Sinir Ağları Temelli Özgün Ayrıklık Sezim Yöntemi
A Novel Anomaly Detection Approach based on Neural Networks

Tolga Ergen ve Mine Kerpiççi
Elektrik ve Elektronik Mühendisliği Bölümü
İhsan Doğramacı Bilkent Üniversitesi
Ankara, Türkiye
{ergen,mine}@ee.bilkent.edu.tr

***Özetçe* —Bu bildiride, etiketsiz çerçevede çalışan ve Uzun Kısa Soluklu Bellek (UKSB) ağları temelli olan bir aykırılık sezim algoritması tanıtılmıştır. İlk olarak, değişken uzunluktaki veri dizileri UKSB temelli yapıdan geçirilerek sabit uzunluktaki dizilere dönüştürülmektedir. Sonra, aykırılık sezimi için, Tek Sınıf Destek Vektör Makinası (TS-DVM) algoritmasına dayanan puanlama fonksiyonu tanıtılmaktadır. UKSB yapısı ve TS-DVM formulasyonu için en ideal parametreleri bulmak amacıyla eğitim aşamasında kullanılan bayır merkezli algoritma tanıtılmaktadır. Orijinal TS-DVM formulasyonu değiştirildiği için, değiştirilmiş halinin orijinal olana yakınsadığını gösteren sonuçlar da gösterilmektedir. Tanıtılan algoritma, değişken uzunluktaki veri dizilerini işleyebilmektedir. Ayrıca, zaman serisi verilerinde oldukça yüksek performans göstermektedir. Sayısal örneklerde, geleneksel metodlara göre yüksek bir performans artışı elde edildiği gösterilmektedir.**

Anahtar Kelimeler*—*Aykırılık sezimi, destek vektör makinası, zaman serisi verisi, denetlenmeyen yapı, uzun kısa soluklu bellek.

***Abstract*—In this paper, we introduce a Long Short Term Memory (LSTM) networks based anomaly detection algorithm, which works in an unsupervised framework. We first introduce LSTM based structure for variable length data sequences to obtain fixed length sequences. Then, we propose One Class Support Vector Machines (OC-SVM) algorithm based scoring function for anomaly detection. For training, we propose a gradient based algorithm to find the optimal parameters for both LSTM architecture and the OC-SVM formulation. Since we modify the original OC-SVM formulation, we also provide the convergence results of the modified formulation to the original one. Thus, the algorithm that we proposed is able to process data with variable length sequences. Also, the algorithm provides high performance for time series data. In our experiments, we illustrate significant performance improvements with respect to the conventional methods.**

Keywords*—*Anomaly detection, support vector machines, time series data, unsupervised framework, long short term memory.

I. GİRİŞ

Ağ görüntüleme ve gözetleme gibi çeşitli alanlardaki mühendislik sorunlarına dayalı uygulamalardan ötürü, aykırılık sezimi çağdaş öğrenim literatüründe oldukça ilgi uyandırmıştır [1], [2]. Bu bildiride, her biri değişken uzunlukta olan, etiketlenmemiş dizilerin aykırı olup olmadıklarına karar vermek için fonksiyon aranarak, etiketsiz bir çerçevede, aykırılık tespit etme problemi üzerinde çalışılmıştır.

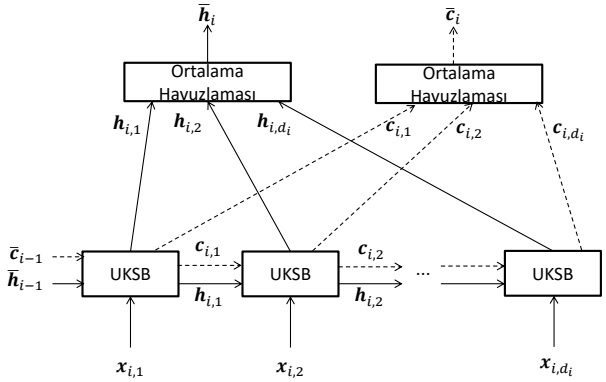
978-1-5386-1501-0/18/$31.00 © 2018 IEEE

Aykırılık seziminde kullanılan genel yöntem, normallik modelini tanımlayan bir karar fonksiyonu bulmaktır [1]. Bu yaklaşımda, bir karar fonksiyonu tanımlanır ve bu fonksiyonun parametreleri tek sınıf destek vektör makinasi (TS-DVM) ve destek vektör veri tanımlaması (DVVT) algoritmaları gibi önceden tanımlanmış nesnel kriterlere göre optimize edilir [3], [4]. Ancak, bu tarz algoritmalar zaman serisi verilerini bir zaman penceresi ile inceler [1] . Zaman penceresinin uzunluğu dikkatle ayarlanmadığında oluşan kısıtlı performansı arttırmak için zaman bilgisini kendilerine ait bellek yapısında saklayabilen ve depolanan bilginin miktarını ayarlayacak kontrol yapısına sahip uzun kısa soluklu bellek (UKSB) ağı tanıtılır [5]. Ancak, sinir ağları tabanlı yaklaşımlar nesnel kriterleri doğrudan optimize edemedikleri için önce bir dizi öngörüp sonra öngörü hatasına bağlı olarak bu dizinin aykırı olup olmadığına karar verirler [1]. Dolayısıyla, hata için olasılığa dayanan bir modele ve bu model için bir eşiğe ihtiyaç duyarlar ki bu da zorlu optimizasyon problemlerine ve performans kısıtlamalarına yol açar [1]. Ayrıca, hem ortak ağlar hem de sinir ağları tabanlı yaklaşımlar genellikle sadece sabit uzunluktaki dizileri işleyebilirler ve bu durum da onların gerçek hayattaki kullanımlarını sınırlar [1].

Bu bildiride, bütün bu sorunları gidermek için, değişken uzunluktaki veri dizilerine uygulanabilen UKSB tabanlı yenilikçi bir aykırılık sezimi algoritması tanıtılmıştır. Bu algoritmada, literatürdeki önceki yaklaşımların aksine, UKSB mimarisi ve TS-DVM formulasyonunun parametreleri birlikte eğitilmiştir. Eğitim için, orijinal TS-DVM formülasyonu değiştirilmiş ve yakınsayan sonuçlar alınmış bayır merkezli bir algoritma önerilmiştir. Geleneksel yaklaşımları izlemek yerine [1], aykırılık tespiti için UKSB mimarisini kullanan uygun bir objektif fonksiyon tanımlanmış ve bu iyi tanımlanmış fonksiyon ile UKSB mimarisinin parametreleri optimize edilmiştir. Bu bildiride tanımlanan aykırılık tespit algoritması değişken uzunluktaki serileri işleyebilmekte ve zaman serisi verileri için yüksek performans sağlayabilmektedir ki zaman serisi verilerinin işlenmesi literatürde oldukça üzerinde durulan bir konudur [6], [7]. Deneylerde, geleneksel metodlara göre [3], [4] yüksek performans artışı gözlenmiştir.

II. MODEL VE PROBLEM TANIMI

Gözlemlenen veri serisi $\{\boldsymbol{X}_i\}_{i=1}^{n}$, $\boldsymbol{X}_i = [\boldsymbol{x}_{i,1} \dots \boldsymbol{x}_{i,d_i}]$, şeklinde tanımlanmıştır. Bu tanımdaki $\boldsymbol{x}_{i,j} \in \mathbb{R}^p$, $\forall j \in \{1, 2, \dots d_i\}$ ve $d_i \in \mathbb{Z}^+$ $\boldsymbol{X}_i$'deki i'ye göre değişebilen kolon sayısıdır. Amaç, gözlemlenen veriye göre $\boldsymbol{X}_i$'nin aykırı olup



Şekil 1: Sabit uzunlukta dizi elde etmek için kurulan UKSB temelli yapı.

olmadığını belirleyecek, normal ve aykırı veri için sırasıyla $+1$ ve -1 sonuçlarını veren karar fonksiyonunu bulmaktır. Karar fonksiyonunu bulmak için TS-DVM [3] ya da DVVT [4] kullanılabilir. Bu algoritmalar sadece sabit uzunluktaki dizileri işleyebilirler. Bu sebeple, her $\boldsymbol{X}_i$ için sabit uzunluktaki vektör gösterimi elde etmek amacıyla UKSB yapısı kullanılmıştır. Şekil 1'deki gibi, $\boldsymbol{X}_i$ öncelikle UKSB yapısına verilmiştir. UKSB içindeki denklemler aşağıda verildiği gibidir [5]:

$$\boldsymbol{z}_{i,j} = g(\boldsymbol{W}^{(z)}\boldsymbol{x}_{i,j} + \boldsymbol{R}^{(z)}\boldsymbol{h}_{i,j-1} + \boldsymbol{b}^{(z)}) \quad (1)$$

$$\boldsymbol{s}_{i,j} = \sigma(\boldsymbol{W}^{(s)}\boldsymbol{x}_{i,j} + \boldsymbol{R}^{(s)}\boldsymbol{h}_{i,j-1} + \boldsymbol{b}^{(s)}) \quad (2)$$

$$\boldsymbol{f}_{i,j} = \sigma(\boldsymbol{W}^{(f)}\boldsymbol{x}_{i,j} + \boldsymbol{R}^{(f)}\boldsymbol{h}_{i,j-1} + \boldsymbol{b}^{(f)}) \quad (3)$$

$$\boldsymbol{c}_{i,j} = \boldsymbol{s}_{i,j} \odot \boldsymbol{z}_{i,j} + \boldsymbol{f}_{i,j} \odot \boldsymbol{c}_{i,j-1} \quad (4)$$

$$\boldsymbol{o}_{i,j} = \sigma(\boldsymbol{W}^{(o)}\boldsymbol{x}_{i,j} + \boldsymbol{R}^{(o)}\boldsymbol{h}_{i,j-1} + \boldsymbol{b}^{(o)}) \quad (5)$$

$$\boldsymbol{h}_{i,j} = \boldsymbol{o}_{i,j} \odot g(\boldsymbol{c}_{i,j}), \quad (6)$$

Bu denklemlerdeki $\boldsymbol{c}_{i,j} \in \mathbb{R}^m$, $\boldsymbol{x}_{i,j} \in \mathbb{R}^p$, ve $\boldsymbol{h}_{i,j} \in \mathbb{R}^m$ Şekil 1'deki UKSB ünitesi için sırasıyla durum, girdi ve çıktı vektörleridir. $\boldsymbol{s}_{i,j}$, $\boldsymbol{f}_{i,j}$ ve $\boldsymbol{o}_{i,j}$ sırasıyla girdi, unutma ve çıktı kapılarıdır. $g(\cdot)$, $\tanh$ gibi hiperbolik tanjant fonksiyon olarak ayarlanır ve girdiye noktasal olarak uygulanır. Benzer şekilde, $\sigma(\cdot)$, sigmoid fonksiyonu olarak ayarlanır. $\odot$ işlemi ise aynı boyuttaki iki vektörün elementlerinin çarpımıdır. $\boldsymbol{W}^{(\cdot)}$, $\boldsymbol{R}^{(\cdot)}$ ve $\boldsymbol{b}^{(\cdot)}$, UKSB yapısının parametreleridir ve boyutları input ve output vektörlerinin boyutlarına göre seçilir. Veri dizisinin her kolonuna UKSB yapısının Şekil 1'deki uygulanmasından sonra her veri dizisi için UKSB çıktılarının ortalamaları alınır ki bu da ortalama havuzlamasıdır. Bu şekilde, sabit uzunlukta yeni bir dizi elde edilir ve $\{\bar{\boldsymbol{h}}_i\}_{i=1}^n$, $\bar{\boldsymbol{h}}_i \in \mathbb{R}^m$ olarak gösterilir.

III. Ayrılık Sezimi Algoritması

Bu bildiride, TS-DVM formulasyonu ve UKSB yapısı temelli olan bir aykırılık sezim algoritması tanıtılmaktadır. Eğitim için de orijinal TS-DVM formulasyonuna yakınsayan sonuçlar veren bayır merkezli bir algoritma tanıtılmaktadır.

TS-DVM algoritmasında, amaç aykırı veriyi normal veriden ayıran bir hiperdüzlem bulmaktır [3]. $\{\bar{\boldsymbol{h}}_i\}_{i=1}^n$ için TS-DVM problemi aşağıdaki şekilde formülleştirilmiştir [3].

$$\min_{\boldsymbol{\theta}\in\mathbb{R}^{n_\theta},\boldsymbol{w}\in\mathbb{R}^m,\xi\in\mathbb{R},\rho\in\mathbb{R}} \frac{\|\boldsymbol{w}\|^2}{2} + \frac{1}{n\lambda}\sum_{i=1}^{n}\xi_i - \rho \quad (7)$$

$$\text{subject to: } \boldsymbol{w}^T\bar{\boldsymbol{h}}_i \geq \rho - \xi_i,\ \xi_i \geq 0,\ \forall i \quad (8)$$

$$\boldsymbol{W}^{(\cdot)T}\boldsymbol{W}^{(\cdot)} = \boldsymbol{I}, \boldsymbol{R}^{(\cdot)T}\boldsymbol{R}^{(\cdot)} = \boldsymbol{I} \text{ ve } \boldsymbol{b}^{(\cdot)T}\boldsymbol{b}^{(\cdot)} = 1. \quad (9)$$

Bu ifadelerdeki ρ ve $\boldsymbol{w}$ ayırıcı hiperdüzlemin parametreleri, $\lambda > 0$ düzenleme parametresi ve ξ ise yanlış sınıflandırmaları cezalandırmak için kullanılan bir gölge değişkendir. UKSB parametreleri $\{\boldsymbol{W}^{(z)}, \boldsymbol{R}^{(z)}, \boldsymbol{b}^{(z)}, \boldsymbol{W}^{(s)}, \boldsymbol{R}^{(s)}, \boldsymbol{b}^{(s)}, \boldsymbol{W}^{(f)}, \boldsymbol{R}^{(f)}, \boldsymbol{b}^{(f)}, \boldsymbol{W}^{(o)}, \boldsymbol{R}^{(o)}, \boldsymbol{b}^{(o)}\}$ olarak $\boldsymbol{\theta} \in \mathbb{R}^{n_\theta}$ içine gruplandırılmıştır ($n_\theta = 4m(m+p+1)$) . UKSB parametreleri bilinmediği ve $\bar{\boldsymbol{h}}_i$ de bu parametrelere bağlı bir fonksiyon olduğu için (7)'deki maliyet fonksiyonu da $\boldsymbol{\theta}$ parametresine göre minimuma indirilir. (7), $\boldsymbol{\theta}$ parametresine göre küçültülürken verinin zamana bağlılığının etkisiz öğrenmesi ve aşırı uyma problemlerinden dolayı mağdur olunabilir [8]. Bu yüzden, (9)'da verilen eşitlikler tanımlanır. (7) ,(8) ve (9)'da verilen optimizasyon problemi çözüldükten sonra, aykırı veriyi sezmek için aşağıda verilen puanlama fonksiyonu kullanılır.

$$l(\boldsymbol{X}_i) = \text{sgn}(\boldsymbol{w}^T\bar{\boldsymbol{h}}_i - \rho) \quad (10)$$

Buradaki $\text{sgn}(\cdot)$ fonksiyonu, girdinin işaretini çıktı olarak verir. (8) göz önünde bulundurularak, gölge değişken farklı bir formda yazılabilir.

$$G(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)) \triangleq \max\{0, \beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)\}, \forall i. \quad (11)$$

Bu eşitlikteki $\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i) \triangleq \rho - \boldsymbol{w}^T\bar{\boldsymbol{h}}_i$. (11), (7)'deki yerine yazılarak (8)'deki koşul ortadan kaldırılır ve aşağıda verilen optimizasyon problemi elde edilir.

$$\min_{\boldsymbol{w}\in\mathbb{R}^m,\rho\in\mathbb{R},\boldsymbol{\theta}\in\mathbb{R}^{n_\theta}} \frac{\|\boldsymbol{w}\|^2}{2} + \frac{1}{n\lambda}\sum_{i=1}^{n} G(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)) - \rho \quad (12)$$

$$\text{s.t.:} \boldsymbol{W}^{(\cdot)T}\boldsymbol{W}^{(\cdot)} = \boldsymbol{I}, \boldsymbol{R}^{(\cdot)T}\boldsymbol{R}^{(\cdot)} = \boldsymbol{I} \text{ ve } \boldsymbol{b}^{(\cdot)T}\boldsymbol{b}^{(\cdot)} = 1. \quad (13)$$

(11) türevlenebilir fonksiyon olmadığı için, (12)'de verilen optimizasyon problemi, bayır merkezli optimizasyon algoritmaları kullanılarak çözülemez. Bu nedenle, (11)'e yaklaşmak için aşağıda verilen türevlenebilir fonksiyon kullanılır.

$$S_\tau(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)) = \frac{1}{\tau}\log\left(1 + e^{\tau\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)}\right) \quad (14)$$

Buradaki, $\tau > 0$ düzgünleştirme parametresidir ve $\log$ doğal logaritmayı temsil etmektedir. (14)'teki τ artarken, $S_\tau(\cdot)$ $G(\cdot)$ ye yakınlaşır. (Bu bölümün sonundaki Önerme 1'e bakılabilir.) Bu nedenle, τ için büyük bir değer seçilir. (14) ile birlikte, optimizasyon problemi aşağıda verildiği şekilde değiştirilir.

$$\min_{\boldsymbol{w}\in\mathbb{R}^m,\rho\in\mathbb{R},\boldsymbol{\theta}\in\mathbb{R}^{n_\theta}} F_\tau(\boldsymbol{w},\rho,\boldsymbol{\theta}) \quad (15)$$

$$\text{s.t.:} \boldsymbol{W}^{(\cdot)T}\boldsymbol{W}^{(\cdot)} = \boldsymbol{I}, \boldsymbol{R}^{(\cdot)T}\boldsymbol{R}^{(\cdot)} = \boldsymbol{I} \text{ ve } \boldsymbol{b}^{(\cdot)T}\boldsymbol{b}^{(\cdot)} = 1 \quad (16)$$

Buradaki $F_\tau(\cdot,\cdot,\cdot)$ amaç fonksiyonudur ve şu şekilde tanımlanmaktadır.

$$F_\tau(\boldsymbol{w},\rho,\boldsymbol{\theta}) \triangleq \frac{\|\boldsymbol{w}\|^2}{2} + \frac{1}{n\lambda}\sum_{i=1}^{n} S_\tau(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)) - \rho.$$

(15) ve (16)'daki ideal parametreleri elde etmek için, $\boldsymbol{w}$, ρ ve $\boldsymbol{\theta}$ yakınsayana kadar güncellenir [9]. $\boldsymbol{w}$ ve ρ güncellemeleri için, amaç fonksiyonun bütün parametrelerine göre birinci dereceden gradyanının hesaplandığı Olasılıksal Gradyan İnişi (OGİ) algoritması kullanılır. $\boldsymbol{w}$ için gradyan aşağıdaki gibi hesaplanır.

$$\nabla_{\boldsymbol{w}} F_\tau(\boldsymbol{w},\rho,\boldsymbol{\theta}) = \boldsymbol{w} + \frac{1}{n\lambda}\sum_{i=1}^{n}\frac{-\bar{\boldsymbol{h}}_i e^{\tau\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)}}{1 + e^{\tau\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)}}. \quad (17)$$

(17) kullanılarak, $\boldsymbol{w}$ aşağıdaki şekilde güncellenir.

$$\boldsymbol{w}_{k+1} = \boldsymbol{w}_k - \mu \nabla_{\boldsymbol{w}} F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})\Big|_{\substack{\boldsymbol{w}=\boldsymbol{w}_k \\ \rho=\rho_k \\ \boldsymbol{\theta}=\boldsymbol{\theta}_k}}. \tag{18}$$

Buradaki k altindisi, k. itreasyondaki herhangi bir parametrenin değerini ve μ ise öğrenme hızını gösterir. Benzer bir şekilde, ρ'nun türevi ve parametrenin güncellenmesi de aşağıdaki şekilde hesaplanır.

$$\frac{\partial F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})}{\partial \rho} = \frac{1}{n\lambda} \sum_{i=1}^{n} \frac{e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}}{1 + e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}} - 1. \tag{19}$$

$$\rho_{k+1} = \rho_k - \mu \frac{\partial F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})}{\partial \rho}\Big|_{\substack{\boldsymbol{w}=\boldsymbol{w}_k \\ \rho=\rho_k \\ \boldsymbol{\theta}=\boldsymbol{\theta}_k}}. \tag{20}$$

UKSB parametreleri için (16)'dan dolayı [9]'da verilen optimizasyon metodu ortogonallik koşulu ile kullanılır. $\boldsymbol{W}^{(\cdot)}$ elemanlarının güncellenmesi için, gradyan aşağıdaki gibi hesaplanır.

$$\frac{\partial F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})}{\partial \boldsymbol{W}_{ij}^{(\cdot)}} = \frac{1}{n\lambda} \sum_{i=1}^{n} \frac{-\boldsymbol{w}^T \left(\partial \bar{\boldsymbol{h}}_i / \partial \boldsymbol{W}_{ij}^{(\cdot)}\right) e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}}{1 + e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}}. \tag{21}$$

Sonra, $\boldsymbol{W}^{(\cdot)}$ (21) kullanılarak aşağıdaki gibi güncellenir.

$$\boldsymbol{W}_{k+1}^{(\cdot)} = \left(\boldsymbol{I} + \frac{\mu}{2}\boldsymbol{B}_k\right)^{-1} \left(\boldsymbol{I} - \frac{\mu}{2}\boldsymbol{B}_k\right) \boldsymbol{W}_k^{(\cdot)}, \tag{22}$$

denklemindeki $\boldsymbol{B}_k = \boldsymbol{M}_k (\boldsymbol{W}_k^{(\cdot)})^T - \boldsymbol{W}_k^{(\cdot)} \boldsymbol{M}_k^T$ ve

$$\boldsymbol{M}_{ij} \triangleq \frac{\partial F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})}{\partial \boldsymbol{W}_{ij}^{(\cdot)}}. \tag{23}$$

Açıklama 1: $\boldsymbol{R}^{(\cdot)}$ ve $\boldsymbol{b}^{(\cdot)}$ için, öncelikle amaç fonksiyonunun seçilen parametreye göre gradyanı (23)'deki gibi hesaplanır. Sonra, $\boldsymbol{B}_k$ seçilen parametreye göre elde edilir ve parametre (22)'deki gibi $\boldsymbol{B}_k$ kullanılarak güncellenir.

Önerme 1: τ artarken, $S_\tau(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i))$ düzgün olarak $G(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i))$'ye yakınsar. Sonuç olarak $F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ yaklaşımı DVM amaç fonksiyonu olan $F(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ ve aşağıda verildiği gibi tanımlanan fonksiyona yakınsar.

$$F(\boldsymbol{w}, \rho, \boldsymbol{\theta}) \triangleq \frac{\|\boldsymbol{w}\|^2}{2} + \frac{1}{n\lambda} \sum_{i=1}^{n} G(\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)) - \rho.$$

Önerme 1'in kanıtı: $\beta_{\boldsymbol{w},\rho}(\bar{\boldsymbol{h}}_i)$ herhangi $\boldsymbol{w}$, $\boldsymbol{\theta}$, $\boldsymbol{X}_i$ ve ρ değerleri için Ω olarak tanımlanır. Öncelikle $\forall \tau > 0$ için $S_\tau(\Omega) \geq G(\Omega)$ eşitsizliği gösterilir.

$$S_\tau(\Omega) = \frac{1}{\tau} \log\left(1 + e^{\tau\Omega}\right) \geq \frac{1}{\tau} \log\left(e^{\tau\Omega}\right) = \Omega$$

eşitliği ve $S_\tau(\Omega) \geq 0$ eşitsizliğinden $S_\tau(\Omega) \geq G(\Omega) = \max\{0, \Omega\}$ sonucu gelmektedir. Bundan dolayı, her $\Omega \geq 0$ değeri için aşağıda verilen ifade tanımlanır.

$$\frac{\partial S_\tau(\Omega)}{\partial \tau} = \frac{-\log\left(1 + e^{\tau\Omega}\right)}{\tau^2} + \frac{\Omega e^{\tau\Omega}}{\tau(1 + e^{\tau\Omega})} < 0$$

Aynı şekilde, her $\Omega < 0$ değeri için de $\partial S_\tau(\Omega)/\partial\tau < 0$, eşitsizliği geçerlidir. Buradan $S_\tau(\Omega)$ fonksiyonunun τ'ya bağlı monoton azalan bir fonksiyon olduğu sonucu çıkarılır. Son aşama olarak, $S_\tau(\Omega) - G(\Omega)$ farkı için üst limit türetilir. Her $\Omega \geq 0$ değeri için, farkın türevi aşağıda verildiği gibidir.

$$\frac{\partial(S_\tau(\Omega) - G(\Omega))}{\partial\Omega} = \frac{e^{\tau\Omega}}{1 + e^{\tau\Omega}} - 1 < 0.$$

Dolayısıyla fark, her $\Omega \geq 0$ değeri için, Ω'ya bağlı azalan bir fonksiyondur. Bu sebeple, maksimum değeri $\log(2)/\tau$ değeridir ve $\Omega = 0$ eşitliğinde gerçekleşir. Benzer şekilde, her $\Omega < 0$ değeri için, farkın türevi pozitiftir ve bu da farkın maksimumun $\Omega = 0$ eşitliğinde gerçekleştiğini gösterir. Bu sonuçtan, aşağıda verilen üst sınır elde edilir.

$$\frac{\log(2)}{\tau} = \max_{\Omega} \left(S_\tau(\Omega) - G(\Omega)\right). \tag{24}$$

(24) kullanılarak, her $\epsilon > 0$ için $S_\tau(\Omega) - G(\Omega) < \epsilon$ eşitsizliğini sağlayan yeterince büyük bir τ değeri seçilebilir. τ değeri arttıkça, $S_\tau(\Omega)$, $G(\Omega)$ fonksiyonuna düzgün olarak yakınsar. (24)'te verilen sınırın, bütün veri noktalarına göre ortalaması alınıp, $1/\lambda$ ile çarpılmasıyla, amaç fonksiyonlarının farklarının sınırı olarak $\log(2)/(\lambda\tau)$ elde edilir. Bu da $F_\tau(\cdot,\cdot,\cdot)$ fonksiyonunun $F(\cdot,\cdot,\cdot)$ fonksiyonuna düzgün yakınsadığını kanıtlar. ■

Teorem 1: $\boldsymbol{w}_\tau$ ve ρ_τ değerlerinin sabit bir $\boldsymbol{\theta}$ için (15)'in çözümleri olduklarını varsayalım. Bu durumda, $\boldsymbol{w}_\tau$ ve ρ_τ tek değerlidirler ve $F_\tau(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta})$, $F(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ fonksiyonunun minimumuna yakınsar.

Teorem 1'in ispatı: $F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ fonksiyonunun $\boldsymbol{w}$ parametresine göre Hessian matrisi aşağıda verildiği gibidir.

$$\nabla^2_{\boldsymbol{w}} F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta}) = \boldsymbol{I} + \frac{\tau}{n\lambda} \sum_{i=1}^{n} \frac{e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}}{\left(1 + e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}\right)^2} \bar{\boldsymbol{h}}_i \bar{\boldsymbol{h}}_i^T.$$

Bu eşitlik tüm sıfırdan farklı $\boldsymbol{v}$ kolon vektörleri için $\boldsymbol{v}^T \nabla^2_{\boldsymbol{w}} F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta}) \boldsymbol{v} > 0$ eşitsizliğini sağlar. Bu sebeple, Hessian matrisi kesin pozitif matristir ve bu da $F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ fonksiyonunun $\boldsymbol{w}$ parametresine bağlı kesin konveks bir fonksiyon olduğunu gösterir. Sonuç olarak, $\boldsymbol{w}_\tau$ çözümü belirli herhangi bir ρ ve $\boldsymbol{\theta}$ için evrensel ve tektir. Ayrıca, ρ parametresine göre ikinci türev aşağıda verildiği gibidir.

$$\frac{\partial^2 F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})}{\partial \rho^2} = \frac{\tau}{n\lambda} \sum_{i=1}^{n} \frac{e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}}{\left(1 + e^{\tau \beta_{\boldsymbol{w},\rho}(\bar{\mathrm{h}}_i)}\right)^2} > 0,$$

Yukarıda verilen sonuç da $F_\tau(\boldsymbol{w}, \rho, \boldsymbol{\theta})$ fonksiyonunun, ρ parametresine bağlı kesin konveks bir fonksiyon olduğunu gösterir. Sonuç olarak, belirli $\boldsymbol{w}$ ve $\boldsymbol{\theta}$ için, ρ_τ çözümü evrensel ve tektir.

$\boldsymbol{w}^*$ ve ρ^* değerlerinin belirli $\boldsymbol{\theta}$ için (12)'nin çözümü olduklarını varsayalım. Önerme 1'in ispatından dolayı aşağıdaki sonuç elde edilir.

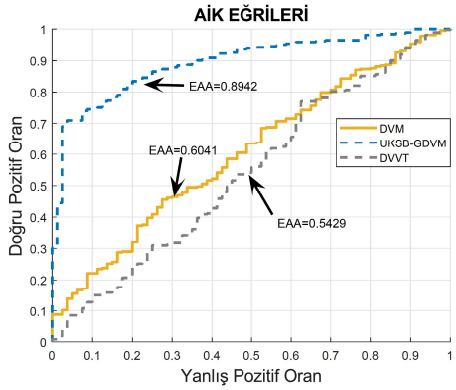
$$\begin{aligned} F_\tau(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}) \geq F_\tau(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta}) &\geq F(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta}) \\ &\geq F(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}). \end{aligned} \tag{25}$$

Önerme 1 sonucu ve (25)'de verilen ifade kullanılarak aşağıda verilen sonuç elde edilir.

$$\begin{aligned} &\lim_{\tau\to\infty} F_\tau(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta}) \leq \lim_{\tau\to\infty} F_\tau(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}) = F(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}) \\ &\lim_{\tau\to\infty} F_\tau(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta}) \geq F(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}), \end{aligned}$$

ve bu sonuçlar da aşağıdaki ifadeyi ispatlar.

$$\lim_{\tau\to\infty} F_\tau(\boldsymbol{w}_\tau, \rho_\tau, \boldsymbol{\theta}) = F(\boldsymbol{w}^*, \rho^*, \boldsymbol{\theta}).$$ ■



Şekil 2: "0" rakamının normal, "9" rakamının aykırı varsayıldığı rakam veri seti için elde edilen AİK eğrileri.

IV. Sayısal Örnekler

Tanıtılan algoritma "UKSB-GDVM" olarak adlandırılmaktadır. DVVT kıyaslama algoritması olarak belirlenmiştir [4]. Aykırılık sezici performansları rakam veri seti [10] kullanılarak ölçülmüştür. Bu veri setinde, tablet üzerine farklı yazarlar tarafından yazılan rakamların piksel örnekleri vardır [10]. Yazma hızı kişiden kişiye değiştiği için, her bir rakamdaki örnek sayısı farklılık gösterebilmektedir. Tanıtılan algoritma, bu tür dizileri işleyebilecek düzeydedir. Ancak, geleneksel TS-DVM ve DVVT algoritmaları bu dizileri doğrudan işleyememektedirler [3], [4]. Bu algoritmalar için, sabit uzunlukta vektör dizisi elde etmek amacıyla her dizinin ortalaması alınır. Performansları değerlendirmek için bir rakam normal ve bir rakam da aykırı olarak seçilerek, örnekler %60'ı eğitim, %40'ı test örnekleri olarak bölünür. Bütün algoritmalar için ideal parametreler, eğitim örnekleri kullanılarak belirlenir. Bu yöntem ile, UKSB-GDVM için $\mu = 0.05$ sonucu elde edilmiştir. Bütün algoritmalar için $m = 2$ ve $\lambda = 0.5$ değerleri seçilmiştir. TS-DVM ve DVVT algoritmaları için LIBSVM kütüphanesi kullanılmıştır ve parametreleri gömülü araçlar kullanılarak seçilmiştir [11].

Performans ölçütü olarak alıcı iletim karakteristiği (AİK) altında kalan alan yani eğri altı alan (EAA) kullanılmıştır [12]. Şekil 2'de "0" rakamının normal ve "9" rakamının aykırı olarak seçildiği örneğe ait AİK eğrileri ve bu eğrilerin EAA değerleri gösterilmiştir. Değişken uzunluktaki veri dizilerini sabit uzunluktaki dizilere dönüştürmek için ortalamaları alındığı için, TS-DVM ve DVVT algoritmaları, tanıtılan algoritmanın ulaştığı EAA değerinden daha düşük EAA değerleri elde etmişlerdir.

Ayrıca HKK oranı veri seti ile deney yapılmıştır. Bu veri seti, bir ABD dolarına karşılık gelen Honk Kong doları miktarını içerir. Aykırılık, ortalaması eğitim verisinin ortalamasıyla aynı, varyansı onun varyansının on katı olan normal dağılımdan alınan örneklerle yapay olarak eklenmiştir. UKSB-GDVM için $\mu = 0.01$ değeri, eğitim verileri kullanılarak belirlenmiştir. Elde edilen EAA değerleri Tablo I'de verilmiştir. Zaman serisi verileri kullanıldığı için, tanıtılan algoritma belleği sayesinde geleneksel algoritmaları geride bırakmıştır.

Son olarak, algoritmaların aykırılık sezim performansları günlük hisse bedeli değerlerini bulunduran Alcoa hisse bedeli veri seti [13] kullanılarak ölçülmüştür. Aykırılık, ortalaması eğitim verisinin ortalamasıyla aynı, varyansı onun varyansının on katı olan normal dağılım örnekleri ile yapay olarak eklenmiştir. UKSB-GDVM için $\mu = 0.01$ değeri seçilmiştir. Alcoa hisse bedeli veri seti için elde edilen EAA değerleri Tablo I'de gösterilmiştir. Tanıtılan algoritmanın, geleneksel metodlardan daha yüksek EAA değerlerine ulaştığı gözlemlenmiştir.

TABLO I: HKK oranı ve Alcoa hisse bedeli veri setlerine ait EAA değerleri

Algoritmalar / Veri Setleri	DVM	DVVT	UKSB-GDVM
HKK	0.8000	0.8500	0.9783
Alcoa	0.7197	0.9390	0.9515

V. Sonuçlar

Bu bildiride, etiketsiz çerçevede aykırılık sezimi üzerine çalışılmış ve UKSB tabanlı bir algoritma tanıtılmıştır. Özellikle, değişken uzunluktaki veri dizilerinin işlenebilmesi için, UKSB tabanlı bir yapı tanıtılmıştır. UKSB tabanlı yapı kullanılarak sabit uzunlukta dizilerin elde edilmesinden sonra, TS-DVM algoritmasına dayanan aykırılık sezici için puanlama fonksiyonu tanıtılmıştır [3]. Sonra UKSB yapısı ve TS-DVM formulasyonunun parametreleri ideal olarak birlikte ayarlanmıştır. Tanıtılan algoritmanın parametrelerinin ideal olarak seçilmesi için TS-DVM formulasyonunun değiştirildiği ve asıl sonuçlara yakınsadığı sonucunun gösterildiği bayır merkezli eğitim metodu tanıtılmıştır. Bu sayede, değişken uzunluktaki veri dizilerini işleyebilen, özellikle zaman serisi verilerinde oldukça etkili olan bir aykırılık sezim algoritması elde edilmiştir. Sayısal örnekler bölümünde, geleneksel metodlara göre [3], [4], önemli performans artışı olduğu gösterilmiştir.

Kaynaklar

[1] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, pp. 15:1–15:58, Jul. 2009. [Online]. Available: http://doi.acm.org/10.1145/1541880.1541882

[2] K. Gokcesu and S. S. Kozat, "Online anomaly detection with minimax optimal density estimation in nonstationary environments," *IEEE Transactions on Signal Processing*, vol. 66, no. 5, pp. 1213–1227, March 2018.

[3] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Computation*, vol. 13, no. 7, pp. 1443–1471, 2001.

[4] D. M. Tax and R. P. Duin, "Support vector data description," *Machine Learning*, vol. 54, no. 1, pp. 45–66, 2004. [Online]. Available: http://dx.doi.org/10.1023/B:MACH.0000008084.60811.49

[5] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997.

[6] H. Ozkan, F. Ozkan, and S. S. Kozat, "Online anomaly detection under markov statistics with controllable type-i error," *IEEE Transactions on Signal Processing*, vol. 64, no. 6, pp. 1435–1445, March 2016.

[7] I. Delibalta, K. Gokcesu, M. Simsek, L. Baruh, and S. S. Kozat, "Online anomaly detection with nested trees," *IEEE Signal Processing Letters*, vol. 23, no. 12, pp. 1867–1871, Dec 2016.

[8] S. Wisdom, T. Powers, J. Hershey, J. Le Roux, and L. Atlas, "Full-capacity unitary recurrent neural networks," in *Advances in Neural Information Processing Systems*, 2016, pp. 4880–4888.

[9] Z. Wen and W. Yin, "A feasible method for optimization with orthogonality constraints," *Mathematical Programming*, vol. 142, no. 1, pp. 397–434, Dec 2013. [Online]. Available: http://dx.doi.org/10.1007/s10107-012-0584-1

[10] M. Lichman, "UCI machine learning repository," 2013.

[11] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 2, pp. 27:1–27:27, 2011, software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.

[12] A. P. Bradley, "The use of the area under the roc curve in the evaluation of machine learning algorithms," *Pattern Recognition*, vol. 30, no. 7, pp. 1145 – 1159, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320396001422

[13] "Summary for alcoa inc. common stock." [Online]. Available: http://finance.yahoo.com/quote/AA?ltr=1