퍼지 추론을 이용한 은닉 마르코프 모델 기반 침입탐지 시스템의 성능향상*

정유석, 박혁장, 조성배
연세대학교 컴퓨터과학과
{j8508, twinkler, sbcho}@candy.yonsei.ac.kr

Improving Intrusion Detection System based on Hidden Markov Model with Fuzzy Inference

Yoo-Suk Jung, Hyuk-Jang Pak, and Sung-Bae Cho
Computer Science Department, Yonsei University

요 약

정보통신의 질적 양적 팽창과 더불어 컴퓨터 시스템에 대한 침입 또한 증가하고 있다. 침입탐지시스템은 이를 해결하기 위한 대표적인 수단으로, 최근 관련된 연구의 방향이 오용탐지 기법에서 비정상행위탐지 기법으로 옮겨가고 있는 상황이다. HMM(hidden Markov model)은 비정상행위탐지 기법에 사용되어 다양한 척도(measure)에 대한 정상행위를 효과적으로 모델링할 수 있는 방법이나, 다양한 척도의 결과값들로부터 침입을 판정하는 방법에 대한 연구는 미흡하다. 본 논문에서는 SOM(self organizing map)을 통해 축약된 데이터를 HMM으로 모델링한 비정상행위기반 침입탐지 시스템의 성능을 향상시키기 위해 퍼지 침입판정 방법을 제시한다. 실험결과 척도에 따른 결과들의 기계적 결합보다 향상된 결과를 얻었으며, 퍼지 관련 파라메터의 개선을 통해 더욱 좋은 효과를 기대할 수 있었다.

1. 서론

최근 정보통신에 대한 관심과 필요성의 증가는 정보통신의 발전에 따르는 긍정적 영향의 증가와 함께, 이와 관련된 문제가 발생했을 시의 부정적인 영향 역시 증가한다는 것을 의미하며, 정보통신 발전의 기본 도구인 컴퓨터 시스템이 사회의 부정적인 요소들로부터 공격 대상이 될 가능성이 커지고 있다는 것을 내포한다.

한국정보보호센터에 따르면 국내의 컴퓨터 시스템에 대한 공격은 인터넷이 보급되기 시작한 98년 이래로 폭발적으로 증가하고 있으며, 한국의 경우 연 평균 300%이상의 증가율을 보인다고 한다. 공격을 위한 도구 또한 예전에는 단순히 시스템의 버그를 이용하는 것들이 주류를 이루었으나, 최근에는 은닉화(stealth), 분산화(distributed), 그리고 자동화(automation)의 특징을 갖는 공격 방법들이 늘어나고 있다[7].

침입탐지 시스템은 컴퓨터 시스템에 대한 공격에 대응하기 위한 대표적인 도구로, 여기에서 사용되는 침입탐지 기법은 알려진 공격에 대한 정보를 구축하고 이를 통해 침입을 판정하는 오용탐지 방법과 사용자나 시스템 혹은 프로그램의 정상 정보를 구축하고 이를 통해 침입을 판정하는 비정상행위탐지방법으로 나뉜다. 기존의 공격방법은 이미 잘 알려져 있어서 오용탐지 방법에 의해 적절히 방어할 수 있었으나 보안기술의 발전과 더불어 이를 극복하기 위한 공격 기술이 발전하고, 새로운 공격모델이 등장하면서 최근 연구의 방향이 비정상행위탐지 방법으로 옮겨가는 상황이다.

HMM을 이용한 정상행위 모델링은 다량의 척도에 적용할 수 있는 방법으로, 시스템 호출관련 척도나 파일 입출력 관련 척도에 따라 정상행위를 모델링할 경우 좋은 결과를 얻은 연구가 있다. 그런데 이 연구에서는 다양한 척도들의 결과값에 대해 기계적인 방법으로 결합하여 침입을 판정했기 때문에, 일반적으로 알려져 있는 척도와 침입행위간의 관계에 대한 고려가 미흡하다[6].

퍼지 추론은 정량화 하기 힘든 전문가의 지식을 반영하는데 효과적인 방법으로 알려져 있다. 침입탐지를 위한 다양한 척도들의 결과값에 퍼지를 적용하여 관련된 정보를 반영한다면 더욱 정확하게 침입을 판정하리라 여겨진다[2].

본 논문에서는 SOM(self organizing map)을 통해 판정을 위한 데이터를 축약하며 퍼지 추론을 이용해 침입판정을 하는 HMM(hidden markov model) 기반의 비정상행위탐지 모델을 제안하고, 실험을 통해 제안한 모델의 가능성을 보이고자 한다.

2. 관련연구

침입탐지시스템은 크게 데이터의 소스를 기반으로 하는 분류방법과 침입 모델을 기반으로 하는 분류 방법으로 나눌 수 있으며, 침입 모델을 기반으로 하는 분류방법으로는 공격 행위들에 대한 공격 특징 정보를 통해 침입을 탐지하는 오용 탐지방법과 정상적인 시스템 사용에 관한 프로파일과 시스템 상태를 유지하고 있는 동안 프로파일에서 벗어하는 행위들을 탐지하는 비정상적인 행위탐지 방법이 있다.

오용탐지 방법은 탐지 방법에 따라 다음과 같이 분류될 수 있다. 패턴 매칭 방법은 알려진 침입 유형들을 감사 자료의 패턴으로 저장하여 비교하고, 전문가 시스템 방법은 "if-then" 규칙을 통하여 공격 패턴들에 대한 지식을 표현하며, 상태 전이방법은 공격 패턴을 특정 시스템의 상태 전이 순서로 표현한다. 그리고 조건부 확률 방법은 침입 감지를 위해 특정 조건하에서

* 본 논문은 (주)정보보호기술의 지원에 의한 것임.

의 침입 확률을 정의한다[4].

비정상행위 탐지를 위해 사용되는 방법들은 다음과 같다. 통계적 방법은 가장 많이 사용되는 기법으로 시간에 따라 샘플링된 여러 변수를 사용하여 침입을 탐지한다. 전문가 시스템 방법은 사용자의 행동을 통계적으로 기술하는 규칙의 집합을 구축하여 탐지한다[3]. 또한 신경망을 통해 사용자나 데몬 등의 행위를 학습하거나[1], 음성인식 등에서 사용되던 HMM을 통해 정상행위를 모델링하는 방법도 있다[5,6].

비정상행위 탐지를 위한 정상행위 수집 방법으로는 사용자의 행위를 기반으로 하거나 프로그램의 행위를 기반으로 모델링하는 방법이 일반적으로 사용되고 있다.

3. HMM기반 침입탐지 시스템

HMM은 침입행위 탐지를 위한 효과적인 비정상행위 탐지 기법의 모델로 가능성을 인정받고 있다. 그런데 현재까지 이에 대한 연구는 어떤 척도(measure)에 따라 정상 행위를 정의하고 어떻게 모델링하는가에 초점이 맞추어져 있으며, 해당 모델들로부터 나온 결과물들을 어떻게 이용하여 침입판정을 할 것인가에 대한 연구는 미비한 상황이다.

침입탐지를 위한 척도는 탐지 목적에 따라 다양하게 선택할 수 있으며, 그 중 시스템 호출, 파일 입출력, 프로세스 관련 정보는 대표적인 척도가 될 수 있는데 이와 같은 다양한 척도의 결과들로부터 침입을 판정하는 것은 단순한 일이 아니다.

3.1 기본 구조

제안하는 침입탐지 시스템은 그림 1과 같이 전처리 과정에서 정상행위 모델인 프로파일을 생성하고 이를 이용해 침입판정 과정에서 실시간 침입탐지를 한다. 전처리 과정은 모델링을 위한 정상행위 감사자료를 필터링하고 축약한 후 정상행위 모델을 생성하며, 침입판정 과정은 프로세스들의 행위궤적을 필터링하고 축약하여 전처리 과정에서 생성한 정상행위 모델과의 비교를 통해 진행된다.

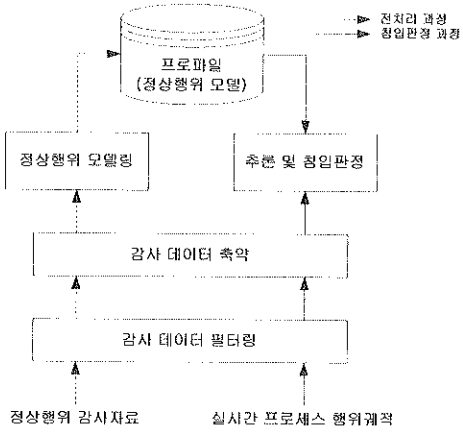

그림 1. 침입탐지시스템의 작동과정

3.2 작동 원리

전처리 과정에서는 통계적 방법과 척도에 따른 감사자료를 축약하는 SOM을 사용해 정상 데이터를 축약하고 이를 이용해 HMM을 모델링한다. 침입판정 과정에서는 프로세스의 실시간 행위궤적을 척도에 따라 축약한 후 전처리 과정에서 모델링한 HMM을 통해 평가 값을 얻고 침입 판정을 한다.

(1) 감사 데이터 축약

실시간 침입탐지를 위해 사용되는 감사자료는 다차원 정보이므로 HMM에 바로 적용시키기 위해 저차원 정보로 변환할 필요가 있다. SOM은 다차원 입력벡터를 유사도 측정을 통해 자기조직화 하고 입력 값에 가장 가까운 대표 값으로 출력해 준다.

(2) 정상행위 모델링

정상행위 모델링은 전처리 과정에서 축약된 감사자료를 이용해 HMM의 파라메터를 결정하는 과정이다. HMM의 파라메터는 축약된 감사자료 시퀀스가 해당 HMM에서 나올 확률 값이 최대가 되도록 조절되는데, 반복적으로 모델을 결정하는 Baum-Welch의 재추정식을 사용한다.

정상행위는 각 척도에 따라 복수 개로 모델링된다. 기존에 알려져 있는 침입판정을 위한 대표적인 척도는 시스템 호출, 파일 입출력, 프로세스 관련 정보 등이며, 이들 중 실험적으로 타당성이 검증된 시스템 호출과 파일 입출력 관련 정보를 통해 정상행위를 모델링한다[6].

4. 퍼지 추론 및 침입판정

추론 및 침입판정 모듈은 정상행위 모델을 통한 프로세스 행위궤적의 평가 값을 얻고 이를 통해 침입판정을 한다. 평가 값을 얻기 위해서는 "forward-backward procedure"나 "Viterbi" 알고리즘 등을 사용하며, 각 척도에 따른 평가 값을 이용해 퍼지 추론을 한다.

퍼지 추론 시스템을 위한 입력 변수는 HMM으로 생성한 각 정상행위 모델들인 시스템 호출(M1), 파일 입출력(M2), 시스템 호출+파일 입출력(M3) 기반 모델들의 평가 값이 되며, 출력 변수는 침입일 가능성 S로 정의한다. HMM의 평가 값은 0에 가까울 수록 정상행위에 가깝다는 것을 의미하며 그 값이 낮을수록 정상행위와 다르다는 것을 의미하므로 입력 변수의 퍼지 집합은 평가 값이 0에 가까운 경우를 나타내는 높음(H)과 정상행위와 구분될 수 있는 영역을 의미하는 낮음(L)과 실제로 가장 낮게 나올 수 있는 HMM 평가 값 α 에 가까운 경우를 나타내는 매우낮음(VL) 그리고 정상인지 침입인지 구분하기 어려운 상태를 나타내는 보통(M)으로 정의한다. 입출력 변수와 변수 범위 및 퍼지집합의 관계는 표 1과 같다.

표 1. 침입탐지를 위한 퍼지집합

구분	변수	변수범위	퍼지집합
입력	M1:시스템호출의 HMM평가값 M2:파일 입출력의 HMM평가값 M3:시스템호출+파일 입출력의 HMM평가값	[0, α]	VL:매우낮음 L :낮음 M :보통 H :높음
출력	S:침입일 가능성	[0, 100]	N :정상 W :경고 A :공격

퍼지추론방식은 실시간 침입탐지를 위한 빠른 계산이 필요하기 때문에 Correlation Minimum 방식을 사용하고, 동일한 이유로 인해 역퍼지화 방법은 간략화된 무게중심 역퍼지화 방법을, 추론을 위한 소속 함수는 삼각형을 사용한다.

정의된 입력 변수와 퍼지집합에 따르면 총 64가지의 퍼지 규칙이 생성될 수 있으나, 시스템에 대한 침입행위와 척도간의 일반적인 관계를 적용할 경우 실제 필요로 하는 규칙은 훨씬 줄어들게 된다. 다음은 침입행위와 정상모델을 위한 척도간의

일반적인 관계로부터 퍼지 규칙을 선별하기 위해 도출한 선규칙(meta rule)이다.

선규칙 1. 특정 척도에서만 탐지될 수 있는 침입행위가 있다.
선규칙 2. 규칙 1의 경우를 제외하면, 다수 척도에 의해 인정되는 결과를 더 신뢰할 수 있다.
선규칙 3. 규칙 1, 2의 경우를 제외하면 각 척도의 결과는 시스템 호출 관련, 파일 입출력 관련, 시스템 호출+파일 입출력 관련의 순서로 우선 순위를 갖는다.

위와 같은 선규칙을 적용하면 표 2.와 같은 퍼지 규칙을 정의할 수 있다. 퍼지 규칙 1-x는 규칙 1과 관련된 규칙이고, 퍼지 규칙 2-x는 규칙 2와 관련된 규칙이며 퍼지 규칙 3-x는 규칙 3과 관련된 규칙이다.

표 2. 퍼지 규칙

규칙No.	내용
1-1	if (M1=VL) then S=A
1-2	if (M2=VL) then S=A
1-3	if (M3=VL) then S=A
2-1	if (M1=H) & (M2=H) then S=N
2-2	if (M2=H) & (M3=H) then S=N
2-3	if (M1=H) & (M3=H) then S=N
2-4	if (M1=L) & (M2=L) then S=A
2-5	if (M2=L) & (M3=L) then S=A
2-6	if (M1=L) & (M3=L) then S=A
2-7	if (M1=M) & (M2=M) then S=W
2-8	if (M2=M) & (M3=M) then S=W
2-9	if (M1=M) & (M3=M) then S=W
3-1	if (M1=H) & (M2=L) & (M3=M) then S=N
3-2	if (M1=H) & (M2=M) & (M3=L) then S=N
3-3	if (M1=M) & (M2=H) & (M3=L) then S=N
3-4	if (M1=M) & (M2=L) & (M3=H) then S=A
3-5	if (M1=L) & (M2=H) & (M3=M) then S=A
3-6	if (M1=L) & (M2=M) & (M3=H) then S=A

5. 실험 결과

실험을 위한 HMM의 상태 수는 10이고, 탐지를 위한 패턴의 길이는 30이며 HMM에 입력되는 이벤트의 종류는 50가지였다. 실험을 위한 정상 데이터는 주로 문서편집, 컴파일 그리고 사용자에 의해 작성된 프로그램의 사용으로 생성되었으며, 침입 데이터는 17회의 u2r 침입으로 생성했다.

실험의 결과, 표 3.에서 나타난 것처럼 퍼지 추론을 통한 다중모델 결합의 경우, 탐지율 100%에서의 긍정적오류율은 단일 척도 시의 시스템 호출이나 다중 척도 시의 다수결 결합 방법 그리고 OR투표 결합 방법의 경우보다 낮게 측정되었다. 또한 전반적인 침입탐지율과 긍정적오류율간의 상관관계를 나타내는 ROC 곡선은 그림 2.에서 보이는 것처럼 퍼지 추론의 경우가 이벤트 ID의 경우보다 좋은 결과를 나타냈다.

표 3. 다중모델 결합의 성능비교

	시스템호출	다수결	OR	퍼지
긍정적오류	13.66	29.47	98.59	12.12

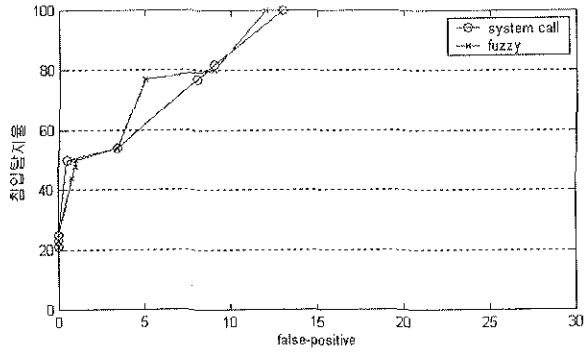

그림 2. 퍼지 추론을 통한 다중모델 결합의 성능비교

6. 결론 및 향후과제

본 연구에서는 SOM을 통해 판정을 위한 데이터를 축약하는 HMM기반의 침입탐지 시스템에서, 다양한 척도의 정상행위로부터 생성된 감사 자료의 결과값을 퍼지 추론하는 침입 탐지 방법을 제안했고, 실험을 통해 제안한 방법이 단일 척도의 경우나 기계적인 계산에 의한 다중 척도의 경우에 비해 좋은 효과가 나타남을 보였다.

실험에 사용된 소속 함수의 변수나 퍼지추론방식 혹은 역퍼지화 방법은 개선의 여지가 있으며 적절한 방법이 선택 될 경우 침입탐지 효과는 더욱 커질 수 있다. 또한 퍼지 규칙을 생성하기 위한 지식인 선규칙을 개선하는 것도 성능 향상을 위한 방법이라 여겨진다.

참고문헌

[1] A. K. Ghosh, A. Schwartzbard and M. Schatz, "Learning program behavior profiles for intrusion detection," *Proc. Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, USA, April 1999.

[2] J. S. R. Jang, C. T. Sun, E. Mizutani, *Neuro-Fuzzy and Soft Computing*, pp. 11-90, 1997

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

[4] S. Kumar and E. H. Spafford, "An application of pattern matching in intrusion detection," *Technical Report CSD-TR-94-013*, 1994.

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

[6] 최종호, 조성배, "순서적 이벤트에 기반한 침입탐지시스템의 성능향상을 위한 다중 HMM의 모델 결합", *2000 한국 정보과학회 춘계학술발표회*, vol 2. pp. 238-240, 2000년 4월.

[7] "99 국내외 해킹현황 분석," *한국정보보호센터*, http://www.certcc.or.kr/statistics/hack/1999/99-hack.htm