# 침입 탐지를 위한 컴퓨터 시스템 상태 기술

## Description of Computer System State for Intrusion Detection

곽미라*, 조동섭**
Mira Kwak*, Dong-Sub Cho**

**Abstract** - We designed an intelligent intrusion detection scheme that works based on target system's operational states and doesn't depend on humans' analysis. As a prior work, we presents a scheme to describe computer system's operational states. For this, Hidden Markov Model is used. As input to modeling, huge amount of system audit trail including data on events occurred in target system connected to network and target system's resource usage monitoring data is used. We can predict system's future state based on current events' sequence using developed model and determine whether it would be in danger or not.

**Key Words** : 침입 탐지(intrusion detection), 은닉 마르코프 모델(Hidden Markov Model), 컴퓨터 시스템 상태

### 1. 서 론

인터넷을 기반으로 하는 지식정보화시대가 본격적으로 열리면서, 업무를 비롯한 일상의 많은 일들이 인터넷과 그것에 연결된 컴퓨터 시스템 상에서 이루어지고 있다. 이에 따라 네트워크에 연결된 컴퓨터 시스템에 대해 행해지는 침입에 효과적으로 대응하는 것이 중요한 문제가 되어 여러 침입 대응 기법이 연구되고 있다.

특히 적절한 순간에 침입의 발생을 탐지하는 것은 침입에 대응하는 절차에서 가장 먼저 이루어져야 하는 일이다. *침입 탐지 기법*들은 전통적으로, 침입유형에 관한 지식을 바탕으로 침입을 찾아내는 *오용 탐지 기법*과 정상행위에 관한 지식을 바탕으로 의심스러운 사건을 찾아내는 *비정상 탐지 기법*으로 나뉜다. 오용 탐지 기법은 이미 알고 있는 침입은 비교적 정확히 탐지하나 알려지지 않은 침입에 무력한 약점을 가진다. 비정상 탐지 기법은 아직 지식베이스에 추가되지 않은 침입도 탐지할 수 있지만, 침입이 아닌 경우임에도 침입으로 간주할 확률이 높아 상용 시스템에 널리 쓰이지 못하고 있다.

우리는 이상적인 침입 탐지 기법을 설계하기 위해, 오용 탐지 기법과 비정상 탐지 기법의 장점을 취하고 약점을 제거하고자 하였다. 오용 탐지 기법과 비정상 탐지 기법은 모두 사람의 이해에 의존하고 있다. 즉, 두 기법의 차이는 컴퓨터 시스템이 처하는 새로운 상황이 침입 발생 상황인지를 판단하는 기준이 침입의 지식인지 침입이 없는 상태의 지식인지의 차이로 요약되며, 두 기법 모두 사람이 침입을 어떻게 이해하고 지식으로 표현하는지에 의존하고 있는 것이다. 사람의 이해를 바탕으로 한 침입 관련 지식 – 침입에 관한 지식이나 침입이 일어나지 않은 상태에 관한 지식 모두 – 은 미루어 짐작함에서 비롯된 오류를 포함하거나 의미 있는 특징을 간과할 수 있고, 수동적으로 갱신되어야 하는 한계를 가진다. 침입 발생 여부를 판단하는 바탕 지식의 구축에서 사람의 개입을 배제하면, 침입이 발생한 상황의 비정상성을 본질적으로 설명할 수 있다.[1] 이에 우리는, 침입 탐지를 위한 바탕 지식으로써, 사람의 이해가 아닌, 시스템의 상태 정보를 사용하고자 하였다.

본 논문에서 우리는 침입의 발생 가능성을 판단할 수 있는 근거로 사용되기 위해 시스템의 상태를 파악하고 표현하는 방법을 설명하고자 한다.

### 2. 컴퓨터 시스템의 상태

#### 2.1. 상태 파악을 위한 수집 정보

일반적으로 *상태*란 사물이나 현상이 처해 있는 현재의 모양 또는 형편을 일컫는다. 이 연구에서 상태는 대상 컴퓨터 시스템에서 일어나고 있는 모든 사건과 자원 소비의 모양을 뜻한다. 우리는 컴퓨터 시스템의 상태를 파악하는 데 있어, 컴퓨터 시스템 내부 뿐 아니라 네트워크 연결을 모두 관찰의 대상으로 한다. 관찰은 계측 가능한 요소들의 값을 측정함으로써 이루어지는데, 그 내용은 다음과 같다.:

- 내부 자원 소비 정보
  - 프로세스 생성량
  - 문맥교환 발생량
  - 중앙처리장치 사용량

저자 소개
* 곽미라: 梨花女子大學敎 컴퓨터學科 博士課程
** 조동섭: 梨花女子大學敎 컴퓨터學科 敎授 · 工學博士

1) 이 논문에서 침입은 일반적으로 받아들여지는 협의의 의미, 즉 특정 대상에게 피해를 입히려는 의도적 행위의 결과를 포함하여, 대상 컴퓨터 시스템과 그것이 제공하는 서비스에 영향을 미치는 위협을 아우르는 의미로 사용된다.

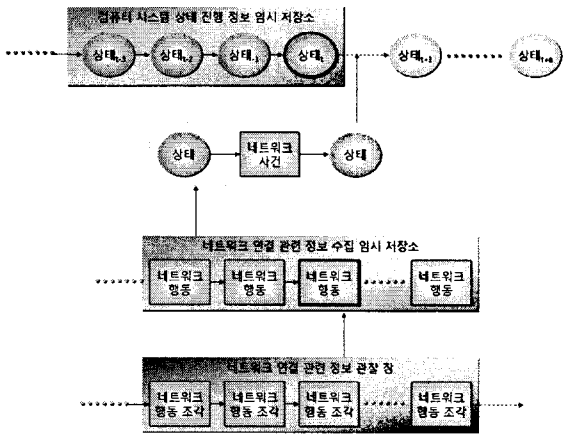


그림 1. 컴퓨터 시스템 상태와 사건

- 인터럽트 발생량
- 메모리 사용 정보: 페이지스왑량, 페이징량, 메모리해제량, 버퍼메모리량, 캐싱메모리양
- 디스크 입출력 정보: 읽기/쓰기 발생량
- 네트워크 인터페이스 정보: 수신/발신 패킷 개수와 크기, 손실 패킷 개수와 크기, 오류량, 사용 소켓 개수
- 커널 테이블 정보: 미사용 캐시 엔트리 개수, 파일 핸들러 개수, inode 핸들러 개수, 수퍼 블록 핸들러 개수
- 실행 큐: 실행 큐 길이, 프로세스 리스트 내 프로세스 개수

• 네트워크 연결 관련 정보
- 연결된 시스템 개수
- 열린 포트 개수
- 연결 시스템에 사용된 포트 개수
- 패킷 개수
- 수신 패킷 비율
- 패킷발신 후 패킷수신 비율
- 수신 패킷 평균 크기
- 패킷 수신 성공 비율
- 수신패킷 출발시간 간격
- 패킷 연속 발신 비율
- 패킷수신 후 패킷발신 비율

### 2.2. 상태 변화를 야기하는 사건

이와 같은 수집 내용은 대상 시스템의 상태를 수치적으로 나타낸다. 이러한 수치들에 대해 전문가들의 경험을 바탕으로 적절한 계산을 수행하여 관측 시점에서 위협 요소를 발견할 수 있다. 그러나 이러한 단편적 관찰은 연속적으로 변화하는 값이 내포하는 값의 변화 추이를 무시한다. 우리는 관찰되는 값과 그 변화 추이를 동시에 고려하여 시스템의 상태를 설명하고, 이렇게 정의된 상태를 사용하여 진행상황의 예측을 가능케 하려 한다.

지속적으로 일어나는 측정값을, 변화 추이를 고려하여 관찰하기 위해, 관찰 시 *창*을 사용하였다. 창의 크기는 가변적이며 의미 있는 일련의 행동들을 관찰할 수 있도록 조절된다. 여기에서 '의미 있는 행동'이란 다음과 같이 정의된다. 그림1은 이 내용을 보조하고 있다.

- 네트워크 행동: TCP 명세에 따라 의미를 가지는 네트워크 패킷 집합의 가장 작은 단위 (예. TCB 생성, SYN 발신, ACK(SYN) 발신 등)
- 네트워크 사건: 네트워크 행동들이 구성하는, 네트워크 통신에 있어 의미를 가지는 기본 단위 (예. 텔넷 세션 초기화, 터미널 옵션 협상 등)
- 네트워크 세션: 네트워크 사건들과 서버-클라이언트 사이에 주고 받는 내용을 담은 패킷들로 이루어지는, 네트워크 어플리케이션 수준에서 의미를 가지는 하나의 완벽한 집합
- 네트워크 세션 집합: 네트워크 어플리케이션의 특성 상 세션이 여럿 모여 서버-클라이언트 사이의 한 번의 작업을 구성하는 경우, 이러한 세션들의 집합

## 3. 컴퓨터 시스템의 상태 모형

우리는 시스템에 대한 침입을 탐지하기 위해, 시스템의 상태를 특성화하고 관찰된 상태 진행을 바탕으로 이후의 상태 변화를 예상할 수 있도록 하고자 한다. 이러한 목적을 만족하도록 모형을 만드는 데에는 *은닉 마르코프 모델(Hiddem Markov Model)*을 사용하는 것이 적합하다. *은닉 마르코프 모델*을 사용하여 우리는 이 연구에서 다음과 같은 문제를 해결할 수 있다.

• 문제1. 컴퓨터 시스템의 상태 모형의 구축:
$P(O|\lambda)$를 최대화 하는 모형 $\lambda=(A,B,\pi)$의 매개변수를 구한다.

• 문제2. 컴퓨터 시스템에 현재 발생하고 있는 사건과 상태의 변화를 바탕으로 이후에 일어날 사건과 상태의 변화를 예상:
관측렬 $O=\{O_1,O_2,O_3,\cdots\}$와 모형$\lambda=(A,B,\pi)$가 주어져 있을 때, 관측렬을 가장 설명하는 최적 상태열 $q=\{q_1,q_2,q_3,\cdots\}$를 찾는다.

본 연구에서는 2.2절에서 의미 있는 행동들을 모형의 관측심볼로 사용하고, 모형의 각 상태에 대해서는 침입 탐지의 측면에서 의미 있는 해석을 하지 않는다.[2)]

### 3.1. 모형 구축

문제1은 *바움-웰치(Baum-Welch) 재추정 알고리즘*을 사용하여 반복적인 과정으로 해결된다. 시간 $t$에 상태$q_i$이다가 시간 $t+1$에 상태 $q_j$일 확률을 $\xi_t(i,j)$, $\lambda$와 $O$가 주어졌을 때 시간 $t$에서 상태 $q_i$일 확률을 $\gamma_t(i)$라 하자. $\xi_t(i,j)$를 $\gamma_t(i)$를 사용하여 풀이하면 다음과 같다.

$$\gamma_t(i)=\sum_{j=1}^{N}\xi_t(i,j)$$

추정되는 매개변수들은 다음과 같다.

2) 은닉 마르코프 모델로 모형을 구축하고 다루는 과정에서 사용되는 *상태*는, 이 연구 전반에서 일반적으로 *상태*라는 표현으로 뜻하는 것과 다르다. 본 논문의 3장에서만 *상태*가 은닉 마르코프 모델의 상태라는 의미로 사용되며, 나머지 부분에서는 컴퓨터 시스템 상태의 의미로 쓰인다.

$\hat{\pi}_i$: 시간 $t=1$에서 상태 $q_i$에 있을 확률

$$\hat{a}_{ij} = \frac{q_i\text{에서 } q_j\text{로 천이할 확률}}{q_i\text{로 천이할 확률}} = \frac{\sum_{t=1}^{T-1}\xi_t(i,j)}{\sum_{t=1}^{T-1}\gamma_t(i)}$$

$$\hat{b_j}(k) = \frac{q_j\text{에서 천이하고 관측·심볼이 } v_k\text{일 확률}}{q_j\text{에 있을 확률}} = \frac{\sum_{t=1,q.t.o_t=v_k}^{T-1}\gamma_t(j)}{\sum_{t-1}^{T-1}\gamma_t(j)}$$

이 모형화는 컴퓨터 시스템이 침입 하에 있는지/그렇지 않은지에 무관하게 이루어진다. 은닉 마르코프 모델을 사용하는 다른 침입 탐지 기법 연구들은 정상행위 및 비정상행위를 구분하여 모형화하고, 각 모형에서 현재 일어나고 있는 사건이 발생 가능한지를 계산하여 침입의 발생 여부를 결정하는 방식을 주로 사용한다. 본 연구는 모형 자체는 정상/비정상의 의미를 가지지 않고 단지 사건의 진행 유형과 그에 따른 변화의 지식이 되도록 한다. 침입의 발생 여부는 모형을 사용하여 컴퓨터 시스템에 일어나는 변화를 예측한 결과에 대한 평가에 따라 결정된다.

### 3.2. 상태 변화 예측

문제2는 *비터비(Viterbi) 알고리즘*을 사용하여 해결된다. 시간 $t$에서 첫 번째 $t$개의 관측과 상태 $q_i$에서 끝나는 단일 패스로 가장 높은 확률 점수를 $\delta_t(i)$라 하고, 이를 최대화하는 상태의 트랙을 배열 $\Psi_t(j)$에 저장, 역추적하며 목표를 탐색한다. 이 과정은 다음과 같다.

- 단계1: 초기화
  $\delta_1(i)=\pi_i b_i(o_q), \quad a \le i \le N$
  $\Psi_1(i)=0 \quad (no\ previous\ states)$
- 단계2: 반복
  $\delta_t(j)=\max[\delta_{t-1}(i)a_{ij}]b_j(o_t), \quad 2 \le t \le T;$
  $\Psi_t(j)=\arg max[\delta_{t-1}(j)a_{ij}] \quad a \le j \le N$
- 단계3: 종료
  $P^*=\max[\delta_T(i)]$
  $q_T^*=\arg max[\delta_T(i)]$
- 단계4: 최적 상태열 역추적
  $q_t^*=\Psi_{t+1}(q_{t+1}^*)t=T-1,t-2,...,1$

구해진 컴퓨터 시스템의 상태 진행 예상 모습을 분석하여 시스템이 처할 상황의 위험하고 안전한 정도를 평가할 수 있다. 이 때 전체적 진행 패스의 어느 시점에서 위험에 해당하는 평가 수준으로 진입하는지, 몇 %의 확률로 그렇게 되는지의 정보를 함께 계산함으로써, 침입 탐지 후 알림 및 대응 과정에 유용한 정보를 제공할 수 있다.

## 4. 결론 및 향후연구과제

본 논문은 컴퓨터 시스템의 상태 관찰을 바탕으로 침입을 탐지하는 시스템을 위해 시스템 상태를 모형화하는 방법을 구상하였다. 현재 몇 유형의 침입이 발생한 시스템의 감사 데이터와 침입이 발생하지 않은 한 시스템의 한 달 동안의 감사 데이터를 사용하여 의도한 대로 동작하는지 검사하는 수준의 제한적 실험을 마친 상태이다. 이 방법의 유효함을 증명하기 위해 대량의 실제 데이터를 사용하여 실험을 수행할 것이다.

본 연구팀이 설계하는 침입 탐지 기법은 기존에 제안된 가법들보다 탐지의 정확성을 높이고 사람의 개입을 줄여 더욱 지능화/자동화하는 것을 목적으로 하고 있다. 그러나, 침입 탐지는 실시간으로 대량의 정보를 처리하는 작업이므로, 제안된 기법이 실세계에서 쓰이기 위해서는 개선 가능성이 있는 수준 이상의 처리 속도를 보여야 한다. 앞으로 우리가 제안하는 기법이 처리 속도 및 처리 방식 구조 면에서 실시간 시스템으로 구현될 수 있음을 증명할 것이다.

## 참 고 문 헌


[1] Yaghmour, K., Dagenais, M. R., "Measuring and Characterizing System Behavior Using Kernel-Level Event Logging," Proceedings of the 2000 USENIX Annual Technical Conference, USENIX, 2000 .

[2] Kim, J., Chung, J., "Reduction of dimension of HMM parameters using ICA and PCA in MLLR framework for speaker adaptation", Proceedings of EUROSPEECH-2003, pp. 1461-1464. September, 2003.

[3] Hseuh, M. C., Iyer, R. K., Trivedi, K. S., "Performance Modeling Based on Real Data: A Case Study," IEEE Transactions on Computers, vol. 37, no. 4, pp. 478-484, April, 1988.

[4] Tsai, T. K., Iyer, R. K., Jewitt, D., "An Approach Towards Benchmarking of Fault-Tolerant Commercial Systems," Proceedings of the Twenty-Sixth Annual International Symposium on Fault-Tolerant Computing (FTCS '96), 1996.

[5] Lazarevic, A., Ozgur, A., Ertoz, L., Srivastava, J., Kumar, V., "A Comparative Study of Techniques for Intrusion Detection, " Proceedings of SIAM Conf. Data Mining, 2003.

[6] Isci, C., Buyuktosunoglu, A., Martonosi, M., "Long-Term Workload Phases: Duration Predictions and Applications to DVFS," IEEE Micro, vol. 25, no. 5, pp. 39-51, Sept/Oct, 2005.