

온라인 서포트벡터기계를 이용한 온라인 비정상 사건 탐지

박혜정¹

¹대구대학교

접수 2011년 1월 11일, 수정 2011년 2월 14일, 게재확정 2011년 2월 28일

요약

신호처리 관련 응용문제에서는 신호에서 실시간으로 발생하는 비정상적인 사건들을 탐지하는 것이 매우 중요하다. 이전에 알려져 있는 비정상 사건 탐지방법들은 신호에 대한 명확한 통계적인 모형을 가정하고, 비정상적인 신호들은 통계적인 모형의 가정 하에서 비정상적인 사건들로 해석한다. 탐지방법으로 최대우도와 베イズ 추정 이론이 많이 사용되고 있다. 그러나 앞에서 언급한 방법으로는 로버스트하고 다루기 쉬운 모형을 추정한다는 것은 쉽지가 않다. 좀 더 로버스트한 모형을 추정할 수 있는 방법이 필요하다. 본 논문에서는 로버스트하다고 알려져 있는 서포트벡터기계를 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법을 제안한다.

주요용어: 비정상 사건 탐지, 서포트벡터기계, 온라인서포트벡터기계.

1. 서론

신호처리 관련 응용문제에서 매우 중요한 비정상적인 사건 탐지문제의 학습과정에서는 정상 군집(normal class) 위주의 자료만을 다루게 되고, 학습 후 얻어진 결정함수(decision function)는 주어진 검정자료(test data)가 정상상태를 나타내는 범주 안에 포함되는지 아니면 범주를 벗어나 비정상 군집(abnormal class)에 속하는지를 판단하게 된다. 비정상적인 사건 탐지문제는 단일 군집 분류 문제(one-class classification problems)로 분류되기도 한다. 비정상 신호 탐지문제의 응용 분야로는 은행 중인 기계의 고장진단이나 컴퓨터 보안과 관련한 침입 탐지 시스템(intrusion detection system)과 같은 분야에도 효과적으로 적용될 수 있다.

비정상적인 사건 탐지문제에 대한 고전적인 접근 방법으로는 학습자료를 이용하여 확률밀도함수(probability density function)를 추정한 후, 검정자료에 대한 추정값이 정해진 경계값(threshold value) 미만이 되는 경우에 비정상 군집으로 판정하는 방법이 있다. 즉 결정함수 $f(x) \geq 0$ 이면 정상으로 $f(x) < 0$ 이면 비정상으로 판정하게 된다. 비정상적인 사건을 탐지하기 위한 접근 방법으로 다음과 같이 나눌 수 있다. 첫 번째는 확률밀도함수 p_0 이 알려져 있고 결정영역 $R = \{x \in \chi | p_0(x) > \eta_r\}$ 일 경우이다. 즉 결정함수 $f(x) = p_0(x) - \eta_r$ 이며, η_r 은 경계값이다. r 은 $0 \leq r \leq 1$ 이며 비정상 사건을 탐지할 비율을 의미한다. 여기에서 r 에 따라 η_r 을 조절한다는 것은 쉽지가 않다. 신호처리 관련 응용프로그램에서는 확률밀도함수 p_0 은 일반적으로 잘 알려져 있지 않다. 두 번째는 확률밀도함수 p_0 의 형태는 알려져 있지만 p_0 의 모수들은 모르는 경우이다. 이런 경우에는 학습자료 $\mathbf{x} = \{x_1, \dots, x_m\}$ 은 모수를 추정하기 위해 사용된다. 이 방법은 Duda와 Hart (1973)에서와 같이 학습자료가 클 경우에 효과적이다. 세 번째는 확률밀도함수 p_0 가 알려져 있지 않은 경우에 직접 함수를 추정하는 경우이다

¹ (712-714) 경상북도 경산시 진량읍 내리리 15번지, 대구대학교, 초빙교수. E-mail: hyjpark@daegu.ac.kr

(Silverman, 1986). 이 방법에서도 η_r 을 조절하는 것이 문제이다. 대응되는 검출 방법으로는 최대우도(maximum likelihood)와 베이스 추정 이론(Bayes estimation theory)이 많이 사용되고 있다. 그러나 이러한 방법은 확률밀도함수의 정확한 추정에 기반을 두고 있으므로, 일반적으로 대량의 학습자료를 필요로 한다. 네 번째는 확률밀도함수 p_0 이 알려져 있지 않으면서 결정영역 R 의 모양이 비정상적인 자료를 포함한 학습자료로부터 추정되는 경우에는 경계값이 주어진 r 에 따라 자동적으로 조절되어진다. 그러나 앞에서 언급한 방법들로 로버스트하고 다루기 쉬운 모형을 추정한다는 것은 쉽지가 않다. 좀 더 로버스트한 모형을 추정할 수 있는 방법이 필요하다. 본 논문에서는 로버스트한 모형 추정을 위해서 앞에서 열거된 항목 중 네 번째 경우를 고려하되 학습자료의 개수가 적은 경우도 고려하여 모형을 추정하고자 한다.

제한된 개수의 학습자료가 주어진 경우에는 확률밀도함수의 추정을 이용하여 정상 군집이 존재하는 영역을 간접적으로 구하는 것보다는 정상 군집이 존재하는 영역을 직접적으로 구하는 방법이 오히려 유리할 수 있다. 이러한 접근 방법을 활용한 가장 대표적인 방법으로 서포트벡터 비정상 탐지(support vector novelty detection, SVND)를 들 수 있다. 서포트벡터기계(support vector machine, SVM)는 함수추정과 분류 문제에서 로버스트하다고 이미 알려져 있다. SVM에 대한 소개와 응용에 관한 내용은 Vapnik (1995, 1998), Smola와 Schölkopf (2004), Schölkopf와 Smola (2002), Suykens와 Vandewalle (1999), Suykens 등 (2002), Shim과 Lee (2009), Shim 등 (2009), Hwang (2010), Seok (2010)에 잘 소개되어 있다. SVM을 이용한 비정상 신호 검출 방법은 최근에 주목 받고 있으며 활발히 연구되어지고 있다. SVND에 관한 내용은 Tax과 Duin (1999)에 잘 안내되어 있다. SVND 방법은 결정 경계로부터 멀리 떨어져 있는 영역의 자료에 대해서는 정확히 추정하려는 불필요한 소모를 없애며, 반대로 경계 근처에 위치한 영역의 자료에 대해서는 추정의 정확도를 높이고 있다. 그러나 SVND 모형으로 실시간으로 발생하는 비정상적인 사건들을 탐지하기 위해서는 대량의 학습자료를 요구하게 된다. 본 논문에서는 SVND 방법을 좀 더 확장하여 실시간으로 발생하는 비정상적인 사건들을 탐지하기 위해 온라인 SVM을 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법을 제안한다. 온라인 SVM을 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법은 명확한 통계 모형을 요구하지 않으며 소량의 자료만을 가지고 실시간으로 발생하는 비정상적인 신호를 탐지할 수 있는 특징을 가지고 있다.

본 논문은 다음과 같이 구성되어 있다. 2절에서는 SVM을 이용한 비정상 신호를 탐지하는 방법을 3절에서는 온라인 SVM을 소개하며 4절에서는 온라인 SVM을 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법을 제안한다. 5절에서는 본 논문에서 제안한 온라인 SVM을 이용한 온라인 비정상 신호 탐지 모형을 적용한 실험과 실험의 결과가 있고 마지막 절에서는 본 논문에 대한 결론으로 마무리한다.

2. SVM을 이용한 비정상 사건 탐지

비정상 신호를 탐지하기 위한 가설은 다음과 같다.

$$H_0 : x_i \sim p_0, i = t_0, \dots, t,$$

$$H_1 : x_i \sim p_0, i = t_0, \dots, t-1, \text{ and } x_t \neq p_0$$

여기에서 p_0 은 확률밀도함수이다. 기호 \sim 는 x_i 가 p_0 에 따라 분포되어 있다는 의미이고, 기호 \neq 는 x_i 가 p_0 에 따라 분포되어 있지 않다는 의미이다. 일반적인 해는 결정영역 R 로 구성되어 있으며 다음과 같다.

$$\int_R p_0(x)dx = 1 - r$$

여기에서 $0 \leq r \leq 1$ 이며, H_1 이 참일 때 H_1 을 채택한 비율을 의미한다. 정상과 비정상을 판별하기 위한 규칙은 결정함수 $f(x) \geq 0$ 이면 H_0 을, $f(x) < 0$ 이면 H_1 을 채택하게 된다. 이전에 알려져 있는 비정상적인 사건들을 탐지하는 방법들은 신호에 대한 명확한 통계적인 모형을 가정하고, 비정상적인 신호들은 통계적인 모형의 가정 하에서 비정상적인 사건들로 해석한다. 대응되는 탐지방법으로는 최대우도와 베이지 추정 이론을 많이 사용되고 있다. 그러나 앞에서 언급한 방법으로는 로버스트하고 다루기 쉬운 모형을 추정한다는 것은 쉽지가 않다. 자유롭게 모형을 추정할 수 있는 방법이 필요하다. 본 논문에서는 로버스트하다고 알려져 있는 SVM을 이용하여, 명확한 통계 모형을 요구하지 않는 기법을 적용하고자 한다. 대표적인 방법으로 서포트벡터 비정상 탐지 (Tax과 Duin, 1999)를 들 수 있다.

SVND는 입력 자료 $\mathbf{x} = \{x_1, \dots, x_m\} \in \chi^m$ 이며, $\mathbf{x} \sim p_0$, p_0 은 알려져 있지 않다고 할 때 새로운 입력값 $x \in \chi$ 가 p_0 에 따라 분포될지 안 될지에 관심을 가지고 있다. SVND에서는 결정영역 R 와 실수 b 에 관한 결정함수 $f_x(x)$ 를 고려하고 있으며, 만약 $x \in R$ 이면 $f_x(x) - b \geq 0$ 가 되고 $x \notin R$ 인 경우에는 $f_x(x) - b < 0$ 이 된다. 결정함수 $f_x(x)$ 는 다음에 설명된 두 가지 조건하에서 추정된다. 첫째, 대부분의 학습자료 $\mathbf{x} = \{x_1, \dots, x_m\}$ 은 비정상인 자료를 제외하고 결정영역 R 에 포함되어야 한다. 둘째, χ 에 포함되는 결정영역 R 이 최소가 되도록 해야 한다. R 을 추정하기 위한 방법으로는 결정함수 $f_x(x)$ 의 공간을 커널 함수 $k(\cdot, \cdot)$ 을 활용하여 커널 특징 공간 (kernel Hilbert space) F 로 변환하는 것이다. 일반적으로 잘 알려져 있는 커널은 가우시안 커널로 다음과 같다.

$$k(x_1, x_2) = \exp \left[-\frac{1}{2\sigma^2} \|x_1 - x_2\|_{\chi}^2 \right].$$

$\|f(\cdot)\|_F^2 = \langle f(\cdot), f(\cdot) \rangle_F$ 이다. 모든 $x \in \chi$ 에 대해서 함수 $k(x, \cdot) : \chi \rightarrow R$ 은 F 에 속한다. 또한 어떤 $f(\cdot) \in F$ 에 대해서 새롭게 생성된 속성은 $\langle k(x, \cdot), f(\cdot) \rangle_F = f(x)$ 를 포함한다. SVND 방법은 다음의 최적화 문제로 $f_x(\cdot)$ 을 구한다.

$$\max_{f(\cdot) \in F, \xi_i, b} -\frac{1}{2} \|f(\cdot)\|_F^2 - \frac{1}{vm} \sum_{i=1}^m \xi_i + b$$

단, $f(x_i) - b \geq -\xi_i, \xi_i \geq 0$.

여기서 $0 < v < 1$ 이다. 여유 변수 ξ_i 는 $f(x_i) \geq b - \xi_i$ ($\xi_i \geq 0$)로 표현하며, 함수 $f_x(\cdot)$ 은 학습자료의 적합을 통해서 선택되어진다. 대부분의 x_i 들은 $f(x_i) - b \geq 0$ ($\xi_i = 0$)인 경우를 만족하며 결정영역 R 안에 위치하게 된다. 그러나 일부 x_i 들은 $-\xi_i \leq f(x_i) - b \leq 0$ ($\xi_i > 0$)인 경우가 있다. 이런 경우는 결정영역 R 안에 포함되지 않는 비정상 자료이다. 비정상 자료의 계수는 $\sum_{i=1}^m \xi_i$ 의 최소화를 통해 작은 값이 되도록 유지해야한다. 위의 문제는 쌍대문제 (dual problem)로 유도할 수 있다. 식은 다음과 같다.

$$\min W(\boldsymbol{\alpha}, b) = \frac{1}{2} \sum_{i=1}^m \sum_{j=1}^m \alpha_i \alpha_j k(x_i, x_j) + b(1 - \sum_{i=1}^m \alpha_i)$$

$$\text{단, } \sum_{i=1}^m \alpha_i = 1, \alpha_i \in \left[0, \frac{1}{vm} \right], \forall i. \quad (2.1)$$

여기서 $0 < v < 1$ 이다. 최적의 결정함수는 라그랑제 배수 (Lagrange multiplier) α 와 b 로 구해지며 다음과 같다.

$$f_{\mathbf{x}}(x) = \sum_{i=1}^m \alpha_i k(x, x_i) - b \quad (2.2)$$

정상과 비정상을 판별하기 위한 규칙은 결정함수 $f(x)$ 가 음이면 H_1 을 채택하고 그렇지 않으면 H_0 을 채택하게 된다. 최적의 상황에서 대부분의 α_i 들이 0이고, 이에 대응되는 학습벡터들은 비서포트벡터 (non-support vector, NSV)라고 한다. 또한 $\alpha_i = 1/(vm)$ 에 속하는 학습벡터들은 비경계서포트벡터 (non-margin support vector, NMSV)라고 부르며, $0 < \alpha_i < 1/(vm)$ 에 속하는 학습벡터들은 경계서포트벡터 (margin support vector, MSV)라고 부른다. $v = 1$ 일 때, 식 (2.2)의 $\sum_{i=1}^m \alpha_i k(x, x_i)$ 은 p_0 을 추정하는 Parzen windows (Parzen, 1962)이다. Parzen windows 추정값은 결정영역 R 의 확실한 형태를 기술한다. Parzen windows와 K -근방 이웃 (K -nearest neighbors)에 의해서 근사적인 수렴은 이루어지지만 유한한 표본 집합 상에서의 행동 양상은 SVM에 비해서 성능이 떨어진다. 일반적으로 $v < 1$ 인 경우에는 SVND가 좋은 효과를 얻기 위해서 Vapnik (1995)의 원칙으로부터 유도되어진다. 추정된 기본적인 확률밀도함수를 사용하는 대신에 $f_{\mathbf{x}}(x)$ 를 유도하여 사용한다. SVND는 결정 경계로부터 멀리 떨어져 있는 영역의 자료에 대해서는 정확히 추정하려는 불필요한 소모를 없애며, 반대로 경계 근처에 위치한 영역의 자료에 대해서는 추정의 정확도를 높이고 있다. 그러나 SVND 모형으로 실시간으로 발생하는 비정상적인 사건들을 탐지하기 위해서는 대량의 학습자료를 요구하게 된다. 본 논문에서는 SVND 방법을 좀 더 확장하여 실시간으로 발생하는 비정상적인 사건들을 탐지하기 위해 온라인 SVM을 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법을 제안한다. 온라인 SVM을 이용하여 온라인으로 비정상적인 신호를 탐지하는 방법은 소량의 자료만을 가지고 실시간으로 발생하는 비정상적인 신호를 탐지할 수 있는 특징을 가지고 있다.

3. 온라인 SVM

시점 t 에서 학습자료 $\mathbf{x}_t = \{x_{t-m}, \dots, x_{t-1}\}$ 와 SVND에서의 가중 값 α_t 와 상수 b_t 는 알려져 있다고 가정하자. 학습자료 \mathbf{x}_t 는 시점 t 이전의 m 개의 자료이다. 온라인 SVM을 이용한 온라인 비정상 사건 탐지 (online abnormality detection by online SVM, OAD-SVM) 방법은 시점 t 에서 추정된 값들을 이용하여 시점 $t+1$ 에서의 입력자료 $\mathbf{x}_{t+1} = \{x_{t-m+1}, \dots, x_t\}$ 에 대응되는 새로운 가중 값 α_{t+1} 와 상수 b_{t+1} 을 계산하기 위해 구성되어 있으며, 시점 $t+1$ 에서의 업데이트 단계에서는 학습자료에 새로운 값 x_t 를 추가하고 이전의 값 x_{t-m} 을 제거하여 시점 $t+1$ 이전의 m 개의 자료가 학습자료가 되도록 한다. 처리 절차는 다음과 같다.

- 1) 조합된 학습자료 $\{x_{t-m}, \dots, x_{t-1}\} \cup \{x_t\}$ 에서 $\tilde{\alpha}_t$ 와 \tilde{b}_t 을 구한다. 또한 식 (2.1)에서는 주어진 α_i 의 상한 경계값이 $1/(vm)$ 으로 유지되어 있다. 새로운 값 x_t 가 추가됨으로 상한 경계값을 $1/(v(m+1))$ 으로 바꾸어 준다.
- 2) α_{t+1} 와 b_{t+1} 을 얻기 위해 조합된 학습자료 $\{x_{t-m}, \dots, x_{t-1}\} \cup \{x_t\}$ 에서 x_{t-m} 을 제거한다. 계수 α_c 는 업데이트 시 x_c 에 따라 변화가 생긴다. $c = t$ 일 때의 첫 번째 삽입 업데이트 단계에서는 학습자료에 새로운 자료가 추가되므로 α_c 에 변화가 생기며, $c = t - m$ 일 때의 두 번째 제거 업데이트 단계에서는 기존 자료가 학습자료에서 제거되므로 α_c 에 변화가 생긴다. 첫 번째 삽입 업데이트 단계에서는 $\sum_{i=1}^m \alpha_i = 1$ 을 유지하기 위해서 α_c 의 초기 값을 0로 하며 식 (2.1)의 조건이 만족될 때까지 조정한다. 두 번째 제거 업데이트 단계에서의 α_c 는 0이 되도록 감소시켜야 한다. 나머지 가중 값 $\alpha_i (i \neq c)$ 는 식 (2.1)의 조건을 유지하기 위해서 조정된다.

α 에서의 MSV와 NMSV에 대응되는 $\{t-m, \dots, t-1\}$ 의 집합을 각각 $M(\alpha)$ 와 $N(\alpha)$ 라고 표기하자. 식 (2.1)에서의 손실 함수 W 의 기울기 g_i 는 다음과 같다.

$$g_i = \frac{\partial W}{\partial \alpha_i} = \sum_{j=t-m}^{t-1} \alpha_j k(x_i, x_j) - b, \quad i = 1, \dots, m$$

기울기 g_i 는 $i \in M(\alpha)$ 이면 $g_i = 0$ 이 되고, $i \in N(\alpha)$ 이면 $g_i < 0$ 이 되고 NSV에 대해서는 $g_i > 0$ 이 된다. α 는 다음의 원칙에 따라 조절된다. 첫째, MSV에서는 가중치 α_i 값들의 변화를 허용하지만 기울기 g_i 는 0으로 유지되게 한다. 둘째, NMSV와 NSV에서의 가중치 α_i 는 각각 $1/(vm)$ 와 0로 유지되게 하고 대응되는 기울기는 변화를 허용한다. α 와 b 의 $\Delta\alpha_c$ 에 따른 변화를 살펴보면 NMSV와 NSV에 속하는 x_i 에 대한 α_i 의 값들은 $\Delta\alpha_c$ 에 따라 변화가 없으며, MSV에서는 g_i 가 $\Delta\alpha_c$ 에 따라 변화 없다.

지금부터는 업데이트 과정 중에 MSV와 NMSV, NSV 집합들이 동일한 집합에 머물러 있는 경우와 그렇지 않은 경우로 나누어 $\Delta\alpha_c$ 의 변화를 살펴보자. 먼저 MSV와 NMSV, NSV 집합들이 업데이트가 진행되는 동안에도 동일한 집합에 머물러 있다고 가정한다. α_c 에서 $\Delta\alpha_c$ 의 변화는 MSV의 가중 값 α_i 에 $\Delta\alpha_i : i \in M(\alpha)$ 로 변화가 발생하게 되며, 손실 함수의 기울기 $g_i : i \notin M(\alpha)$ 에 $\Delta g_i : i \notin M(\alpha)$ 로, 상수 b 에 Δb 로 변화가 발생하게 된다. $\Delta\alpha_{MSV}$ 는 $\Delta\alpha_i : i \in M(\alpha)$ 에 대응되는 전체 벡터이다. 온라인 처리 과정을 얻기 위해서는 $\Delta\alpha_{MSV}$ 와 $\Delta g_i : i \notin M(\alpha)$ 의 명확한 관계성을 알아야만 한다. 식 (2.1) 조건 하에서 다음과 같이 정리할 수 있다.

$$\mathbf{Q}_{MSV} \begin{bmatrix} -\Delta b \\ \Delta\alpha_{MSV} \end{bmatrix} = - \begin{bmatrix} 1 \\ \mathbf{k}_{MSV,c} \end{bmatrix} \Delta\alpha_c, \quad \mathbf{Q}_{MSV} = \begin{bmatrix} 0 & \mathbf{1}^T \\ \mathbf{1} & \mathbf{K}_{MSV} \end{bmatrix}. \quad (3.1)$$

여기에서 \mathbf{K}_{MSV} 는 MSV에서의 커널 행렬이며, $\mathbf{k}_{MSV,c}$ 는 MSV와 새로운 입력 자료 x_c 사이의 커널 행렬이다. 식은 다음과 같이 다시 정리할 수 있다.

$$\Delta b = -\beta_b(c)\Delta\alpha_c, \quad \Delta\alpha_j = \beta_j(c)\Delta\alpha_c, \quad (3.2)$$

$$\begin{bmatrix} \beta_b(c) \\ \beta_{MSV}(c) \end{bmatrix} = -\mathbf{Q}_{MSV}^{-1} \begin{bmatrix} 1 \\ \mathbf{k}_{MSV,c} \end{bmatrix},$$

$j \notin M(\alpha)$ 에 대해서는 $\beta_j(c) = 0$ 이다. 식 (3.2)을 식 (3.1)에 대입하면 다음과 같이 $\Delta\alpha_c$ 와 Δg_i 의 관계는 쉽게 확인할 수 있다.

$$\begin{aligned} \Delta g_i &= \gamma_i(c)\Delta\alpha_c, \quad \forall i \in \{1, \dots, m\} \cup \{c\}, \\ \forall i \notin M(\alpha), \gamma_i(c) &= k(s_i, x_c) + \sum_{j \in M(\alpha)} k(x_i, x_j)\beta_j(c) + \beta_b(c), \\ \forall i \in M(\alpha), \gamma_i(c) &= 0. \end{aligned}$$

다음으로 MSV와 NMSV, NSV 집합의 자료들이 업데이트가 진행되는 동안에 집합의 변화가 있다고 가정한다. 즉 NMSV에 속했던 자료가 업데이트가 진행되는 동안 MSV로 이동을 한다든가 아니면 MSV에 속했던 자료가 NMSV나 NSV로 이동했다고 가정한다. MSV에 새로운 자료 x_d 가 추가되었다

고 하자. 식 (3.1)은 다음과 같이 수정된다.

$$\tilde{\mathbf{Q}}_{MSV} \begin{bmatrix} -\Delta b \\ \Delta \boldsymbol{\alpha}_{MSV} \\ \alpha_d \end{bmatrix} = - \begin{bmatrix} 1 \\ \mathbf{k}_{MSV,c} \\ k_{d,c} \end{bmatrix} \Delta \alpha_c,$$

$$\tilde{\mathbf{Q}}_{MSV} = \begin{bmatrix} 0 & \mathbf{1}^T & 1 \\ \mathbf{1} & \mathbf{K}_{MSV} & \mathbf{k}_{MSV,d} \\ 1 & \mathbf{k}_{MSV,d}^T & k_{d,d} \end{bmatrix}$$

모수들을 업데이트하기 위해서는 \mathbf{Q}_{MSV}^{-1} 을 계산해야 한다. \mathbf{Q}_{MSV}^{-1} 은 Herbrich (2002)의 Woodbury formula를 이용하여 다음과 같다.

$$\tilde{\mathbf{Q}}_{MSV}^{-1} = \begin{bmatrix} \mathbf{Q}_{MSV}^{-1} & \mathbf{0} \\ \mathbf{0}^T & 0 \end{bmatrix} + \frac{1}{\gamma_d(d)} \begin{bmatrix} \beta_b(d) \\ \boldsymbol{\beta}_{MSV}(d) \\ 1 \end{bmatrix} \times \begin{bmatrix} \beta_b(d) & \boldsymbol{\beta}_{MSV}^T(d) & 1 \end{bmatrix}. \quad (3.3)$$

식 (3.3)은 자료 x_d 가 $d > \max_{\alpha} M(\boldsymbol{\alpha})$ 이며 MSV 집합에 포함될 때 사용한다. 일반적으로 식 (3.3)에서 0과 1은 $M(\boldsymbol{\alpha})$ 에서 d 가 정렬된 후 삽입되었다는 의미이다. 반대로 자료 x_d 가 MSV 집합에서 제거될 경우의 \mathbf{Q}_{MSV}^{-1} 은 Herbrich (2002)의 Woodbury formula를 이용하여 다음과 같다.

$$\mathbf{Q}_{MSV}^{-1} = [\tilde{\mathbf{Q}}_{MSV}^{-1}]_{\overline{d+1}, \overline{d+1}} - [\tilde{\mathbf{Q}}_{MSV}^{-1}]_{d+1, d+1} [\tilde{\mathbf{Q}}_{MSV}^{-1}]_{\overline{d+1}, d+1} \times [\tilde{\mathbf{Q}}_{MSV}^{-1}]_{d+1, \overline{d+1}}.$$

$[\mathbf{A}]_{a,b}$ 은 벡터 \mathbf{A} 의 a 번째 행과 b 번째 열에 위치한 값을 나타내며, $[\mathbf{A}]_{\overline{a}, \overline{b}}$ 은 벡터 \mathbf{A} 의 a 번째 행과 b 번째 열에 위치한 값을 제거하였음을 의미한다.

4. 온라인 SVM을 이용한 온라인 비정상 사건 탐지

이번 절에서는 비정상 사건 탐지의 기준이 되는 비정상 인덱스 \mathbf{I}_t 를 정의하고자 한다. 시점 t 에서, m 개의 이전 자료 $\mathbf{x}_t = \{x_t - m, \dots, x_t - 1\}$ 을 이용하여 SVND를 학습시켜 $\boldsymbol{\alpha}_t$ 와 b_t 을 계산한다. 비정상 인덱스 \mathbf{I}_t 는 다음과 같다.

$$\mathbf{I}_t = -\log \left[\sum_{i=1}^m \alpha_{i,t} k(x_{t-(m+1)+i}, x_t) \right] + \log [b_t] \quad (4.1)$$

여기에서 α_{i,t_1} ($i = 1, \dots, m$)의 척도는 α_{i,t_2} 와 다르지만 b_t 는 \mathbf{I}_{t_1} 과 \mathbf{I}_{t_2} 사이의 가능한 비교를 만들어 줌으로 α_i 의 척도 요인으로 해석된다. \mathbf{I}_t 의 표준화는 다음과 같다.

$$\mathbf{I}_t = -\log \left[\frac{\langle \mathbf{w}_t, \mathbf{x}_t \rangle}{b_t} \right] = -\log \left[\frac{\|\mathbf{w}_t\|}{b_t} \cos(\widehat{\mathbf{w}_t, \mathbf{x}_t}) \right]$$

여기에서 $\|\mathbf{x}_t\| = 1$ 이며, b_t 는 \mathbf{w} 의 척도 요인이다. $\cos(\hat{\theta}_t) = b_t / \|\mathbf{w}_t\|$ 이라 할 때 \mathbf{I}_t 의 다음과 같이 간소화 시킬 수 있다.

$$\mathbf{I}_t = -\log \left[\frac{\cos(\widehat{\mathbf{w}_t, \mathbf{x}_t})}{\cos(\hat{\theta}_t)} \right]$$

\mathbf{I}_t 는 \mathbf{x}_t 가 학습자료로부터 얼마나 멀리 위치해 있는가를 측정하는 것이다. $\mathbf{I}_t > 0$ 은 $f_{\mathbf{x}_t}(x_t) < 0$ 에 대응된다. 따라서 비정상적인 사건은 $\mathbf{I}_t > 0$ 경우에 탐지된다. 사실상 \mathbf{I}_t 는 경계값 $\eta > 0$ ($\eta \approx -\log(\eta')$),

$\eta' < 1$ ($\eta' \approx 1$)과 비교되며, 경계값 b 를 $\eta'b$ 로 하여 \mathbf{I}_t 의 하한 값에 대응된다. η' 은 일반적으로 0.99이다. 또한 \mathbf{x}_t 는 평균 μ_t 와 공분산 $v_t^2 \mathbf{I}$ 을 가진 가우시안 분포를 따르고, 모수 σ 를 가진 가우시안 커널을 사용한다고 할 때 근사적으로 다음 식을 수반한다.

$$\mathbf{I}_t \geq \eta \Leftrightarrow \frac{\|\mathbf{x}_t - \mu_t\|}{v_t} \geq C \left(\frac{\sigma}{v_t}, \eta, \nu \right).$$

여기에서 $\nu = 1$ 이며 $C(\sigma/v_t, \eta, \nu)$ 는 경계값이 된다. 이와 같은 경우에 본 논문의 검출 방법이 평균이 μ_t 이고 분산이 v_t 인 거리 비교로 구성된 표준 방법 즉 $\|\mathbf{x}_t - \mu_t\|/v_t \geq 3$ 와 동일하다. OAD-SVM 알고리즘은 다음과 같다.

[단계1:초기화]

- m, ν, η 와 $k(\cdot, \cdot)$ 를 선택한다.
- $t \leftarrow m + 1$ 로 설정한다.

[단계2:온라인 검출]

- 입력 자료 $\mathbf{x}_t = \{x_{t-m}, \dots, x_{t-1}\}$ 을 가지고 SVND를 학습시킨다. 학습된 SVND를 통해 $\alpha_{i,t} (i = 1, \dots, m)$ 와 b_t 를 구한다.
 - \mathbf{x}_t 에 대해 식 (4.1)을 이용하여 \mathbf{I}_t 를 구한다. $\mathbf{I}_t \leq \eta$ 이면 x_t 는 정상이고, $\mathbf{I}_t > \eta$ 이면 비정상이다.
 - $t \leftarrow t + 1$ 로 설정한다1.
-

5. 실험

실험에서는 사운드 파일을 이용하여 본 논문에서 제안한 OAD-SVM 모형의 성능을 평가하고자 한다. 제안한 OAD-SVM 모형의 성능 평가를 위해 사용된 사운드 파일은 파일포맷이 Wav인 피아노 연주곡 파일을 이용하였으며, 사운드 파일의 일부를 학습용과 검정용으로 각각 50개의 자료를 사용하였다. 입력 변수 x_i 는 추정하고자 하는 값의 이전 2개의 값으로 하였다. 학습자료를 이용하여 모형을 학습시켰으며, 학습된 모형의 성능 평가를 위해 검정자료에 적용하였다. 또한 검정자료에서는 일정한 간격으로 임의의 값을 추가하여 비정상적인 자료가 발생되도록 하였다. 좀 더 쉽게 확인하기 위해 검정자료의 19, 39번째 자료에 비정상적인 자료가 발생되도록 임의의 값을 추가하였다. 또한 실험에서는 가우시안 커널을 사용하였으며, CV (cross validation) 방법을 이용하여 모형 추정에 결정적인 영향을 주는 벌칙모수와 커널모수의 값을 결정하였다. 실험을 통해 벌칙모수 $1/(vm)$ 은 300, 커널모수 σ 는 0.01로 구해졌다. 비정상 사건 탐지의 기준이 되는 비정상 인덱스 \mathbf{I}_t 는 OAD-SVM 알고리즘을 통해 학습된 후 구해졌다. 비정상 인덱스 \mathbf{I}_t 의 값은 3의 값을 경계로 하였다. 비정상 인덱스 \mathbf{I}_t 의 값이 3보다 큰 경우 ($\mathbf{I}_t > 3$)에는 비정상적인 신호로 그 외에는 정상적인 신호로 구분한다.

제안한 OAD-SVM 모형에 대한 성능 평가 결과는 그림 5.1과 표 5.1에 잘 나타나 있다. 그림 5.1에서의 왼쪽 그림은 학습자료의 실험 결과이며, 오른쪽 그림은 학습 후 검정자료를 이용한 실험 결과이다. 그림 5.1에서는 추정하고자 하는 목표 자료를 점으로 표시하였으며, 제안된 OAD-SVM 모형은 실선으로 표시하였다. 그림 5.1의 오른쪽 그림에서 보면 19번째, 39번째 값이 정상적인 자료에 임의의 값을 추가하여 이상치가 발생한 것을 쉽게 확인할 수 있다. 또한 표 5.1에서는 검정자료를 이용하여 비정상 인덱스 \mathbf{I}_t 의 값을 구한 후 \mathbf{I}_t 의 값이 $\mathbf{I}_t > 3$ 인지 아닌지를 쉽게 확인할 수 있도록 나타내었다. 표 5.1에서는 정상인 경우는 0로 비정상인 경우는 1로 표기하였다. 표 5.1에서도 19번째와 39번째의 자료가 비정상 사건으로 처리되었다.

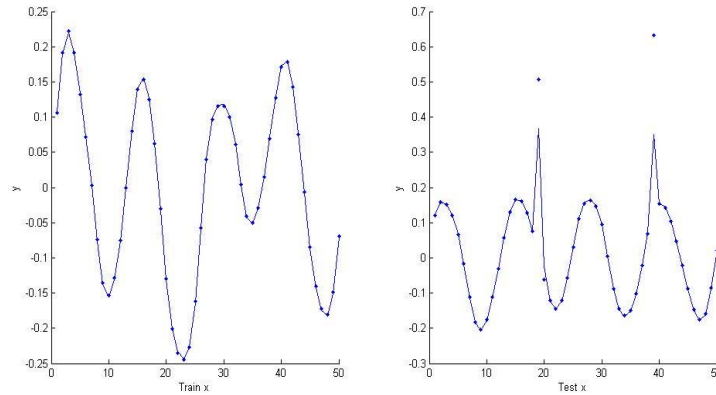


그림 5.1 제안한 OAD-SVM 모형의 추정 결과 (:·: 목표값, 실선: OAD-SVM 모형)

표 5.1 온라인 비정상 사건 탐지 결과 (1: 비정상신호, 0: 정상신호)

I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Sign	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
I	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Sign	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
I	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	
Sign	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	

6. 결론

본 논문에서는 비정상적인 사건 탐지를 위해 SVM을 활용한 온라인 서포트벡터 비정상 사건 탐지방법을 제안하였다. 제안한 모형의 성능을 평가하기 위해 Wav 자료 방식의 사운드 파일을 이용하여 실험하였다. 실험에서는 비정상적인 사건이 발생하도록 하기 위해 임의적으로 2개의 자료 값에 임의의 값을 추가하여 비정상적인 사건이 발생하도록 조정하였다. 실험의 결과는 그림 4.1과 표 4.1을 통해 확인할 수 있다. 그림 4.1의 오른쪽 그림을 보면 검정자료 19, 39번째에서 비정상적인 사건이 발생하였음을 알 수 있으며, 본 논문에서 제안한 OAD-SVM 모형을 통해 추정된 값이 허용범위보다도 더 많이 벗어남으로 비정상적인 자료로 감지되었다. 표 4.1에서는 비정상 인덱스 I_t 를 기준 경계값과 비교하여 경계값보다 큰 값들을 비정상적인 신호 1로 표기하도록 하였다. 표 4.1을 통해 19, 39번째 자료가 비정상적인 자료임을 확인할 수 있었다. 실험의 결과를 통해 본 논문에서 제안한 OAD-SVM 모형이 자료에 포함된 비정상적인 사건 탐지에 좋은 결과를 보임을 확인할 수 있었다.

참고문헌

- Duda, R. O. and Hart, P. E. (1973). *Pattern classification and scene analysis*, Wiley, New York.
- Herbrich, R. (2002). *Learning kernel classifiers- Theory and algorithms*, MIT Press, Cambridge, MA.
- Hwang, H. (2010). Fixed size LS-SVM for multiclassification problems of large data sets. *Journal of Korean Data & Information Science Society*, **21**, 1561-567.
- Parzen, E. (1962). On the estimation of a probability density function and the mode. *Annals of Mathematical Statistics*, **33**, 1065-1076.

- Schölkopf, B. and Smola, A. (2002). *Learning with kernels- Support vector machines, regularization, optimizations, and beyond*, MIT Press, Cambridge, MA.
- Seok, K. H. (2010). Semi-supervised classification with LS-SVM formulation. *Journal of Korean Data & Information Science Society*, **21**, 461-470.
- Shim, J. and Lee, J. T. (2009). Kernel method for autoregressive data. *Journal of Korean Data & Information Science Society*, **20**, 949-964.
- Shim, J., Park, H. J. and Seok, K. H. (2009). Variance function estimation with LS-SVM for replicated data. *Journal of Korean Data & Information Science Society*, **20**, 925-931.
- Silverman, B. (1986). *Density estimation for statistics and data analysis*, Chapman and Hall, New York.
- Smola, A. J. and Schölkopf, B. (2004). A tutorial on support vector regression. *Statistics and Computing*, **14**, 199-222.
- Suykens, J. A. K. and Vandewalle, J. (1999). Least squares support vector machine classifiers. *Neural Processing Letters*, **9**, 293-300.
- Suykens, J. A. K., Gastel, T. V., Bravanter, J. D., Moore, B. D. and Vandewalle, J. (2002). *Least squares support vector machines*, World Scientific.
- Tax, D. and Duin, R. (1999). Support vector domain description. *Pattern Recognition Letters*, **20**, 1191-1199.
- Vapnik, V. (1995). *The nature of statistical learning theory*, Springer, New York.
- Vapnik, V. (1998). *Statistical learning theory*, Wiley, New York.

Online abnormal events detection with online support vector machine

Hye Jung Park¹

¹Daegu University

Received 11 January 2011, revised 14 February 2011, accepted 28 February 2011

Abstract

The ability to detect online abnormal events in signals is essential in many real-world signal processing applications. In order to detect abnormal events, previously known algorithms require an explicit signal statistical model, and interpret abnormal events as statistical model abrupt changes. In general, maximum likelihood and Bayesian estimation theory to estimate well as detection methods have been used. However, the above-mentioned methods for robust and tractable model, it is not easy to estimate. More freedom to estimate how the model is needed. In this paper, we investigate a machine learning, descriptor-based approach that does not require a explicit descriptors statistical model, based on support vector machines are known to be robust statistical models and a sequential optimal algorithm online support vector machine is introduced.

Keywords: Abnormal event detection, online support vector machine, support vector machine.

¹ Invitation Professor, Daegu University, Jillyang, Gyeongsan, Gyeongbuk 712-714, Korea.
E-mail: hyjpark@daegu.ac.kr