베이지안 네트워크 기반의 변형된 침입 패턴 분류 기법☆

Modificated Intrusion Pattern Classification Technique based on Bayesian Network

차 병 래* 박 경 우** 서 재 현***
Byung-Rae Cha Kyoung-Woo Park Jae-Hyeon Seo

요 약

프로그램 행위 침입 탐지 기법은 데몬 프로그램이나 루트 권한으로 실행되는 프로그램이 발생시키는 시스템 호출들을 분석하고 프로파일을 구축하여 변형된 공격을 효과적으로 탐지한다. 본 논문에서는 베이지안 네트워크와 다중 서열 정렬을 이용하여 여러 프로세스의 시스템 호출간의 관계를 표현하고, 프로그램 행위를 모델링하여 변형된 이상 침입 행위를 분류함으로써 이상행위를 탐지한다. 제안한 기법을 UNM 데이터를 이용한 시뮬레이션을 수행하였다.

Abstract

Program Behavior Intrusion Detection Technique analyses system calls that called by daemon program or root authority, constructs profiles, and detectes modificated anomaly intrusions effectively. In this paper, the relation among system calls of processes is represented by bayesian network and Multiple Sequence Alignment. Program behavior profiling by Bayesian Network classifies modified anomaly intrusion behaviors, and detects anomaly behaviors. we had simulation by proposed normal behavior profiling technique using UNM data.

Key Words : Intrusion Pattern Classification, Bayesian Network

1. 서 론

최근 컴퓨터와 통신 기술의 급속한 발전으로 컴퓨터 시스템에 대한 해킹 방법이 다양해지고 있으며 새로운 기법들이 개발되고 있다. 이러한 추세에 의해서 비인가된 사용자로부터 불법적인 정보의 조작과 접근을 방지하기 위해서 인증과 접근제어 등의 보안 기술에 추가하여, 정보보호의 2차 방어선으로 침입 탐지 시스템(Intrusion Detection System)이 개발되어 졌다. 침입 탐지 시스템은 오용 탐지(Misuse Intrusion Dtection)와 이상 탐지(Anomaly Intrusion Detection)로 분류가 된다.

이상 탐지는 정상 시스템의 행위로부터 주목할 만한 특이한 행위 패턴을 침입으로 규정하여 침입을 탐지한다. 오용 탐지는 알려진 침입 기술을 수집하여 지식 베이스에 유지하고, 동일한 침입 기술을 지식 베이스 검색을 통해 침입을 탐지하는 방법이다. 이상 탐지를 위한 방법들은 연구 초기단계이며 일반적으로 상업화되어 오용탐지 방법이 많이 사용되지만 오용 탐지의 단점으로는 새로운 침입 패턴은 탐지할 수 없는 문제점이 있다[1].

시스템 호출을 이용한 이상탐지 기법에는 크게 열거형 방법, 빈도 기반의 방법, 데이터마이닝 접근 방법 그리고 유한상태 기계 방법으로 분류할 수 있다. 열거형 순차 방법은 정상행위를 경험적으로 추적하여 결과적으로 알려지지 않은 패턴을 모니터링하여 이상을 탐지한다. 빈도 기반의 방법은 다양한 이벤트의 빈도 분포를 모델로하여 이

* 준회원 : 목포대학교 컴퓨터공학과
chabr69@empal.com(제1저자)
** 정회원 : 목포대학교 정보공학부
kwpark@mokpo.ac.kr(공동저자)
*** 정회원 : 목포대학교 정보공학부
jhseo@mokpo.ac.kr(공동저자)
☆ 이 논문은 2002년도 정보통신부 기초기술연구지원사업에 의하여 연구되었음.

상을 탐지한다. 데이터마이닝 접근 방법은 정상행위 데이터로부터 발생하는 공통의 원소를 작은 규칙집합으로 특징을 기술하는 능력을 제공한다. 유한 상태 기계 방법은 기계 학습 기법으로 프로그램을 추적하여 인식하는 유한 상태 기계를 구축하여 이상을 탐지한다[2].

또한, 이상 침입 탐지에는 사용자 행위 기반 이상 탐지와 프로그램 행위 기반 이상 탐지로 분류한다. 프로그램 행위 이상 침입 탐지 기법은 데몬 프로그램이나 루트 권한으로 실행되는 프로그램이 발생시키는 시스템 호출들을 분석하고 프로파일을 구축하여 잠재적인 공격을 효과적으로 탐지한다. 시스템 호출을 이용한 침입탐지는 사용자 행위의 이상 탐지보다는 많은 다양성과 변이를 보이지 않고 고정된 특별한 몇 개의 시스템 호출의 순차로 구성된다. 그러므로, 각각의 프로그램마다 시스템 호출을 이용하여 프로그램 행위를 모델링할 수 있다.

시스템 호출을 이용한 이상 탐지는 단지 그 프로세스가 이상(anomaly)임을 탐지할 뿐 그 프로세스에 의해 영향을 받는 여러 부분에 대해서는 탐지하지 못하는 문제점을 갖는다[3,7]. 본 논문에서는 이러한 문제점을 개선하는 방법이 베이지안 네트워크와 다중 서열 일치를 이용하여 관련된 여러 프로세스의 시스템 호출간의 관계를 표현하고, 프로그램 수준의 프로세스간 이상이 미치는 범위까지 이상 침입을 탐지 및 분류한다.

본 논문에서는 베이지안 네트워크와 다중 서열 일치를 이용한 정상 행위 프로파일링과 변형된 침입을 탐지하는 기법을 제안한다.

베이지안 네트워크를 이용한 침입 탐지 모델은 베이지안 이론을 기본으로 전후 관계를 확률값으로 추정하며, 전후 관계를 그래프 형태인 베이지안 네트워크로 표현한다.

행위의 전후 관계를 다중 서열 일치와 패턴 생성 구문을 정의하여 행위 패턴을 간결하게 기술하며, 베이지안 네트워크를 이용한 프로파일에 의해서 변형된 침입 행위의 탐지가 가능하다.

은닉 마코프 모델에 비해서 계산 복잡도가 크지 않다는 장점과 N-gram의 단점인 프로파일 데이터의 크기 및 오버헤드가 매우 크다는 점을 극복할 수 있다. 제안한 모델을 Sendmail 데몬의 행위 기반 UNM 데이터를 이용하여 시뮬레이션 하였다.

2. 관련 연구

2.1 시스템 호출을 이용한 이상탐지 기법

침입 탐지를 위해 프로그램 행위를 분석하여 프로파일을 구축하는 기법들은 사용자 행위 침입 탐지 기법의 대안으로 연구되어 왔다. 프로그램 행위 프로파일은 정상적인 프로그램이 수행되면서 발생시키는 시스템 호출들을 수집 및 분석하여 구축한다.

열거형 순차 방법은 열거된 순차에 의존하는 방법으로 lookahead pairs, tide (time-delay embedding) 그리고 stide (sequence time-delay embedding) 등이 있다. 이 방법들은 정상 행위를 경험적으로 추적하여 결과적으로 알려지지 않은 패턴을 모니터링한다. 초기에 이 기법들은 패턴에 대한 통계적 분석이 적용되지 않았다[2].

빈도 기반의 방법들은 다양한 이벤트의 빈도 분포를 모델로 하며, 텍스트 문서를 분류하는데 사용된 N-그램 벡터(N-gram vector)가 여기에 속한다. 프로그램 행위 기반 침입 탐지 기법의 전제는 대부분의 공격은 프로그램 오용 때문에 가능하다는 것이고 프로그램이 오용될 때는 프로그램의 정상적인 사용과는 그 행위가 다르다는데 있다. 그러므로, 프로그램의 행위가 적합하게 표현될 수 있다면 침입 탐지를 위한 행위 특성에 이용될 수 있다.

프로그램의 정상행위를 자동적으로 발굴하고 정의하기 위한 대표적인 것은 뉴 멕시코 대학의 Forrest 연구팀에서 개발한 N-gram 기법이다. 이 기법은 면역학의 개념을 응용하여 침입탐지에 적용하였다. N-gram 기법은 프로그램에 의해 발생되

는 시스템 호출들을 고정된 길이의 순차(sequence)로 분할하고 이 순차들을 정상행위로 간주하여 프로파일을 구축한다. 만약, 임의의 순차가 프로파일에 존재하지 않는다면 이상행위로 간주한다. 세션내의 총 스트링의 개수에 대해 이상 행위로 간주된 스트링의 개수의 비율이 매우 크다면, 그 세션을 비정상으로 판정한다[2,4,5]. N-gram 기법은 단순한 알고리즘과 높은 탐지율을 보이지만, 프로파일 데이터의 크기 및 오버헤드가 매우 크다는 단점을 갖고 있다. 시스템 호출 추적의 방법으로 이 기법은 프로그램이 종료되어야 추적 벡터를 계산할 수 있기 때문에 온라인 테스팅에서는 부적절하다. 또한 벡터의 크기를 결정하는데 어려움이 있으며, 동일한 프로그램의 정상 행위와 비정상 행위를 추적하기 위한 충분한 정밀도를 제공하지 못한다.

데이터마이닝 접근법은 많은 수집된 데이터로부터 가장 중요한 특징을 결정하기 위해 설계되었다. 이상 침입 탐지에서는 발생된 정상 행위의 모든 패턴을 단순하게 나열하여 얻기보다는 간결하게 정의할 수 있는 정상 행위 패턴을 발견하는데 있다. 데이터마이닝 접근법으로 RIPPER는 정상 행위 데이터로부터 발생하는 공통의 원소를 작은 규칙 집합으로 특징을 기술하는 능력을 제공한다[2].

유한 상태 기계 방법은 기계 학습 접근법으로 프로그램을 추적하여 인식하기 위하여 유한 상태 기계(Finite State Machines)를 구축하여 이상을 탐지한다. 매우 강력한 유한 상태 기계로는 은닉 마코프 모델이 있으며, 이 모델은 이중 추정 통계적 과정으로 기술된다. 여러 모델중에서 가장 이상탐지 능력이 뛰어난 것으로 판명되었으나, 단지 계산 복잡도가 크다는 단점을 갖고 있다[2] .

이상 탐지 모델dpj 발생하는 문제점들은 통계적 분석의 필요, 실시간 처리의 어려움, 정상 행위의 간결한 정의, 계산 복잡도 문제 등이다. 시스템 호출을 이용한 이상탐지에 베이지안 기법를 적용하여 통계적 분석과 계산 복잡도의 문제점들을 부분적으로 해결할 수 있다. 더불어, 각각의 시스템 호출 정보를 이용한 베이지안 네트워크를 구축하여 프로세스간의 관련성을 표현함으로써 프로그램 수준의 변형된 침입을 탐지가 가능하다[8].

2.2 프로파일링

이상 침입을 탐지하기 위해서는 이상과 정상을 구분할 행위를 기술하여야 한다. 시스템 또는 사용자의 행위를 기술하는 것을 행위 프로파일링이라 한다. 행위 프로파일링은 객체에 대한 주체 행위의 특징을 기술하거나 주-객체간의 정상 행위 기술, 또는 이상 징후를 제공한다. 행위 프로파일링 방법으로 행렬과 통계적 모델 들이 존재한다.

행렬 방법은 주기적으로 누적된 측정된 값을 표현하여 이상 탐지에 정보를 제공한다. 행렬방법은 대부분이 3가지 형태로 정의하는데, 이벤트 계수기, 이벤트의 간격 시간 그리고 사용된 자원 측도로 구성한다. 통계적 모델은 모든 지식을 행위를 관측함으로써 정보를 획득하며, 행위에 대한 기본 분포를 가정하지 않아도 된다. 통계적 모델의 IDS는 운영적 모델, 평균과 표준 편차 모델, 다변량 모델, 마코프 프로세스 모델 그리고 시계열 모델로 구분한다[1].

운영적 모델은 고정된 제한과 새로운 관측을 비교하여 비정상을 결정하는 모델이다. 평균과 표준 편차 모델은 이벤트의 합, 합 제곱, 평균, 표준 편차 등의 정보를 이용하여 임의의 신뢰구간을 벗어나면 비정상으로 간주한다. 장점은 정상 행위의 제한 설정에 대한 사전 지식이 필요하지 않다는 점이다. 또한 신뢰구간은 증가된 지식을 반영하며, 관측된 데이터에 의존한다. 다변량 모델은 행위 행렬간의 상관관계를 기반으로 좋은 식별 능력은 제공한다. 행위 개별적인 측정보다는 관련된 측정의 조합에 의해 얻어진다. 마코프 프로세스 모델은 여러 이벤트 형태를 상태 변수, 상태간의 전이 빈도로 특징을 기술하는 상태전이행렬을 사용한다. 어떤 명령과 명령 순차간의 전이 조사에 매우 유용한 모델이다. 시계열 모델은 시간

측면에서 행위의 경향을 측정한다. 장점은 행위의 중요한 변화를 단계적 탐지할 수 있다는 점이다. 단점은 평균과 표준 편차 모델에 비해 비용증가가 크다는 점이다.

2.3 다중 서열 정렬

바이오인포메틱스에서 DNA 서열의 패턴을 추출하기 위해서 다중 서열 정렬(MSA : Multiple Sequence Alignment), 일치 서열(Consensus sequences) 그리고 위치 특이 득점 행렬 (PSSM : Position Specific Scoring Matrice) 방법 등이 쓰인다.

다중 서열의 정렬은 DNA 서열이나 단백질의 특징이나 구조, 화학적 반응에 결합된 특별한 영역을 탐지하는 방법 중의 하나이다. 그러한 영역에 의해 표현된 정보를 서열 정렬을 이용하여, 새로운 서열 또는 유사한 서열을 데이터베이스에서 검색하는 방법이다[15].

바이오인포메틱스에서 사용된 서열 탐색기법들을 이용하여 이상 행위 탐지를 위한 프로그램 행위 패턴 생성에 적용할 수 있다. 프로그램 행위 패턴이란 하나의 프로세스 아이디에 의한 호출된 시스템 호출의 순차로 정의한다. 하나의 프로세스 아이디가 하나의 패턴이 되며, 프로세스 아이디가 호출한 시스템 호출은 패턴의 속성이 된다.

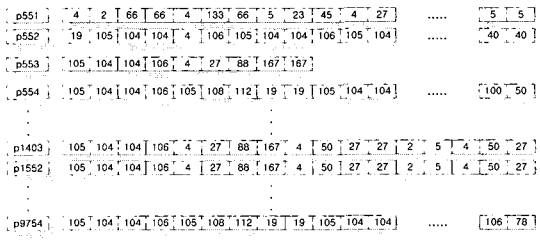
3. 침입 패턴 탐지를 위한 베이지안 네트워크

프로그램 이상 행위를 탐지하기 위해서는 먼저, 정상 행위 데이터를 이용한 프로그램의 정상 행위에 대한 프로파일링의 구축과 프로그램 행위를 기술하는 프로그램 행위 패턴 생성과정이 필요하다.

3.1 베이지안 네트워크를 이용한 프로파일링

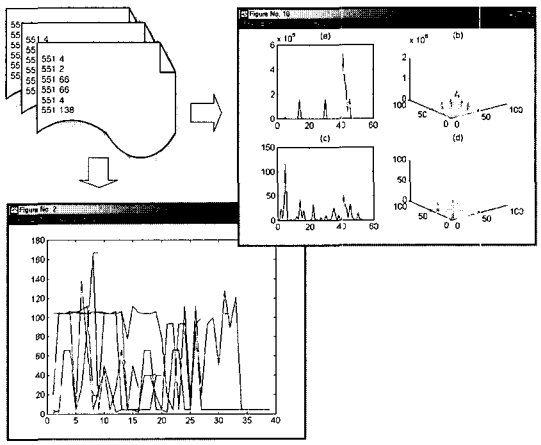
베이지안 네트워크를 이용한 시스템 호출의 이상을 탐지하기 위해서 사전정보와 정상 행위 패턴 정보들을 프로파일로 구축하며, 베이지안 네트워크를 적용하여 이상을 탐지한다. 시스템 호출 정보로 생성된 패턴들이 진정한 침입인지 아니면 정상적인 수행인지를 파악하는 사후 감사과정을 진행한다.

뉴 멕시코 대학(UNM : Univ. of New Mexico)의 Sendmail 시스템 호출 데이터를 이용하여 베이지안 네트워크를 구축한다. Sendmail 데몬의 시스템 호출 데이터를 이용한 프로세스 아이디별 시스템 호출의 순차를 나열하면 다음의 그림 1과 같다.



(그림 1) UNM 데이터의 PID별 시스템 호출 순차

시스템 호출 발생 확률 $P(E)$는 Senmail 데몬의 시스템 호출들을 모니터링 하므로 써 그림 2와 같이 사전 정보로써 확률 값들을 얻을 수 있으며, 시간의 흐름에 따라 값은 변경된다.



(그림 2) 확률 $P(E)$, 시스템 호출 순차

시스템 호출 과정은 대부분이 무작위의 순서로 이루어지지 않으며, 일정한 순서를 갖는 것으로 알려졌다. 시스템 호출의 각 상태는 전후의 순서 관계가 존재하며 모든 시스템 호출 과정은 순서에 의해 상태 전이 그래프인 베이지안 네트워크와 확률값으로 상태 변화 과정이 도출이 가능하다.

시스템 호출의 연속적인 이벤트($E_1, \cdots, E_{i-1}$, E_i)에 대해서 시스템 상태의 침입 확률($P(I|E_1, \cdots, E_i)$)은 결합 확률 함수를 이용하여 다음과 같이 식(1)로 바꿔 쓸 수 있으며,

$$P(I|E_1, \cdots, E_i) = P(I|E_1, \cdots, E_{i-1}) \frac{P(E_i|I, E_1, \cdots, E_{i-1})}{P(E_i|E_1, \cdots, E_{i-1})} \quad (1)$$

위의 식(1)로부터 다음과 같이 정의한다[13].

정의 1) 연속적인 이벤트 $E = (E_1, \cdots, E_{i-1}, E_i)$에 대한 침입 확률값 계산은 $P(I|E_1, \cdots, E_{i-1}, E_i)$으로 정의한다.

정의 2) P_{j-1}상태에서 분기시 침입확률값 계산은 $P_j = P(I|E_j, E_{j-1}, \cdots)$와 $P_{j+1} = P(I|E_j, E_{j-1}, \cdots)$이고, P_j와 P_{j+1}의 침입 확률값은 동일한 것으로 정의한다.

정의 3) P_{k-1}과 P_k의 상태에서 병합시 침입 확률값 계산은 $P_{k-1} = P(I|E_{k-1})$와 $P_k = P(I|E_k)$의 결합확률함수로써, $P_{k+1} = P(I|P_{k-1}, P_k)$으로 정의한다.

정의 4) 시스템 호출 과정의 각 상태를 연결, 역, 접두사, 접미사, 길이 그리고 반복으로 표현이 가능하다.

4-1) 연결(concatenation)은 두 개의 상태 P_v와 P_w를 연결하는 것은 P_v의 상태 뒤에 P_w의 상태를 붙이는 연산으로 정의한다.

4-2) 역(reverse)은 어떤 상태의 역순은 주어진 목적들을 거꾸로 나열한 것으로 정의한다. 상태 P_v와 P_w에 대해 $(P_v P_w)^R = P_w^R P_v^R$이 성립한다.

4-3) 접두사(prefix)와 접미사(surfix)는 만약 $P_z = P_v P_w$라면 P_v는 P_w의 접두사가 되고 P_w는 P_v의 접미사라고 정의한다. 어떤 상태에서 접두사나 접미사를 제거함으로써 이루어지는 상태를 '서브 상태'이라 한다.

4-4) 상태의 길이는 상태 전이 전과정에 포함된 단위 상태의 개수로 정의한다. $|P_v|$와 같이 절대값을 써서 나타낸다.

4-5) 반복은 P_v가 상태일 때 P_v^n이란 P_v를 n번 연결한 것으로 정의한다.

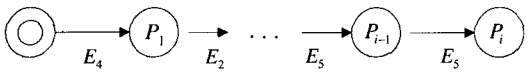
베이지안 네트워크를 이용한 프로파일링 방법은 다음과 같은 절차로 이루어지다.

1) Senamil 데몬의 정상 행위 시스템 호출을 DAG를 이용한 기본 베이지안 네트워크 생성.
2) 생성된 기본 베이지안 네트워크를 MSA의 알고리즘에 의해 확장된 베이지안 네트워크를 생성.
3) 확장된 베이지안 네트워크에서 중복된 반복 부분을 제거하여 최적화된 베이지안 네트워크 프로파일링을 생성.

시스템 호출 과정을 DAG(Direct Arc Graph)를 이용해서 베이지안 네트워크를 표현한다. DAG는 초기상태(◎), 방향성 아크(→), 시스템 호출(이벤트)의 집합(E), 상태(○) 그리고 상태의 확률(P)로 구성된다.

정의 1) 을 이용하여 프로세스 아이디(프로세스 아이디 : Process ID)에 의한 시스템 호출 과정을 이용하여 기본 베이지안 네트워크를 구성한다.

Sendmail의 프로세스 아이디 551의 시스템 호

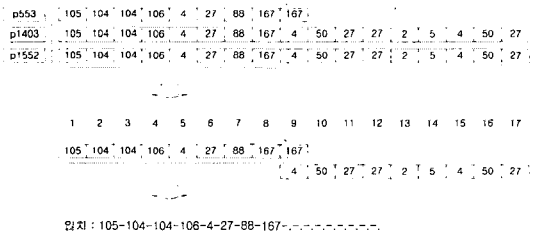


(그림 3) 프로세스 아이디 551의 기본 베이지안 네트워크

출은 {4, 2, 66, 66, 4, 138. 66. 5. 23. 45. 4. 27, 66, 5, 4, 2, 66, 66, 5, 4, 2, 66, 66, 5, 5, 85, 5, 5}으로 구성된다. 프로세스 아이디 551의 기본 베이지안 네트워크를 그래프로 표현하면 그림 3과 같다.

정의2) 와 정의 3)을 이용하여 정의 1)에 의해 구성된 기본 베이지안 네트워크를 프로세스 아이디와 무관하게 다중 서열 정렬(Multiple Sequence Alignmant)에 의해 베이지안 네트워크를 확장한다.

프로세스 아이디 1403과 1552은 시스템호출 과정이 거의 일치하여 동일하다. 그러나 553 프로세스는 시스템 호출 과정의 후반부에서 동일하지 않는다. 이러한 점을 감안하여 다중 서열 정렬(Multiple Sequence Alignment)에 의한 정상 행위 패턴을 추출하며, 다음의 그림 4와 같다.

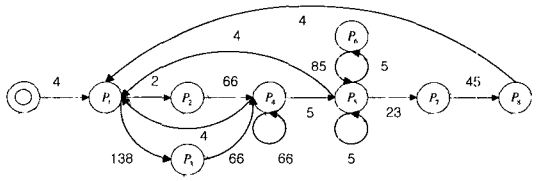


(그림 4) 시스템호출의 MSA

다중 서열 정렬에 의해서 확장된 베이지안 네트워크를 구축함으로써, 각각 시스템 호출의 매칭에 의한 이상 탐지에서 탈피하여, 시스템 호출간의 관련성에 의한 프로그램 행위 수준의 이상 탐지가 가능하게 된다. N-gram 방식의 이상 탐지는 정상 행위 패턴에 등록되지 않은 패턴을 임계치 이상 발생하면 이상으로 탐지하지만, 제안한 방법은 어플리케이션 행위를 프로파일링하여 변형된 이상 침입을 분류한다.

확장된 베이지안 네트워크를 최적화된 베이지안 네트워크로 표현하기 위해 재구성한다. 정의 4)를 이용하여 확장된 베이지안 네트워크를 최적화시켜서 재구성한다. 즉, 반복된 부분을 제거하고, 모든 가능한 순차를 베이지안 네트워크로 표현하게 된다. 이 과정에 의해서 시스템 호출에 의한 이상 행위의 변형된 행위의 탐지가 가능하게 된다.

프로세스 아이디 551의 경우에는 몇 개의 그룹화된 시스템 호출이 반복되는 것을 발견할 수 있다. 시스템 호출을 단순히 순차적으로 열거하기보다는 반복부분을 구분하여 제거하는 등의 과정으로 베이지안 네트워크의 최적화를 수행하며, 그림 5와 같다.



(그림 5) 최적화된 베이지안 네트워크

각각의 시스템 호출에 의해 생성된 기본 베이지안 네트워크를 분기, 병합 그리고 반복된 부분의 제거 등의 과정을 수행함으로써 프로그램 수준의 정상 행위 베이지안 네트워크가 생성된다. 이러한 베이지안 네트워크로 표현된 정상 행위 패턴들을 모아서 정상 행위 프로파일로 구축한다.

각각의 시스템 호출에서는 단지 프로세스 아이디에 의한 이상을 갖는 하나의 프로세스밖에는 탐지하지 못한다. 그러나, 하나의 프로그램은 여러 개의 프로세스에 의해 구성되기 때문에 하나의 이상 프로세스에 관련된 프로세스들은 탐지하지 못한다. 즉, 시스템에 이상이 발생했다는 것밖에는 탐지하지 못한다. 프로그램을 구성하는 임의의 프로세스가 이상 현상을 보이면 결국에는 그 프로세스로 이루어진 프로그램에 이상이 탐지되는 것이다. 한 프로세스 아이디의 이상 탐지에 멈추지 않고 프로세스 아이디의 조합에 의한 프

로그램 수준의 이상 탐지가 가능하다. 또한, 임의의 변형된 시스템 호출에 대해서도 정상과 이상의 탐지가 가능하다.

3.2 프로그램 행위 패턴 생성

최적화된 베이지안 네트워크는 프로그램 수준의 정상 행위 프로파일링으로 사용한다. 정상 행위 프로파일링과 새로운 프로그램 행위간의 이상을 탐지하기 위해서는 프로그램 행위를 표현하는 방법이 필요하다.

본 논문에서 사용하는 프로그램 행위 패턴 표현법은 다음과 같다[15].

- 시스템 호출에 대한 시스템 호출 번호를 사용
- 패턴의 시작과 끝은 각각 <와 >으로 표시한다.
- 각각의 시스템 호출들은 '-'에 의해 구분한다.
- 심볼 X는 모든 시스템 호출에 대응한다.
- [ ]중괄호는 다양한 시스템 호출을 의미한다.
- { }중괄호는 제외된 시스템 호출을 의미한다.
- 괄호()는 반복을 의미한다.
- 임의 심볼은 특이 패턴을 정의한다.

그러므로, 프로세스 553의 패턴은 <105-104(2)-106-4-27-88-167(2)>이 된다. 프로세스 1403와 1552는 <105-104(2)-106-4-27-88-167-4-50-27-2-5-4-50-27>이 된다. 간략하게 표현하기 위해서 다음과 같이 패턴을 기술하면

A = <105-104(2)-106-4-27-88-167>
프로세스 553 : <A-167>,
프로세스 1403, 1552 : <A-4-50-27-2-5-4-50-27>

이 된다.

최적화된 베이지안 네트워크와 시스템호출 순차에 의한 생성된 프로그램 행위 패턴의 차이점은 시스템호출의 순차 패턴은 한 프로세스의 행위 패턴이고, 최적화된 베이지안 네트워크는 프로세스로 구성된 프로그램 수준의 행위를 프로파일링한 것이다. 그러므로 입력된 새로운 프로그램 패턴이 시스템호출 서열의 패턴과 완벽하게 일치하지 않고 최적화된 베이지안 네트워크 안에 존재하면 이것을 변형된 패턴으로 분류한다.

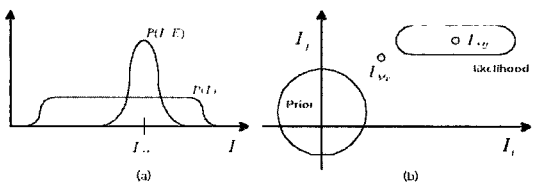
4. 변형된 침입패턴 분류 기법

베이지안 확률값 계산은 사전 확률과 사후 확률, 우도 함수 등을 이용하여 다음과 같은 식(2)로 제시할 수 있다.

$$P(I|E) = \frac{P(E|I)P(I)}{P(E)} = P(I)\frac{P(E|I)}{P(E)} \qquad (2)$$

사전확률 $P(I)$는 침입의 발생 빈도에 의해 좌우되며, 침입에 대한 완전한 정보를 제공하지 못한다. 그러나 사후 확률 $P(I|E)$는 이벤트 E라는 조건에 의한 그림 6의 (a)와 같이 가장 유력한 침입 $P(I|E)$ 부분에서 집중적인 확률 분포를 보일 것이다.

사후 확률 $P(I|E)$은 사전 확률 $P(I)$와 우도 함수 $P(E|I)$의 곱에 이벤트의 확률 $P(E)$로 나눔으로써 계산되며, 위의 관계를 그림으로 나타내면 그림 6의 (b)와 같다. 즉, 두 침입 I_i와 I_j에 대해서 사전 정보와 최우도 함수값에 의한 0과 1 사이의 확률값으로 가장 가능한 침입과 이벤트의 정보를 획득할 수 있다. 가장 가능한 침입 I_j는 확률값 $P(I_j|E)$가 1에 근사하므로 가장 유력한 침입이 되며, 침입 I_i는 확률값 $P(I_i|E)$가 0에 근사하므로 침입과는 무관하게 된다.



(그림 6) 침입에 대한 확률 관계

일반적인 침입 패턴분류 방법은 침입 패턴이 어떤 형태인지는 알지만 약간 변경된 형태의 침입과 새로운 침입 패턴들을 분류하지 못한다. 베이지안 방법을 이용하면 침입에 대해 알고 있는 것은 침입의 사전 확률 분포이다. 사전 확률분포는 기존의 침입에 대한 임의의 사전 지식을 반영하는 형태를 취한다. 여러 침입 사례로부터 사전 확률 분포의 정보를 얻고 사전 확률 분포의 정보로부터 사후 확률 분포 정보를 도출함으로써 다양한 침입 패턴, 변형된 침입 패턴의 분류가 가능하다.

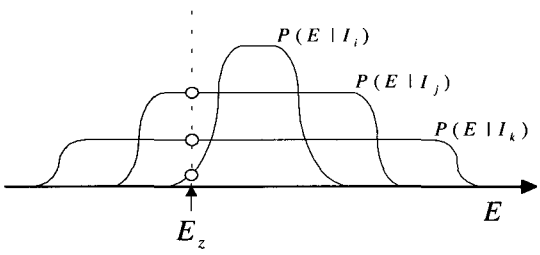
베이즈 정리의 식(2)과 (3)를 이용하여 식(4)을 유도해 낼 수 있다.

$$P(I|E) = P(\sum_i I_i|E) \quad (3),$$

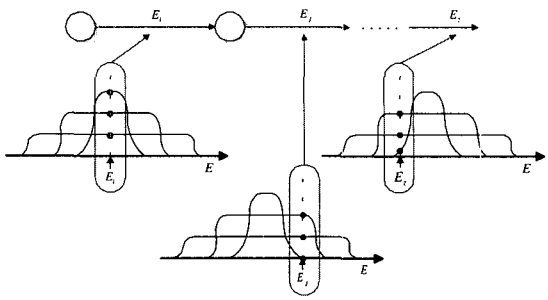
$$P(I_i|E) = \frac{P(E|I_i)P(I_i)}{P(E)} = \frac{P(I_i)P(E|I_i)}{P(E)} \quad (4)$$

시스템 호출 순차 패턴 E를 관측하여 다양한 침입 행위 $I = \sum_i I_i = (I_1, \cdots, I_i, I_j, \cdots)$들의 사후 확률 분포를 계산할 수 있다. 여기서 $P(I_i)$는 침입 행위 I_i의 사전 확률이고, $P(E|I_i)$는 I_i의 확률이면서 명백하게 침입 행위 I_i의 조건에 의존한다. 만약 다른 침입 행위에 대해 다른 사전 확률을 할당하지 않는다면, 이는 각각 침입 행위의 확률 분포를 기저로 한 다른 침입 행위들 간의 연관 확률들을 비교할 수 있다.

그림 7의 시스템 호출 패턴 E_z의 한 시점에서 침입 행위 각각에 대한 우도함수의 분포 행위 확률값을 계산함과 동시에 각각의 침입 행위의 확률값을 비교함으로써 시스템 호출 순차 패턴 E_z의 한 시점에 의한 가장 유력한 침입 행위를 찾을 수 있다. 더불어 어느 정도 변형된 침입 행위의 분류 및 탐지가 가능하게 된다.

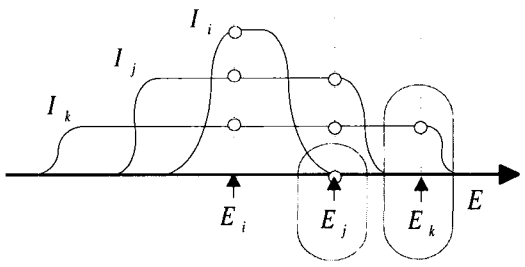


(그림 7) 이벤트에 의한 우도함수의 분포 모델 비교


(그림 8) 이벤트 패턴 조건의 우도함수를 이용한 침입 모델 추정

침입 행위은 단지 하나의 시스템 호출 패턴에 의해 이루어지기보다는 시스템 호출 순차 패턴의 집합과 순서에 의해 침입 패턴의 행위가 구성된다. 그러므로 그림 8과 같이 각각의 연속적인 시스템 호출 패턴의 우도 함수 분포 모델을 비교함으로써 침입 행위를 분류할 수 있다. 연속된 시스템 호출 패턴 $\cdots, E_i, E_j, \cdots, E_z \cdots$ 에 대해 각각의 시스템 호출에 대한 우도 확률 함수를 계산함으로써 침입 행위를 분류 및 탐지할 수 있다. 시스템 호출 패턴 E_i에 의한 침입 행위의 우도 확률 함수의 계산은 $P(E_i|I_i), P(E_i|I_j), P(E_i|I_k)$이 된다. 그리고 시스템 호출 순차 패턴 $E_j, \cdots, E_z \cdots$ 에 대해서도 동일한 과정을 수행함으로써 침입 행위를 탐지 및 분류할 수 있다.

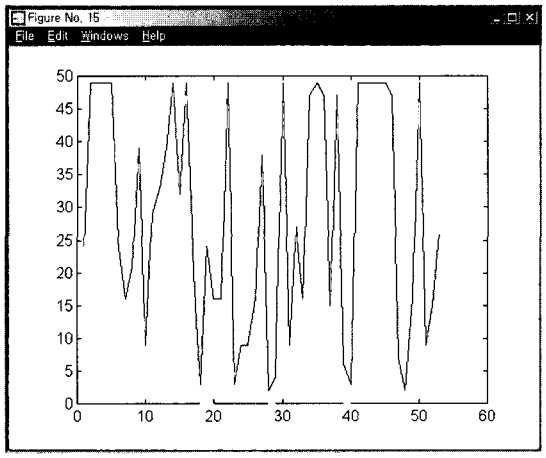
더불어 새로운 연속적인 시스템 호출 패턴으로 인한 침입은 새로운 침입 행위의 우도 확률 분포를 생성 및 등록함으로써 침입 행위를 탐지 및 분류가 가능하게 된다. 프로파일에 등록할 침입 행위 패턴 정보의 특징 선택은 침입 패턴 분류에 두드러지는 특징을 나타내는 시스템 호출 순차 패턴 중에서 그림 9의 시스템 호출 패턴 E_j 및 E_k 와 같은 특징을 이용하여 침입 패턴의 특징을 선택하여 프로파일에 등록한다.



(그림 9) 침입패턴의 두드러진 특징 추출

시스템 호출 패턴 $E = \sum_{i=1}^{n} E_i$중에서 E_i의 확률값은 침입 행위마다 약간씩의 값의 차이가 있을 뿐 모든 침입 행위에 나타나는 침입 패턴이라 할 수 있다. E_i의 각각의 침입 행위에 대해서 확률값은 큰 차이가 있지만, 이것은 불확실성에 대한 약간의 신뢰성을 제공하는 임의의 값에 불과하다. 즉 E_i는 침입 행위 I_i일 신뢰성이 크다는 것을 보여주지, 결코 침입 행위 I_i라는 것을 보장하지는 않는다. 그러므로 우도함수 $P(E_i|I_i)$에 의해서 다른 침입 행위에 대한 우도함수($P(E_i|I_j)$와 $P(E_i|I_k)$)에 비교해서 신뢰성이 좀더 있다는 정보를 제공한다. E_j는 침입 행위 I_k와 I_j에는 나타나나 I_i에는 거의 나타나지 않는 시스템 호출 패턴이라 할 수 있다. 시스템 호출 패턴 E_j의 발생은 침입 행위 I_i가 아님을 의미한다. 그러나 패턴 중 E_k는 여러 침입 행위 중에서 I_k 침입 행위에서만 나타나는 특징으로서 특징 선택에서 필수적으로 선택된다. 시스템 호출 패턴 E_j와 E_k는 특징 선택의 항목에 포함되며 침입 패턴 분류에 명확한 분류 정보를 제공한다.

그림 10은 정상 및 이상 패턴 탐지를 위한 특징 선택을 위한 시스템 호출 분포 데이터를 나타낸다. Sendmail의 정상과 비정상 행위 데이터에서 침입 모델 분류에 사용될 시스템 호출은 두 가지 측면에서 선택한다. 하나는 많은 시스템 호출을 갖는 경우와 또다른 하나는 매우 적은 시스템 호출을 갖는 경우이다.



(그림 10) 정상 및 이상 패턴을 탐지 위한 특징 선택

많은 시스템 호출을 갖는 경우에는 직관적으로 많은 변형이 가능하고 침입 모델 분류에 각각의 모델마다 특이하게 나타날 특징을 추출할 수 있다. Sendmail의 정상 행위 데이터에서는 최고 49개의 시스템 호출을 갖는 경우가 15개의 시스템 호출 정보가 나타났으며, 비정상 행위 데이터에서는 최고 23개 및 9개의 시스템 호출을 갖는 경우가 11개의 시스템 호출 정보를 추출하였다.

적은 시스템 호출을 갖는 경우에는 그 시스템 호출만을 갖는 두드러진 특징으로 침입 모델을 분류할 정보로 사용할 수 있다. Sendmail의 정상 행위 데이터에서는 최저 2, 3 그리고 4개의 시스템 호출을 갖는 경우가 6개의 시스템 호출 정보를 추출하였고, 비정상 행위 데이터에서는 최저 1, 2개의 시스템 호출을 갖는 경우에 22개의 시스템 호출 정보를 추출하였다.

비정상 행위 데이터에서 시스템 호출 번호 5, 2, 4, 14, 16, 22, 35, 41, 42, 43, 45인 경우에는 많은 시스템 호출 정보를 포함하므로 다양한 변형된 침입 패턴을 갖을 확률이 크다. 이러한 정보를 이용하면 이상 침입 모델 분류 정보로 사용 가능하다. 시스템 호출 번호 1, 6, 7, 9, 10, 21, 25, 31, 47, 48, 51, 53과 9, 11, 13, 17, 24, 32, 33, 52는 매우 적은 시스템 호출 정보를 포함하므로 침입 모델의 두드러진 특징 정보로 사용 가능하다.

5. 시뮬레이션

베이지안 네트워크를 이용하여 뉴 멕시코 대학 면역 시스템의 Sendmail 데몬의 시스템 호출 데이터를 이용하여 이상 탐지 과정을 시뮬레이션 한다.

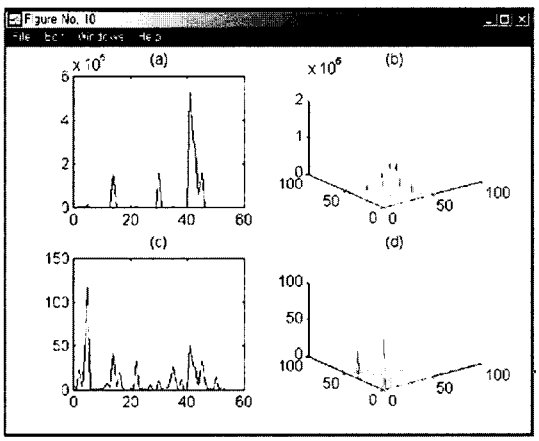
뉴 멕시코 대학의 Sendmail 시스템 호출 데이터의 구성을 보면, 많은 양의 정상 행위 데이터가 존재하는 반면에, 비정상 데이터는 상대적으로 협소하게 구성되어 있다. 그러므로, 정상 행위 데이터에 대해 베이지안 네트워크를 이용하여 정상 행위 프로파일을 작성하고, 비정상 행위 데이터로는 단지 정상과 이상을 분류하기 위한 베이지안 확률값만 산출하여 사용한다.

시뮬레이션 과정은 먼저, 정상 행위 데이터에 대해 베이지안 네트워크를 이용한 프로파일을 구축한다. 이어서, 비정상 행위 데이터에 대해 베이지안 확률값을 이용하여 이상 침입을 탐지한다.

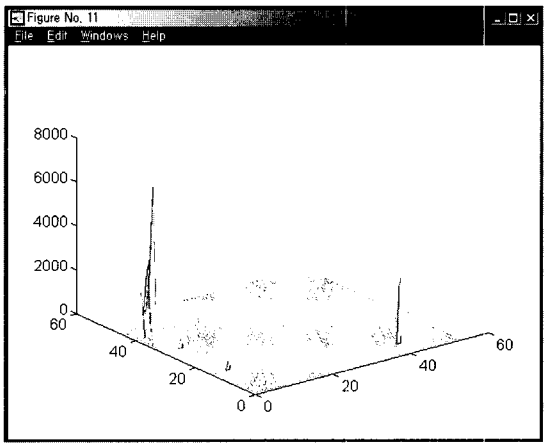
그림 11의 (a)와 (b)는 정상 행위의 데이터를, 그림 11의 (c)와 (d)는 이상 행위 데이터를 이용하여 베이지안 확률값의 분포를 그래프로 표현한 것이다. 그림 11의 (a)와 (c)의 그림에서 정상 행위의 시스템 호출 분포하고 이상 행위 시스템 호출의 분포를 비교할 수 있는데, 정상 행위는 몇몇 시스템 호출에 밀집된 형태를 취하는 반면에, 이상 행위 시스템 호출은 비교적 넓게 분포한 것을 보여준다. 이런 점을 착안하여 시스템 호출의 이상탐지에 베이지안 확률값의 분포에 의한 특징 선택이 가능하게 된다. 그러므로, 모든 시스템 호출을 이용한 이상 탐지보다는 몇몇 시스템 호출로 특징을 선택함으로써 많은 오버헤드 감소와 빠른 이상 탐지가 가능하게 되었다. 그림 11의 (b)와 (d)의 시뮬레이션 결과에 의해 정상행위의 베이지안 확률분포는 몇몇 시스템 호출간의 매우 밀접한 전후관계가 존재함을 파악할 수 있다. 이상행위의 베이지안 확률분포 역시, 넓은 분포를 보이지만 서로 연관 시스템 호출간의 전후관계가 명확하게 존재함을 파악할 수 있다.

Sendmail 시스템 호출 데이터를 이용한 최적화된 베이지안 네트워크 구축한 다음, 프로그램 행위 패턴 표현법에 의해서 UNM의 이상 데이터 집합에서 행위 패턴들을 생성한다. Sendmail의 최적화된 베이지안 네트워크에 의해서 변형된 패턴들의 분포는 그림 12와 같다.

몇몇 시스템 호출을 제외한 나머지의 많은 시스템 호출들은 빈번하게 나타나지 않으며, 같은 이벤트를 반복하더라도 확장된 베이지안 네트워크에 의해서 베이지안 확률값의 변화는 매우 미비하게 나타나게 되므로 같은 이벤트가 반복되거나 임의의 시스템 호출에 의한 간섭이 주어지더 라도 변형된 침입을 같은 부류로 분류가 가능하였다.



(그림 11) 정상 및 이상행위의 분포와 베이지안 확률값



(그림 12) 변형된 패턴들의 분포

6. 결론 및 추후 연구방향

프로그램 행위 침입 탐지 기법은 데몬 프로그램이나 루트 권한으로 실행되는 프로그램이 발생시키는 시스템 호출들을 분석하고 프로파일을 구축하여 잠재적인 공격을 효과적으로 탐지한다.

본 논문에서는 시스템의 호출을 이용하는 이상 침입 탐지에 베이지안 네트워크와 다중 서열 정렬을 적용하였다. 다중 서열 정렬을 이용하여서는 정상 행위 패턴을 생성하였고, 베이지안 네트워크를 이용하여서는 최적화된 어플리케이션에 근접한 동작을 모델링하였다. 베이지안 방법을 이용하여 침입의 각 상태의 확률값을 계산하여 정상과 이상을 탐지하였다. 더불어 베이지안 네트워크를 확장하여 프로세스의 이상 탐지에서 벗어나 어플리케이션 단계에 근접한 이상 탐지가 가능하도록 하였다. 즉, 이상 침입 패턴에 같은 이벤트를 반복하더라도 베이지안 확률값의 변화는 매우 미비하게 나타나게 되고, 다른 시스템 호출의 간섭에 의한 변형된 침입도 확률값의 변화에 미비하게 영향을 미치므로, 같은 부류로 분류가 되었다.

베이지안 네트워크와 위치 특이 득점 행렬의 적용에 의해서 입력된 패턴에 대해 변형된 패턴을 구별하여 탐지가 가능하였다. 즉, 시스템호출 서열이 순차가 일치하지 않는 침입 패턴에 대한 확률값의 요약정보에 의해 변형된 패턴을 분류하고 탐지할 수 있다.

추후 연구방향으로는 침입 패턴 계보 분류에 대한 프레임 워크에 대한 연구와 베이지안 확률값에 의한 이상 침입 패턴을 평가하는 기준을 제시하고, 이상 침입 패턴을 표현하는 프로파일링 방법을 연구하고자 한다.

참 고 문 헌

[1] Dorothy E. Denning, An Intrusion-Detection Model, IEEE Transaction on Software Engineering, Vol. SE-13, No.2, p222~232, February 1987.

[2] Christina Warrender, Stephanie Forrest, Barak Pearlmutter, "Detecting Intrusion Using System Calls : Alternative Data Models", 1998.

[3] Sreven L. Scott, "A Bayesian Paradigm for Designing Intrusion Detection Systems To Appear in Computational Statistics and Data Analysis", June 20, 2002.

[4] S. Forrest, S. Hofmeyr, A. Somayaji ad T. Longstaff, "A sense of self for unix processes", IEEE Symposium on Security and Privacy, pp. 120~128, 1996.

[5] S. A. Hofmeyr, A. Somayaji and S. Forrest, "Intrusion Detection using Sequences of System Calls", Journal of Computer Security, Vol.6, pp. 151~180, 1998.

[6] Christoper M. Bishop, Neural Networks for Pattern Recognition, Oxford Press, pp. 385~433, 1995.

[7] K. Jain, R. Sekar, "User-Level Infrastructure for System Call Interposition : A Platform for Intrusion Detection and Confinement", 1999.

[8] Mehdi Nassehi, Characterizing Masqueraders for Intrusion Detection, Computer Science/ Mathematics, 1998.

[9] Paolo Garbolino, Franco Taroni, "Evaluation of scientific evidence using Bayesian networks", Forensic Science International 125, pp. 149~155, 2002.

[10] E. Biermann, E. Cloete, L.M. Venter, "A comparison of Intrusion Detection systems", Computers & Security, 20, pp. 676~683, 2001.

[11] Terran Lane, Carla E. Brodley, "An Application of Machine Learning to Anomaly Detection", February 14, 1997.

[12] Terran Lane, Carla E. Brodley, "Temporal

Sequence Learning and Data Reduction for Anomaly Detection", 1999.

[13] 차병래, 박경우, 서재현, "베이지안 방법을 이용한 침입탐지", 한국컴퓨터오에이학회 논문지, p , 2003.

[14] Richard O. Duda, Peter E. Hart, David G. stork, Pattern Classification, 2nd, Wiley, 2001.

[15] Marco Pagni, "Introduction to Patterns, Profiles and Gidden Markov Models", Swiss Institute of Bioinformatics(SIB), August 30, 2002.

◐ 저 자 소 개 ◑

차 병 래

1995년 호남대학교 수학과 졸업(학사)
1997년 호남대학교 대학원 컴퓨터공학과 졸업(석사)
2002년 목포대학교 대학원 컴퓨터공학과 수료(박사)
1997~현재 : 여수대학교 전산학과 시간강사
관심분야 : 정보보호, 컴퓨터 네트워크, 신경망 etc.
E-mail : chabr69@empal.com

박 경 우

1986년 전남대학교 계산통계학과 졸업(학사)
1988년 전남대학교 대학원 전산통계학과 졸업(석사)
1994년 전남대학교 대학원 전산통계학과 졸업(박사)
1995. 3~현재 : 목포대학교 정보공학부 컴퓨터공학 전공 부교수
관심분야 : 분산시스템, 시스템 소프트웨어, 정보보호 etc.
E-mail : kwpark@mokpo.ac.kr

서 재 현

1985년 전남대학교 계산통계학과 졸업(학사)
1988년 중앙대학교 대학원 전자계산학과 졸업(석사)
1996년 전남대학교 대학원 전산통계학과 졸업(박사)
1996. 9~현재 : 목포대학교 정보공학부 정보보호 전공 부교수
관심분야 : 시스템 및 네트워크 보안, 컴퓨터 네트워크, 네트워크 관리 etc.
E-mail : jhseo@mokpo.ac.kr