Journal of Korean Institute of Intelligent Systems, Vol. 24, No. 5, October 2014, pp. 495-503
http://dx.doi.org/10.5391/JKIIS.2014.24.5.495

베이지안 네트워크 개선을 통한 탐지율 향상의 IDS 모델

IDS Model using Improved Bayesian Network to improve the Intrusion Detection Rate

최보민* · 이정식** · 한명묵***†
Bomin Choi, Jungsik Lee, and Myung-Mook Han†

*한국인터넷진흥원, **국방과학연구소, ***† 가천대학교
*Department of Security Technology Team, Korea Internet & Security Agent
Agency for Defense Development *† Department of Computer Engineering, Gachon University

요 약

최근 보안 분야에서는 네트워크 패킷이나 로그와 같은 네트워크 정보를 수집하고 분석함으로써 네트워크 위협에 대응할 수 있는 침입탐지 시스템에 대한 연구를 활발히 진행되고 있다. 특히, 베이지안 네트워크는 주어진 몇 몇 자료만으로도 정확도 높은 침입에 대한 추론이 가능한 이점으로 이를 이용한 침입탐지 시스템의 모델링 기법들이 이전에도 진행되어 왔다. 그러나 이전 연구들에서는 네트워크 패킷간의 복잡성 문제와 이용되는 패킷 데이터의 연속성 문제를 반영하지 못하고 있기 때문에 높은 탐지정확도 산출에 한계가 있다. 따라서 본 논문에서는 이전 모델들이 갖는 문제들의 개선을 통하여 탐지율을 향상시키기 위해 K-means 클러스터링 기반의 두 가지 방법론을 제안한다. 첫 번째로는 K-means 클러스터링 기반의 정교한 노드구간 범위를 설정방법을 제안하여 연속성 데이터 처리 문제를 개선할 수 있다. 또한, 두 번째로는 K-means 클러스터링 기반으로 산출된 가중치를 학습에 적용하여 보다 견고한 CPT를 산출하여 탐지성능을 향상 시킬 수 있다. 제안하는 방법론들의 성능을 입증하기 위하여 방법론 모두를 적용한 K_WTAN_EM에 대한 탐지율을 이전 모델들과 비교 실험을 수행하였다. 실험 결과 제안하는 모델의 탐지율이 이전의 순수베이지안 네트워크기반(NBN) 모델 보다는 약 7.78%의 향상도를 보였고 트리확장 순수베이지안 네트워크(TAN) 모델 보다는 약 5.24%의 향상도를 산출하여 제안하는 방법의 우수성을 입증하였다.

키워드 : 침입탐지 시스템, 베이지안 네트워크, K-means 클러스터링, 침입 탐지율

Abstract

In recent days, a study of the intrusion detection system collecting and analyzing network data, packet or logs, has been actively performed to response the network threats in computer security fields. In particular, Bayesian network has advantage of the inference functionality which can infer with only some of provided data, so studies of the intrusion system based on Bayesian network have been conducted in the prior. However, there were some limitations to calculate high detection performance because it didn't consider the problems as like complexity of the relation among network packets or continuos input data processing. Therefore, in this paper we proposed two methodologies based on K-menas clustering to improve detection rate by reforming the problems of prior models. At first, it can be improved by sophisticatedly setting interval range of nodes based on K-means clustering. And for the second, it can be improved by calculating robust CPT through applying weighted-leaning based on K-means clustering, too. We conducted the experiments to prove performance of our proposed methodologies by comparing K_WTAN_EM applied to proposed two methodologies with prior models. As the results of experiment, the detection rate of proposed model is higher about 7.78% than existing NBN(Naive Bayesian Network) IDS model, and is higher about 5.24% than TAN(Tree Augmented Bayesian Network) IDS mode and then we could prove excellence our proposing ideas.

Key Words : Intrusion Detection System(IDS), Bayesian Network, K-means Clustering, Intrusion Detection Rate

접수일자: 2014년 1월 14일
심사(수정)일자: 2014년 3월 15일
게재확정일자 : 2014년 9월 13일
† Corresponding author
본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [10044938, 악성코드 프로파일링 및 대용량 보안이벤트 분석을 통한 공격징후 탐지기술 개발]

1. 서 론

침입탐지 시스템은 통신에서 발생하는 네트워크 트래픽이나 패킷 데이터들을 수집하여 분석함으로써 네트워크의 악의적인 행위들을 찾아내는 보안 솔루션이다. 침입탐지에서 주로 이용되고 있는 트래픽이나 패킷 데이터들은 해당 네트워크의 출발지 주소나 발생시간, 서비스 종류 등의 다양한 정보필드로 구성되어 있다. 그렇기 때문에 이들의 속성 정보들을 분석을 통해 네트워크의 비정상 행위에 대한 패턴을 추출해 낼 수 있다. 이러한 네트워크 정보의 특징을 고려하여 볼 때 다양한 정보들을 체계적으로 표현할 수 있는 베이지안 네트워크(Bayesian network)는 침입탐지 모델링에 유리한 이점이 있다.

침입탐지 분야에서 베이지안 네트워크는 몇몇 관측치 만으로도 불확실한 침입의 가능성을 예측할 수 있는 추론기능을 주로 이용하여 네트워크의 정상 또는 비정상 가능성을 판단한다. 또한, 학습기능을 통해 변화하는 공격들의 특징이나 패턴을 추출해 낼 수 있기 때문에 다양한 학습 알고리즘의 적용을 통해 탐지 정확도를 높일 수도 있다. 그러나 이러한 이점에도 불구하고 베이지안 네트워크의 각 노드가 갖는 상호 독립적 특성은 현실세계에서 네트워크 정보들이 상호간에 갖는 관계성을 반영하지 못하는 한계가 있다.

또한 베이지안 네트워크의 각 노드는 네트워크 트래픽이나 패킷과 같은 연속성 데이터들을 다룰 때 이를 범주형 파라미터로 처리하고 있다. 그렇기 때문에 이들 노드 상태의 효율적인 범주 설정에 따라 최적화된 관측치를 입력 받을 수 있다. 따라서 이용되는 데이터들의 특성을 바탕으로 각 노드 상태범주의 구간이 설정되면 보다 정확도 높은 탐지결과를 얻을 수 있을 것이다. 그러나 이전 연구들에서는 노드구간 설정 문제를 고려하지 못하고 있어 침입탐지 모델들이 보다 높은 탐지율을 산출하는 데 있어 한계를 보이고 있다.

따라서 본 논문에서는 기존 베이지안 네트워크 침입탐지 모델의 한계점을 개선하고자 K-means 클러스터링을 활용한 두 가지 방법론을 제안한다. 첫 번째로는 K-means 클러스터링 기반의 정교한 노드구간 범위 설정을 통하여 연속성을 가진 데이터 처리 문제를 개선하고, 두 번째로는 K-means 클러스터링을 기반으로 산출된 가중치를 학습에의 적용하여 각 속성 필드가 갖는 중요성이 반영된 CPT를 구성할 수 있게 한다. 따라서 이 두 가지 방법 모두를 적용할 경우 최종적으로 향상된 탐지율을 가진 침입탐지 모델을 산출해 낸다.

본 논문의 구성으로 2장에서는 제안하는 방법의 배경이 되는 관련연구들을 제시하고, 3장에서는 제안하는 침입탐지 개선 방법론들을 소개한다. 그리고 4장에서는 제안한 방법론들을 적용한 침입탐지 모델을 바탕으로 탐지 실험을 수행하여 기존의 모델들과 성능을 비교 평가 하며, 5장에서는 결론 및 향후 연구방향을 논의한다.

2. 관련 연구

2.1 침입 탐지 모델

침입탐지 시스템은 컴퓨터 시스템의 비정상적인 사용이나 오·남용 등을 규정하는 시스템으로 침입의 시도뿐만 아니라 이미 발생하고 있는 침입자의 악의적 행위를 확인해주는 시스템을 의미한다. 여기에서 의미하는 침입이란 악의적인 목적을 가진 해커가 네트워크나 컴퓨터 시스템 자원의 무결성, 비밀성, 그리고 가용성을 저해하는 행위들의 집합 또는 보안 정책을 파괴하는 행위를 의미한다[1].

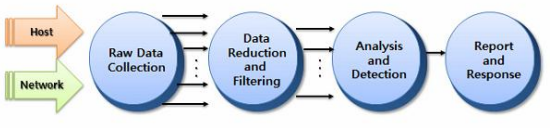


그림 1. 침입탐지 모델의 주요 기능 및 절차
Fig. 1. Main Functionality and Process of Intrusion Detection System

이러한 침입탐지 시스템은 대게 통신에서 발생하는 트래픽이나 패킷정보들을 수집하고 분석하여 공격 패턴을 추출한다. 그리고 공격 패턴이 추출되면 이를 기반으로 침입을 탐지하여 적절한 대응을 취할 수 있게 하고 있다[2]. 침입탐지 시스템의 실행단계로는 그림 1과 같으며 주로 침입 분석 및 탐지 단계가 견고하게 수행되어야 높은 탐지성능을 산출해 낼 수 있다.

2.2 베이지안 네트워크

베이지안 네트워크(Bayesian Network)는 믿음 네트워크(Belief Network)라고도 불리며 베이즈 정리(Bayes' Theorem)의 확률이론과 그래프 이론의 결합으로 만들어진 그래픽 모델이다[3]. 베이지안 네트워크의 구성은 변수를 표현하는 노드(node)와 변수들 간의 의존관계를 표현하는 호(arc)의 방향성 비순환 그래프(Directed Acyclic Graph)로 이루어진다. 또한 각 노드는 부모노드와 자식 노드간의 연관관계가 나타내는 원인과 결과간의 의존도를 조건부 확률표(Conditional Probability Table)를 통해 표현하고 있다[4]. 여기서 베이지안 네트워크를 B라고 정의할 때 B는 (G,θ)로 표현될 수 있으며, 여기서 G는 호의 방향을 통해 노드들 간의 의존성을 표현한 비순환 그래프(DAG)를 지칭한다. 그리고 θ는 G에 포함된 변수들 간의 조건부 확률분포를 기술하고 있는 확률 값들의 집합인 CPT를 의미한다. 이러한 베이지안 네트워크는 복잡한 현실세계의 정보를 체계적으로 시각화 하여 다룰 수 있는 방법론이며 주요기능으로는 추론(inference)기능과 학습(learning)기능이 있으며 다음 절을 통하여 이를 설명한다.

2.2.1 베이지안 네트워크의 추론

베이지안 네트워크의 추론은 어떤 현상의 추이를 직접적으로 재단하지 않고서도 현재 관찰자가 알고 있는 사실과 새로이 관찰된 몇 가지 증거치 간의 상호작용을 바탕으로 해당 대상의 사후확률을 판단한다. 이는 사전확률(prior probability) $P(A)$와 우도확률(likelihood probability) $P(B|A)$가 주어졌을 때 사후확률(posterior probability) $P(A|B)$를 알 수 있는 베이즈이론(Bayes' Theorem)을 기반으로 하고 있다. 베이즈 이론을 바탕으로 한 추론은 각 사건의 독립성과 명확한 사전확률이 요구된다. 그렇기 때문에 매우 복잡한 상황을 해결하는 데에는 한계가 있지만, 좁은 영역의 문제를 해결하는 데에는 유용하다[5]. 식(1)은 베이지안 네트워크 추론의 기반이 되는 베이즈 이론을 수학적으로 표현한 것이다.

$$P(A|B) = \frac{P(A,B)}{P(B)} = \frac{P(A|B)P(B)}{P(B)} \qquad (1)$$

2.2.2 베이지안 네트워크의 학습

베이지안 네트워크의 학습은 주어진 평가 척도에 따라 데이터의 훈련 집합(training set)에 가장 적합한 네트워크를 구하는 것이다[6]. 베이지안 네트워크 학습의 종류에는 주어진 학습 데이터를 이용하여 베이지안 네트워크의 토폴로지(topology)를 구성하는 구조학습(structure learning)과 각 노드마다 설정된 CPT를 구성하는 파라미터학습(parameter learning)의 두 가지로 분류되고 있다. 구조학습은 변수간의 상관관계를 나타내는 호를 데이터로부터 직접 학습하여 네트워크의 전체적인 구조를 설계하고, 파라미터 학습은 각 노드의 확률을 데이터로부터 학습하여 높은 추론치를 산출 할 수 있는 CPT를 구성하는 데 주로 이용되고 있다. 따라서 효율적인 학습을 위해서는 네트워크의 구조나 관찰데이터의 존재 유무에 따라 적합한 학습방법을 선택하여 적용해야 한다. 표 1은 조건에 따라 다르게 적용되는 베이지안 네트워크 학습방법을 표로 정리한 한 것이다[7].

2.3 제안하는 배경

2.3.1 이전 베이지안 침입탐지 모델의 한계

베이지안 네트워크 기반의 침입탐지 방법에는 주로 네트워크 이상탐지에 대한 사전 정보를 이용하여 패킷을 분류하는 Naive Bayes 분류기가 대표적이며 다양한 학습 방법론들이 적용되어 분류기의 정확도를 향상시키기 위한 노력이 선행되어 왔다. F Jemili는 그의 연구에서 Self Adaptive Bayesian Algorithm을 제안하여 시간의 흐름에 따라 변화하는 공격 패턴들을 익히고 분류 정확도 및 false positive 문제를 개선시키고자 하였다.[8]. 그리고 KC Khor는 다양한 방법의 feature selection 방법의 제안을 통해 침입탐지 시스템의 복잡성을 단순화 하고 침입탐지에 가장 영향력 있는 특징들만으로 토폴로지(topology)를 구성하여 탐지 성능을 개선하고자 하였다[9]. F Jemili의 연구에서는 학습을 통한 파라미터의 개선을, KC Khor의 연구에서는 불필요한 정보들을 제거함으로써 침입탐지에 영향력 있는 정보들만을 추출하는 feature selection에 초점을 맞추어 탐지율 향상에 노력을 보여 왔다. 그러나 이들 방법론들은 베이지안 네트워크 노드들 간의 독립성을 기반으로 하고 있는 구조를 바탕으로 하고 있어 현실세계의 복잡성이 반영되지 못한 한계를 보인다.

표 1. 조건에 따라 적용되는 베이지안 네트워크의 학습 방법 분류

Table 1. Under the terms of the classification learning method of Bayesian Network

Method	Structure		Observability	
	Known	Unknown	Full	Partial
Maximum Likelihood Estimation	○		○	
EM(or Gradient Ascent)	○			○
Search Through Model Space		○	○	
EM-Search Through Model Space		○		

이를 개선하기 위해서 Najafi의 연구에서는 TAN(Tree Augmented Naive Bayesian Network) 기반의 침입탐지 모델을 제시함으로써 보다 고차원적인 현실세계의 복잡성을 반영한 모델을 제시하였다[10]. 이는 각 데이터 필드간이 갖는 관계성이 추가된 네트워크 구조로의 확장을 통해 이전 모델들 보다 현실세계에 가까운 침입탐지 모델을 설계하여 탐지율 개선 효과를 보일 수 있었다. 그러나 Najafi의 연구에서는 노드간의 연관성만 반영되었을 뿐, 각각의 노드가 탐지 결과에 영향을 미치는 중요도를 고려하지 못하였다.

2.3.2 노드 상태구간 설정 문제

베이지안 네트워크는 각 노드의 상태 파라미터를 통해 관측치를 입력받는 데, 여기에서 이용되는 데이터의 속성은 범주형과 연속형의 혼합된 형태로 존재한다[11]. 이는 침입탐지에서 주로 이용되고 있는 네트워크 패킷 데이터 속성에도 해당되는 것으로 각 노드의 상태 구간 설정에 따라 추론이나 학습의 효과가 개선될 수 있다. 그러나 이전 연구들에서는 이러한 문제들이 고려되지 못하고 그림 2와 같이 일률적인 간격으로 노드상태의 구간을 설정하여 모델을 설계하였다. 제시된 그림의 노드는 입력되는 네트워크 패킷 데이터가 갖는 범주에 대한 특성이 고려되지 못하고 단순 일정한 간격으로 노드의 상태 파라미터 구간이 설정 되어 있다. 이러한 문제점으로 CPT 구성의 데이터 편중 현상을 야기되고 있기 때문에 탐지 정확도를 저하시키는 원인이 될 수 있다.

2.4 K-means 클러스터링

본 논문에서는 앞서 언급된 베이지안 기반의 침입탐지 모델들의 한계를 개선하고자 K-means 클러스터링을 통한 가중치 학습방법과 노드상태 구간을 정교하게 설정할 수 있는 방법을 제안한다. 다음 2.2.1절의 클러스터링에 대한 개념을 바탕으로 K-means클러스터링 특징과 알고리즘 수행과정을 이해할 수 있다.

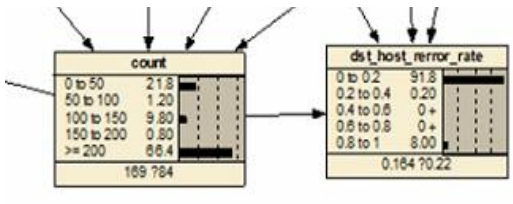


그림 2. 일률적으로 설정된 기존 노드 State의 예제

Fig. 2. An example of the existing node set uniformly

2.4.1 클러스터링

클러스터링(clustering)은 분류되지 않은 집단에 있는 데이터들 간에 유사성을 추출하여 의미 있는 집단들로 분류하는 기법이다. 클러스터링을 통해 생성된 동일한 클러스터 내의 객체들은 유사성을 보이고 서로 다른 클러스터 간의 객체들은 상이성을 보이는 구조적 특징을 가지고 있다. 따라서 클러스터링을 수행하여 객체들은 유사한 객체들 끼리 각각의 클러스터를 형성하는 데 이 과정에서 가장 중요한 것은 객체들 간의 유사도 또는 거리를 측정하는 기준이다.

또한 클러스터링은 비감독 학습(unsupervised learning) 알고리즘에 속하여 학습 데이터의 질에 상관없이 우수한 분류 결과를 얻을 수 있는 이점이 있다. 이러한 클러스터링의 이점을 침입탐지에 이용할 경우 변동가능성이 다분한 네트워크 패킷 데이터들을 분류하거나 이에 대한 패턴을 추출하는데 유용하게 작용할 수 있다.

2.4.2 K-menas 클러스터링

다양한 클러스터링 알고리즘 중에서도 본 논문에서는 분할 접근의 대표적 기법이자 숫자속성(numeric attribute) 데이터를 군집화 하는데 잘 알려진 K-means 클러스터링을 채택하였다. K-means 클러스터링은 객체의 집합 내에 선정된 k개의 중심점(centroid)을 기준으로 그 점에서 가장 근접한 항목들을 각 클러스터에 할당한다. 할당된 모든 노드들의 평균점은 새로운 중심점으로 설정되고 이에 대하여 객체들의 재 할당을 수행한다. 평균점의 변동이 일어나는 동안에는 이 과정을 계속 반복하고 더 이상의 새로운 할당이 일어나지 않으면 이 과정을 중단하고 새로운 중심점을 산출하여 클러스터를 구성한다.

K-means 클러스터링은 직관적이며 계산이 간편한 이점이 있다. 그러나 이용되는 초기 중심점이 클러스터링의 성능에 중대한 역할을 하므로 적절한 초기 중심점의 설정이 중요하다. 클러스터링의 성능은 각 클러스터 내의 거리가 최소화(minimization)되고 각 클러스터 간의 거리가 최대화(maximization)를 가정할 때 가장 높은 성능을 나타내는 것으로 평가될 수 있다. 표 2는 K-means 클러스터링의 수행 과정을 알고리즘화 하여 정리한 것이다.

표 2. K-menas 알고리즘의 수행 과정
Table 2. The process of K-means algorithm

k-means Algorithm

Input: Object Set $X=\{x_1, x_2, \cdots, x_N\}$,
Cluster Number k
Output: Centriod of a Cluster C
Algorithm:

1. initialize the Centriod Set $Z=\{z_1, z_2, \cdots, z_k\}$
2. while(TRUE) {
for ($i=1$ to N)
allocate x_i at the centriod of the closet Cluster.
if (this allocation position equals to allocation position of before) break;
for($j=1$ to k) z
replace z_j as average of samples which is allocated at z_j.
}

3. 탐지율 개선을 위한 제안하는 방법

3.1 제안하는 침입탐지 시스템 모델링

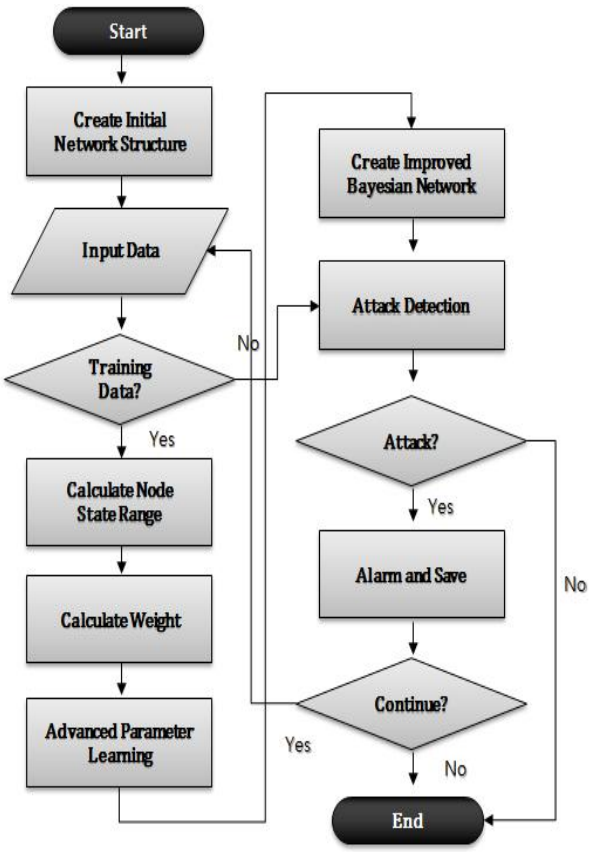


그림 3. 제안하는 침압탐지 모델의 프로세스 처리 흐름도
Fig. 3. Flow chart of proposed intrusion detection model

본 논문에서는 베이지안 네트워크의 노드구간 범위 산출 방법과 각 노드가 지닌 중요성을 반영하기 위한 가중치 적용 학습을 통해 이전 침입탐지 모델들의 한계를 보완하고 탐지율을 개선할 것을 제안하고 있다. 그림 3은 제안하는 침입탐지 모델의 프로세스 처리 흐름을 나타낸 것이다.

침입탐지 모델의 프로세스가 시작되면 초기 침입탐지 네트워크를 형성한다. 초기 네트워크 설정시 네트워크의 구조는 Khor의 연구에서 제시된 feature selection과 Najafi에서 제안된 현실세계를 보다 고차원 적으로 반영한 베이지안 네트워크의 확장모델인 TAN구조를 기본으로 한다.

초기 네트워크가 생성되면 데이터를 입력 받게 되는데, 입력 데이터는 test 데이터와 training 데이터의 두 가지가 있다. training 데이터로 판단되는 경우에는 이를 분석하여 K-means 클러스터링 기반의 노드구간 범위와 가중치를 산출하고 산출된 가중치는 학습에의 적용되어 보다 견고한 CPT를 산출할 수 있게 된다. 또한, test 데이터로 판별된 데이터들은 침입탐지를 수행하며 공격으로 의심되는 경우

에는 관리자에게 이를 보고하고, 이상 데이터는 데이터 저장소에 보관되어 향후 learning 데이터로 이용될 수 있다. 본 프로세스는 다음 패킷 데이터의 입력이 끝날 때까지 지속적으로 반복 수행되며 더 이상의 입력이 없을 경우 종료된다.

3.2 제안하는 방법

3.2.1 정교한 노드구간 범위산출

실세계의 트래픽이나 패킷과 같은 네트워크 정보를 담은 데이터들은 수치의 연속성을 띄고 있다. 그렇기 때문에 이들을 이산화 하는 것은 매우 중요한 문제이다. 여기에서 의미하는 이산화란, 구간 $[x_1, x_n]$을 가질 수 있는 도메인 값 N에 대하여 중복되지 않는 m개의 구간을 나누는 과정을 의미한다. 일반적으로 이러한 연속성 데이터들을 이산화 문제는 기계학습이나 데이터마이닝을 이용한 전처리(pre-processing)과정에서 주로 다루어지고 있다. 그러나 비교적 실시간 처리를 요구하는 침입탐지 시스템의 특성상 이들의 복잡한 연산시간은 성능 저하의 요인이 될 수 있다.

본 논문에서는 이러한 연속성 데이터 처리 문제를 베이지안 네트워크의 특성과 K-means 클러스터링을 이용하여 처리하고자 한다. 베이지안 네트워크에서는 입력되는 데이터가 연속성 특징을 가질 때 각 노드의 상태파라미터가 범위형 변수로 표현 될 수 있다. 그렇기 때문에 데이터가 갖는 구간적 속성을 반영한 정교한 노드구간의 범위 산출을 통해 기존의 복잡한 데이터 이산화 문제를 별도의 전처리를 거치지 않고 처리할 수 있다.

즉, 입력되는 데이터셋(learning dataset)에 포함된 각각의 필드를 하나의 도메인으로 간주하여 볼 때, 각 도메인은 클러스터링을 통하여 k개의 클러스터를 산출하게 된다. 각각의 클러스터는 대게 공격 유형의 분류에 기반한 특성을 갖게 되며, 각 클러스터의 중심이 되는 공간점 p는 서로 다른 도메인의 클러스터를 구분 짓는 경계 값이 될 수 있다. 따라서 클러스터의 변화가 없을 때가지 클러스터링을 수행하여 최종적으로 산출된 p는 각 노드의 상태 구간의 범위로 적용 될 수 있다. 표 3은 제안하는 노드구간 산출 방법을 알고리즘화 하여 정리한 것이다.

표 3. 제안하는 노드구간 범위 산출 알고리즘
Table 3. The proposed algorithm of node interval range

Adjusting node ranges algorithm based on K-means
input: Learning Dataset, number of node state k output: node state range 1. Set k intial average value at the input Dataset (in this paper $k=5$) 2. Calculate similarity d based on of Euclid between k and objects $d = \sum_{i=1}^{k} \sum_{p \in C_i} \lvert p - m_i \rvert^2$ (p: space point of object, m_i: centriod of clusters, C_i: average) 3. Allocate cluster based on d 4. Update $means$ of cluster 5. Repeat step 2.~4. while there are not changes 6. Calculate node state range based on categorical $centroid$ between cluster fields

3.2.2 K-means 클러스터링을 이용한 가중치 산출

ⅰ. 모든 속성들이 서로 독립이다.
ⅱ. 모든 속성들이 동일한 중요도를 갖는다.

베이지안 네트워크는 위의 두 가지 조건을 가정한다. 그러나 현실세계의 데이터는 각 속성들 간에 다양한 관계성을 가지고 있다. 특히 네트워크 데이터 정보를 담은 패킷과 같이 수많은 속성필드를 지닌 데이터들은 각 필드간의 서로 다른 중요도가 그 결과에 영향을 줄 수 있다. 그렇기 때문

표 4. 제안하는 가중치 산출과정
Table 4. The process of proposed weighted value calculation

K-means weighted value calculation algorithm
input: Learning Dataset, number of attack k output: weighted value for the each clusters w_i 1. Set average of k Dataset 2. Calculate similarity d based on Euclid between k and object $d = \sum_{i=1}^{k} \sum_{p \in C_i} \lvert p - m_i \rvert^2$ (p: space point of the object, m_i: centriod of the cluster, C_i: average) 3. Allocate Cluster upon similarity d 4. Update $means$ of cluster 5. Repeat step 2.~4. while there are not changes 6. Calculate node state range based on categorical $centroid$ between cluster fields 7. Calculate weighted value w_i using rank()

에 각각의 노드가 갖는 중요도를 반영한 학습이 이루어질 경우 학습의 질 뿐 아니라 베이지안 네트워크의 추론 성능을 향상시킬 수 있다. 이에 본 논문에서는 K-means 클러스터링을 기반으로 산출된 가중치를 부여한 파라미터 학습 방안을 제안한다.

(1) 제안하는 가중치 산출 방법

본 논문에서는 침입탐지 모델의 탐지 정확도 향상을 위하여 K-means 클러스터링을 통해 산출된 가중치 적용하여 파라미터 학습을 수행한다. 표 4는 제안하는 가중치를 산출 방법의 알고리즘이다. 표 4에 따르면 K-menas 클러스터링은 입력된 훈련 데이터 셋(Learning Dataset)에 대하여 Dos, Probe, R2L, U2R, Normal 공격 유형의 특징에 따라 서로 다른 중심점을 가진 클러스터를 산출한다. 각 공격 유형의 속성에 기반하여 서로 다른 중심점을 갖는 특징 필드들은 분류된 클러스터 내의 중심점 간의 거리를 비교하여 가중치를 산출할 수 있다. 즉, 먼 거리를 갖는 클러스터(특징 필드 또는 노드)일수록 높은 rank의 가중치를 산출할 수 있다. 각 클러스터 내 거리가 최소화 될 때와 각 클러스터 간의 거리가 최대화 되는 조건에 수렴할 때 가장 높은 가중치가 산출될 수 있는데, 이는 클러스터의 특징을 기반으로 하고 있는 것이다. 이렇게 산출된 가중치는 학습에 적용되어 서로 다른 중요도를 갖는 노드를 구성한 베이지안 침입탐지 모델을 산출해 낼 수 있다.

(2) 가중치를 부여한 학습 방법

본 논문의 제안하는 침입탐지 시스템의 학습에는 EM(Expectation Maximization) 학습 알고리즘을 이용한다. EM 학습은 어떤 숨겨진 정보에 대하여 가장 그럴듯한 모델을 추정할 때 효과적인 알고리즘으로 숨겨진 분포함수를 대상으로 최적의 파라미터를 찾아내어 안정적인 CPT 구성을 가능하게 해준다. 이러한 이점을 바탕으로 특정 패킷 데이터 필드의 부재가 발생 가능한 상황을 고려하여 학습에의 EM 알고리즘을 선정하여 적용하였다.

표 5. EM 알고리즘의 수행 과정
Table 5. The process of EM algorithm

EM(Expectation Maximization) Algorithm

Repeat until convergence is reached
{
E step:
In Expectation step if there is a $\theta^{(t)}$, it defines Q expected result of likelihood.
$Q(\theta\|\theta^{(t)}) = E_{Z\|X,\theta^{(t)}}[\log L(\theta;X,Z)]$
$= \sum_{Z} p(Z\|X,\theta^{(t)}) \log L(\theta;X;Z)$
M step:
In Maximization step it calculates new parameter $\theta^{(t+1)}$ which is maximizing Q.
$\theta^{(t+1)} = \arg\max_{\theta} Q(\theta\|\theta^{(t)})$
 	
}

표 5는 EM알고리즘을 정리한 것으로, 먼저 E단계에서는

표 5. EM 알고리즘의 수행 과정
Table 5. The process of EM algorithm

EM(Expectation Maximization) Algorithm

Repeat until convergence is reached
{
E step:
In Expectation step if there is a $\theta^{(t)}$, it defines Q expected result of likelihood.
$Q(\theta\|\theta^{(t)}) = E_{Z\|X,\theta^{(t)}}[\log L(\theta;X,Z)]$
$= \sum_{Z} p(Z\|X,\theta^{(t)}) \log L(\theta;X;Z)$
M step:
In Maximization step it calculates new parameter $\theta^{(t+1)}$ which is maximizing Q.
$\theta^{(t+1)} = \arg\max_{\theta} Q(\theta\|\theta^{(t)})$
 	
}

이미 조성된 베이지안 네트워크를 통해 결여된 데이터들의 값을 모두 추론해 내는 작업을 한다. 결여된 값이 없을 경우에는 기존의 설정된 수치들을 이용하여 기댓값 Q가 정의되는데, 산출된 가중치 w_i는 E단계의 기댓값을 Q를 구하는 공식에 적용되어 학습이 이루어질 수 있다. 산출된 가중치는 기본 Q를 산출하는 과정에서 각 속성 필드 θ_i에 대하여 $\{w|w_i$일 때, $0 < w \leq 1\}$의 조건을 만족하는 w_i를 곱을 해주어 해당 필드 θ_i의 기대치 값을 증가시켜 가중치가 적용된다.

4. 실험 및 평가

4.1 실험 환경

표 6은 본 연구의 실험환경을 표로 정리한 것으로, Intel Core i5 3GHz의 CPU와 8G의 RAM을 사용하였고 Window7 64bit의 운영체제를 기본으로 사용하고 있다. 또

표 6. 실험 환경
Table 6. Experimental environment

CPU	Intel Core i5 3GHz
RAM	8.0 GB
OS	Windows 7 Enterprise(64bit)
S/W	· Netica 5.12 · WEKA 3.6.10
Develope Platform	JDK 1.7.0_45
Dataset	KDD Cup 99 - 10%

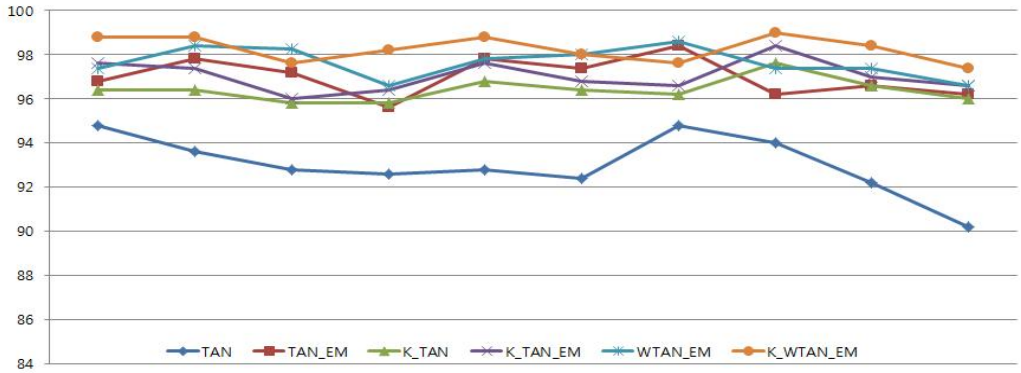


그림 4. 탐지 모델들 간의 정확도 비교
Fig. 4. Comparison of intrusion detection accuracy among detection models

한, WEKA를 이용하여 클러스터링을 산출하였으며 Netica를 이용하여 베이지안 네트워크의 그래픽 모델을 산출할 수 있었다.

4.2 실험 데이터

본 연구에서 수행되는 모든 실험데이터 자료는 KDD Cup 99 데이터 셋을 이용한다. KDD Cup 99는 침입탐지 연구 분야에서 성능평가를 위해 널리 사용되고 있는 데이터 집합으로 총 41개의 특징 필드를 포함하고 있고 정상적인 연결기록과 비정상적인 연결기록을 수집한 네트워크 패킷 데이터 집합이다[12]. 실제 실험에서 사용되고 있는 KDD Cup 99 10% 버전 데이터의 구성은 총 494,021개의 TCP 패킷 연결 정보를 담고 있으며 표 7은 각 공격유형에 따른 데이터의 구성을 표로 정리한 것이다. 또한 본 실험에서는 객관적인 실험평가를 위하여 각 실험 결과의 수치들을 랜덤으로 500개씩 추출한 10개의 실험데이터 셋을 대상으로 10회 수행한 결과의 평균을 산출하여 제시하고 있다.

4.3 제안하는 시스템의 탐지 정확도 측정

본 절에서는 실험을 통하여 제안하는 방법의 우수성을 입증하고자 한다. 실험은 TAN, K_TAN, WTAN_EM, K_WTAN_EM을 대상으로 한다. TAN은 기존 연구에서 제시된 모델로 Najafi의 연구에서 제시된 Tree Augmented Naive Bayesian Network 기반의

표 7. KDD Cup 99 10% 버전 데이터의 구성
Table 7. Composition of KDD Cup 10% data

Attack Type	the number of Attack
DoS	391,458
Probe	4,107
R2L	1,126
U2R	52
Normal	97,278
Total	494,021

IDS 모델이다. 기존 TAN을 개선하고자 K_TAN은 제안하는 노드상태 범위 설정 방법을 적용하였고, WTAN_EM은 제안하는 가중치 산출 방법론을 적용하였다. 마지막으로, 제안하는 두 가지 방법 모두를 적용한 K_WTAN_EM 모델의 정확도 측정 결과를 통해 제안하는 방법의 우수성을 입증 할 수 있었다. 표 8은 실험에 이용되는 모델들의 특징을 정리한 것이다.

실험에서의 정확도 산출은 해당 모델이 정상(normal)과 비정상(abnormal: Dos, Probe, U2R, R2L) 행위를 얼마나 정확히 탐지해 낼 수 있는가를 판단하는 적중률을 이용한다. 적중률의 산출은 식 (2)와 같다.

$$Accuracy\ Rate = \frac{Total\ Number\ of\ Correct\ Classified\ Attributes}{Total\ Number\ of\ Attributes} \quad (2)$$

표 9는 이들 모델들 간의 10회 평균 탐지 정확도 테스트 결과를 보여준다. 10회 평균값을 기준으로 TAN < K_TAN < WTAN_EM < K_WTAN_EM 순으로 적중률이 향상 되었으며, 이전 모델인 TAN보다 제안하는

표 8. 이용되는 침입탐지 모델들의 특징
Table 8. The characteristic of used Intrusion Detection Models

	node setting		applying weighted value
	existing method	proposed method	
TAN	✓		
K_TAN		✓	
WTAN_EM			✓
K_WTAN_EM		✓	✓

표 9. 침입탐지 모델 간의 탐지 정확도 비교 1
Table 9. Comparison1 of intrusion detection accuracy among intrusion detection models

	TAN	K_TAN	WTAN_EM	K_WTAN_EM
1	94.8	96.4	97.4	98.8
2	93.6	96.4	98.4	98.8
3	92.8	95.8	98.28	97.6
4	92.6	95.8	96.6	98.2
5	92.8	96.8	97.8	98.8
6	92.4	96.4	98	98
7	94.8	96.2	98.6	97.6
8	94	97.6	97.4	99
9	92.2	96.6	97.4	98.4
10	90.2	96	96.6	97.4
평균	93.02	96.4	97.648	98.26

(measure: %)

K_WTAN_EM 모델이 평균 적중률 5.648%의 향상된 결과를 산출하였다.

그림 4는 본 연구의 실험에서 사용되는 모든 모델들의 탐지성능을 그래프로 표현한 것이다. 제안하는 두 가지 방법 모두를 적용한 K_WTAN_EM 모델의 그래프가 평균적으로 가장 우위에 위치하고 움직임의 폭이 적은 것으로 보아 성능의 안정성 및 탐지율 개선 효과를 입증하는 바이다.

또한, 표 10은 제안하는 최종모델인 K_WTAN_EM의 T/N(True/Negative), F/N(False/Negative), F/P(False/Positive), T/P(True/Positive) 값을 산출한 것이다.

· T/N(True/Negative): 비정상 중 정상 탐지율
· F/N(False/Negative): 비정상 중 비정상 탐지율
· F/P(False/Positive): 정상 중 비정상 탐지율
· T/P(True/Positive): 정상 중 정상 탐지율

10개 실험 데이터 셋 대상 1개 셋에 포함된 Normal의 개수는 약 96.4개, Abnormal의 개수는 약 403.6개로 구성되어 있다. 표 10에서 약 1% 미만으로 산출된 F/P로 보아 제안하는 시스템의 오탐율에 대한 우수성을 보일 수 있다. 상대적으로 높이 산출된 T/N의 수치로 미탐에는 취약 할 수 있으나, 향후 차단 룰 설정을 통해 개선된 미탐율을 산출할 수 있을 것으로 판단된다.

표 10. K_WTAN_EM모델의 탐지 성능 평가
Table 10. The Detection Performance Evaluation of K_WTAN_EM

Performance	T/N	F/N	F/P	T/P
Average	23.36	2.57	0.49	76.64

(measure: %)

5. 결론 및 향후 연구

5.1 결론

컴퓨터와 스마트 기기의 발전에 따른 네트워크 이용의 증가는 우리 삶의 많은 부분을 편리하게 만들어 주고 있다. 그러나 이에 따라 증가하고 있는 네트워크 패킷의 다양한 정보를 악용하여 네트워크에 연결된 시스템에 침입해 개인의 정보를 위협하거나 서비스를 마비시키는 등의 악의적인 위협과 고역의 발생 빈도 또한 높아지고 있다. 이에 본 연구에서는 몇몇 네트워크 패킷 속성 정보만으로도 공격 유무를 판단하고 각 공격에 대하여 정확도 높은 분류가 가능한 베이지안 네트워크와 이를 개선시키기 위하여 K-means 클러스터링을 이용한 탐지율 개선 방법론을 제안하였다. 즉, 기존 베이지안 침입탐지 모델들의 한계를 개선하고자 'K-means 클러스터링 기반의 정교한 노드상태 설정방법'과 'K-menas 클러스터링 기반 가중치 산출 및 학습에의 적용방법'을 제안하고 방법의 적용을 통해 높은 탐지율을 갖는 침입탐지 모델을 설계하였다.

제안하는 방법의 성능을 검증하기 위하여 이전 모델들과의 비교실험을 통해 탐지율을 평가하였고, 실험결과 제안하는 두 가지 방법 모두를 적용한 K_WTAN_EM 모델이 가장 높은 탐지율과 성능의 안정성을 보였다. K_WTAN_EM 모델의 탐지율은 이전 모델인 순수베이지안 네트워크 기반 모델(NBN) 보다는 약 7.78%를 향상시켰고, 트리확장 순수베지이지안 네트워크 모델(TAN) 보다는 약 5.24%의 향상된 결과를 산출하여 제안하는 방법의 우수성을 입증하였다. 이는 제안하는 방법의 적용이 학습의 질을 개선시켜 보다 정교한 CPT의 구성을 가능하게 하고, 이를 통해 높은 탐지 성능을 산출 할 수 있었음을 의미한다.

5.2 향후 연구

본 연구를 통해 이전보다 향상된 탐지율을 가진 침입탐지모델이 제시되었다. 그러나 네트워크에 대한 위협은 기술의 발전과 함께 끊임없이 진화하고 있기 때문에 지속적으로 확장된 연구가 요구된다. 특히, 베이지안 네트워크 기반의 침입탐지 시스템의 경우 주로 학습을 통하여 탐지율 개선의 연구가 진행되고 있지만 학습 방법론뿐만 아니라 학습 데이터의 질 또한 탐지 성능을 높이는 데 주요 요소가 될 수 있다. 즉, 본 논문에서 이용했던 KDD Cup 99의 경우에도 DoS 공격이 전체 공격 데이터 비율의 80%이상을 차지하고 있어 기타 Probe나 U2R, R2L과 같은 공격 특성의 학습효과가 상대적으로 낮은 학습효과를 보여 왔다. 이에 향후에는 열악한 학습 데이터의 한계를 극복하여 보다 높은 탐지율을 갖는 침입탐지 모델의 연구가 지속되어야 할 것이다.

References

[1] Tsuchiya, Paul F. "The IP Network Address Translator (Nat): Preliminary Design," work in progress, 1991.

[2] Kim Hyun-Woo, Shin Seong-Jun, Lee Seung-Min, and Jeong Seok-Bong, "Network-based Intrusion Detection Scheme using Markov Chin Model," Journal of Decision Science, vol.20, no.1, pp.75-88, Nov. 2012.

[3] Chickering, David Maxwell, "Learning equivalence classes of Bayesian-network structures," *The Journal of Machine Learning Research,* no.2, pp.445-498, 2002.

[4] M. Julia Flores, José A, Gámez, Ana M, Martínez, José M, and PuertaFlores, "Handling numeric attributes when comparing Bayesian network classifiers: does the discretization method matter?," Applied Intelligence, vol.34, no.3, pp.372-385, 2011.

[5] Bayes, Thomas, "An essay toward solving a problem in the doctrine of chances," *Philosophical Transactions of the Royal Society of London 53*, 1984.

[6] Jun-hyeng choi, Joong-bae Kim, Dae-su Kim and Kee-wook Rim, "Bayesian Model for Probabilistic Unsupervised Learning," *Proceedings of KIIS Conference*, vol.11, no.9, pp.849-854, 2011.

[7] Murphy, Kevin. "A brief introduction to graphical models and Bayesian networks," 1998.

[8] Jemili, Farah, Montaceur Zaghdoud, and M. Ben Ahmed, "A framework for an adaptive intrusion detection system using Bayesian network," *Intelligence and Security Informatics*, pp.66-70, 2007.

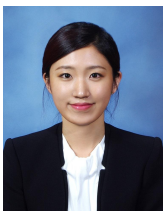
[9] Khor, Kok-Chin, Choo-Yee Ting, and Somnuk-Phon Amnuaisuk, "From feature selection to building of Bayesian classifiers: A network intrusion detection perspective," *American Journal of applied sciences,* vol.6, no.11, 2009.

[10] Najafi, R., and Mohsen Afsharchi. "Network Intrusion Detection Using Tree Augmented Naive-Bayes." *The Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS'12),* 2012.

[11] Ian H. Witten, Eibe Frank, "Data Mining," *Morgan Kaufmann Publishers*, pp.238-246, 2000.

[12] Kayacik, H. Günes, A. Nur Zincir-Heywood, and Malcolm I. Heywood. "Selecting features for intrusion detection: a feature relevance analysis on KDD 99 intrusion detection datasets," *Proceedings of the third annual conference on privacy, security and trust,* 2005.

저 자 소 개



최보민(Bomin Choi)

2014년 2월 : 가천대학교 전자계산학과 석사졸업(공학석사)
2014년~현재 : 한국인터넷진흥원 연구원

관심분야 : Security, Algorithm, Big Data
Phone : +82-2-150-5206
E-mail : bmchoi@kisa.or.kr

이정식 (Jungsik Lee)

1996년 2월 : 숭실대학교 전자계산학과 석사 졸업(공학석사)
1996년~현재 : 국방과학연구소 연구원

관심분야 : Fuzzy, Recognition, Soft Computing
Phone : +82-2-3400-2687
E-mail : godsider@add.re.kr

한명묵(Myung-Mook Han)

1980년 : 연세대학교 공과대학 졸업 (공학사)
1987년 : 뉴욕공과대학교 컴퓨터공학과 석사 졸업 (공학석사)
1997년 : 오사카시립대학교 정보공학부 졸업(공학박사)
1998년~현재 : 가천대학교 IT대학 컴퓨터공학과 교수
1998년~현재 : 한국지능시스템학회 이사

관심분야 : Security, Data Mining, Algorithm
Phone : +82-10-7343-5120
E-mail : mmhan@gachon.ac.kr