본 논문에서는 자기조직화 신경망을 사용하여 저차원 정보로 축약·변환함으로써 여러 정상행위 모델링방법의 전처리단계로 사용될 수 있도록 한다.

정상행위 모델링을 위한 감사기록의 축약과정은 사용되는 척도들의 크기를 줄이고 다차원 정보를 저차원 정보로 변환하는 과정이다. 이를 위해서 주로 사용되는 척도들의 정보를 이용하여 정보의 크기를 축약하고 정규화 시킨 후 마지막단계에서 SOM의 입력으로 사용하여 고정된 크기를 갖는 대표값을 생성해낸다. 여기서 생성된 대표값들을 하나의 이벤트로 하는 시퀀스를 생성하면 정상행위 모델링에 유용하게 사용할 수 있다.

3. 척도의 결정

침입을 탐지하기 위해서 BSM에서 사용될 수 있는 데이터는 다양하다. 어떤 감사기록 정보가 침입탐지를 위해 유용한가에 대해서는 아직 확실한 답은 없다. 많은 양의 감사기록 정보가 침입탐지를 위해 사용될 경우 침입에 중요한 척도의 변화가 다른 중요하지 않은 척도의 변화에 의해 가려질 수 있기 때문에 오히려 역효과를 가져올 수도 있다. 미국 콜롬비아대학[1]과 퍼듀대학[7, 8]에서는 시스템 호출과 명령어만을 척도로 사용하고 있다.

효율적 척도의 추출은 침입탐지 시스템의 성능을 좌우하는데 기존의 시스템들에서 사용된 척도들을 살펴보면 CPU 사용시간, 파일접근(생성, 삭제, 수정), 시스템 호출, 네트웍 행동, 로그인/로그아웃 등으로 다양하다[10]. 척도의 선택은 탐지 목적에 따라 달라지는데 호스트 기반의 침입을 탐지하는 경우 BSM과 같이 시스템에서 제공하는 모듈로 탐지가능하며 네트웍 기반 침입탐지의 경우 tcpdump 등을 이용해 네트웍 패킷을 분석함으로써 네트웍 트래픽을 조사한다.

본 논문에서는 침입탐지시스템에서 사용할 최적의 척도들을 결정하기 위해 침입에서 주로 사용되는 값들인 시스템호출, 파일관련 및 프로세스 관련 정보들을 조합하여 침입탐지 성능에 어떤 영향을 미치는지를 조사하고 중요한 정보를 추출한다. 이를 위해 SOM을 이용하여 BSM에서 추출된 자료를 저차원 정보로 축약한 후, HMM을 이용한 모델링으로 침입탐지성능에 미치는 영향을 밝히고자한.

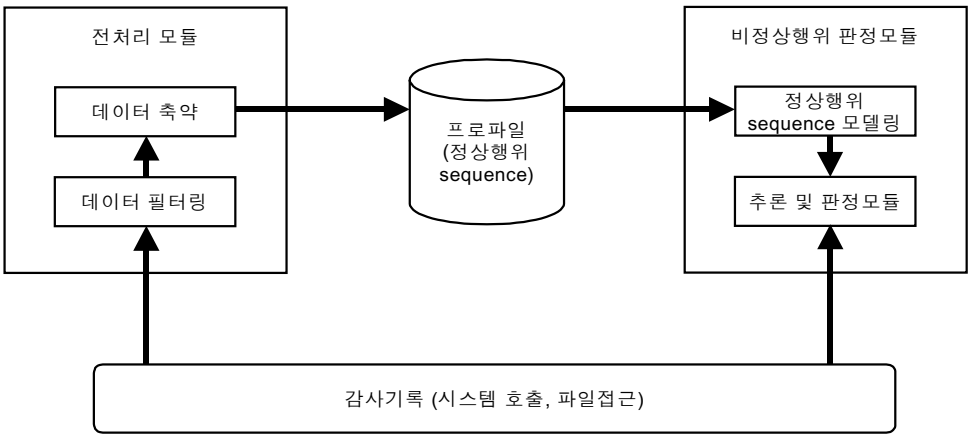

그림 1. 침입탐지 시스템의 구조

4. 감사자료의 축약

감사기록의 문제점은 감사범위에 따라 다르지만 그 양이 방대하다는 점이다. 모든 이벤트에 대해 감사를 할 경우 하루에도 수 백 Mbyte이상의 감사기록을 남기게 된다. 따라서 이러한 감사기록에서 필요한 데이터를 추출하고 축약할 필요가 있다.

방대한 양의 감사기록을 축약하기 위해 추출된 정보의 통계적 특성을 이용하는 경우가 많다. 본 논문에서는 감사기록에서 추출된 정보의 지역성(Locality)에 근거하여 각 정보의 크기를 축약한다. 크기가 축약된 정보들은 다차원 정보이기 때문에 정상행위 모델링은 통계적 기법이나 데이터 마이닝 기법이 사용될 수 있지만 다양한 모델링방법에 적용되기 위해서는 이를 저차원 정보로 축약할 필요가 있다.

BSM감사기록에서 추출될 수 있는 정보는 많지만 추출가능한 모든 정보를 그대로 사용하지 않고 필요한 정보만을 추출해야 한다. 여기서 필요한 정보의 개수는 실시간 탐지에 있어서 탐지시간과 관련되는 중요한 변수로 볼 수 있다. BSM감사기록에서 추출된 정보의 축약에는 데이터에 의한 자료축약과 추출된 다차원 정보를 작은 크기의 새로운 정보로 변환하는 축약방법이 있다. 데이터에 의한 자료축약은 $x_1, x_2, x_3, \dots, x_n \rightarrow x_1', x_2', x_3', \dots, x_k' \ (k < n)$ 과 같이 한 척도의 크기($0 \sim n$)를 k ($k < n$)로 줄이는 것이다. 척도들이 사용되는 값의 범위를 테이블로 저장하고 사용되는 값을 테이블 내에 저장되어 있는 값의 위치로 매핑시키면 간단하게 척도의 크기를 줄일 수 있다.

본 논문에서는 표 1과 같이 BSM감사기록에서 중요한 정보로 볼 수 있는 시스템호출 관련 정보, 파일 관련정보 그리고 프로세스 관련정보를 사용한다.

척도	정보
시스템호출 관련	시스템 호출 ID, Return value, Return status
프로세스 관련	프로세스 ID, IPC ID, IPC, permission, exit value, exit status
파일 액세스 관련	파일접근, 접근 경로, 파일 시스템 ID, 파일 액세스 모드

표 1. 사용된 척도들

4.1 SOM에 의한 축약

다차원 정보를 수학적으로 저차원정보로 축약하는 경우 비선형적 다차원정보를 선형적인 일차원 정보로 모델링하기 어렵다. 다차원 정보를 저차원 정보로 변환하기 위해 비교사 학습신경망인 자기조직화 신경망을 이용한다.

자기조직화 신경망은 통계학적인 클러스터링 알고리즘을 병렬처리 및 학습기능 지원가능한 신경망 형태로 구현한 것이라 할 수 있다. 그림 2와 같이 3×3으로 연결된 출력노드에 2개의 특징값으로 구성된 입력이 들어오면 이와 가장 유사한 대표값에 해당하는 노드가 출력값을 내는 방식으로 작동한다. 이를 감사기록 데이터에 적용하면 대량의 데이터를 그 대표값이 된 출력노드로 매핑할 수 있어 효과적으로 데이터를 축약할 수 있을 것이다.

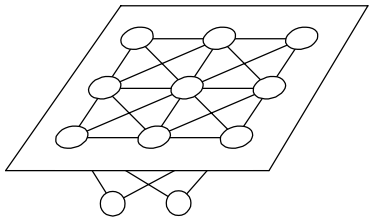

그림 2. 3×3 SOM

SOM의 일반적인 학습 알고리즘은 다음과 같다[6]. 수식에서 $i(x)$는 입력에 가장 잘 일치하는 값이며, Λ_i는 이웃함수, η 는 학습률을 의미한다.

1. 가중치 벡터들($w_j(0)$)의 초기화 (n=0).
2. 유사도 비교.

$$i(\mathbf{x}) = \arg\min_j \left\| \mathbf{x}(n) - \mathbf{w}_j \right\|$$

3. 가중치 벡터들의 갱신.

$$\mathbf{w}_j(n+1) = \mathbf{w}_j(n) + \eta(n)\Lambda_{i(\mathbf{x})}(n, j)\left(\mathbf{x}(n) - \mathbf{w}_j(n)\right)$$

4. 조건을 만족할 때까지 2 ~ 3반복.

BSM감사기록에서 정보들은 하나의 감사레코드로부터 추출되는데 이러한 정보들이 정규화되어 SOM의 입력으로 사용되고 이러한 다변량 정보에 대한 대표값이 출력된다. 즉 BSM감사기록중 하나의 레코드에 대하여 하나의 대표값이 생성된다. 이러한 정보들은 다양한 정상행위 모델링에 사용되어 질 수 있는데 HMM에 적용할 경우 이러한 대표값들로 구성된 시퀀스를 생성하여 HMM의 입력으로 사용할 수 있다.

4.2 HMM을 이용한 정상행위 모델링[11]

HMM은 실제적인 생성모델을 알 수 없고 단지 생성된 시퀀스에 의해서만 확률적으로 관측할 수 있는 이중으로 확률적인 절차로서, 고정된 값인 관찰 시퀀스의 길이, 상태수, 심볼수와 학습에 의해 조정되는 전이확률, 관측확률, 초기상태분포로 구성이 되며 사용자의 행위시퀀스를 모델링하기에 유용한 도구이다.

HMM은 상태라 불리는 N개의 노드와 노드간에 방향성을 갖는 전이를 나타내는 아크로 구성된 그래프 구조이다. 이 그래프의 각 노드에 공간적인 특성을 모델링하는 관측 심볼 확률분포와 초기상태 확률분포가 저장되어 있고, 각 아크에는 관측열의 시간적인 특성을 모델링하는 상태전이 확률분포가 저장되어 있다. HMM은 주어진 관측열(순서적 이벤트)에 대해 비록 외부에서 그 상태 전이과정을 직접적으로 관찰할 수는 없어도 마르코프 과정의 확률함수로 모델링할 수 있다. 그림 3은 4개의 노드가 우향으로 연결된 HMM의 구조를 보여준다.

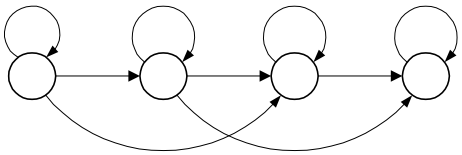

그림 3. HMM의 예

HMM은 다음과 같이 표현되며, 모델 λ는 간략히 (A, B, π) 로 표현될 수 있다.

- T : 관찰 시퀀스의 길이
- N : 모델의 상태수
- M : 관찰 심볼의 수
- $Q = q_1, q_2, \ldots, q_N$: 상태들
- $V = v_1, v_2, \ldots, v_M$: 가능한 관찰심볼의 이산적인 집합
- $A = \{a_{ij}\}, a_{ij} = \Pr(q_j \text{ at } t+1 | q_i \text{ at } t)$: 상태전이 확률분포
- $B = \{b_j(k)\}, b_j(k) = \Pr(v_k \text{ at } t | q_j \text{ at } t)$: 관측 심볼 확률분포
- $\pi = \{\pi_i\}, \pi_i = \Pr(q_i \text{ at } t=1)$: 초기 상태 분포

4.2.1 정상행위 모델링

정상행위 모델링은 전처리 단계에서 생성된 정상행위 시퀀스를 기반으로 HMM의 매개변수를 결정하는 과정이다. HMM의 매개변수 결정은 주어진 시퀀스 O가 해당 모델 λ로부터 나왔을 확률인 $\Pr(O|\lambda)$ 값이 최대가 되도록 $\lambda = (A, B, \pi)$ 를 조정한다. 이를 계산하는 해석적인 방법은 알려져있지 않고 반복적으로 λ를 결정하는 방법으로 Baum-Welch의 재추정식이 있다[9].

4.2.2 비정상행위 판정

비정상행위 판정에서는 이미 구축되어 있는 정상행위별 HMM에 사용자행위시퀀스를 입력으로 넣어 각 정상행위에서 현재 행위가 생성되었을 확률을 구한다. 확률을 구하는 방법으로는 forward- backward procedure나 Viterbi 알고리즘을 사용할 수 있다[9]. 각 모델별로 구해진 확률은 판정모듈에 전달되어 비정상행위인지 판정한다.

5. 실험결과 및 고찰

5.1 실험환경

본 논문에서는 침입탐지를 위해 사용될 척도의 선택을 위해 하루동안 3명 사용자의 프로그램 작업, 문서편집 및 네트워킹 작업에 대한 감사기록으로부터 몇 가지 척도들을 추출하고 자기조직화 신경망에 의해 저차원 정보로 변환한 다음 탐지성능에 미치는 영향을 조사한다. 실험에서 사용된 척도들은 시스템 호출관련(시스템 호출 ID, 시스템 호출 반환 값, 시스템 호출 반환상태), 프로세스 관련(프로세스 ID, IPC ID, IPC permission, exit value, exit status), 파일 액세스 관련 (중요파일 접근 여부, 중요패스 접근여부, 파일 액세스 모드, 인자길이) 등이며 이를 조합한 7가지에 대해 SOM을 통해 축약된 정보를 이용하여 HMM으로 모델링하고 난 후 17회 u2r시도에 대한 탐지성능을 평가하였다.

SOM의 맵 크기 변화에 따라 탐지 성능이 달라질 수 있기 때문에 맵 크기 실험결과[10]를 이용하여 맵의 크기를 5×5, 6×6, 7×7로 하여 실험하였다. HMM에 의한 정상행위 모델링을 위해서는 상태수를 10으로 하고 심볼수는 SOM의 맵 크기와 일치하도록 25, 36, 49로 하였다. 또한 하나의 시퀀스 길이는 30으로 하였으며 시퀀스의 생성을 위해 이전에 생성된 시퀀스를 완전 중복시키는 방법을 사용하였다[11].

5.2 실험결과

그림4에서 그림6은 SOM의 맵 크기에 따라서 BSM에서 추출된 척도들이 탐지 성능에 미치는 영향을 보여주고 있다. 맵의 크기가 비교적 작은 5×5의 경우 시스템 호출과 관련된 척도, 프로세스와 파일 액세스 관련 척도의 조합 및 모든 척도의 조합이 다른 맵 크기에 비해 더 나은 성능을 보여주고 있다. 파일 액세스의 경우에는 맵의 크기가 6×6일 때 가장 좋은 성능을 보인다. 실험결과에서 탐지에 영향을 주지 못했던 프로세스와 관련된 척도는 편의상 그래프로 나타내지 않았다.

이러한 결과는 척도들이 사용되는 행위가 지역적이라는 처음 가정과 일치하며 척도마다 다름을 의미한다. 정상행위 모델링을 이용한 비정상행위 탐지의 경우, 정상행위를 학습할 때 모델링되지 않은 정상행위도 비정상행위로 간주하기 때문에 정상행위를 비정상행위로 판별하는

False-positive 오류가 커지게 된다. 이러한 것은 가능한 모든 정상행위를 수집하는 것이 어렵기 때문에 발생하는 오류라고 할 수 있다. 따라서 비정상행위 탐지에서 탐지 성능을 관찰하기 위해서는 False-positive오류도 중요한 요인으로 고려하면서 탐지율을 살펴 보아야한다.

False-positive 오류가 클 경우 시스템의 사용자는 정상행위를 함에도 불구하고 빈번히 비정상행위로 간주됨으로써 시스템의 정지현상이 발생할 수 있다. 따라서 정상행위를 이용한 비정상행위 탐지의 경우 False-positive 오류를 낮은 값으로 유지하면서 탐지율을 향상시키는 방법을 주로 사용한다[7,8]. 이를 위해 False-positive 오류의 변화에 따른 탐지성능을 그래프로 나타내었다.

5.2.1 맵의 크기가 5×5일 때

그림 4는 SOM의 맵 크기가 비교적 작은 5×5에서 각 척도에 의한 탐지성능을 보여주고 있다. 시스템 호출관련 척도의 경우 False-positive 오류가 3.2일 때 100%의 탐지 성능을 보이고 있어 이러한 맵 크기에서 시스템 호출이 침입탐지에 유용한 척도임을 알 수 있다. 반면 파일 액세스 관련 척도의 경우 16.76%의 False-positive 오류에서 100%의 성능을 나타내고 있어 거의 사용될 수 없음을 알 수 있다. 프로세스와 파일 시스템 관련 척도들의 조합은 비교적 높은 7.64%의 False-positive 오류에서 100%의 탐지 성능을 냄을 알 수 있다. 또한 사용 가능한 척도를 모두 조합한 경우에 5.91%의 False-positive 오류에서 100%의 탐지 성능을 보여주고 있다.

여기 그래프에서 생략된 프로세스 관련된 척도에 의한 탐지결과는 0%로 나타났으며 시스템 호출과 프로세스 관련된 척도들의 조합 역시 0%의 탐지 성능을 나타냈다. 또한 시스템 호출과 파일 액세스 관련 척도들의 조합도 0%의 탐지 성능을 보여주었다.

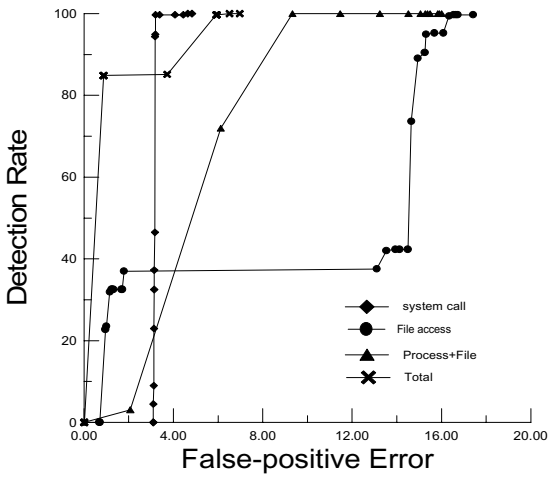

그림 4. SOM의 맵 크기가 6×6일 때 척도들의 탐지성능

5.2.2 맵의 크기가 6×6일 때

그림 5를 보면 시스템 호출 관련 척도의 맵의 크기가 5×5인 경우에 비해 낮은 탐지결과인 4.73%의 False-positive 오류에 대해 100%의 탐지 성능을 보여주고 있으며, 파일 액세스의 경우 2.99% False-positive 오류에서 100%의 탐지 성능을 나타내고 있어 침입탐지에 유용하게 사용될 수 있음을 보여준다. 시스템 관련 척도와 파일 액세스 관련 척도들의 조합 결과는 5.58%의 False-positive 오류에서 100%의 탐지 성능을 보여주고 있으며, 전체를 조합한 경우 25.88%의 False-positive 오류를 보이고 있어 침입탐지에 거의 사용될 수 없다.

5.2.3 맵의 크기가 7×7일 때

그림 6에서 볼 수 있듯이 이러한 맵 크기에서 뚜렷한 탐지성능의 향상을 볼 수 없으며 오히려 탐지 성능이 저하됨을 알 수 있다. 실험을 통해 맵 크기의 증가가 척도들의 특성을 잘 반영하는 대표값을 생성하지 않음을 알 수 있다.

5.3 고 찰

본 논문에서 침입을 탐지하는 척도들의 중요도를 조사하기 위해 HMM을 이용하여 정상행위를 모델링하고 이를 이용해 정상행위 시퀀스에서 얼마나 벗어나는지를 평가하였다. 실험결과 시스템 호출관련 척도 및 파일 관련 척도들은 SOM의 맵 크기를 조정하면 침입탐지에 효율적으로 사용될 수 있음을 보았다.

그러나 이러한 축약된 척도정보가 모든 정상행위 모델링 방법에 의해 유용하게 사용될 수 있다고는 할 수 없다. 사용되는 모델링 방법에 관계없이 침입탐지에서 사용되는 척도가 중요함을 입증하기 위해서는 여러 모델링 방법에 의한 검토가 이루어져야 할 것이다.

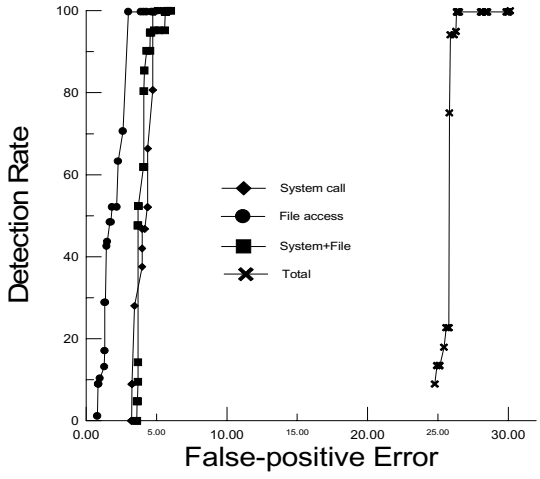

그림 5. SOM의 맵 크기가 6×6일 때 척도들의 탐지성능

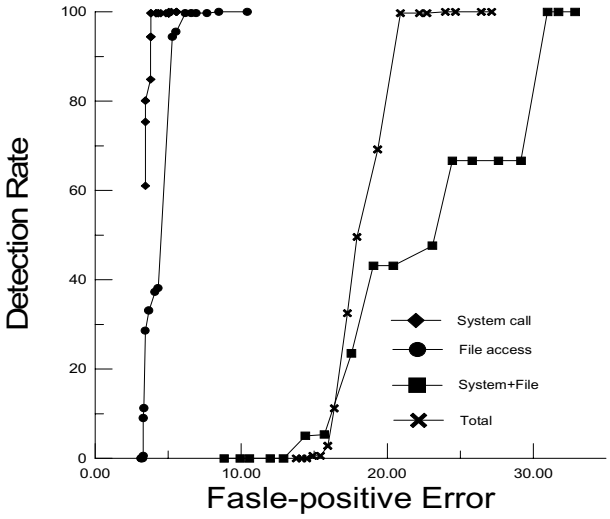

그림 6. SOM의 맵 크기가 7×7일 때 척도들의 탐지성능

6. 결 론

본 논문에서는 침입탐지 시스템에서 감사기록을 처리하기 위하여 감사기록에서 추출한 정보의 크기를 축약하고 다차원의 정보를 저차원의 정보로 변환함으로써 다양한 정상행위 모델링방법에 적용될 수 있도록 하는 전처리과정을 다루고 있다. 전처리과정에서 중요한 것은 침입탐지를 위한 척도의 선정과 이들의 손실없는 축약이다. 이 중에서 탐지를 위한 척도선정은 침입탐지성능을 좌우하는 중요한 요인으로 축약된 척도들이 실제 탐지성능에 미치는 영향을 조사함으로써 각 척도의 중요도를 살펴보았다.

실험결과 시스템 호출 및 파일액세스 관련 척도들이 False-positive 오류를 줄이면서 탐지성능을 높임을 알 수 있었다. 또한 각 척도들의 탐지 성능이 좋은 맵 크기가 다름을 알 수 있었는데 시스템 호출 관련 척도나 척도들의 조합의 경우 맵의 크기가 비교적 작은 5×5에서 높은 탐지성능을 나타냄을 알 수 있었고 파일관련 척도의 경우는 6×6에서 좋은 탐지성능을 나타냄을 알 수 있었다. 이는 크기가 축약되고 SOM에 의해 저차원 정보로 축약·변환된 대표값이 큰 정보손실 없이 침입 탐지에 사용될 수 있음을 의미한다.

참고문헌

[1] Debar, H., Becker, M. and Siboni, D., "A neural network component for an intrusion detection system," *Proc. of IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 240~250, 1992.

[2] Ghosh, A.K., Schwartzbard, A. and Schatz, M., "Learning program behavior profiles for intrusion detection," *Proc. of WIDNM'99*, 1999.

[3] Frank, J., "Artificial intelligence and intrusion detection: current and future directions," *Proc. 17th National Computer Security Conference*, 1994.

[4] Jackson, K., DuBois, D. and Stallings, C., "An expert system application for network intrusion detection," *Proc. 14th National Computer Security Conference*, pp. 215~225, 1991.

[5] Javitz, H.S. and Valdes, A., "The SRI IDES statistical anomaly detector," *Proc. of IEEE Symposium on Research in Security and Privacy*, 1991.

[6] Kohonen, T., *Self-Organizing Maps*, Springer press, 1995.

[7] Lane, T. and Brodley, C.E., "Temporal sequence learning and data reduction for anomaly detection," *Proc. of ACCS'98*, pp. 150~158, 1998.

[8] Lane, T. and Brodley, C.E., "An application of machine learning to anomaly detection," *Proc. of NISSC'97*, pp. 366~380, 1997.

[9] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, no. 2, pp. 257~286, Febebuary 1989.

[10] 서 연규, 조 성배, "자기조직화 신경망을 이용한 침입탐지 시스템의 BSM감사기록 축약," 한국정보처리학회 추계 학술발표대회, 1999.

[11] 최 종호, 조 성배, "은닉 마르코프 모델을 이용한 침입탐지 시스템의 모델링 성능분석," 한국정보처리학회 추계학술발표대회, 1999.

[12] 한국 정보보호센터, *호스트 기반 실시간 침입탐지 시스템 개발을 위한 SunSHIELD Basic Security Module의 분석*, 1998.