Journal of the Faculty of Engineering and Architecture of Gazi University 32:2 (2017) 459-468

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Simetrik α-kararlı gürültü altında akıllı şebeke güvenliği için durağan durum kestirimi ve veri enjeksiyon saldırılarının tespiti

Alirıza Yavuz[1], Mehmet Emre Çek[2*], Olcay Akay[2]
[1]TEİAŞ Batı Anadolu Yük Tevzi İşletme Müdürlüğü, 35070, İzmir, Türkiye
[2]Dokuz Eylül Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, 35160, İzmir, Türkiye

Ö N E Ç I K A N L A R

- Akıllı şebekelerde veri güvenliği
- $\alpha -$ kararlı dağılımlı gürültü altında durum kestirimi
- Veri enjeksiyonu saldırılarının CUSUM yöntemi ile tespiti

Makale Bilgileri
Geliş: 21.03.2016
Kabul: 15.11.2016

DOI:
10.17341/gazimmfd.322171

Anahtar Kelimeler:
Akıllı şebeke güvenliği, α-kararlı dağılımlar, veri enjeksiyonu saldırılarının tespiti

ÖZET

Bu çalışmada, Gauss olmayan ortamlarda akıllı şebekeler için durağan durum kestirimi problemi ele alınmıştır. Durum kestiriminde gürültünün Gauss dağılıma sahip olduğu yaygın olarak kabul edilir. Fakat bazı gerçek dünya uygulamalarında gürültü dürtüsel bir dağılıma da sahip olabilmektedir. Gürültünün Gauss dağılımla modellendiği sistemlerde, durum kestirimi için genellikle en küçük kareler (LS) yöntemi kullanılmaktadır. Bu çalışmada ise dürtüsel bileşenler içeren gürültü α-kararlı dağılımla modellenmiş, durağan durum kestirimi için gürbüz süzgeçler seçilmiş ve bu süzgeçlerin performansları, LS yöntemi ile kıyaslanmıştır. Buna ilave olarak, akıllı şebekelerde baraların ölçüm değerlerine yapılan kötü niyetli veri enjeksiyonu saldırılarının en hızlı şekilde tespit edilebilmesi için kümülatif toplam (CUSUM) tekniği kullanılmış ve performansı α-kararlı gürültü altında irdelenmiştir. Veri enjeksiyonu saldırılarının hızlı tespitinde, tespit hızı ile tespit güvenilirliği arasında bir tercih söz konusudur. CUSUM tekniğinde, seçilen eşik değeri, kötü niyetli saldırıların tespitinin performansını belirlemektedir. Bu çalışmada, seçilen eşik değerinin, doğu tespit oranı, yanlış alarm oranı ve ortalama tespit süresi üzerindeki etkisi farklı α değerleri için detaylı olarak irdelenmiştir.

Static state estimation and detection of data injection attacks for smart grid security under symmetric α −stable noise

H I G H L I G H T S

- Data security in smart grids
- State estimation under $\alpha -$ stable distributed noise
- Detection of data injection attacks by CUSUM method

Article Info
Received: 21.03.2016
Accepted: 15.11.2016

DOI:
10.17341/gazimmfd.322171

Keywords:
Smart grid security, α-stable distributions, detection of data injection attack.

ABSTRACT

In this study, static state estimation problem in smart grid is considered for non-Gaussian environments. The noise model in state estimation is widely assumed to possess Gaussian distribution. However, in some real-world applications, noise may also possess an impulsive distribution. Method of least squares (LS) is generally used for state estimation in systems where noise is modeled by using Gaussian distribution. In this study, noise which contains impulsive components is modeled by α-stable distributions. Robust filters are chosen for static state estimation and performances of these filters are compared against the performance of LS. In addition, cumulative sum (CUSUM) technique is employed and its performance is investigated under α-stable distributed noise for quickest detection of malicious data injection attacks which might be launched at measurement values of buses in smart grids. In quickest detection, there is a trade-off between detection speed and detection reliability. The chosen threshold value for CUSUM determines the probability of detection for malicious attacks. In this study, impact of the threshold value on detection rate, false alarm rate, and average run length is examined in detail for different α values.

*Sorumlu Yazar/Corresponding Author: emre.cek@deu.edu.tr / Tel: +90 232 301 7683

1. GİRİŞ (INTRODUCTION)

Akıllı güç şebekelerinin güvenilirliğinin ve etkinliğinin artırılması için, ileri seviyede güç, iletişim, sinyal işleme ve kontrol tekniklerinin güç şebekelerine entegre edilmesi günümüzde popüler bir çalışma alanıdır. Gerçek zamanlı enerji yönetim sistemleri için durum kestirimi oldukça önemlidir. Akıllı şebekelerde durum kestirimi, güç şebekesindeki bir baradan voltaj genliği ve faz açısı bilgisinin alınması olarak tanımlanır. Literatürde durum kestirimi için izlenen işlem basamakları [1]'de detaylı olarak belirtilmektedir. Durum kestirimi durağan bir model üzerinden gerçekleştirilebileceği gibi dinamik bir modelleme ile de gerçekleştirilebilir. [1]'de, durağan durum kestirimi için en küçük kareler (LS) yöntemi kullanılmıştır. Dinamik durum kestiriminde ise Kalman süzgeci kullanılmakta olup durum geçiş matrisinin modeline göre genişletilmiş Kalman süzgecinin ve kokusuz Kalman süzgecinin kullanımı olası saldırıların tespitini de içerecek şekilde [2]'de verilmektedir. Durağan ve dinamik durum kestirimindeki en önemli varsayım, modellemedeki mevcut gürültünün Gauss dağılıma sahip olmasıdır. Kalman süzgeci Gauss dağılımlı gürültü için tanımlanmış olup Gauss olmayan dağılımlarda performans kaybına uğramaktadır. Aynı şekilde, durağan durum kestiriminde kullanılan LS yönteminin Gauss olmayan dağılımlar altında performans kaybına uğraması beklenir. Bu çalışmada, Gauss olmayan dürtüsel gürültü altında durağan DC durum kestirimi için gürbüz süzgeçleme yöntemleri uygulanmış olup Gauss olmayan dürtüsel gürültüyü modellemek için α-kararlı dağılım modeli kullanılmıştır. α-kararlı dağılımın seçilmesinin nedeni, Gauss dağılımı da içeren daha genel bir gürültü modeli üzerinde çalışılmasını olanaklı kılması ve literatürde üç fazlı voltaj sinyallerindeki kısa süreli bozulmaların dürtüsel gürültü olarak modellenmesidir [3]. Uygulanan gürbüz süzgeçler ise Medyan, Myriad [4] ve Meridian [5] süzgeçleridir. Bu süzgeçlerin performansları LS yöntemi ile kıyaslanmıştır. Çalışmanın ikinci kısmında, durum kestiriminin dürtüsel gürültü dağılımlarını da kapsayacak şekilde gerçekleştirilmesi yanında kötü niyetli veri saldırılarının tespiti de analiz edilmektedir. Burada kritik olarak ayrıştırılması gereken nokta, durum değişkenindeki değişimin saldırı sonucu mu yoksa fiziksel nedenlerden kaynaklanan bozulma sonucu mu olduğunun belirlenmesidir.

Bunun için yakın zamanda makine öğrenmesi tabanlı bir ayrıştırma algoritması tanımlanmıştır [6]. Kötü niyetli kişiler, durum kestirimi işlemi sırasında kendilerini belli etmeden zararlı veriyi sisteme enjekte edip enerji kontrol merkezini yanıltabilir ve kendilerine avantaj sağlayabilirler. Bu işlem ise genelde mevcut durum değişkeninin değerinde bir DC kayma oluşturarak gerçekleştirilmektedir [7]. Yakın geçmişte, veri enjeksiyonu saldırılarının analizi, çeşitli güncel çalışmaların da konusu olmuştur. [8]'de güç sistemi topolojisi içerisindeki en zayıf düğüm noktalarına yapılacak saldırılar için koruma ve kestirim tabanlı savunma yöntemleri üzerinde çalışılmıştır. [9]'da güç şebekesi üzerindeki ölçümlerin zamansal olarak ilintisinden veri enjeksiyon saldırılarının kestirimi matris ayrıştırma problemi şeklinde irdelenmiştir. [10]'da, güç sistemlerinde tanımlanamayan saldırı kavramı irdelenmiş, [11]'de ise indirgenemez siber saldırılar tanımlanıp karakterize edilmiştir. Temel bileşenler analizi kullanarak gözü kapalı veri enjeksiyonu saldırıları [12]'nin konusu olmuştur. [13]'te de veri enjeksiyonu saldırılarının tespiti için yeni bir yöntem önerilmiştir. Kablosuz haberleşme sistemlerinde saldırı tespiti de [14]'te incelenmiştir. Saldırı kestiriminde kullanılan yöntem kadar önemli bir başka nokta ise hasarın en aza indirgenebilmesi için saldırının en hızlı şekilde tespit edilebilmesidir. Kümülatif toplam (CUSUM) en hızlı tespit yöntemi [15], saldırının yapıldığı zamanla tespit zamanı arasındaki gecikmenin en aza indirilmesi hedefine yönelik olarak kullanılabilir. CUSUM tekniğini kullanan saldırı kestirimi, yakın zamanda [16]'in konusu olmuştur. Hızlı tespit ile yüksek performanslı tespit arasında bir seçim söz konusudur. Bu çalışmada da kullanılan CUSUM yönteminde, eşik değeri seçimi tespit işleminin performansını belirlemektedir.

2. DURAĞAN DURUM KESTİRİMİ (STATIC STATE ESTIMATION)

Durum kestirimi, ölçümler ve şebeke ile ilgili parametrelerin işlenmesi sonucunda enerji sisteminin mevcut durumunun doğru bir şekilde şebeke operatörüne sunulmasını hedefler. Durağan durum kestirimi, belirli bir anda elde edilen voltaj genliği ve faz açısı bilgilerini içerir. Q baralı bir sistemde i numaralı baraya ait karmaşık voltaj değeri V_i ile gösterildiği takdirde, Q uzunluğundaki durum vektörü $\mathrm{x} = [V_1, \cdots, V_Q]^T$ şeklinde yazılabilir. Genellikle SCADA sistemi aracılığı ile elde edilen ölçümler, z, içerisinde L tane doğrusal olmayan fonksiyon içeren $\mathrm{h}(\cdot)$ fonksiyon seti kullanılarak Eş. 1'deki doğrusal olmayan denklem sistemi üzerinden ilintilendirilebilir [1]

$$\mathrm{z} = \mathrm{h}(\mathrm{x}) + \mathrm{w}. \tag{1}$$

Öte yandan, yukarıdaki doğrusal olmayan denklem sistemi, literatürde sıklıkla kullanılan DC güç akış modeli ile doğrusallaştırılmaktadır [7]. Bu şekilde doğrusallaştırılmış sistem modeli Eş. 2 ile ifade edilir

$$\mathrm{z} = \mathrm{H}\mathrm{x} + \mathrm{w}. \tag{2}$$

Yukarıda, $L > Q$ olmak üzere, $\mathrm{H} \in \mathbb{R}^{L \times Q}$ sistem operatörlerince bilindiği varsayılan DC güç akış matrisini, w ise ölçüm gürültü vektörünü göstermektedir. Gözlem vektörü z'de yer alan ölçümler, şebeke elemanlarındaki senkronize olmayan aktif ve reaktif güç akışlarını, baralara enjekte olan güçleri, hat akımlarının ve bara voltajlarının genliklerini içerir. LS yöntemi kullanılarak kestirilen durum vektörü $\hat{\mathrm{x}} = (\mathrm{H}^T\mathrm{H})^{-1}\mathrm{H}^T\mathrm{z}$ formülü aracılığıyla bulunur.

3. α-KARARLI DAĞILIMLAR (α-STABLE DISTRIBUTIONS)

Gauss dağılım, sinyal işlemede gürültüyü modellemek için yaygın olarak kullanılmaktadır. Fakat dürtüsel bozulmaların

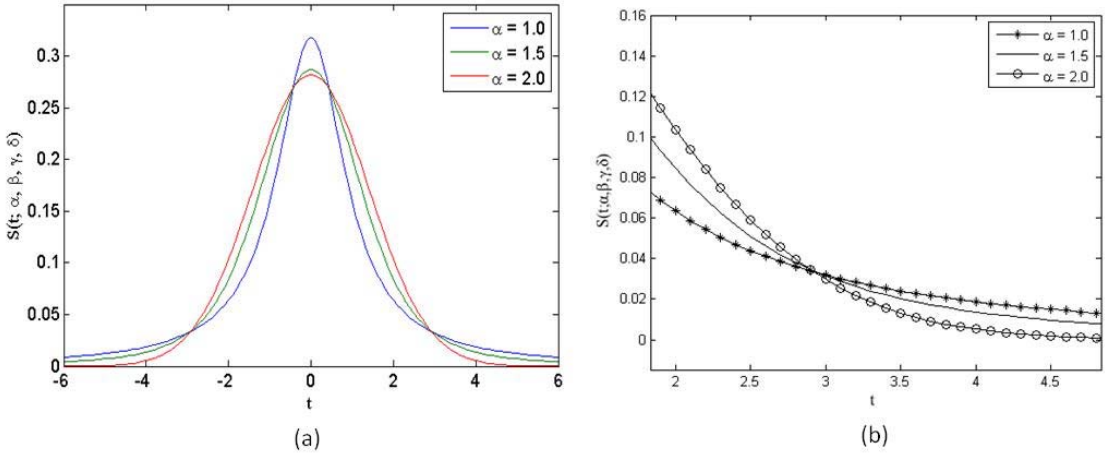
temsil edilmesinde yetersiz kalmaktadır. Bu nedenle, bu çalışmada dürtüsel gürültünün modellenmesinde kullanılan α-kararlı dağılım, karakteristik fonksiyonu cinsinden Eş. 3'deki gibi ifade edilir [17].

$$\varphi(\omega;\alpha,\beta,\gamma,\delta) = \begin{cases} \exp\left[j\omega\delta - |\gamma\omega|^{\alpha}\left(1 - j\frac{2}{\pi}\beta\,\mathrm{sgn}(\omega)\log|\omega|\right)\right], \alpha = 1 \\ \exp\left[j\omega\delta - |\gamma\omega|^{\alpha}\left(1 - j\beta\,\mathrm{sgn}(\omega)\tan\left(\pi\frac{\alpha}{2}\right)\right)\right], \alpha \neq 1. \end{cases} \quad (3)$$

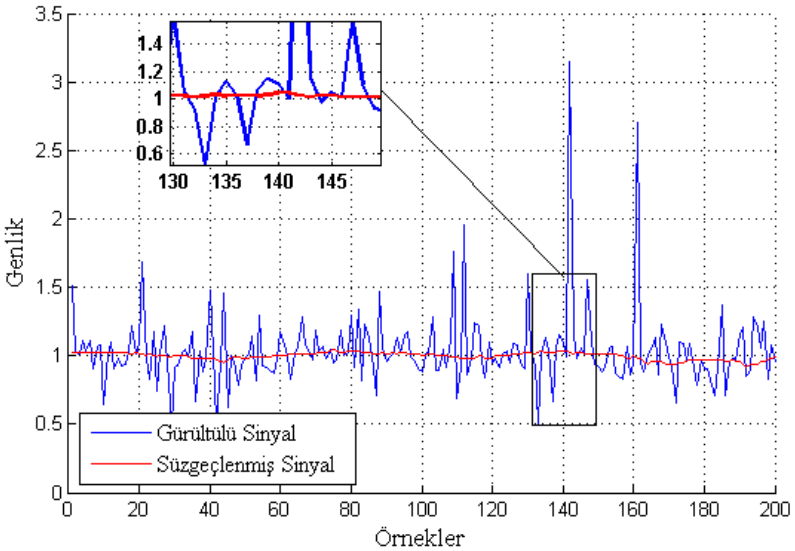
α-kararlı dağılım dört farklı parametre ile $S(t;\alpha,\beta,\gamma,\delta)$ şeklinde gösterilebilir. Karakteristik üstel $\alpha \in (0,2]$, dağılımın dürtüsellik derecesini, simetri parametresi $\beta \in [-1,1]$, dağılımın sağa veya sola eğik olmasını belirlerken, saçılım parametresi $\gamma > 0$, dağılımın şiddetini belirler ve Gauss dağılımdaki varyansa benzer bir işlev görür. Kayma parametresi $-\infty < \delta < +\infty$, dağılımın yatay eksendeki pozisyonunu belirler. Şekil 1a ve Şekil 1b'de görüldüğü üzere α küçüldükçe dağılım ağır kuyruklu bir yapıya dönüşmektedir. Simetrik dağılımda $\beta = 0$ olup, simetrik α-kararlı (SαS) dağılımın karakteristik fonksiyonu Eş. 4'teki gibidir,

$$\varphi(\omega;\delta,\gamma,\alpha) = \exp[\,j\omega\delta - |\gamma\omega|^{\alpha}\,] \quad (4)$$

Durum kestirimi için her bir baradaki karmaşık voltajın bulunması gerekmektedir. Yaptığımız çalışmada daha gerçekçi bir yaklaşım için karmaşık bara voltaj değerleri üzerine karmaşık gürültü eklenmiştir. Bu sebeple, gürültü izotropik karmaşık SαS rassal değişken kullanılarak modellenmiştir [17].



Şekil 1. a) Farklı α değerlerinde olasılık yoğunlukları ($\beta = 0,\ \gamma = 1,\ \delta = 0$) b) Farklı α değerlerinde olasılık kuyruk yoğunlukları ($\beta = 0,\ \gamma = 1,\ \delta = 0$)
(a) Probability densities for different α values ($\beta = 0,\ \gamma = 1,\ \delta = 0$).) (b) Tail probability densities for different α values ($\beta = 0,\ \gamma = 1,\ \delta = 0$))



Şekil 2. Dürtüsel gürültü ($\alpha = 1{,}8$) eklenmiş DC sinyal ve medyan süzgeç çıkışı
(Impulsive noise ($\alpha = 1{,}8$) added DC signal and the output of median filter)

4. GÜRBÜZ SÜZGEÇLER (ROBUST FILTERS)

Gürbüz süzgeçler, ölçüm verilerindeki gürültünün Gauss dağılımdan sapmasına karşı dayanıklı olma özellikleri ile karakterize edilebilirler. Aşağıda, bu çalışmada kullanılan üç farklı gürbüz süzgeç kısaca tanıtılmaktadır.

4.1. Medyan Süzgeç (Median Filter)

Medyan süzgeç, $s[.]$ kesikli zaman sinyali üzerinde simetrik bir pencere vasıtasıyla yatay eksen boyunca ilerler. Süzgeç, bulunduğu noktada sağındaki ve solundaki verilerden eşit sayıda alarak, bu verileri küçükten büyüğe sıralar ve ortanca değeri süzgeç çıkışına verir [4]. Bu işlem için gözlem aralığını belirleyen ve zamanla ilerleyen sabit uzunlukta bir pencere vektörü oluşturulur. Merkezi n anında olmak üzere pencere vektörü Eş. 5'deki gibi ifade edilir

$$\mathrm{s}[n] = [s[n-M_l], \dots, s[n], \dots, s[n+M_r]]^{\mathrm{T}}. \quad (5)$$

Eş. 5'te, M_l ve M_r negatif olmayan tamsayılar olmak üzere sırasıyla pencere vektörünün merkezden sola ve sağa doğru uzunluklarını belirtir. Pencere vektörünün toplam uzunluğu $M = M_l + M_r + 1$ şeklinde hesaplanır. Çoğunlukla pencere vektörü simetrik yapıda olduğundan $M_l = M_r = M_1$ olarak alınır. Simetrik bir gözlem vektörü için, zamana bağlı olarak medyan süzgeç çıkışı Eş. 6'da verilmektedir

$$y_{med}[n] =$$

$$\text{MEDYAN}\,(s[n-M_1], \dots, s[n], \dots, s[n+M_1]). \quad (6)$$

Şekil 2'de genliği 1 olan DC sinyalin üzerine, dürtüsel bileşenlerin yoğun olduğu α-kararlı dağılıma sahip ($\alpha = 1{,}8$) gürültü eklenmiş ve bu gürültülü sinyale medyan süzgeç işlemi uygulanmıştır. Görüldüğü üzere, $\alpha < 2$ iken medyan süzgeç dürtüsel sapmaları büyük oranda sönümlemiştir.

4.2. Meridian Süzgeç (Meridian Filter)

Sıfır ortalamalı Laplace dağılıma sahip bağımsız iki rassal değişkenin oranlanması ile elde edilen rassal değişkenin dağılımı meridian dağılım olarak tanımlanır [18]. M tane birbirinden bağımsız ve özdeş dağılıma sahip örnekler $s[n-M_1], \cdots, s[n], \cdots, s[n+M_1]$ olsun ve her biri ortak ölçek parametresi Δ (medyanlık) ile meridian dağılıma uysun. Örnek meridian, $y_{mer}[n]$, Eş. 7'deki denklem ile hesaplanır

$$y_{mer}[n] = \text{MERIDIAN}\begin{pmatrix}\Delta;\ s[n-M_1], \dots, \\ s[n], \dots, s[n+M_1]\end{pmatrix}$$

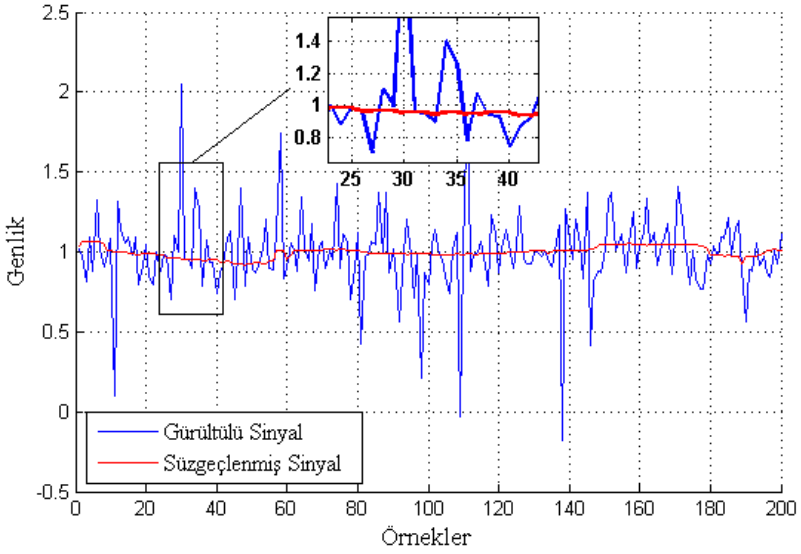
$$= \arg\min_{\eta\in\Re} \textstyle\sum_{i=n-M_1}^{n+M_1} \log[\Delta + |s[i]-\eta|]. \quad (7)$$

Yukarıda η, konum parametresi olarak adlandırılır. Δ, meridian süzgecin davranışını belirleyen ayarlanabilir bir parametredir. Dürtüsel ortamlarda medyanlık (Δ) düşük değerler alıyorsa, süzgeç daha güvenilir sonuç veriyor demektir [18]. Şekil 3'te de görüldüğü üzere $\alpha < 2$ iken medyan süzgece benzer şekilde meridian süzgeç de dürtüsel bileşenleri büyük oranda elimine etmiştir.

4.3. Myriad Süzgeç (Myriad Filter)

Myriad süzgeç, belirli bir dağılım altında maksimum olabilirlik kestirimine dayanan konum belirleme amaçlı bir süzgeç olup Gauss olmayan dağılımlar için uygun bir süzgeçtir. M tane birbirinden bağımsız ve özdeş dağılıma sahip örnekler $s[n-M_1], \cdots, s[n], \cdots, s[n+M_1]$ olsun.

Buna göre, $y_{myr}[n]$ Eş. 8 ile hesaplanır



Şekil 3. Dürtüsel gürültü ($\alpha = 1{,}8$) eklenmiş DC sinyal ve meridian süzgeç çıkışı
(Impulsive noise ($\alpha = 1{,}8$) added DC signal and the output of meridian filter)

$$y_{myr}[n] = \text{MYRIAD}\,(K;\, s[n-M_1], \ldots, s[n], \ldots, s[n+M_1])$$

$$= \arg\min_{\rho \in \Re} \sum_{i=n-M_1}^{n+M_1} \log[K^2 + (s[i]-\rho)^2]. \quad (8)$$

Yukarıda ρ, konum parametresi olarak adlandırılır. Gürültülü sinyalin ortalamasından aşırı derecede sapan örneklerden kaynaklanan yüksek hataların etkisi logaritma fonksiyonu tarafından zayıflatılır. Ölçek parametresi K'nın küçük bir değere sahip olması, süzgecin daha güvenilir sonuçlar vermesini sağlar [4]. Şekil 4'te de görüldüğü üzere $\alpha < 2$ iken myriad süzgeç de önceki gürbüz süzgeçler gibi dürtüsel bileşenleri büyük oranda sönümlemiştir.

5. VERİ ENJEKSİYONU SALDIRILARININ EN HIZLI TESPİTİ (QUICKEST DETECTION OF DATA INJECTION ATTACKS)

Eş. 2'de yer alan gözlenen durum değişkeni **z**'deki bozulmaların sebebi, güç sistemlerindeki fiziksel problemlerden kaynaklanabilen geçici ölçüm hataları olabileceği gibi, art niyetli birimlerin farklı amaçlarla sisteme yanlış veri enjekte etmesi şeklindeki saldırılar da olabilir. Bu durumun olabildiğince hızlı tespit edilmesi maddi ve fiziksel kayıpların önüne geçebilmek için önem taşımaktadır. Veri enjeksiyonu saldırısı altında ölçüm vektörünün modellenmesi aşağıda açıklanmaktadır.

5.1. Veri Enjeksiyonu Modeli (Data Injection Model)

DC güç akış modeline dayanan ve tek bir noktadan yapıldığı kabul edilen siber veri enjeksiyonu saldırısı durağan durum varsayımı altında Eş. 9'da modellenmektedir [7].

$$\mathrm{z} = \mathrm{Hx} + \mathrm{a} + \mathrm{w}. \quad (9)$$

Burada a, kötü niyetle enjekte edilmiş veriyi temsil eder. Eğer saldırı yapacak birim, H matrisi yani güç şebekesi hakkında ön bilgiye sahipse, ölçüm vektörü üzerine $\mathrm{a} = \mathrm{Hc}$ şeklinde bir vektör ekleyerek operatörü yanıltabilir. Bu durumda ölçüm vektörü Eş. 10'daki gibi olur [7].

$$\mathrm{z} = \mathrm{H}(\mathrm{x} + \mathrm{c}) + \mathrm{w}. \quad (10)$$

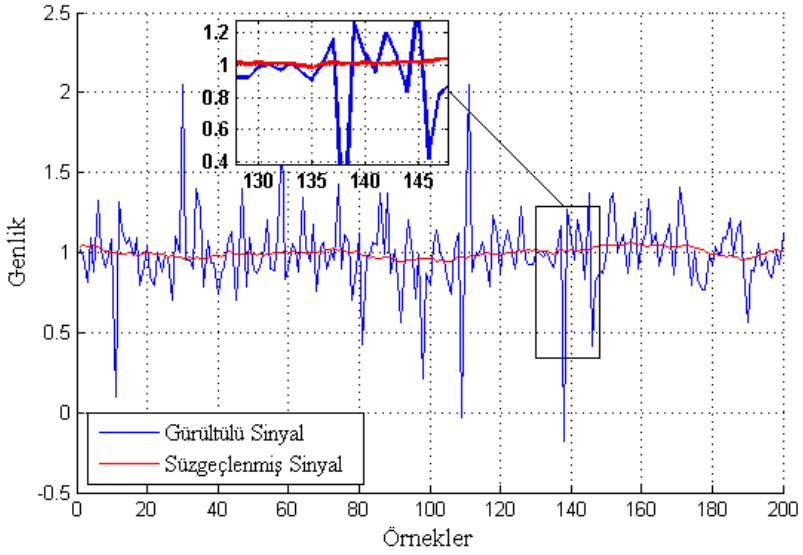
Böylelikle, operatör gerçek durum vektörünün $(\mathrm{x}+\mathrm{c})$ olduğuna inanır. Saldırı vektörü c, H matrisinin değer kümesi uzayı içinde yer alıyorsa, geleneksel istatistik testleri ile algılanamaz. Saldırı yapıldığı zaman, ölçüm vektörünün ortalama değeri bir sapma gösterecektir. Gürültü vektörü w, $S\alpha S$ dağılıma sahipse, saldırı öncesi δ_0 olan konum değeri, saldırı sonrası δ_1'e dönüşecektir. Bu durumda, ikili karar hipotezi Eş. 11 ile ifade edilir.

$$\begin{cases} H_0: \ \mathrm{z} \sim \mathrm{S}(\alpha, 0, \gamma, \delta_0) \\ H_1: \ \mathrm{z} \sim \mathrm{S}(\alpha, 0, \gamma, \delta_1). \end{cases} \quad (11)$$

a_τ'nun rassal bir τ zamanında yapılan bilinmeyen bir saldırı vektörünü, T_h'nin ise değişimin tespit edildiği zamanı temsil ettiği varsayılmak üzere, eğer $T_h < \tau$ ise henüz saldırı yokken alarm verilmiş demektir ve bu durum yanlış alarm olarak adlandırılır. $T_h > \tau$ durumunda ise $T_d = T_h - \tau$ zamansal gecikmeyi ifade eder. Saldırı zamanı, τ rassal değişkeni ile modellenirse, saldırı tespitindeki olası en büyük zaman gecikmesi Eş. 12'deki şekilde ifade edilebilir [19].

$$T_d = \sup_{\tau \geq 1} E_\tau[T_h - \tau |\, T_h \geq \tau]. \quad (12)$$

Yukarıda, $E_\tau[\cdot]$, τ cinsinden beklenen değer operatörünü temsil eder. Zamansal gecikmenin mümkün olduğunca azaltılması, kümülatif toplam (CUSUM) en hızlı tespit algoritması aracılığıyla gerçekleştirilebilir.



Şekil 4. Dürtüsel gürültü ($\alpha = 1{,}8$) eklenmiş DC sinyal ve myriad süzgeç çıkışı
(Impulsive noise ($\alpha = 1{,}8$) added DC signal and the output of myriad filter)

5.2. CUSUM En Hızlı Tespit Algoritması
(CUSUM Quickest Detection Algorithm)

CUSUM, değişim tespiti için geliştirilmiş bir analiz tekniğidir ve gecikmenin en aza indirgenmesinde oldukça etkilidir [19]. Bu çalışmada, tek bir noktadan yapıldığı varsayılan veri enjeksiyon saldırısı sonucunda ölçüm vektöründe meydana gelen değişimlerin tespiti için iki yönlü CUSUM yöntemi kullanılmıştır. Başlangıçta saldırı olmadığı kabul edilir ve bu durumda ortalama değer, ölçüm sonucunda bilindiği varsayılan α −kararlı dağılımın konum parametresi δ_0'a eşittir. Saldırı olduğunda bu değer $\delta_1{}^+ = \delta_0 + \mu\gamma$ veya $\delta_1{}^- = \delta_0 - \mu\gamma$ olur. Burada μ, ölçüm vektöründe saldırının gerçekleştiği elemanda tespit edilmek istenen kaymanın miktarı olup, γ ise α-kararlı gürültünün saçılım parametresidir. İki yönlü CUSUM algoritması kullanılarak saldırı tespit zamanı T_h, sırasıyla üst ve alt karar istatistikleri olan $g_n{}^+$ ve $g_n{}^-$ kullanılarak Eş. 13, Eş. 14 ve Eş. 15 ile bulunabilir [19].

$$T_h = \min\{n : (g_n{}^+ \geq \theta) \cup (g_n{}^- \geq \theta)\}, \quad (13)$$

$$g_n{}^+ = \max\left(0,\ g_{n-1}{}^+ + z_n - \delta_0 - \frac{v}{2}\right), \quad (14)$$

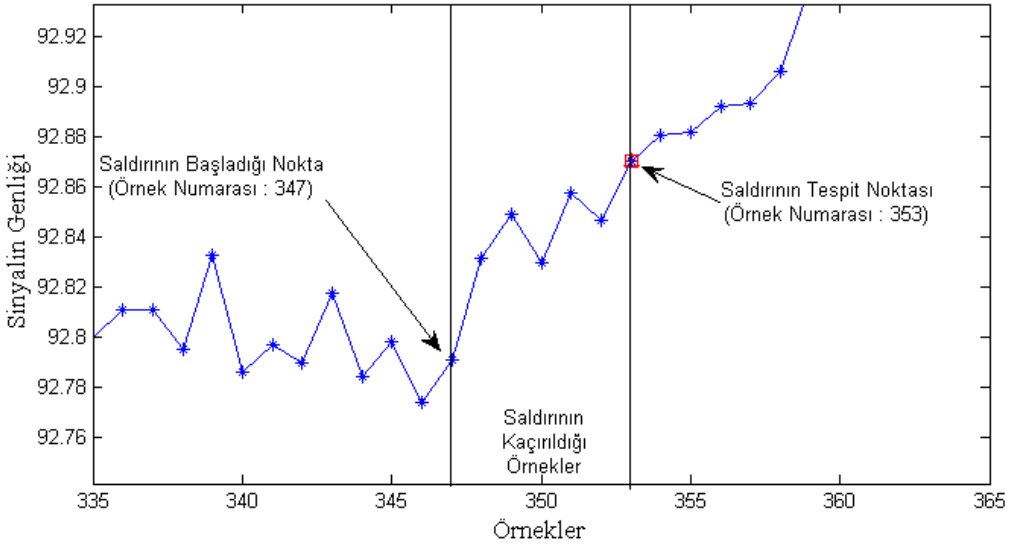
$$g_n{}^- = \max\left(0,\ g_{n-1}{}^- - z_n + \delta_0 - \frac{v}{2}\right). \quad (15)$$

Yukarıdaki denklemlerde, n örnekleme anını göstermekte olup başlangıç değerleri $g_0{}^+ = 0$ ve $g_0{}^- = 0$ olarak alınmıştır. z_n, ölçüm vektörünün saldırıya uğrayan elemanının n örnek noktasındaki ölçüm değerini ifade eder. v parametresi, algoritma tarafından kontrol edilen genlik değişimini temsil eder ve değeri genlikte oluşabilecek minimum sıçrama miktarına karşılık gelecek şekilde seçilebilir. Eğer $g_n{}^+$ veya $g_n{}^-$ belirlenen eşik değer θ'yı geçerse enjekte edilen veri saldırısı tespit edilmiş demektir. Şekil 5'te, bilinmeyen bir örnek noktasında meydana gelen saldırı ve belli bir süre sonra saldırının yakalandığı örnek noktası gösterilmektedir. Gösterimde, iki dikey çizgi arasında kalan örnekler ise saldırının tespit edilemediği örnekleridir ve bu aralığa karşılık gelen zamana ortalama tespit süresi denir. Amaç, ortalama tespit süresini en aza indirgemektir. Fakat CUSUM algoritmasında tespit süresi ile tespit güvenilirliği arasında bir seçim söz konusudur. Bundan dolayı, operasyon hassasiyetine en uygun eşik değeri, θ, seçilmelidir. Büyük seçilen eşik değerleri, tespit süresini artırmakla birlikte, tespit güvenilirliğinin de artmasını sağlamaktadır. Küçük seçilen eşik değerleri ise tespit süresini kısaltırken, yanlış alarmların sayısını artırır. Son olarak vurgulamak isteriz ki, olası bir veri enjeksiyon saldırısı önceden bilinmesi mümkün olmayan herhangi bir ölçüm barasından gerçekleştirilebileceği için iki yönlü CUSUM saldırı tespit algoritmasının ölçüm alınan tüm baralara uygulanması gerekmektedir.

6. BENZETİM SONUÇLARI (SIMULATION RESULTS)

6.1. Durum Kestirimi Sonuçları (State Estimation Results)

Bu çalışmada dürtüsel gürültü altında, LS ve gürbüz süzgeçler kullanılarak durum kestirimi yapılmıştır. Eş. 2'de yer alan sistem modelinde H matrisi için IEEE 3 baralı sistem güç akış matrisi kullanılmıştır. Karmaşık değerli bara voltajları "*MATLAB Matpower Toolbox*"ında [20] oluşturulmuş ve üzerine karmaşık değerli izotropik $S\alpha S$ gürültü eklenmiştir. Simülasyonlarda kullanılan veri $N = 1000$ örnek içermektedir. Her bir baradaki süzgeçleme sonucu, gürültünün dürtüselliğini gösteren karakteristik üstel α'ya bağlı olarak aynı istatistiksel davranışı göstereceğinden, süzgeç performansları tek bir baradaki ölçümler kullanılarak



Şekil 5. Saldırı noktası, saldırının kaçırıldığı örnekler ve tespit noktası
(Attack point, missed attack samples and detection point)

irdelenmiştir. Gürbüz süzgeçlerin formülasyonlarında H matrisine ihtiyaç olmamakla birlikte, süzgeçlemeye giren veri, H matrisi kullanılarak oluşturulmuş olan gürültülü ölçüm verisidir. Dolayısıyla, en küçük kareler yönteminin sonucunu bulurken, $\hat{\mathrm{x}} = (\mathrm{H}^T\mathrm{H})^{-1}\mathrm{H}^T\mathrm{z}$ formülü uyarınca gürültülü verinin oluşturulmasında yer alan ve sistem operatörlerince bilindiği varsayılan H matrisi kullanılmıştır. DC sinyal genliği A olmak üzere, sinyalin gürültüye oranını göstermek için α-kararlı dağılımlarda gürültü şiddetini tanımlayan saçılım parametresi, γ, kullanılmış olup, Sinyal-Saçılım Oranı (SSO) desibel cinsinden Eş. 16'daki şekilde ifade edilmiştir

$$\mathrm{SSO} = 10\log_{10}\frac{A^2}{2\gamma^{2/\alpha}}. \qquad (16)$$

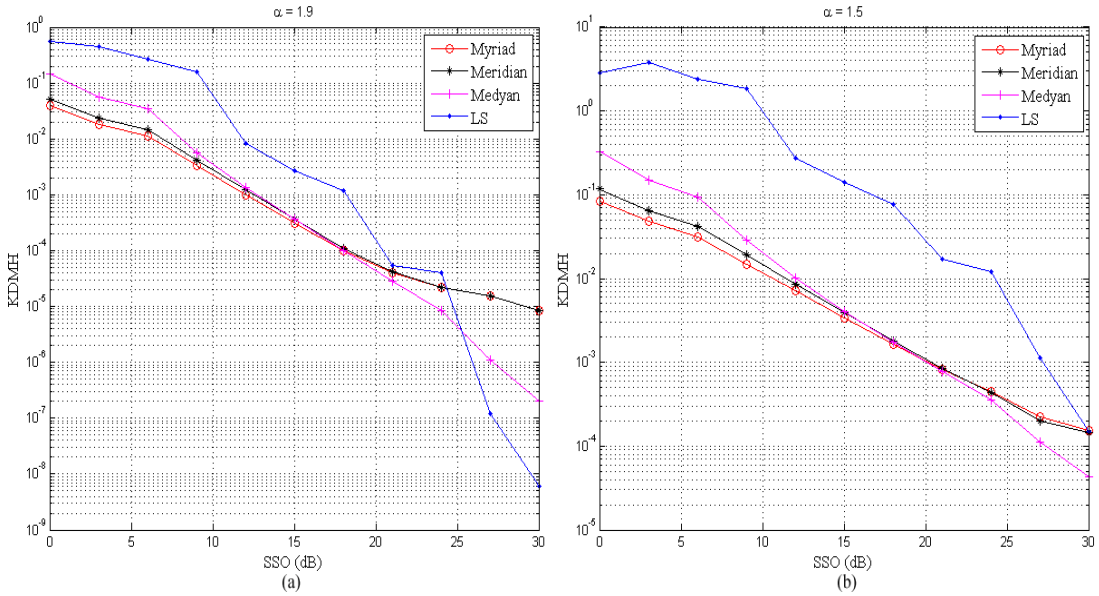
Kullanılan süzgeçler için her SSO noktasında birbirinden bağımsız 200 benzetim yapılmıştır. $\alpha = 1{,}9$ ve $1{,}5$ değerleri için benzetim sonuçları incelenmiş ve süzgeç performansları birbirleri ile kıyaslanmıştır. Bütün gürbüz süzgeçler için pencere genişliği $M = 21$ örnek alınmıştır. Grafiklerde yatay eksen, SSO'yu gösterirken, dikey eksen ise Eş. 17'de logaritmik olarak tanımlanan "Kesirli Düşük Mertebeden Hata"yı (KDMH) göstermektedir

$$\mathrm{KDMH} = 10\log_{10}\left(\frac{1}{N}\sum_{n=1}^{N}|y[n]-A|^p\right), \quad p < \alpha. \qquad (17)$$

Eş. 17'de, bu çalışmada kullanılan tüm gürbüz süzgeçlerin çıkış sinyalleri ortak bir isimle $y[n]$ olarak gösterilmiş olup, $p = \alpha - 0.01$ olarak alınmıştır. Şekil 6a'da $\alpha = 1{,}9$ ve $p = 1{,}89$ alınmış olup $S\alpha S$ gürültünün dağılımının Gauss $(\alpha = 2)$ dağılımına yakın olduğu söylenebilir. Myriad ve meridian süzgeçlerin benzer performans gösterdiği, medyan süzgeç ve LS'nin yüksek SSO'lar için daha iyi sonuçlar verdiği görülmektedir. Diğer üç süzgeç ise genel anlamda LS'den daha iyi performans göstermektedirler. Şekil 6b'de ise, $\alpha = 1{,}5$ ve $p = 1{,}49$ için dürtüselliğin arttığı bir durumda, myriad ve meridian süzgeçler genel olarak en iyi performansı gösterirken, medyan süzgeç SSO'nun yüksek olduğu 20 - 30 dB aralığında en iyi performansı vermektedir.

6.2. En Hızlı Tespit Algoritması (CUSUM) Performans Sonuçları
(Performance Results of Quickest Detection Algorithm (CUSUM))

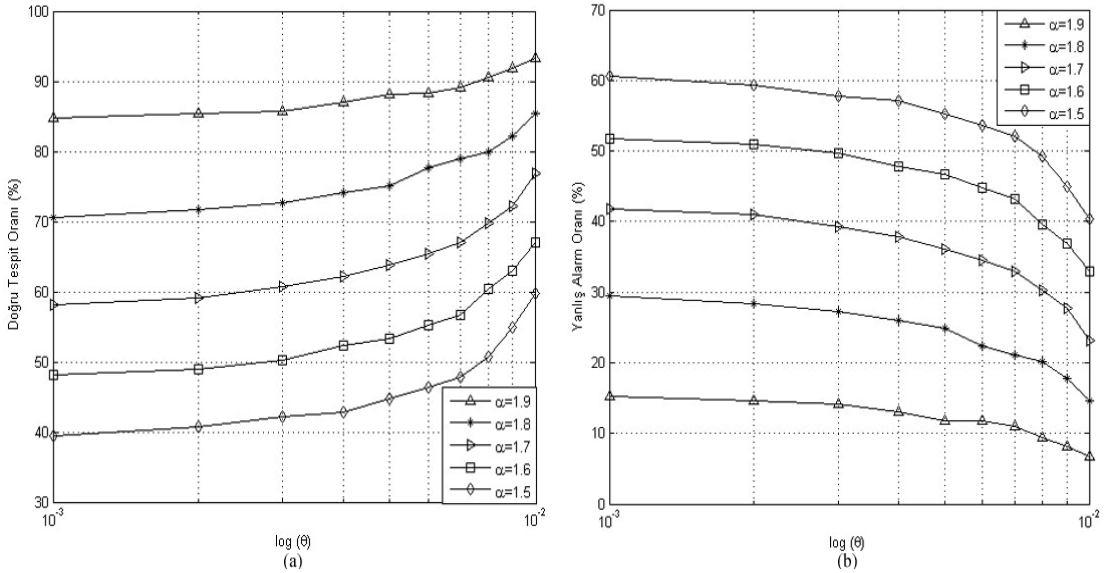
Farklı α değerleri için CUSUM algoritmasının performans testleri yapılmış ve CUSUM tekniğinin dürtüsel ortamlardaki davranışı incelenmiştir. Simülasyonlarda veri uzunluğu $N = 1000$ örnektir. $\alpha = 1{,}5,\ 1{,}6,\ 1{,}7,\ 1{,}8$ ve $1{,}9$ değerleri için birbirinden bağımsız 10000 saldırı gerçekleştiği varsayılmıştır. Aşağıdaki sonuçlardan da görüleceği gibi dürtüselliğin artması, CUSUM tekniğinin saldırı tespit performansını düşürmektedir. Bu tarz gürültünün güçlü olduğu ortamlarda doğru tespit oranını artırmak için eşik değeri, θ, daha büyük seçilebilir. Şekil 7(a)'da görüldüğü gibi α'nın düşmesi dürtüselliği artırmış ve bunun sonucunda CUSUM tekniğinin saldırı tespit performansını düşürmüştür. Saldırıdan önce gözlenen gürültü kaynaklı dürtüsel bileşenler CUSUM tekniğinin erken sonlandırılmasına sebep olmuştur. Yani belirlenen eşik değeri dürtüsel gürültü bileşenleri yüzünden aşılmış, saldırının tespiti başarısız olmuştur. α değerinin düşmesinin yanlış alarm oranını artırdığı Şekil 7b'de görülmektedir. Yanlış alarmlardan kaçınmak için eşik değeri, θ, daha büyük seçilebilir. Fakat eşik değerinin büyük seçilmesinin ortalama tespit süresini artıracağı unutulmamalıdır. Şekil 8'de görüldüğü gibi α'nın büyük değerler alması, ortalama tespit süresini artırmaktadır. Dolayısıyla, dürtüsel ortamlarda



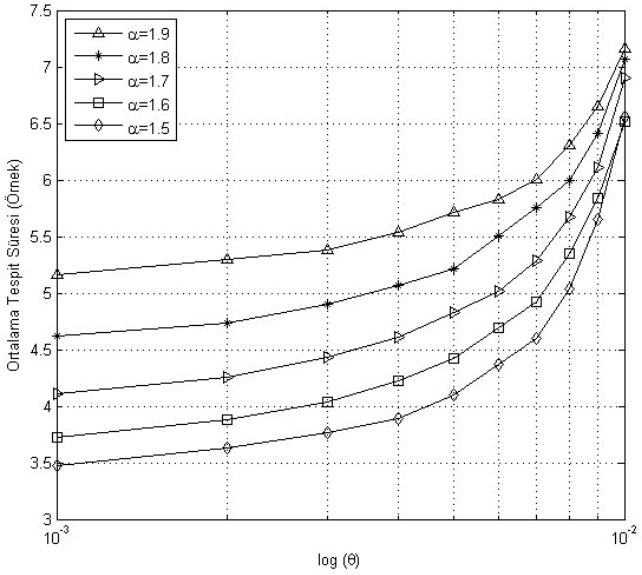
Şekil 6. a) $\alpha = 1{,}9$ $p = 1{,}89$ b) $\alpha = 1{,}5$ $p = 1{,}49$ için süzgeçlerin hata performansları
(Error performances of filters for a) $\alpha = 1.9$ $p = 1.89$ b) $\alpha = 1.5$ $p = 1.49$)

CUSUM tekniğinin doğru karar vermesi zorlaşmaktadır. Daha önce de belirtildiği gibi ortalama tespit süresi ile doğru tespit oranı arasında bir seçim söz konusudur. Uygulamanın hassasiyetine göre bir eşik değeri seçilmelidir. Çok büyük bir eşik değerinin seçilmesi, saldırı tespiti için gereğinden fazla zaman harcanmasına sebep olabileceği gibi, çok küçük seçilen eşik değeri de doğru tespit oranını önemli miktarda düşürebilir. Yakın geçmişte literatürde yer alan bir çalışmada [21], Gauss gürültüsü varsayımı altında, veri enjeksiyon saldırılarının tespitinde "Chi kare testi" ve "kosinüs benzerlik eşleştirme yaklaşımı" yöntemleri kullanılmıştır. Şekil 9a ve Şekil 9b'de, makalemizde kullanılan CUSUM yönteminin performansının Doğru Tespit Oranı ve Ortalama Tespit Süresi açısından bu iki yöntemle kıyaslanması gösterilmektedir. [21]'de gürültü Gauss dağılımı ile modellenmiş olup bu makaledeki $\alpha-$kararlı dürtüsel gürültü daha genel bir olasılık yoğunluk fonksiyonuna sahiptir. Gürültü modelimizin Gauss olmayışı nedeniyle, her iki yöntemin de CUSUM tekniğine kıyasla daha düşük performans gösterdiği gözlemlenmiştir. Chi kare testi, ölçülen değerlerin karelerinin toplamının bir eşik değeri ile karşılaştırılması esasına dayanır [21].

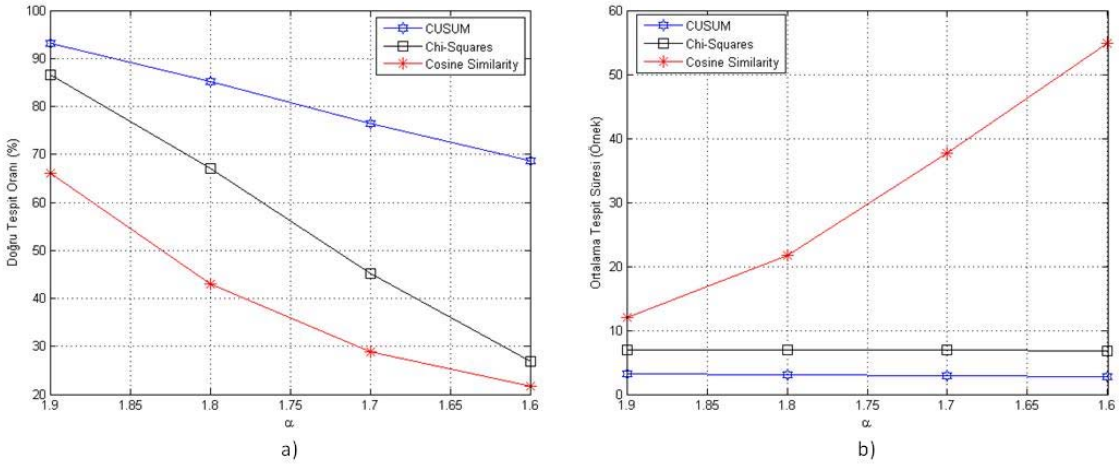
Ancak, $\alpha-$kararlı dağılıma sahip örneklerin sonlu bir varyansı olmamasından dolayı bilhassa azalan α değerlerinde (artan dürtüsellikte) Chi kare testinin doğru tespit oranının düştüğü gözlemlenmiştir. [21]'de önerilen kosinüs benzerlik eşleştirme yaklaşımı ise Kalman süzgeci kullanımını içermekte olup, bu süzgeç Gauss gürültü modeli varsayımı altında geliştirilmiş bir süzgeçtir.



Şekil 7. a) Doğru tespit oranı b) Yanlış alarm oranı eşik değeri ilişkisi (a) Detection ratio (b) False alarm ratio versus threshold value)



Şekil 8. Ortalama tespit süresi ve eşik değeri ilişkisi (Average run length versus threshold value)



Şekil 9. Performans karşılaştırması a) Doğru Tespit Oranı b) Ortalama Tespit Süresi
(Performance comparison a) Detection Ratio b) Average Run Length)

Öte yandan, bu makalede $\alpha-$kararlı gürültü modeli kullanıldığı için, kosinüs benzerlik eşleştirme yaklaşımı Kalman süzgeci yerine en küçük kareler yöntemi kullanılarak uygulanmıştır. Karakteristik üstel, α, azaldıkça (dürtüsellik arttıkça), bu yaklaşımın da Doğru Tespit Oranı'nın azaldığı Şekil 9a'da görülebilir. Ortalama Tespit Süre'leri kıyaslandığında ise yüksek dürtüsel bileşenlere bağlı olarak en fazla performans düşümü kosinüs benzerlik eşleştirme yaklaşımında görülmüştür. Bu yöntemlerin hepsinin performansının aynı ölçekte gösterilebilmesi için Şekil 9a ve Şekil 9b'de gürültü şiddetine karşılık gelen saçılım parametresi $\gamma = 0{,}0005$ olarak alınmıştır. Bu nedenle, Şekil 9a ve Şekil 9b'de elde edilen değerler saçılım parametresinin $\gamma = 0{,}001$ olarak seçildiği Şekil 7 ve Şekil 8'de elde edilmiş olan Doğru Tespit Oranı ve Ortalama Tespit Süresi değerleri ile farklılık göstermektedir.

7. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, α-kararlı dağılımla modellenmiş gürültü altında durağan durum kestirimi ve veri enjeksiyonu saldırısı tespiti problemleri irdelenmiştir. Durum kestirimi için genellikle tercih edilen LS yöntemine alternatif olarak gürbüz süzgeçler (meydani meridian, myriad) incelenmiş ve dürtüsel ortamlarda gürbüz süzgeçlerin LS'ye kıyasla daha iyi sonuçlar verdiği görülmüştür. Veri enjeksiyonu saldırısını tespit etmek için kullanılan CUSUM tekniğinde eşik değerinin seçimi, sonucu doğrudan etkilemektedir. Bu çalışmada veri enjeksiyonu saldırısının tek bir noktadan yapıldığı varsayımı altında CUSUM tekniği kullanılarak saldırının tespiti gerçekleştirilmiştir. Literatürde yer alan iki farklı yöntemle performans karşılaştırması yapılmış ve CUSUM tekniğinin daha iyi sonuç verdiği görülmüştür.

KAYNAKLAR (REFERENCES)

1. Huang Y.F., Werner S., Huang J., Kashyap N., Gupta V., State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid, IEEE Signal Processing Magazine, 29 (5), 33-43, 2012.
2. Yang Q., Chang L., Yu W., On False Data Injection Attacks Against Kalman Filtering in Power System Dynamic State Estimation, Security and Communication Networks – Special Issue, 9 (9), 833-849, 2013.
3. Khalili A., Rastegarnia A., Sanei S., Robust Frequency Estimation in Three-Phase Power Systems Using Correntropy-Based Adaptive Filter, IET Science, Measurement & Technology, 9 (8), 928-935, 2015.
4. Arce G.R., Nonlinear Signal Processing: A Statistical Approach, John Wiley & Sons Inc., New Jersey, USA, 2005.
5. Aysal T.C., Barner K.E., Meridian Filtering for Robust Signal Processing, IEEE Transactions on Signal Processing, 55 (8), 3949-3962, 2007.
6. Anwar A., Mahmood A.N., Shah Z., A Data-Driven Approach to Distinguish Cyber-Attacks from Physical Faults in a Smart Grid, Proceedings of the 24th ACM International Conference on Information and Knowledge Management (CIKM'15), Melbourne-Australia, 1811-1814, 19-23, 2015.
7. Cui S., Han Z., Kar S., Kim T.T., Poor H.V., Tajer A., Coordinated Data-Injection Attack and Detection in the Smart Grid: A Detailed Look at Enriching Detection Solutions, IEEE Signal Processing Magazine, 29 (5), 106-115, 2012.
8. Yang Q., Yang J., Yu W., An D., Zhang N., Zhao W., On False Data-Injection Attacks Against Power System State Estimation: Modeling and Countermeasures, IEEE Transactions on Parallel and Distributed Systems, 25, (3) 717-729, 2014.
9. Liu L., Esmalifalak M., Ding Q., Emesih V.A., Han Z., Detecting False Data Injection Attacks on Power Grid by Sparse Optimization, IEEE Transactions on Smart Grid, 5 (2), 612-621, 2014.
10. Qin Z., Li Q., Chuach M.C., Defending Against Unidentifiable Attacks in Electric Power Grids, IEEE

Transactions on Parallel and Distributed Systems, 24, (10) 1961-1971, 2013.

11. Giani A., Bitar E., Garcia M., McQueen M., Khargonekar P., Poolla K., Smart Grid Data Integrity Attacks, IEEE Transactions on Smart Grid, 4 (3), 1244-1253, 2013.

12. Yu Z.H., Chin W.L., Blind False Data Injection Attacks Using PCA Approximation Method in Smart Grid, IEEE Transactions on Smart Grid, 6 (3), 1219-1226, 2015.

13. Chaojun G., Jirutitijaroen P., Motani M., Detecting False Data Injection Attacks in AC State Estimation, IEEE Transactions on Smart Grid, 6 (5), 2476-2483, 2015.

14. Samet R., Çelik Ö.F., Fake GSM Base Station Attack Detection Algorithm, Journal of the Faculty of Engineering and Architecture of Gazi University, 31 (1), 161-169, 2016.

15. Poor H.V., Hadjiliadis O., Quickest Detection, Cambridge University Press, Cambridge, UK, 2008.

16. Li S., Yılmaz Y., Wang X., Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids, IEEE Transactions on Smart Grid, 6 (6), 2725-2735, 2015.

17. Samorodnitsky G., Taqqu M.S., Stable Non-Gaussian Random Processes: Stochastic Models with Infinite Variance, CRC Press, Florida, USA, 1994.

18. Pander T., Przybyła T., Impulsive Noise Cancellation with Simplified Cauchy-Based P-norm Filter, Signal Processing, 92 (9), 2187–2198, 2012.

19. Basseville M., Nikiforov I.V., Detection of Abrupt Changes, Prentice Hall, New Jersey, USA, 1993.

20. Zimmerman R.D., Murillo-Sanchez C.E., Gan D., MATPOWER, A MATLAB Power System Simulation Package, http://www.pserc.cornell.edu//matpower/. Yayın Tarihi; Aralık 16, 2016. Erişim Tarihi: Nisan 26, 2017.

21. Rawat D.B., Bajracharya C., Detection of False Data Injection Attacks in Smart Grid Communication Systems, IEEE Signal Processing Letters, 22 (10), 1652-1656, 2015.