퍼지 및 지능시스템학회 논문지 2003, Vol. 13, No. 2, pp. 237-242

SVM과 클러스터링 기반 적응형 침입탐지 시스템

Adaptive Intrusion Detection System Based on SVM and Clustering

이한성* · 임영희** · 박주영*** · 박대희*

Hansung Lee*, Younghee Im**, Jooyoung Park***, and Daihee Park*

* 고려대학교 컴퓨터정보학과

** 대전대학교 컴퓨터정보통신공학부

*** 고려대학교 제어계측공학과

요 약

본 논문에서는 클러스터링을 기반으로 하는 새로운 침입탐지 알고리즘인 Kernel-ART를 제안한다. Kernel-ART는 개념벡터(concept vector)와 SVM(support vector machine)의 머서 커널(mercer-kernel)을 온라인 클러스터링 알고리즘인 ART(adaptive resonance theory)에 접목시킨 새로운 알고리즘으로서 교사학습 기반 침입탐지 시스템의 단점을 극복할 뿐만 아니라, 클러스터링 기반 침입탐지 시스템에서 요구되는 모든 평가 기준들을 만족한다. 본 논문에서 제안하는 알고리즘은 클러스터를 점증적으로 생성함으로써 여러 가지 다양한 침입 유형들을 실시간으로 탐지할 수 있다.

Abstract

In this paper, we propose a new adaptive intrusion detection algorithm based on clustering: Kernel-ART, which is composed of the on-line clustering algorithm, ART (adaptive resonance theory), combining with mercer-kernel and concept vector. Kernel-ART is not only satisfying all desirable characteristics in the context of clustering-based IDS but also alleviating drawbacks associated with the supervised learning IDS. It is able to detect various types of intrusions in real-time by means of generating clusters incrementally.

Key Words : intrusion detection, ART, mercer kernel, concept vector

1. 서 론

인터넷을 이용한 전자상거래가 현대사회의 산업구조에서 점점 더 중요한 위치를 차지하게 됨에 따라 네트워크상의 컴퓨터 및 자원에 대한 위협요소(threat)와 범죄 행위가 나날이 증가하고 있다. 또한, 최근의 해킹(hacking) 및 침입(intrusion) 유형은 그 수나 방법을 예측하기 어려울 정도로 다양해지고 있으며, 해킹 도구들은 일반인들도 쉽게 사용할 정도로 보편화되고 있는 추세이다. 따라서 스스로 새로운 침입 유형을 탐지해내고 탐지 영역을 확장할 수 있는 적응형(adaptive) 침입탐지 시스템에 대한 요구가 증가하고 있다.

전통적인 규칙 기반(rule based) 및 교사학습(supervised learning) 기반의 침입탐지 시스템들은 학습되지 않은 새로운 공격 유형에 대한 침입탐지에 어려움을 가지고 있으며, 새로운 공격 유형이 발견될 때마다 수동으로 규칙 베이스(rule base)를 갱신(update)하거나 시스템을 새롭게 재학습 시켜야 한다는 문제점을 가지고 있다[1][3][4]. 결과적으로 시스템이 새롭게 갱신되지 않는 한, 새로운 공격 유형에 대해서는 무방비 상태에 빠지게 되며, 규칙 베이스를 갱신한다 하여도 또 다른 새로운 침입 유형에 대해서는 대비할 수 없다는 단점을 가지고 있다. 교사학습 기반 침입탐지 알고리즘의 문제점들을 정리하면 다음과 같다[1][3]:

1. 침입탐지를 위해서는 학습과정이 반드시 필요하므로 시스템의 안정적 성능이 나오기까지 많은 비용이 든다.
2. 시스템 학습을 위해 많은 양의 분류되어있는 데이터(labeled data)를 필요로 하며, 학습 데이터의 질에 의해 시스템의 성능이 크게 좌우된다.
3. 현재 침입탐지에 사용되고 있는 많은 알고리즘은 방대한 데이터의 처리(ability in scalable) 및 점증적 학습(incremental learning)을 동시에 수행하기가 어렵다
4. 학습된 데이터 이외의 침입 유형에 대한 탐지 및 침입 유형에 대한 정보 제공이 어려우며, 새로운 침입유형의 발견 시 시스템을 재학습 시켜야 한다.

한편, 비교사 학습 알고리즘인 클러스터링을 이용한 침입탐지 알고리즘들이 최근 학계에서 제안되고 있다[1][3][4]. 침입탐지를 위한 클러스터링 기법은 그 성격상 범용의 클러스터링 기법과는 매우 다르므로, 자체 성격을 잘 반영한 새로운 평가 기준이 요구된다. 다음은 침입탐지를 위한 클러스터링 알고리즘이 가져야하는 특징들을 기술한 것이다:

1. 침입유형의 개수를 예측할 수 없기 때문에 초기 클러스터 개수의 지정 없이 적응적(adaptively)으로 클러스터의 개

접수일자 : 2002년 10월 15일
완료일자 : 2003년 2월 26일
본 과제(결과물)는 정보통신부의 정보통신학술기초연구지원사업(정보통신연구진흥원)으로 수행한 연구 결과입니다.

수를 자동 설정할 수 있어야 한다.
2. 실시간으로 발생하는 이벤트를 처리하여 침입탐지를 수행하여야 하기 때문에, 클러스터링 알고리즘에 입력되는 입력 데이터의 순서(order)에 상관없이 동일한 성능을 보여야 한다.
3. 방대한 양의 데이터 처리가 요구되므로 수렴 속도가 빨라야 하며, 점증적 갱신이 가능하여야 한다.

일반적으로, 인공지능 분야에서 개발된 기존의 클러스터링 알고리즘들은 실시간 처리가 요구되는 대규모 집합에 적용하기 어려우며, 침입탐지를 위해 개발된 최근의 알고리즘들[1][3]도 위의 기준들 중 일부 항목만을 만족하고 있다. 따라서 본 논문에서는 침입탐지를 위한 클러스터링 알고리즘이 갖추어야 할 기본 요건들을 최대한 충족시킬 수 있는 새로운 알고리즘의 개발에 초점을 맞추고 있다. 본 논문에서 제안하는 적응형 침입탐지 시스템은 새로운 침입 유형을 발견하고 이를 시스템에 반영하고자 한다는 점에서는 기존의 연구들[1][3][4][5]과 맥락을 같이한다. 그러나, 본 논문에서 제안하는 방법은 온라인 상의 침입탐지과정에서 직접 새로운 공격유형을 발견하고 이를 시스템에 반영하여 스스로 탐지 능력 및 탐지 범위를 확장한다는 점에서 기존의 연구들과 차별화될 수 있다. 결과적으로 본 논문에서 제안하는 방법은 시스템의 주기적인 갱신이 필요 없는 방법으로 시스템의 유지 보수 측면에서 비용 절감을 가져올 수 있을 뿐만 아니라, 발견되지 않은 침입 유형에 대한 침입 사고를 미연에 방지할 수 있는 새로운 방법론이라 하겠다.

본 논문의 구성은 다음과 같다. 2장에서는 클러스터링 알고리즘의 입력으로 사용될 데이터의 표현 및 유사도함수에 대해 설명한다. 3장에서는 Kernel-ART의 근간을 이루는 개념 벡터와 SVM의 커널 함수에 대해 기술하고, 본 논문에서 새롭게 제안하는 Kernel-ART에 대해 자세히 설명한다. 4장에서는 실험결과 및 분석을 기술한다. 마지막으로 5장에서는 결론 및 향후 연구과제에 대해 논한다.

2. 입력데이터의 표현형태 및 유사도 측정함수

일반적으로 실세계의 데이터들은 여러 가지 속성(attributes)들이 혼합되어 있다. 숫자형 데이터(numeric data) 뿐만 아니라 기호형 데이터(symbolic data)도 침입탐지를 위한 중요한 정보를 가지고 있다는 관점아래 본 논문에서는 두 가지 타입의 데이터를 모두 사용하여 클러스터링의 성능을 높이고자 한다. 즉, n개의 입력데이터 $X=\{\underline{x}_i\}_{i=1}^{n}$, 는 k차원의 실수 영역 데이터와 m 차원의 기호 영역 데이터로 구성된다.

$$\underline{x}_i=\underline{x}_i^R+\underline{x}_i^S;\ \underline{x}_i^R\in R^k, \underline{x}_i^S\in S^m \tag{1}$$

여기서 R^k는 k 차원의 실수 영역을 의미하고, S^m 은 m 차원의 기호 영역을 의미한다. 실수 범위의 데이터들이 서로 다른 항목에 대하여 바이어스(bias)되는 현상을 방지하기 위하여 실수 범위의 데이터에 대하여 L2 정규화를 수행한다.

$$\underline{x}_i^R=\frac{\underline{x}_i^R}{\|\underline{x}_i^R\|};\ \|\underline{x}_i\|=\sqrt{\sum_{j=1}^{k}x_{ij}^2} \tag{2}$$

본 논문에서는 실수형 데이터에 대해서는 코사인(cosine) 유사도를 적용하고, 기호형 데이터에 대해서는 일치하는 항목의 수를 기호형 데이터의 항목수로 나누어 이 둘을 결합하는 유사도 측정 함수를 사용하고자 한다. 유사도 측정 함수의 출력 값은 [0,1]의 범위가 된다.

$$S(\underline{x}_i,\underline{x}_j)=\lambda\cdot\langle\underline{x}_i^R,\underline{x}_j^R\rangle+(1-\lambda)\cdot\frac{\sum_{l=1}^{m}\delta(x_{il}^S,x_{jl}^S)}{m} \tag{3}$$

여기서 m 은 기호형 데이터의 차원이고, λ는 두 유사도 사이의 가중치를 조정하는 변수이며, [0,1]의 범위에서 선택된다. $\delta(\cdot)$는 델타 함수로 아래와 같이 정의된다.

$$\delta(x_{il}^S,x_{jl}^S)=\begin{cases}1, & \text{if } x_{il}^S=x_{jl}^S\\ 0, & otherwise\end{cases} \tag{4}$$

숫자형 두 백터 사이의 각(angle)은 $0\le\theta(\underline{x}_i^R,\underline{x}_j^R)\le1$ 범위이며, 숫자형 데이터는 단위 백터로 정규화 되어 있음으로 두 벡터 사이의 코사인 유사도는 두 백터 사이의 내적(inner product)으로 쉽게 구할 수 있다.

$$\begin{aligned}\langle\underline{x}_i^R,\underline{x}_j^R\rangle &= \|\underline{x}_i^R\|\cdot\|\underline{x}_j^R\|\cdot COS(\theta(\underline{x}_i^R,\underline{x}_j^R))\\ &= COS(\theta(\underline{x}_i^R,\underline{x}_j^R))\end{aligned} \tag{5}$$

3. Kernel-ART

본 장에서는 우선 개념 벡터와 머서 커널에 대한 기본적인 개념에 대하여 설명하고, 이들 개념을 온라인 클러스터링 알고리즘인 ART와 결합시킨 Kernel-ART에 대하여 자세히 설명한다.

3.1 개념 벡터

개념 벡터는 단위 노름(unit norm)을 갖는 클러스터의 중점 벡터를 의미한다. 개념벡터는 각 클러스터에 대해 지역화되므로, 각 클러스터의 중점은 입력 데이터 집합의 구조를 나타낸다[10]. 즉, 각각의 클러스터의 중점은 해당 침입 유형의 데이터 성격을 잘 표현하게 되므로, 본 논문에서는 각각의 클러스터가 해당 침입유형의 대표적인 성격을 표현하도록 하기 위하여 개념 벡터를 사용한다.

입력데이터들이 c개의 클러스터 $\pi_1, \pi_2, \pi_3, \ldots, \pi_c$로 나누어진다고 가정하면 클러스터 π_j의 중점 벡터 $\underline{m}_j$ 는 숫자형 데이터의 중점과 기호형 데이터의 중점으로 다음과 같이 정의된다.

$$\underline{m}_j=\underline{m}_j^R+\underline{m}_j^S;\quad \underline{m}_j^R\in R^k, \underline{m}_j^S\in S^m \tag{6}$$

여기서 $\underline{m}_j^R=\frac{1}{n_j}\sum_{\underline{x}^R\in\pi_j}\underline{x}^R$는 숫자형 데이터 항목에 대한 중점을 의미하고, $\underline{m}_j^S$ 는 기호형 데이터 항목에 대한 중점을 의미한다. 기호형 데이터 항목에 관한 중점은 각 항목 중 가장 빈번히 나타나는 기호를 그 항목의 중점으로 간주한다.

숫자형 데이터 중점을 단위 벡터로 정규화 하여, 정규화 중점 벡터 $\underline{c}_j$를 다음과 같이 정의한다.

$$\underline{c}_j = \frac{\underline{m}_j^R}{\|\underline{m}_j^R\|} + \underline{m}_j^S = \underline{c}_j^R + \underline{m}_j^S \quad ; \ \underline{m}_j^R \in R^k, \ \underline{m}_j^S \in S^m \tag{7}$$

여기서 $\underline{c}_j^R$ 은 개념 벡터이다.

개념 벡터 $\underline{c}_j^R$ 는 다음과 같은 중요한 특성을 갖는다. $R^d \geq 0$ 상의 임의의 단위 벡터 $\underline{z}$ 에 대해, 다음의 Cauchy-Schwarz 부등식을 유도할 수 있다.

$$\sum_{\underline{x} \in \pi_j} \underline{x}^T \underline{z} \leq \sum_{\underline{x} \in \pi_j} \underline{x}^T \underline{c}_j \tag{8}$$

따라서 개념 벡터 $\underline{c}_j^R$ 는 클러스터 π_j 에 속해 있는 모든 벡터들에 대해 가장 근접한 코사인 유사도를 갖는 벡터임을 알 수 있다. 이러한 개념 벡터는 간단한 계산만으로 코사인 유사도나 클러스터의 응집력 등을 계산할 수 있다. 따라서 개념 벡터는 수행 속도에 상당히 민감한 침입탐지 분야에서 클러스터링의 복잡도를 줄여줄 수 있다. 결과적으로 개념 벡터는 앞서 언급한 침입탐지를 위한 클러스터링 알고리즘의 여러 가지 요구 조건들 중 속도의 개선을 만족할 뿐 아니라 클러스터로 표현되는 침입유형들이 잘 구분될 수 있도록 하는 근거를 제시한다.

3.2 머서 커널(mercer-kernel)

머서 커널(mercer-kernel)의 기본적인 아이디어는 다음과 같다. 입력공간(input space)에서 선형 분할(linear separable)이 잘 이루어지지 않는 데이터에 대하여 비선형 함수(nonlinear function)를 통하여 특징공간(feature space)이라는 도트 프로덕트 스페이스로(dot product space) 매핑(mapping)을 하면 선형 분할이 잘 이루어져 선형 함수를 통하여 분류를 할 수 있다는 것이다. 많은 경우 기계학습을 위한 유사도 함수에는 입력 데이터의 내적(inner product)이 사용된다. 이때 입력 데이터를 선형 공간으로 매핑한 후 내적을 구하는 것은 계산 비용이 많이 들기 때문에 입력공간에서 특징 공간의 내적을 직접 계산할 수 있는 커널의 개념을 도입하고 있다[6][7]. 즉, 입력공간에서의 유사도 측정함수의 내적 부분을 커널 함수 $K(\cdot)$로 대치함으로써 특징공간에서의 유사도 측정함수를 얻을 수 있다. 식 (3)의 입력공간에서의 유사도 측정함수에서 내적 부분을 커널 함수 $K(\cdot)$로 대치함으로써 특징공간에서의 유사도 측정함수 식(9)을 얻을 수 있다

$$S(\underline{x}_i, \underline{x}_j) = \lambda \cdot K(\underline{x}_i^R, \underline{x}_j^R) + (1-\lambda) \cdot \frac{\sum_{l=1}^{m} \delta(x_{il}^S, x_{jl}^S)}{m} \tag{9}$$

여기서 RBF (radial basis function) kernel, $K(\underline{x}_i, \underline{x}_j) = \exp\left\{-\frac{1}{c}\|\underline{x}_i - \underline{x}_j\|^2\right\}$ 를 사용하게 되면 특징공간에서의 유사도 측정함수는 다음의 식(10)과 같다.

$$S(\underline{x}_i, \underline{x}_j) = \lambda \cdot \exp\left\{-\frac{1}{c}\|\underline{x}_i^R - \underline{x}_j^R\|^2\right\} + (1-\lambda) \cdot \frac{\sum_{l=1}^{m} \delta(x_{il}^S, x_{jl}^S)}{m} \tag{10}$$

3.3 Kernel-ART

본 절에서는 개념 벡터와 머서 커널을 ART(adaptive resonance theory)모델에 접목한 새로운 점증적 클러스터링 알고리즘인 Kernel-ART을 제안하고자 한다. Kernel-ART는 개념 벡터의 특성상 메모리 측면의 효율성이 높을 뿐만 아니라 클러스터링 수행 후, 각 클러스터의 내용 요약을 위해 별도의 대표 벡터 계산 없이 개념 벡터를 바로 사용하여 클러스터의 레이블링(labeling)을 수행할 수 있다는 장점을 가지고 있다. 한편 머서 커널의 도입은 분류성질이 좋지 않은 데이터에 대해서도 특징 공간으로 데이터를 매핑하여 분류 성질을 높임으로써 발견하기 힘든 패턴의 발견 가능성을 높여준다는 장점을 가지고 있다.

초기화 : 초기 클러스터의 개수를 1로 초기화하고, 입력데이터에 대하여 L2 정규화를 수행한다. 또한 첫 번째 입력 데이터를 초기 가중치 벡터에 할당한다.

$$\underline{w}_1 = \underline{x}_1 = \underline{w}_1^R + \underline{w}_1^S = \underline{x}_1^R + \underline{x}_1^S \tag{11}$$

입력 패턴과 가중치 벡터 사이의 매칭 정도는 코사인 유사도에 의해 측정되므로, 첫 번째 입력 데이터와 초기 클러스터 유닛 사이의 코사인 값은 항상 1이 된다. 따라서 사용자가 어떤 값의 경계 변수($\rho \in [0,1]$)를 주더라도 첫 번째 입력 데이터가 항상 첫 번째 클러스터에 할당됨을 보장할 수 있다.

활성화 함수 : 활성화 함수는 특징공간에서의 유사도 측정함수로서 정의한다.

$$AF(\underline{x}_i, \underline{\hat{w}}_j) = \lambda \cdot \exp\left\{-\frac{1}{c}\left\|\underline{x}_i^R - \underline{\hat{w}}_j^R\right\|^2\right\} + (1-\lambda) \cdot \frac{\sum_{l=1}^{m} \delta(x_{il}^S, w_{jl}^S)}{m} \tag{12}$$

이때 $\underline{\hat{w}}_j$ 는 클러스터 π_j 의 정규화 중점 벡터이며, $\underline{\hat{w}}_j^R = \frac{\underline{w}_j^R}{\|\underline{w}_j^R\|}$ 는 클러스터 π_j 의 개념 벡터이다.

매칭 함수 : 만약 활성화 함수 $AF(\cdot)$와 매칭 함수 $MF(\cdot)$가 다음의 식(13)을 만족하도록 선택되어진다면,

$$MF(\underline{w}_1, \underline{x}_i) > MF(\underline{w}_2, \underline{x}_i) \Leftrightarrow AF(\underline{w}_1, \underline{x}_i) > AF(\underline{w}_2, \underline{x}_i) \tag{13}$$

최대 활성화 함수 값을 갖는 클러스터에 대해 매칭 함수가 경계 변수 조건을 만족하지 않으면 별도의 탐색 과정 없이 곧바로 새로운 클러스터를 생성하고, 해당 입력 패턴을 가중치 벡터로 할당한다[9]. 식(13)의 조건을 만족하는 가장 간단한 매칭 함수의 선택은 활성화 함수를 매칭 함수로 정의하는 것이다.

$$AF(\underline{w}_j, \underline{x}_i) \equiv MF(\underline{w}_j, \underline{x}_i) \tag{14}$$

Resonance 유닛의 선택 : 매칭 함수를 활성화 함수로 정의함으로서 resonance 유닛은 다음과 같이 결정된다.

$$AF(\underline{w}_{j*}, \underline{x}_i) \geq \rho \tag{15}$$

$$\text{where } j* = \arg \max_{j=1,\cdots,c} \{AF(W_j, X_i)\}.$$

만약 최적의 매칭 템플릿(best-matching template)이 경

계변수 조건을 만족하지 않을 경우, 별도의 탐색과정 없이 새로운 클러스터를 생성하고 입력 데이터를 할당하게 된다. 이 조건은 클러스터링 알고리즘 속도의 향상을 가져오는 요인이 된다.

가중치 벡터 갱신 : 식(15)에 의해 클러스터 $j*$ 가 결정되면, 입력 데이터는 클러스터 $j*$ 에 할당되고 다음의 식에 의해 가중치 벡터가 갱신된다.

$$\begin{aligned} \underline{w}_{j*}^{R(i)} &= \underline{w}_{j*}^{R(i-1)} + \underline{x}_i^R \\ \underline{w}_{j*}^{S(i)} &= \textit{Most frequent symbol} \end{aligned} \tag{16}$$

클러스터 $j*$ 의 가중치 벡터는 해당 클러스터에 소속되어 있는 입력 데이터들의 합으로 정의됨으로 가중치 벡터의 학습계수 파라미터(parameter)를 고려하지 않아도 된다. Kernel-ART는 가중치 벡터가 각각의 클러스터에 소속되어 있는 입력 데이터들의 정규화 중점 벡터를 기억하고 있기 때문에 클러스터링 결과가 Fuzzy ART 보다 입력 데이터들의 순서에 덜 민감한 특징을 가지고 있다. 다음의 그림 1은 제안된 알고리즘의 의사 코드(pseudo code)이다.

Step0. Normalize input pattern with L2 norm. Initialize Weights:

$$\underline{w}_1 = \underline{x}_1 = \underline{w}_1^R + \underline{w}_1^S = \underline{x}_1^R + \underline{x}_1^S$$

Step1. While Stopping Condition is false, do Step 2-7

Step2. For each training input, do Step 3-6

Step3. Set activation of all F2 to zero

Step4. Compute Activation Function:

$$AF(\underline{x}_i, \underline{w}_j) = \lambda \cdot \exp\left\{-\frac{1}{c}\,\|\underline{x}_i^R - \underline{\hat{w}}_j^R\|^2\right\} + (1-\lambda)\cdot\frac{\sum_{l=1}^{m}\delta(x_{il}^S, w_{jl}^S)}{m}$$

Step5. Find $j*$ with max activation

Step6. Test for reset:

If $AF(W_{j*}, X_i) \geq \rho$ then

$$\begin{aligned} \underline{w}_{j*}^{R(i)} &= \underline{w}_{j*}^{R(i-1)} + \underline{x}_i^R \\ \underline{w}_{j*}^{S(i)} &= \textit{Most frequent symbol} \end{aligned}$$

else new processing element

allocation: c = c + 1

$$\begin{aligned} \underline{w}_{j*}^{R(i)} &= \underline{w}_{j*}^{R(i-1)} + \underline{x}_i^R \\ \underline{w}_{j*}^{S(i)} &= \textit{Most frequent symbol} \end{aligned}$$

Step7. Test for stopping condition

그림 1. Kernel-ART 알고리즘
Fig. 1. Kernel-ART Algorithm

4. 실험 결과 및 분석

본 논문에서는 침입탐지 알고리즘을 테스트하기 위하여 침입탐지 분야의 연구에서 가장 유명하며, 널리 사용되고 있는 KDD CUP 99 데이터[11][12]를 실험 데이터로 사용한다. 본 데이터는 1998 DARPA Intrusion Detection Evaluation Program에 의해 표준 데이터 집합을 얻기 위하여 미국 군사 네트웍(military network) 상에서 시뮬레이션(simulation)을 통해 만들어진 데이터이다. 본 논문에서는 이 데이터 집합 중 실험의 결과를 정확히 분석하기 위하여 Correct 데이터 집합을 이용하여 실험을 하였다. 테스트용 데이터는 7개의 기호형(symbolic) 속성(attribute)과 34개의 숫자형(numeric) 속성으로 구성되어있다. 클러스터 라벨은(cluster label)은 클러스터링 결과를 분석할 때만 사용하며, 알고리즘 수행 시는 사용되지 않는다. 데이터는 DOS, R2L, U2R, probing 등 크게 4개의 공격 유형으로 구분되며, 세부적인 공격 유형은 총 37이다. 전체 데이터 중 각 공격 유형별 176개 정상 데이터, 총 880개의 데이터를 추출하여 테스트 데이터를 만들어 실험을 수행하였다.

4.1 다른 클러스터링 알고리즘과의 성능 비교

본 실험은 Kernel-ART의 클러스터링 알고리즘 자체의 성능을 평가하기 위하여 다른 클러스터링 알고리즘과의 성능을 비교한 결과이다. 본 실험을 위해서 Kernel-ART 외에 K-Means 알고리즘, Fuzzy-ART에 대한 실험을 수행하였다. 각 실험은 기본 성능 테스트 및 분류 성능 테스트를 수행하여 그 결과를 나타내었다. 실험결과에서 DR은 탐지율, FP는 False Positive 오류율을 의미하며, FN은 False Negative 오류율을 의미한다. 각 알고리즘별 실험 조건은 표 1에 요약 정리하였으며, 표 2는 기본 성능 테스트 결과를 표 3은 분류 테스트 결과를 보여주고 있다.

표 1. 알고리즘별 실험 조건.
Table 1. The condition of experiments.

K-means	# of cluster = 39, repeat 30 experiments, using min-max normalization
Fuzzy ART	$\alpha = 0.00001$, $\beta = 1.0$, varying ρ from 0.35 to 0.95
Kernel-ART	$\lambda = 0.5$, c from 0.01 to 0.1, varying ρ from 0.35 to 0.95

위의 실험 결과, 기본 성능 면에서는 모든 알고리즘들이 비슷한 성능을 나타내고 있으나 Kernel-ART가 다른 클러스터링 알고리즘 보다 시스템 분류 성능 면에서 뛰어남을 알 수 있다. Kernel-ART의 경우에는 입력 패턴의 순서가 바뀌더라도 인식률에서 큰 차이를 보이지 않는다. 또한 경계 변수와 RBF 커널 함수의 c 변수를 조정함으로서 클러스터의 세분화와 구체적인 클러스터의 생성을 조종할 수 있다.

표 2. 기본 성능 테스트.
Table 2. The experimental results of basic test.

Item / Method	Average			Best		
	DR	FP	FN	DR	FP	FN
K-means	90.62	20.45	9.37	93.89	24.43	6.10
Fuzzy ART $\rho=0.9$	93.96	38.73	6.03	96.73	17.61	3.26
Kernel-ART < > : $\rho=0.9$ $c=0.1$ ( ) : $\rho=0.6$ $c=0.01$	97.74	12.68	5.25	<93.03> (96.87)	<3.40> (19.88)	<6.98> (3.12)

표 3. 분류 성능 테스트
Table 3. The experimental results of extended test.
0 : Normal, 1 : DOS, 2 : R2L, 3 : U2R, 4 : Probing

Item / Method	분류 성능 테스트					
	Average			Best		
K-means	클래스 별 탐지율		정분류율	클래스 별 탐지율		정분류율
	0	79.54	60.08	0	75.56	68.89
	1	55.11		1	64.20	
	2	30.11		2	32.95	
	3	72.15		3	81.81	
	4	82.95		4	96.59	
Fuzzy ART $\rho=0.9$	클래스 별 탐지율		정분류율	클래스 별 탐지율		정분류율
	0	61.26	71.44	0	82.38	82.95
	1	86.36		1	93.75	
	2	30.11		2	62.33	
	3	75.00		3	84.09	
	4	94.31		4	99.43	
Kernel-ART $\rho=0.9$ $c=0.1$	클래스 별 탐지율		정분류율	클래스 별 탐지율		정분류율
	0	87.31	81.41	0	96.59	88.63
	1	90.71		1	93.18	
	2	55.58		2	73.86	
	3	80.77		3	87.50	
	4	98.57		4	100	

4.2 다른 연구와의 성능 비교

Wenke Lee[4] 등은 본 논문에서 사용한 데이터와 상당히 유사한 DARPA 데이터집합에 대하여 그들이 제안한 분류기를 이용하여 실험을 수행하였다. KDD CUP 99년도 우승자인 Dr. Bernhard [12] 는 C5 알고리즘을 이용하여 본 논문에서 사용한 correct 데이터에 대하여 분류실험을 수행하였다. 각각의 실험결과에 대한 비교를 표 4에 정리하였다. KDD CUP 99 데이터는 네트워크 패킷(network packets)을 기반으로 만들어진 데이터이다. 따라서, 호스트 기반의 공격유형(host-based attacks)인 R2L과 U2R은 매우 비슷한 성격을 가지며 정상 데이터와 구별이 어려운 데이터이다. 각 실험결과의 비교는 본 논문에서 제안한 Kernel-ART가 일반적인 분류 성능 면에서 다른 실험 결과에 필적할 뿐만 아니라 특히 유사한 패턴에 대해서는 보다 좋은 분류 성능을 보여준다.

표 4. 다른 연구와의 실험결과 비교
Table 4. Comparison of three experimental results : Wenke Lee's, Dr. Bernhard's and Our method

DR(%) / Class	Wenke Lee	Dr. Bernhard	Kernel-ART
Normal	-	99.5	96.59
Dos	79.9	97.1	93.18
R2L	60.0	8.4	73.86
U2R	75.0	13.2	87.50
Probing	97.0	83.3	100

5. 결론 및 향후 연구과제

본 논문의 주된 공헌은 점증적으로 클러스터를 생성함으로써 실시간으로 여러 가지 침입유형을 탐지하는 강건하고 효율적인 침입탐지 모델의 개발에 있다. 본 논문에서 제안하는 방법은 시스템의 주기적인 갱신이 필요 없는 방법으로 시스템의 유지 보수 측면에서 비용 절감을 가져올 수 있을 뿐만 아니라, 발견되지 않은 침입 유형에 대한 침입 사고를 미연에 방지할 수 있는 새로운 방법론이라 하겠다.

제안된 알고리즘인 Kernel-ART는 점증성과 확장성, 알고리즘의 빠른 수행속도 그리고 입력 데이터의 순서에 민감하지 않은 성질 등 1장에서 언급한 요구사항을 모두 만족할 뿐만 아니라 실험에서 보여준 바와 같이 유사한 패턴의 세분화 능력의 향상 등 클러스터링 관점에서의 성능도 향상시킨 새로운 알고리즘이다. 결과적으로 Kernel-ART는 교사학습 기반의 침입탐지 알고리즘의 가지고 있는 단점을 상당부분 극복하고 있다. 결론적으로 Kernel-ART는 침입탐지 알고리즘의 견지에서 보았을 때 계산의 효율성, 각 공격유형에 대한 정보 제공, 학습되지 않은 침입유형의 발견 등 여러 가지 장점을 가지고 있다.

본 연구의 향후 연구 과제로는 Kernel-ART의 데이터마이닝 분야에 대한 다각적인 적용분야에 대한 연구와 Kernel-ART 알고리즘에 적용할 수 있는 다양한 유사도 측정 방법 및 커널 함수에 대한 연구가 필요하며, 침입탐지시스템에 대한 연구로는 Kernel-ART에 의해서 생성되는 클러스터링 결과를 다각적으로 분석/대응 할 수 있는 방법에 대한 연구가 필요하다.

참고문헌

[1] Leonid Portnoy, Eleazar Eskin, and Salvatore J. Stolfo. "Intrusion detection with unlabeled data

using clustering", *Proceedings of ACM CSS Workshop on Data Mining Applied to Security* (DMSA-2001), Philadelphia, PA: November 5-8, 2001.
[2] Jack Marin, Daniel Ragsdale, and John Shurdu, "A hybrid approach to the profile creation and intrusion detection", *Proceedings of DARPA Information Survivability Conference and Exposition, IEEE*, 2001.
[3] Nong Ye and Xiangyang Li, "A scalable clustering technique for intrusion signature recognition", *2001 IEEE Man Systems and Cybernetics Information Assurance Workshop*, West Point, NY, June 5-6, 2001.
[4] Wenke Lee, Salvatore J. Stolfo, and Kui W. Mok, "A data mining framework for building intrusion detection models", *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, pp. 120-132, 1999.
[5] Jianxiong Luo and Susan M. Bridges, "Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection", *International Journal of Intelligent Systems*, vol. 15, pp. 687-703, 2000.
[6] Nello Cristianini and John Shawe-Taylor, *An introduction to support vector machines and other kernel-based learning methods*, Cambridge University PRESS, 2000.
[7] Mark Girolami, "Mercer kernel based clustering in feature space", *IEEE Transactions on Neural Networks*, vol. 13, no. 4, pp. 780-784, 2002.
[8] Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers, 2001.1.
[9] A. Baraldi and E. Chang, "Simplified ART : A new class of ART algorithms", International Computer Science Institute, TR 98-004, 1998.
[10] I. S. Dhillon and D. S. Modha, "Concept decomposition for large sparse text data using clustering", Technical Report RJ 10147(95022), IBM Almaden Research Center, 1999.
[11] KDD CUP 1999 DATA, Available in http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html and http://www-cse.ucsd.edu/users/elkan/kdresults.html
[12] Results of the KDD '99 Classifier Learning Contest, Available in http://www-cse.ucsd.edu/users/elkan/clresults.html
[13] 유신근, 이남훈, 심영철, "침입탐지시스템 평가 방법론", *한국정보처리학회 논문집*, vol. 7, no. 11, pp. 3445-3461, 2000.

저 자 소 개

이한성(Han-Sung Lee)
1996년 : 고려대학교 전산학과(학사)
1996년~1999년 : (주)대우엔지니어링 근무
2002년 : 고려대학교 전산학과(석사)
2002년~현재 : 고려대학교 전산학과 박사과정

관심분야 : 기계학습, 데이터마이닝, 인공지능, 인공신경망, SVM, 침입탐지, 퍼지 이론
E-mail : mohan@korea.ac.kr

임영희(Young-Hee Im)
1994년 : 고려대학교 전산학과(학사)
1996년 : 고려대학교 전산학과(석사)
2001년 : 고려대학교 전산학과(박사)
2001년~현재 : 대전대학교 컴퓨터정보통신공학부 강의전담교수

관심분야 : 인공지능, 정보 검색, 텍스트 마이닝, 데이터 마이닝, 데이터베이스 보안
E-mail : yheeim@dju.ac.kr

박주영(Joo-Young Park)
1983년 : 서울대학교 전기공학과(공학사)
1985년 : 한국과학기술원 (공학석사)
1985년 3월~1988년 7월 : 한국전력 월성원자력 발전소 근무
1992년 : University of Texas at Austin 전기 및 컴퓨터공학과(공학박사)
1992년 8월~1993년 2월 : 한국전력 전력경제연구실 근무
1993년 3월~현재 : 고려대학교 제어계측공학과 교수

관심분야 : 신경망, 퍼지 제어, 비선형시스템
E-mail : parkj@korea.ac.kr

박대희(Dai-Hee Park)
1982년 : 고려대학교 수학과(학사)
1984년 : 고려대학교 수학과(석사)
1989년 : 플로리다 주립대학 전산학과(석사)
1992년 : 플로리다 주립대학 전산학과(박사)
1993년~현재 : 고려대학교 컴퓨터정보학과 교수

관심분야 : 인공지능, 지능 데이터베이스, 데이터마이닝, 인공신경망, 퍼지 이론
E-mail : dhpark@korea.ac.kr