2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

베이지안 네트워크를 이용한 비정상행위 탐지 기법 연구

정일안, 김민수, 노봉남
전남대학교 전산학과
e-mail:mir@athena.chonnam.ac.kr

A Study of Anomaly Detection Method Using Bayesian Network

Il-An Cheong, Min-Soo Kim, Bong-Nam Noh
Dept of Computer Science, Chonnam National University

요약

일반적으로 비정상행위를 탐지하는데 통계적인 기법을 사용하여 왔다. 본 논문에서는 통계적인 기법의 단점을 보완하기 위해 베이지안 네트워크(Bayesian Network)의 장점들을 이용한 비정상행위에 대한 판정 및 분석에 효과적인 방법을 연구하고자 한다. 리눅스 시스템의 감사자료(LSM audit data)로부터 사용자의 정상행위에 대해 베이지안 네트워크 학습에 효율적인 Sparse Candidate 알고리즘을 사용하고, 감사자료의 일부가 결여되어 있는 경우에도 추론이 가능하도록 Gibbs Sampling 방법을 적용하여 시스템 사용자의 비정상행위를 판정하는데 도움이 되도록 한다.

1. 서 론

기존의 연구들 중에서는 비정상행위를 탐지하는데 일반적으로 통계적인 기법을 사용하였다. 그러나 이 방법을 사용하게 되면 감사 자료를 통계적인 수치 값으로만 표현하므로 데이터의 손실이 발생할 수 있다는 문제점이 있다. 그리고 감사 자료의 일부가 결여되어 있는 경우에 정상행위에 대해 학습한 프로파일과의 비교에서 비정상행위 판정 여부의 효율성이 떨어지므로 정확한 탐지에 어려움이 있게 된다. 또한, 행위의 인과관계를 알 수 없으므로 시스템 사용자의 비정상행위를 분석하는데 어려움이 있게 된다. 그러나 베이지안 네트워크의 장점들을 이용하게 되면 감사 자료의 일부가 결여되어 있는 경우에도 다양한 추론 알고리즘에 의해 비정상행위를 판정하는데 도움이 될 수 있고, 사용자가 비정상행위를 했을 때 베이지안 네트워크의 인과 관계를 이용하여 그 행위에 대한 타당한 근거를 제시해 주므로 원인 분석을 가능하게 해준다. 따라서 사용자의 비정상행위에 대한 분석에 도움이 될 것으로 기대된다. 또한, 베이지안 네트워크로 구성하게 되면 이전 모델에서보다 이벤트간의 인과관계를 유지하면서 효율적으로 그래프를 재구성하는데 적합하게 된다.

본 논문에서는 리눅스 시스템의 감사자료(LSM)[1]를 이용하여 사용자의 정상행위를 베이지안 네트워크(Bayesian Network)로 학습한 후, 새로운 이벤트 감사자료에 대한 비정상행위 여부를 판정하는데 효과적인 방법을 연구하고자 한다. 감사자료에 대한 사용자의 정상행위 학습은 대규모의 베이지안 네트워크를 구성하는데 효율적인 Sparse Candidate 알고리즘을 사용하고, 감사 자료의 일부가 결여되어 있는 경우에도 추론이 가능하도록 Gibbs Sampling 방법을 적용하여 비정상행위 판정에 도움이 되도록 하고자 한다.

2. 관련 연구

2.1 기존 연구방법

Bayes 이론을 바탕으로 비정상행위를 탐지하기 위한 연구로 Liepins는 확률 모델(Bayes 이론)을 적용하여 misuse와 anomlay 탐지를 하는데 두 가지 접근 방법(frequentist approach와 W&S)에 관한 연구를 하였다[2]. 또한 George Mason 대학의 Center for Secure Information Systems에서는 비정상행위 탐지 시스템에 기반한 ADAM(Audit Data Analysis and Mining)시스템을 제안하였다. 이 시스템에서는

가능한 한 많은 false alarm rate를 감소시키면서 새로운 공격을 탐지하는 비정상행위 탐지 시스템의 능력을 향상시키기 위해 pseudo-Bayes estimators 방법을 사용하였다[3].

2.2 베이지안 네트워크

베이지안네트워크는 광범위한 데이터를 변수간의 관계에 따라 그래프로 표시함으로써 단순히 분류하거나 예측하는데에서 간과할 수 있는 데이터의 특성을 이해할 수 있게 해 준다. 베이지안 네트워크는 변수에 해당하는 노드와 그 노드(변수)들간의 인과관계를 나타내는 간선들로 구성된 DAG(Directed Acyclic Graph)이며 변수들간의 결합확률분포(joint probability distribution)를 효율적으로 표현할 수 있는 그래프 모델이다.

조건부 독립성을 나타내는 DAG를 사용하여 많은 변수들간의 다양한 확률분포를 비교적 축약된 형태로 표현하기 때문에 변수들간의 상관관계를 쉽게 이해하고자할 때 유용하게 쓰인다[4].

2.3 베이지안 네트워크의 이점

모든 변수들간의 의존관계(dependency)를 표현하기 때문에 결측치가 많이 포함된 데이터를 자연스럽게 처리할 수 있고, 성분들간의 인과관계를 알 수 있으므로 특정 조건하에서의 결과를 예측할 수 있도록 해 준다. 또한, 인과관계의 분석에서 모델 자체가 원인(causality)과 확률적의미(probabilitsic semantics)를 표현하고 있기 때문에 사전 지식(prior knowledge)과 학습 데이터를 결합하는데 적합하다. 베이지안 네트워크에 베이즈 통계기법을 적용함으로써 데이터를 나눌 필요가 없으므로 데이터 과대적합(data overfitting)을 막을 수 있다. 따라서, 베이지안 네트워크를 이용하면 성분들간의 인과관계를 이용하여 비정상행위의 근거를 제시해 줄 수 있다. 기존 방법들은 단순한 수치값만을 사용하여 비교하여 비정상행위를 판단하는 정도의 수준에 지나지 않았지만, 베이지안 네트워크를 이용하면 사용자가 비정상행위를 했다고 판정했을 때 타당한 근거를 제시하므로 원인 분석이 가능하게 된다. 따라서 사용자의 비정상행위를 분석하는데 도움이 될 것으로 기대된다. 또한, 베이지안 네트워크로 구성하게 되면 이전 모델에서보다 이벤트간의 인과관계를 유지하면서 효율적으로 그래프를 재구성하기에 적합하다.

2.4 베이지안 네트워크 학습

데이터로부터 베이지안 네트워크를 학습하는 과정은 파라미터 학습과 구조학습로 나누어 생각할 수 있다. 파라미터 학습은 각 노드의 확률을 데이터로부터 학습하는 것이고, 구조학습은 베이지안 네트워크를 구성하는 것이다. 구조학습을 위해 그동안 제시되었던 여러 가지 방법들이 있는데, 그 중에서 탐색과 평가함수(score function)을 이용한 방법을 이용한다. 이 방법은 통계적으로 유도된 평가함수(score function)을 구한 후, 이 함수의 값을 최대로 하는 구조를 선택하는 방법이다. 이런 통계적 평가함수로 가장 많이 쓰이는 것은 베이지안 평가(Bayesian scores)함수와 MDL 평가함수가 있다. 베이지안 평가함수의 가장 큰 특징은 결측치(missing value)가 없는 데이터에서 분리성(decomposability)을 가진다는 점이다. 이런 분리성은 지역적 탐색(local search)를 가능케 한다. 베이지안 네트워크 학습을 최적화하는 경우 베이지안 네트워크의 구조가 데이터에 적합한 정도를 나타내는 점수를 선정한 후 데이터에 가장 적합한 베이지안 네트워크의 구조를 탐색하게 된다. 베이지안 네트워크의 적합도를 나타내는 점수로는 MDL(Minimum Description Length) 계열, BD(Bayesian Dirichlet)계열 등이 있으며 데이터의 개수가 많아지면 두 점수는 점근적으로 같아지게 된다. 점수를 선정한 후 베이지안 네트워크 구조의 학습은 가능한 탐색 공간에서 점수가 가장 좋은 네트워크 구조를 찾는다[5]. 노드의 개수가 증가함에 따라 구조 학습 시간도 지수적으로 증가하는 단점이 있다. 이 문제를 해결하기 위해 각 노드의 부모 노드의 후보를 미리 정해 놓고 이 공간에서만 greedy search를 함으로써 탐색 시간을 줄이고 더 좋은 구조를 찾을 가능성을 높인 Sparse Candidate 알고리즘이 있다[6]. 이 알고리즘에서 Markov Blanket은 그 노드를 다른 노드로부터 확률적으로 조건부 독립으로 만드는 노드들의 집합을 의미하고 다음과 같이 수식으로 표현할 수 있다.

$$P(X_i|BL(X_i)) = P(X_i|X-\{X_i\})$$

여기서, X_i는 i번째 변수, $BL(X_i)$는 X_i의 Markov Blanket이다. 주어진 감사자료 D와 초기 네트워크 구조 S_0, BDe점수를 가정한다. 수렴할 때까지 Markov Blanket을 선정하는 전체 노드에 대한 지역 탐색 단계와 전체 네트워크에 대한 구조 T_n에 포함된 네트워크 구조 중 점수가 높은 베이지안 네트워크 구조 S_n을 탐색하는 전역 탐색 단계를 반복하여 학습한다.

3. 베이지안 네트워크를 이용한 탐지 모델

3.1 비정상행위 탐지 모델 개요

본 논문에서 사용된 비정상행위 탐지를 위한 모델은 그림1과 그림2와 같이 두 가지 모드로 구성되어 있다.

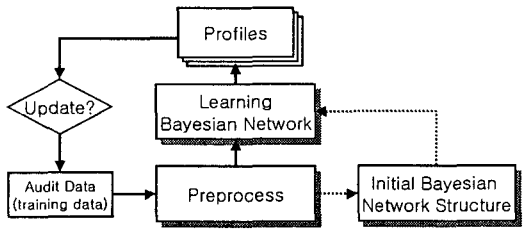

그림 1 Learning Mode

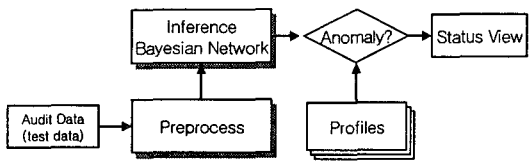

그림 2 Inference Mode

위 모델은 리눅스 시스템의 감사자료(LSM audit data)로부터 베이지안 네트워크를 구성하기 위한 학습 모드(Learning Mode)와 각 사용자의 시스템 사용으로 생성된 감사자료에 대한 비정상행위를 판정하기 위한 추론 모드(Inference Mode)로 구성되어 있다.

3.2 Preprocess

본 논문에서는 표1에서와 같이 시스템 사용자의 행위에 의해 발생하는 시스템 호출번호들 중에서 학습 과정과 비정상행위 판정시에 적절하다고 판단되는 주요 시스템 호출번호만을 선택하여 사용한다.

번호	시스템호출	번호	시스템호출	번호	시스템호출
0	null	33	access	23	setuid
1	exit	37	kill·	24	getuid
2	fork	38	rename	94	fchmod
5	open	39	mkdir	95	fchown
6	close	40	rmdir	182	chown
8	creat	43	times	190	vfork
9	link	46	setgid	1025	socket*
10	unlink	47	getgid	1027	connect*
11	execve	48	signal	1029	accept*
12	chdir	49	geteuid	-번호 항목은 해당 시스템호출번호를 의미함 -시스템호출 항목의 * 표시는 LSM에서 사용자지정 시스템 호출 번호임	
13	time	50	getegid		
15	chmod	61	chroot		
16	lchown	64	getppid		
20	getpid	65	getpgrp		

표 1 주요 시스템 호출

또한 사용자의 시스템 사용시간, 주요 파일 접근, 내외부로부터 접속이 이루어졌을 때의 IP번호 등을 각 사용자별로 분리하여 척도(measure)로 사용한다.

3.3 Learning Mode

학습 모드에서는 사용자가 시스템 사용으로 생성된 감사자료를 전처리 과정을 거쳐 사용자별로 분리하여 학습을 통해 베이지안 네트워크를 구성한다. 베이지안 네트워크를 구성할 때 초기에는 생성된 구조가 없으므로 edge가 없는 구조를 가정(그림1에서 점선으로 표시된 단계)한다. 그리고 Sparse Candidate 알고리즘에 의해 지역 탐색 단계와 전역 탐색 단계를 거쳐 베이지안 네트워크 구조로 학습한다. 생성된 베이지안 네트워크를 각 사용자별로 프로파일을 생성하고, 주기적으로 위와 같은 과정을 반복하여 각 사용자의 프로파일을 갱신한다.

3.4 Inference Mode

추론 모드에서는 사용자의 시스템 사용으로 생성된 감사자료를 학습 모드에서와 같이 전처리 과정을 거친 후, 감사자료의 일부가 결여되어 있는 경우 직접적인 주변확률의 계산이 어렵기 때문에 MCMC(Markov Chain Monte Carlo)의 일종인 Gibbs Sampling 방식으로 간접적인 방법을 사용하여 BDe점수를 계산한다[7]. 여기서 BDe(Bayesian Dirichlet metric)점수는 다음과 같이 표현된다.

$$P(A,S)=$$

$$P(S)\left[\prod_{i=1}^{n}\left\{\prod_{j=1}^{q_i}\frac{\Gamma(\alpha_{ij})}{\Gamma(\alpha_{ij}+N_{ij})}\left(\prod_{k=1}^{r_i}\frac{\Gamma(\alpha_{ijk}+N_{ijk})}{\Gamma(\alpha_{ijk})}\right)\right\}\right]$$

$$\alpha_{ij}\equiv\sum_{k=1}^{r_i}\alpha_{ijk}\qquad N_{ij}\equiv\sum_{k=1}^{r_i}N_{ijk}$$

여기서 A는 감사자료, S는 베이지안 네트워크의 구조이다. n은 학습의 수, q_i는 노드 i의 부모 노드의 집합이 가질 수 있는 상태의 개수이며, r_i는 노드 i의 상태 개수이다. N_{ijk}는 감사자료에서 노드 i가 부모노드의 j번째 상태 하에서 k번째 상태를 가지는 횟수이다. α_{ijk}는 노드 i의 Dirichlet prior이다(여기서는 1.0값을 사용). $P(S)$는 네트워크 구조에 대한 사전확률이다. $\Gamma(\cdot)$함수의 값은 매우 커질 수 있으므로 log함수를 취한 값을 사용한다. 이 단계에서의 베이지안 네트워크 구조 추론은 위에서 계산된 값들 중 BDe점수가 가장 높은 네트워크 구조를 찾는 과정이라 할 수 있다.

4. 비정상행위 판정

테스트 사용자가 시스템 사용으로 생성된 감사자

료를 추론 모드에서 계산된 베이지안 네트워크의 확률값과 학습 모드에서 생성된 해당 사용자의 프로파일의 값을 비교하고 임의로 설정한 임계치(threshold value)를 넘어서는가에 따라 비정상행위 여부를 결정하게 된다. 더 나아가 여러 가지 척도(measure)에 대해 베이지안 네트워크의 인과관계를 이용한 종합적인 분석으로 사용자의 비정상행위를 분석하는데 도움이 될 것으로 기대된다.

5. 결론 및 향후연구

본 논문에서는 베이지안 네트워크의 장점을 이용하여 비정상행위를 판정하는데 효과적인 방법을 연구하였다. 대규모의 베이지안 네트워크를 학습하는데 노드의 수가 증가함에 따라 학습 시간이 증가하는 문제점에 대해 효율적인 Sparse Candidate 알고리즘을 사용하고, 감사자료의 일부가 결여되어 있을 때에도 베이지안 네트워크 추론이 가능하도록 Gibbs Sampling 방법을 적용하였다.

비정상행위 탐지를 위해 학습 모드와 추론 모드로 모델을 구성하였다. 본 논문에서는 리눅스 시스템의 감사자료를 사용하고, 전처리 과정을 거친 후 학습 모드에서 Sparse Candidate 알고리즘을 사용하여 각 사용자에 대한 정상행위를 학습한다. 추론모드에서는 감사자료를 Gibbs Sampling 방법을 통해 추론하고, 학습 모드에서 생성된 프로파일과의 비교로 비정상행위 여부를 판정하고자 하였다.

향후 연구에서는 본 논문에서 제시한 방법을 사용하여 각 사용자에 대한 비정상행위 탐지의 효율성을 실험을 통해 알아보고자 한다.

참고문헌

[1] 박남열, "리눅스 보안 모듈 설계 및 구현," 제1회 정보보호 연구회 논문발표집, 2001.

[2] G. Liepins and H. Vaccaro., "Intrusion detection: Its role and validation," Computeres and Security, 11:247-355, 1992.

[3] Barbara, D., Wu, N., and Jajodia, S., "Detecting Novel Network Intrusions Using Bayes Estimators," Proceedings of the First SIAM Int. Conference on Data Mining, (SDM 2001), Chicago, IL, April 2001.

[4] Heckerman, D., Meek, C., and Coooper, G., "A Bayesian Apraoch to Causal Discovery," Technical Report MSR-TR-97-05, Microsoft Research February, 1997.

[5] Friedman, N. and Goldszmidt, M., "Learning Bayesian networks with local structure, Learning in Graphical Models," pp.421-459, 1998.

[6] Friedman, N., Nachman, I., and Peer, D., "Learning Bayesian network structure from massive dataset: the 'sparse candidate' algorithm," In *Proceedings of UAI'97*.

[7] D. Heckerman. "A tutorial on learning Bayesian networks," Technical Report MSR-TR-95-06, Microsoft Research, Redmond, Washington, 1995.