베이지안 네트워크와 통합 감사 자료를 이용한 사용자의 비정상행위 탐지에 관한 연구

정일안*, 노봉남

*전남대학교, 전산학과

A study of user's anomalous behavior analysis using Bayesian Network and integrated audit data

Il-An Cheong*, Bong-Nam Noh

*Department of Computer Science Chonnam National Univ.

요 약

본 논문에서는 베이지안 네트워크와 통합 감사자료를 이용하여 시스템 사용자에 대한 비정상행위를 탐지하고 분석하는데 효과적인 모델을 제안하고자 한다. 이를 위해 리눅스 시스템에서의 여러 가지 감사자료들을 통합한 감사자료로부터 사용자의 행위에 대해 베이지안 네트워크로 구성하고자 한다. 베이지안 네트워크를 구성할 때 효율적인 학습이 가능한 Sparse Candidate 알고리즘을 적용하고, 감사자료의 일부가 결여되어 있는 경우에도 추론이 가능하도록 MCMC(Markov Chain Monte Carlo)의 일종인 Gibbs Sampling 방법을 적용한다.

I. 서론

사용자가 컴퓨터 시스템을 사용하게 되면 시스템에서는 여기저기에 각종 로그 파일들을 남기게 된다. 그리고 각각의 로그 파일에서 얻을 수 있는 정보와 형태도 다양하다. 이러한 감사 자료들의 정보를 종합하여 분석하면 사용자의 시스템 사용에 대한 행위 분석이 가능하다. 일반적으로 비정상행위를 탐지하는데 통계적인 기법을 사용한다. 그러나 이 방법을 사용하게 되면 감사 자료를 통계적인 수치 값으로만 표현하므로 데이터의 손실이 발생할 수 있다는 문제점이 있고, 행위의 인과관계를 알 수 없으므로 시스템 사용자의 비정상행위를 분석하기가 어렵다. 그러나 베이지안 네트워크의 장점들을 이용하게 되면 감사 자료의 일부가 결여되어 있는 경우에도 다양한 추론 알고리즘에 의해 비정상행위를 판정하는데 도움이 될 수 있고, 컴퓨터 시스템 사용에 대해 사용자가 비정상행위를 했을 때 베이지안 네트워크의 인과 관계를 이용하여 그 행위에 대한 타당한 근거를 제시해 줄 수 있으므로 사용자에 대한 행위 분석을 가능하게 해준다.

본 논문에서는 리눅스 시스템에서의 여러 가지 감사자료들을 통합하여 사용자의 행위를 베이지안 네트워크(Bayesian Network)로 학습한 후, 새로운 이벤트 감사자료에 대해 사용자의 비정상행위 여부를 판정하고 분석하는데 효과적인 방법을 연구하고자 한다. 여러 가지 감사자료들로부터 사용자에 대한 행위 학습은 대규모의 베이지안 네트워크 구조를 구성하는데 효율적인 Sparse Candidate 알고리즘을 사용하고, 실제 사용자의 시스템 사용에 대한 추론은 감사 자료의 일부가 결여되어 있는 경우에도 추론이 가능하도록 Gibbs Sampling 방법을 적용하고자 한다.

II. 본문

1. 기존 연구 방법

지금까지의 기존 연구들 중에서는 베이즈 이론(Bayes thoery)을 적용하여 사용자의 비정상 행위를 탐지하기 위한 시도가 있었다. Liepins는 확률 모델(Bayes 이론)을 적용하여 misuse와 anomlay 탐지를 하는데 두 가지 접근 방법(frequentist approach와 W&S)에 관한 연구를 하였고[1], 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[2].

2. 베이지안 네트워크

1) 베이지안 네트워크의 개념

베이지안 네트워크는 변수들간의 결합 확률 분포(joint probability distribution)를 효율적으로 표현할 수 있는 그래픽 모델로서 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 결합 확률 분포를 효율적으로 표현할 수 있다. 조건부 독립성을 나타내는 DAG를 사용하여 많은 변수들간의 다양한 확률분포를 비교적 축약된 형태로 표현하기 때문에 변수들간의 상관관계를 쉽게 이해하고자할 때 유용하게 쓰인다[3]. 변수 집합 $\mathbf{X}=\{X_1, \ldots, X_n\}$에 대한 베이지안 네트워크는 다음 두 부분으로 구성된다.

(1) 집합 **X**의 변수들간의 조건부 독립 가정(conditional independence assertion)을 표현하는 네트워크의 구조 S

(2) 각 변수들과 연관되어 있는 지역 확률 분포(local probability distribution)집합 P

주어진 구조 S에 대해서 **X**의 결합 확률 분포는 다음과 같이 주어진다.

$$p(x) = \Pi_{i=1}^{n} p(x_i|Pa_i)$$

지역 확률 분포 P는 위의 식의 Π안의 각 항에 대응된다. 결과적으로 확률분포 p(x)를 나타내기 위해서는 (S, P)가 필요하게 된다.

2) 베이지안 네트워크의 이점

모든 변수들간의 의존관계(dependency)를 표현하기 때문에 결측치(missing value)가 많이 포함된 데이터를 자연스럽게 처리할 수 있고, 성분들간의 인과관계를 알 수 있으므로 특정 조건 하에서의 결과를 예측할 수 있도록 해 준다. 또한, 인과관계의 분석에서 모델 자체가 원인(causality)과 확률적 의미(probabilistic 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 측정된 수치값만을 사용하여 비정상행위를 판단하였지만, 베이지안 네트워크를 이용하면 사용자가 비정상행위에 대한 타당한 근거를 제시할 수 있으므로 원인 분석도 가능할 것으로 기대된다. 또한, 베이지안 네트워크로 구성하게 되면 이전 모델에서보다 이벤트간의 인과관계를 유지하면서 효율적으로 그래프를 재구성하는데 적합하게 된다.

3) 베이지안 네트워크 구조의 구성과 학습

베이지안 네트워크의 구조를 구성하는 방법에는 크게 두 가지 방법이 있다. 첫 번째 방법은 사람이 직접 각 변수들간의 인과 관계(causal relationship)를 이용하여 네트워크의 구조를 결정하는 방법이다. 우선 문제 해결에 중요한 변수에 해당하는 노드들을 직접 결정하고, 그 노드들 중 인과 관계가 있다고 생각되는 노드들을 화살표로 연결하는 것이다. 두 번째 방법은 대량의 데이터를 이용해서 네트워크의 구조를 결정하는 방법이다. 이 경우에는 우선 필요한 변수들을 설정하고 이 변수들간의 인과 관계를 대량의 데이터를 이용하여 찾아내는 것이다. 여기에는 각 모델들의 적합도(fitness)를 결정할 수 있는 기준(criterion)이 필요하며 이 기준을 이용해서 필요한 모델들을 찾아낼 수 있는 탐색 기법(searching method)이 필요하다. 베이지안 네트워크 학습을 최적화하는 경우 베이지안 네트워크의 구조가 데이터에 적합한 정도를 나타내는 점수를 선정한 후 데이터에 가장 적합한 베이지안 네트워크의 구조를 탐색하게 된다[4]. 여기에서는 각 노드의 부모 노드의 후보를 미리 정해 놓고 이 공간에서만 greedy search를 함으로써 탐색 시간을 줄이고 더 좋은 구조를 찾을 가능성을 높인 Sparse Candidate 알고리즘을 사용한다[5].

3. 베이지안 네트워크를 이용한 탐지 모델

1) 비정상행위 분석 모델의 개요

본 논문에서 제안한 각 사용자에 대한 비정상행위 분석을 위한 모델은 그림 1과 같이 구성되어 있다.

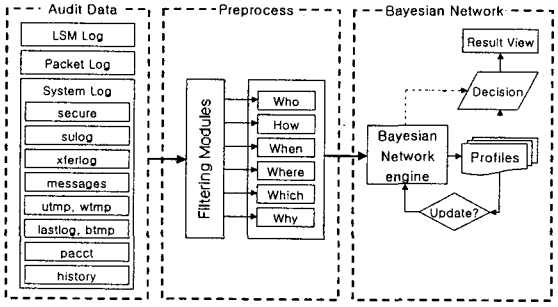

그림 1 비정상행위 분석 모델

제안한 모델은 리눅스 시스템에서의 여러 가지 감사자료들로부터(Audit Data 부분) 필요한 정보만을 5W1H 형식으로 필터링 및 축약하고(Preprocess 부분) 베이지안 네트워크를 구성하기 위한 학습 모드(Learning Mode)와 실제 사용자의 시스템 사용으로 생성된 감사자료에 대해 비정상행위를 분석하기 위한 추론 모드(Inference Mode)로 구성된 Bayesian Network 부분으로 되어 있다.

2) Preprocess

시스템 호출 정보를 기록하는 LSM(LINUX Security Module)[6] 로그와 네트워크의 패킷 정보를 기록하는 Packet 로그, 사용자나 프로세스의 시스템 사용을 기록하고 있는 System log 로그 정보를 감사자료로 하여 필요한 정보만을 5W1H 형식에 맞게 필터링하고 축약한다. 이 정보를 이용하여 베이지안 네트워크를 구성하도록 한다. 표 1은 감사자료를 필터링하고 축약하려는 정보를 나타낸 것이다.

5W1H	how	who	where	which	when	why
Logger Type	Message type	ID	address	protocol	Event time	기타
Packet Logger	Packet의 Flag bit	Source IP, Source MAC address	Dest IP, Dest MAC address	Dest Port, Source Port	Capture time	Data size Packet count 추가 정보
System log Parser	Message name	PID, UID	Incoming host IP address (wtmp)	Daemon name	Syslog time	Message별 추가 정보
LSM Logger	System call Event type	PID, PPID SID, UID	-	Return value	System call Time	System call 별 추가정보

3) Learning Mode

학습 모드에서는 사용자가 정상적인 시스템 사용으로 생성된 감사자료를 전처리 과정을 거쳐 사용자별로 분리하여 학습을 통해 베이지안 네트워크를 구조를 구성한다. 베이지안 네트워크를 구조를 구성할 때 초기에는 생성된 구조가 없으므로 edge가 없는 구조를 가정(그림 2에서 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 사용자에 대한 프로파일을 갱신한다.

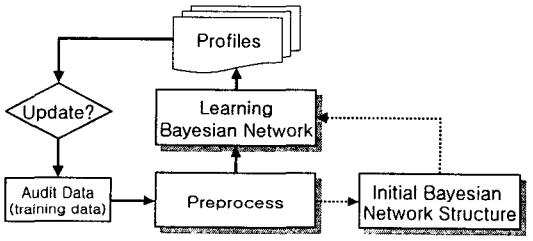

그림 2 Learning Mode

4) Inference Mode

추론 모드에서는 사용자의 시스템 사용으로 생성된 감사자료를 학습 모드에서와 같이 전처리 과정을 거친 후, BDe(Bayesian Dirichlet metric)점

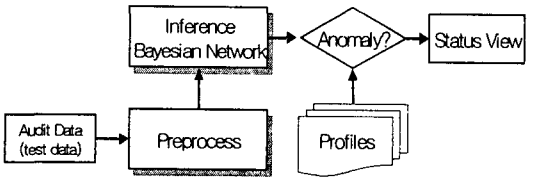

그림 3 Inference Mode

수를 계산한다[7]. 여기서 감사자료의 일부가 결여되어 있는 경우 직접적인 주변확률의 계산이 어렵기 때문에 MCMC(Markov Chain Monte Carlo) 중 간단한 형태의 Gibbs Sampling 방법을 사용한다[8, 9]. BDe점수는 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.

5) 비정상행위 판정

테스트 사용자가 시스템 사용으로 생성된 감사자료를 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. 또한, 베이지안 네트워크의 인과관계를 이용한 종합적인 분석으로 사용자의 행위를 분석하는데 도움이 될 것으로 기대된다.

4. 결론 및 향후연구

본 논문에서는 베이지안 네트워크의 장점과 시스템에서 생성된 각종 감사 자료를 이용하여 사용자의 비정상행위를 분석하는데 효과적인 방법을 제안하였다. 그리고 방대한 양의 감사자료로부터 대규모의 베이지안 네트워크를 학습할 때 노드의 수가 증가함에 따라 학습 시간이 증가하는 문제점에 대해 효율적인 Sparse Candidate 알고리즘을 사용하고, 감사자료의 일부가 결여되어 있을 경우에도 베이지안 네트워크 추론이 가능하도록 Gibbs Sampling 방법을 적용하였다.

본 논문에서는 리눅스 시스템의 여러 가지 감사자료들을 통합하여 사용하고, 전처리 과정을 거친 후 사용자의 행위에 대해 학습하는 학습 모드와 비정상행위를 판정하고자 하는 추론 모드로 구성하였다. 학습 모드에서 Sparse Candidate 알고리즘을 사용하여 각 사용자에 대한 정상행위를 학습하고, 추론모드에서는 감사자료를 Gibbs Sampling 방법을 통해 추론하여 학습 모드에서 생성된 프로파일과의 비교로 비정상행위 여부를 판정하고자 하였다.

향후 연구에서는 본 논문에서 제안한 모델을 적용하여 사용자에 대한 비정상행위 탐지의 효과성과 효율성을 실험을 통해 알아보고자 한다. 그리고 보다 더 효과적으로 사용자의 행위를 분석하는 방법에 대해 연구하고자 한다.

참고문헌

[1] G. Liepins and H. Vaccaro, "Intrusion detection: Its role and validation," *Computers and Security*, vol. 11, pp.247-355, 1992.

[2] 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)*, Apr. 2001.

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

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

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

[6] 박남열, 송춘환, 김정일, 노봉남, "리눅스 보안 모듈 설계 및 구현," 제 1회 정보보호 연구회 논문 발표집, pp.51-54, 2001년 2월.

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

[8] Radford M. Neal, "Probabilistic Inference Using Markov Chain Monte Carlo Methods," *Technical Report CRG-TR-93-1*, Dep. of Computer Science Univ., 25 Sep. 1993.

[9] http://www.mrc-bsu.cam.ac.uk/bugs