제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

# HMM을 이용한 패킷 내용기반 공격 탐지에 관한 연구

김동성*, 염동복*, 박종서*
*한국항공대학교 컴퓨터공학과
e-mail : {dskim,mutacker,jspark}@mail.hangkong.ac.kr

# A Study on Packet payload based Attack Detection using HMM

Dong Seong Kim*, Dong Bok Yeom*, Jong Sou Park*
*Dept. of Computer Engineering, Hankuk Aviation University

요 약

기존의 네트워크 기반의 IDS 는 쉘코드를 단순 매칭함으로써 침입여부를 판별한다. 이러한 방식은 알려진 공격에 대해서만 탐지할 수 있으며, 다형 쉘코드 및 IDS 우회 방법을 사용할 경우 탐지하지 못하는 문제점을 가진다. 따라서 본 논문에서는 Hidden Markov Model 을 이용하여 자동화되고 효율적인 패킷 내용 기반의 침입 탐지기법을 제안한다.

## 1. 서론

인터넷의 보급 및 확산으로 인해 컴퓨터 사용 인구의 급격히 증가하고 있다. 이와 더불어 인터넷을 통한 각종 해킹 기술의 공개 및 확산되고 있으며, 심각한 보안 침해 사고가 급격한 증대되고 있다. 이와 더불어 최근의 발생한 인터넷 대란 등으로 인하여 정보 보안에 대한 인식이 높아지고 있다. 인터넷과 네트워크로부터 발생하는 침입의 상황에 대한 정보와 각종 대응 방법에 대한 효과적인 대책이 필요하다. 이를 효과적으로 대처하기 위해 방화벽이 먼저 등장하였다. 그러나 방화벽은 다양한 공격에 대처하고 내부 침입자에 효과적으로 대응하기 어렵다. 따라서 외부 공격자뿐만 아니라 내부 침입자를 효과적으로 대응하고 위해 침입탐지 시스템을 사용하고 있다. 침입탐지 시스템(IDS)은 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 규정하는 시스템으로 가능하면 실시간으로 처리하는 시스템으로 정의되었다[1]. Kumar 의 분류에 의해 IDS 는 침입모델을 기반으로 오용 탐지, 비정상탐지, 하이브리드 탐지로 나누어지고, 감사자료의 위치에 따라 호스트 기반, 네트워크 기반, 하이브리드 기반으로 나누어진다[2]. 오용탐지 모델은 지식기반 접근방법으로 알려진 공격을 패턴화하는데 주력하였고 이는 알려지지 않은 새로운 공격에 효과적으로 대처하지 못하는 문제점을 가진다. 이를 극복하기 위한 최근에는 기계학습을 이용한 비정상 탐지 방법이 연구되고 있다. 대표적인 예로, 신경망[3], 컴퓨터 면역 시스템[4], 데이터 마이닝 방법이다[5]. 그러나 이러한 연구들은 대부분 호스트 기반으로 침입을 탐지하는데 초점을 맞추고 있다. 호스트 기반의 IDS 는 네트워크 공격을 탐지하기 어렵고, 운영체제에서 의존적이며, 개발비용이 높아 대부분의 상용 IDS 는 네트워크 기반의 IDS 이다[6]. 네트워크 기반의 IDS 에서의 비정상 탐지 방법은 네트워크 패킷 헤더정보를 이용하여 침입을 판별하는 비정상 탐지 방법이 연구되고 있다[7]. 그러나 이러한 네트워크 기반 IDS 는 내용기반의 침입 탐지를 시도하고 있지 않으며, DoS 나 Probe 공격은 높은 탐지율을 가지지만, U2R, R2L 공격에 대해서 낮은 탐지율을 가진다[8]. 또한 NIDS 를 우회하는 방법이 등장하고 있으며, 다형 쉘코드를 생성하므로 단순한 패턴 매칭 방법은 한계가 있다. 따라서 이를 효과적으로 대처하기 위한 방법이 필요하다. 본 논문에서는 Hidden Markov Model(HMM)을 이용한 패킷의 내용 기반 네트워크 침입 탐지 방법을 제안한다. HMM 은 음성인식분야나 DNA 시퀀스 모델링분야에서 광범위하게 사용되는 확률적인 모델링기법으로 우수한 성능을 나타낸다[9]. 감사자료로 공격에 사용되는 쉘코드를 사용하며 HMM 을 이용하여 침입을 탐지하는 기법을

제안한다.

## 2. 관련 연구

네트워크 기반의 침입 탐지 시스템은 단순한 패턴 매칭 방법을 이용한 침입 탐지를 수행하고 있다. 공격자들은 이를 우회하는 방법들을 개발하였고, 이를 공개하였다. 이 장에서는 다형 쉘코드, 침입 탐지 시스템 우회방법을 간략히 소개하고, HMM 의 개념에 대해 소개한다.

### 2.1 다형 쉘코드와 IDS 우회

특정 시스템을 공격하기 위해서는 먼저 그 시스템의 운영체제 정보와 사용중인 서비스 목록 중에서 취약한 서비스를 공격한다. 이 중에서 가장 많은 사용되는 공격은 프로그래밍 상의 오류를 이용한 공격이며[10], 이들 공격은 악의적인 코드인 쉘코드(shellcode)를 대부분 사용한다. 쉘코드는 메모리의 임의영역에 주입되는 악의적인 기계어 코드로 주로 쉘을 실행한다[11][12]. 스택기반의 버퍼넘침 공격은 공격자가 메모리의 스택영역에 저장되는 복귀주소를 쉘코드가 있는 주소로 바꾸어서 쉘코드가 실행되게 함으로써 이루어진다. 이러한 쉘코드는 공격 대상 머신의 환경에 따라서 달라진다. HP 와 Spark, intel 머신의 경우 쉘코드가 달라지며, 운영체제, 사용자의 컴파일 환경에 따라서도 달라진다. 그러나 상용 NIDS 는 알려진 공격의 쉘코드를 공격 데이터베이스에 저장하고 단순 패턴 매칭 방법으로 공격을 탐지한다. 그림 1 은 상용 IDS 인 snort 에서의 쉘코드 탐지 룰에 대한 한 예(Ramen 바이러스에서 사용되었던 LPRng 버그)이다. 그림 1 에서 룰에서 패턴을 매칭하는 부분인 content: " /..../"의 내용은 실제 사용된 exploit 의 쉘코드 중에서 일부분만을 사용하고 있다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT LPRng overflow";
flags: A+; content: "|43 07 89 5B 08 8D 4B 08 89 43 0C B0 0B CD 80 31 C0 FE
C0 CD 80 E8 94 FF FF FF 2F 62 69 6E 2F 73 68 0A/"; reference:bugtraq,1712;)
```

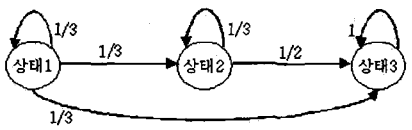
그림 1. snort 에서의 쉘코드 탐지 룰의 예.

만약 공격자가 위의 exploit 중에서 쉘코드를 변형하여 사용한다면, IDS 를 쉽게 통과할 수 있다. 실제로 공격자는 변형된 쉘코드인 다형(polymorphic) 쉘코드를 만들어서 IDS 를 우회하며[13], Insertion, Evasion 기술을 사용하여 IDS 를 우회 하는 방법도 존재한다[14]. 따라서 본 논문에서는 이러한 다형 쉘코드 및 침입탐지시스템 우회 방법을 사용할 경우에도 침입을 탐지할 수 있는 방법을 HMM 을 사용하여 제안한다.

### 2.2 은닉 마르코프 모델

HMM 은 기저가 되는 생성 모델을 가정하지 않으며, 단지 관찰열에만 의존해서 확률적으로 대상을 모델링하여 특정 관찰열이 구축된 모델로부터 생성되었을 확률 및 최적의 전이 상태를 구할 수 있다. HMM 의 모델링과 평가를 위한 절차들은 잘 정립된 수학적 배경을 가지고 있어서, 음성인식을 포함한 여러 분야에서 소스가 알려지지 않은 대상을 모델링하는데 널리 유용성을 인정받고 있다[15].

HMM 은 실제적인 생성모델을 알수 없고 단지 생성된 관찰열에 의해서만 확률적으로 관찰할 수 있는 이중으로 확률적인 절차로서[9], 순서 정보를 모델링하기에 유용한 도구이다. 이 모델은 상태라고 불리는 $N$ 개의 노드와 상태간의 전이를 표현하는 가지(edge)로 구성된 그래프로 볼 수 있다. 각 상태 노드에는 초기 상태 분포와 해당 상태에서 $M$ 개의 관찰 가능한 심볼 중 특정 심볼을 관찰할 확률분포가 저장되어 있으며, 각 가지에는 한 상태에서 다른 상태로 전이할 상태전이 확률분포가 저장되어 있다. 그림 2 는 상태수가 3 인 우향(left-to-right)모델의 HMM 을 보여주고 있다.




Pr('a'|상태1)=1/2 Pr('a'|상태2)=1/3 Pr('a'|상태3)=1/2
Pr('b'|상태1)=1/2 Pr('b'|상태2)=2/3 Pr('b'|상태3)=1/2

그림 2. 우향모델 HMM 의 예

$0 = 0_1, 0_2, ...., 0_T$ 라는 입력열이 주어지면 HMM 은 비록 외부에서 그 상태전이 과정을 직접적으로 알지는 못하지만 자체의 확률 매개변수를 이용하여 이를 마르코프 과정의 확률함수로 모델링할 수 있다. 또한, 일단 모델링 과정을 통해 모델이 구축되며 임의의 입력열이 모델로부터 생성되었을 확률을 계산할 수 있다. HMM 은 다음과 같은 매개변수 $\lambda = (A, B, \pi)$로 표현된다.

- 상태전이 확률분포 $A = \{a_{ij}\}$ (상태 $S_i$ 에서 $S_j$ 로 이동할 확률)
- 관찰심볼 확률분포 $B = \{b_j(k)\}$ ( 상태 $S_j$ 에서 심볼 $v_k$ 를 관찰할 확률)
- 초기상태 분포 $\pi = \{\pi_i\}$ (초기 상태가 $S_i$ 가 될 확률)

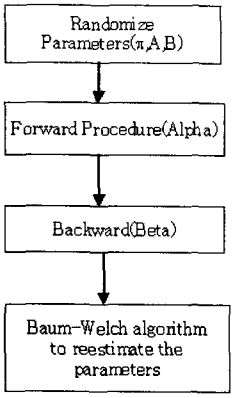



그림 3. HMM 의 훈련과정

그림 3 은 HMM 의 훈련과정을 나타낸 것이다. 주어진 관찰 심볼을 이용하여 최적의 모델을 구하기 위하여 그림 3 과 같은 절차가 순서대로 수행된다. 먼저 구하고자하는 임의의 모델 $(\pi, A, B)$ 을 설정한다. 그 다음 $P(B|\lambda)$ 을 구하여야 하는데, 계산 복잡도를 낮추기 위하여 forward-backward 알고리즘을 사용한다. 다음으로 알려진 관찰 심볼에 대응하는 알려지지 않은 최적의 상태 시퀀스를 구하기 위하여 Viterbi 알고리즘을 사용한다. 마지막으로 $P(B|\lambda)$ 을 최대화하는 모델의 파라미터 $\lambda=(A,B,\pi)$ 를 구하기 위하여 Baum-Welch 알고리즘을 사용하여 파라미터를 재평가한다.

## 3. 제안 모델

### 3.1 제안 모델의 전체구조

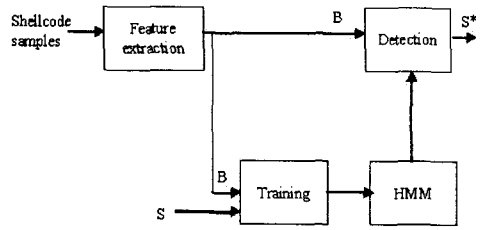



그림 4. 제안 모델의 전체 블록 다이어그램

그림 4 는 본 논문에서 제안하는 HMM 을 이용한 패킷 내용 기반 침입 탐지 방법의 전체 블록 다이어그램이다. 제안 모델의 전체 과정은 4 단계로 나누어질 수 있다. 첫 번째는 감사자료를 수집단계이다. 두 번째는 수집된 쉘코드의 특징을 추출하는 단계이다. 세 번째는 특징이 추출된 쉘코드를 HMM 의 훈련과정을 통하여 훈련시키고 최적의 모델을 구하는 단계이다. 네 번째는 훈련과정을 통하여 구해진 모델을 실제 쉘코드를 통하여서 검증하는 단계이다. 만일 탐지율이 일정수준의 이하라고 하면 1 단계에서 3 단계가 반복되어 수행하여 체적의 모델 파라미터를 찾아야한다.

각 단계를 보다 구체적으로 설명한다. 첫 번째 감사자료 수집단계에서는, 감사자료로 알려진 쉘코드 예제를 수집한다. 일반적으로 쉘코드는 특정 머신의 종류와 운영체제에 따라서 분류되며, 그 하위로 알려진 취약점에 대한 exploit 이 제공된다. 네트워크 기반 IDS 는 네트워크 망의 허브나 라우터 단에 설치되며, 모든 패킷을 스니퍼링하여 공격여부를 탐지할 수 있어야 하므로 머신의 종류와 운영체제의 종류에 관계없이 네트웍을 통과하는 모든 쉘코드를 탐지할 수 있어야 한다. Irix/MIPS, Solaris/sparc, solaris/x86, linux/x86 등에서 사용되던 쉘코드를 각각 수집되어야 하며, 각각의 쉘코드는 분석되어야 한다. 두 번째 단계에서는 수집된 감사자료의 특징을 추출하는 것이다. 이 단계에서는 각 머신에 따라 다른 쉘코드의 구조를 각각 분석하여 하며 쉘코드를 우회하는 다형 쉘코드에 대한 분석이 병행되어야 한다[13]. 예를 들어 0x90 의 연속적인 흐름을 탐지할 수 있어야 하며, 0x90 에 대한 룰을 회피하기 위해 만들어진 XOR 기법을 이용한 쉘코드에 대한 분석도 진행되어야 한다. 또한 이 단계에서 특징을 추출하는 방법 중 얼마만큼의 길이로 쉘코드의 시퀀스를 샘플링 할 것인가에 대한 실험이 진행되어야 한다. 세 번째 단계인 HMM 훈련 과정에서는 특징이 관찰된 쉘코드를 바탕으로 침입 여부를 판단하는 상태가 있어야 한다. 쉘코드에 따라 공격 혹은 정상의 두 상태로 나타내거나 좀 더 세부적인 상태값을 찾아낼 수 있을 것이다. 네 번째 단계인 검증단계에서는 훈련과정에서 사용되어진 쉘코드 외에 새롭게 변형된 쉘코드를 만들고 이에 대해서 얼마나 잘 탐지하는지에 대한 실험이 필요하다.

### 3.2 제안 구조의 실험시 필요사항

제안 구조의 필요사항을 각 단계별로 요약해본다.

- *1 단계 감사자료 수집 단계.* 각 머신과 운영체제의 따라서 쉘코드를 수집한다. 이때 가능한 다양한 경우의 변형된 쉘코드를 수집해야 한다.

- *2 단계 특징 추출 단계.* 머신과 운영체제에 따른 쉘코드의 구조를 분석하여야 하며, 다형쉘코드와 우회 방법을 대처하기 위한 연구가 병행되어야 한다. 또한 특징 추출시 쉘코드의 추출길이의 가변 혹은 고정 여부를 정해야 하며, 최적의 샘플링 길이도 구하여야 한다.

- *3 단계 HMM 훈련.* forward-backward 알고리즘과 Viterbi 알고리즘, Baum-welch 알고리즘을 사용하여 최적의 모델을 구해야 한다.

- *4 단계 탐지.* 새로운 쉘코드, 다형 쉘코드를 이용하여 구하여진 최적의 모델의 침입 탐지 능력을 점검하여야 하며 샘플링 길이에 따른 실험 등 다양한 실험이 필요하다.

## 4. 결론 및 향후 연구

본 논문에서는 Hidden Markov Model(HMM)을 이용한 패킷의 내용 기반 네트워크 침입 탐지 방법을 제안하였다. 감사자료로 리모트 공격이나 로컬 공격에서 사용되는 exploit 의 쉘코드를 사용한다. 기존의 침입 탐지 시스템의 문제점을 분석하였고, HMM 을 간략히 소개하였다. HMM을 이용한 침입 탐지 모델의 전체 블록다이어그램을 제시하였고 각 단계에 필요한 사항들을 명시하였다. 이를 바탕으로 HMM 툴인 HTK[16]을 이용하거나 직접 구현하여 다양한 실험을 통하여 확인하는 작업이 필요하다.

## 참고문헌

[1] D. Denning, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, 13(2), Feb. 1987.
[2] S. Kumar. "Classification and Detection of Computer Intrusions", PhD thesis, Department of Computer Sciences, Purdue University, August 1995.
[3] Ryan, J., Lin, M., and Mikkulainen,R., 1998, "Intrusion Detection with Neural Networks", Advances in Neural Information Processing Systems, vol. 10, MIT Press.
[4] S. Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation Journal Vol. 8, No. 4, pp. 443-473. 2000.
[5] Wenke Lee, Sal Stolfo, and Kui Mok, "A Data Mining Framework for Building Intrusion Detection Models", In Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, CA, May 1999
[6] H. Debar, M. Dacier, and A. Wepsi, "A Revised Taxonomy for Intrusion-Detection Systems", IBM Research Report. 1999.
[7] Network Traffic Anomaly Detection Based on Packet Bytes by Matthew V. Mahoney, to appear in Proc. ACM-SAC, Melbourne FL, 2003
[8] Results of the KDD'99 Classifier Learning Contest, www.cs.ucsd.edu/users/elkan/clresults.html
[9] L. R. Rabiner, "A Tutorial on Hidden Markov Models and selected applications in speech recognition", proceedings of th IEEE, vol. 77, no. 2, pp. 257~286, February 1989
[10] 2003 년 2 월 통계, http://www.certcc.or.kr
[11] Alpha one, "Smashing The Stack For Fun And Profit", Phrack 49
[12] Murat Balaban, "Designing Shellcode Demystified"
[13] Polymorphic Shellcodes vs. Application IDSs, http://www.ngsec.com
[14] Ptacek, Thomas & Newsham, Timothy. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection". Secure Networks, January 1998.
[15] 침입 탐지시스템을 위한 은닉 마르코프 모델의 적용, 정보과학회 논문지 : 소프트웨어 및 응용 제 28 권 제 6 호(2001.6)
[16] Hidden Markov Model Toolkit (HTK), http://htk.eng.cam.ac.uk/