İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

GSM ŞEBEKELERİNDE İSTATİSTİKSEL ÖĞRENME YÖNTEMLERİ İLE AKSAKLIK YÖNETİMİ

YÜKSEK LİSANS TEZİ

Mehmet Onur SARKAN

Anabilim Dalı : Bilgisayar Bilimleri

Programı : Bilgisayar Bilimleri

HAZİRAN 2011

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ BİLİŞİM ENSTİTÜSÜ

GSM ŞEBEKELERİNDE İSTATİSTİKSEL ÖĞRENME YÖNTEMLERİ İLE AKSAKLIK YÖNETİMİ

YÜKSEK LİSANS TEZİ
Mehmet Onur SARKAN
(704041012)

Tezin Enstitüye Verildiği Tarih : 20 Aralık 2010
Tezin Savunulduğu Tarih : 22 Haziran 2011

Tez Danışmanı : Doç. Dr. Zehra ÇATALTEPE
Diğer Jüri Üyeleri : Yrd. Doç. Dr. Feza BUZLUCA
Yrd. Doç. Dr. Güneş KURT

HAZİRAN 2011

Bu çalışma, desteklerini hiçbir zaman esirgemeyen annem ve eşime adanmıştır. Katkılarından dolayı tez danışmanım Doç. Dr. Zehra Çataltepe'ye en içten teşekkürlerimi sunarım.

ÖNSÖZ

Mobil teknolojilerin hayatımızın ayrılmaz bir parçası haline gelmesi ve artan rekabet koşullarında müşterilerin şebeke işletmecisi firmalardan aldıkları hizmetlerin kalitesi konusunda beklentilerinin çok yükselmesi ile aksaklık yönetimi süreçlerinin önemi yükselmiştir. Mobil haberleşme şebekelerinde kesintisiz ve kaliteli hizmetin verilmeye devam edilebilmesi için karşılaşılan aksaklıkların azalması ve aksaklıklarla karşılaşıldığında müşterilere mümkün olan en az şekilde hissettirilip hızlıca çözülmeleri gerekmektedir. Gelişen teknoloji ile birlikte mobil haberleşme şebekelerinde kullanılan cihazlar çeşitlenmekte ve şebekelerin boyutları çok büyümektedir. Ülkemizde bulunan mobil şebeke işletmecisi firmalar her gün şebekelerindeki cihazlardan yüz binlerce alarm almaktadırlar. Hizmet kalitesinin devamı için bu alarmların uzman kişiler tarafından incelenmesi ve gerekli çözüm aksiyonlarının alınması gerekmektedir. İncelenmesi gereken alarm sayısının yüksekliği şebeke gözlem uzmanlarının harcaması gereken zamanı arttırdığı gibi önemli problemlerin geç farkedilip müdahalelerin gecikmesine neden olabilmektedir. Yüksek alarm sayısı ile mücadelede en yaygın kullanılan yöntem farklı çeşitlerde alarm filtrelerinin üretilmesidir. Şebeke gözlem uzmanları, milyonlarca alarm içeren alarm tarihçesini inceleyerek kullanılacak alarm filtrelerinin kurallarına karar vermektedir. Alarm sayılarını düşürmeye yönelik filtre kurallarının belirlenmesi çok zaman alan bir süreçtir ve birçok muhtemel filtre adayı gözlem uzmanlarının gözünden kaçabilmektedir. Sürekli değişen ve gelişen haberleşme şebekelerinde, oluşan alarmlar da zamanla değiştiği için eski alarm filtre kurallarının da güncellenme ihtiyacı olabilmektedir. Tez çalışmamız kapsamında, yüksek alarm sayısını düşürmek için yaratılan alarm filtrelerinin otomatik üretimi için şebeke gözlem uzmanlarına ihtiyaç duyulmadan alarm tarihçesini kullanan çeşitli istatistiksel öğrenme yöntemleri önerilmiştir.

Haziran 2011

Mehmet Onur Sarkan

Telekomünikasyon Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

AIS **:** Alarm Indication Signal (Uyarı Belirtme Sinyali)
ATM **:** Asynchronous Transfer Mode (Asenkron Transfer Modu)
BSC **:** Base Station Controller (Baz İstasyon Kontrol Birimi)
BTS **:** Base Transceiver Station (Baz Alıcı Verici Sistemi)
CORBA **:** Common Object Request Broker Architecture (CORBA Protokolü)
GSM **:** Global System for Mobile Communication
HLR **:** Home Location Register (Abone Ana Kütüğü)
MGW **:** Media Gateway (Ortam Geçidi)
MMS **:** Multimedia Messaging Services (Çoğulortam Mesajlaşma Servisi)
MSC **:** Mobile Switching Center (Mobil Anahtarlama Merkezi)
NTT **:** Nippon Telegraph and Telephone (Nippon Telgraf ve Telefon)
OSI **:** Open Systems Interconnection (Açık Sistemler Arabağlaşımı)
PDA **:** Personal Digital Assistant (Elektronik Ajanda)
POS **:** Point of Sale (Satış Noktası)
SMS **:** Short Message Service (Kısa Mesaj Servisi)
SNMP **:** Simple Network Management Protocol (SNMP Protokolü)
SS7 **:** Signal System #7 (SS7 Protokolü)
STP **:** Signal Transfer Point (Sinyal İletim Noktası)

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

GSM ŞEBEKELERİNDE İSTATİSTİKSEL ÖĞRENME YÖNTEMLERİ İLE AKSAKLIK YÖNETİMİ

ÖZET

Bu çalışmada, GSM şebekeleri aksaklık yönetimi sistemlerine gelen alarmlar için istatistiksel öğrenme yöntemleri ile otomatik filtre kuralları üretimi için algoritmalar geliştirilip, Türkiye'nin en büyük GSM şebeke işletmeci firmasının alarm veri tabanı üzerinde deneysel testleri yapılmıştır. Çalışma iki farklı ihtiyaca odaklanmıştır: Geçici alarmların filtrelenmesi ve ilintili alarmların filtrelenmesi.

Geçici alarm filtrelerinin üretiminde dağılımdan bağımsız olasılık kestirimi yöntemlerinden *Histogram Analizi* ve *Parzen Penceresi Analizi* yöntemlerinden faydalanılmıştır. Alarm tarihçesi incelenerek her bir alarm tipi için birikimli alarm yaşam süresi histogramları ve yoğunluk fonksiyonları üretilmiştir. Histogramlar ve yoğunluk fonksiyonları incelenerek geçici alarm tipleri ve bu alarm tipleri için uygun alarm bekletme filtreleri tahmin edilmeye çalışılmıştır. Literatürde bu konuda daha önceden gerçekleştirilmiş bir çalışma olmadığı için geçici alarm filtrelerinin üretimi için önerilen iki yöntem türünün ilk örnekleri durumundadır. *Histogram Analizi* ve *Parzen Penceresi Analizi* yöntemlerinin geçici alarm filtreleri üretimi konusundaki başarı performansları karşılaştırmalı olarak incelenmiştir. *Parzen Penceresi Analizi* içindeki çekirdek fonksiyonun yumuşatma etkisi sayesinde incelenen alarm örnek sayısının düşük durumlarda daha başarılı iken, alarm örnek sayısının yüksek olduğu durumlarda *Histogram Analizi* daha başarılı sonuçlar sergilemiştir.

İlintili alarmları filtrelemek amacıyla kullanılan filtreleri üretebilmek için alarm tipleri arasındaki ihtimalsel ilişkilerden faydalanılmıştır. Alarm tarihçesindeki alarmlar kayan zaman penceresi yöntemi ile incelenerek eş kaynaktan yakın zamanlarda gelen alarm tipi gruplarının beraber gözlemlenme frekansları hesaplanmıştır. Hesaplanan gözlemlenme frekansları kullanılarak *Pazar Sepet Analizi* tekniklerinde kullanılan en yaygın altı benzerlik ölçütü hesaplanmış ve hesaplanan benzerlik ölçütleri ile alarm filtrelerinde kullanılacak ilintili alarm tiplerinin öğrenilmesi konusunda deneysel çalışmalar yapılmıştır. Kullanılan benzerlik ölçütleri *Etki, Maksimum Güven, Minimum Güven, Tutarlılık, Cosine* ve *Kulczynski* benzerlikleridir. İlintili alarm filtreleri üretilmesi konusunda önerilen altı benzerlik ölçütünün de başarılı sonuçlar verdiği gözlemlenmiştir. Benzerlik ölçütlerini beraber kullanarak daha başarılı sonuçlar elde etmek için *S Biçimli Sınıflandırma* yöntemi kullanılmış ve benzerlik ölçütlerinin tek başlarına sağlayabilecekleri sonuçlardan daha başarılı sonuçlar elde edilmiştir. Bu çalışmanın sonunda alarm ilintilendirme kurallarının öğrenilmesi amacıyla farklı benzerlik ölçümlerinin gücünü birleştirdiği ve benzerlik eşiklerinin de öğrenilmesini sağladığı için *S Biçimli Sınıflandırma* en başarılı yöntem olarak tavsiye edilmiştir.

GSM NETWORK FAULT MANAGEMENT BY USING STATISTICAL LEARNING METHODS

SUMMARY

In this study, new algorithms are presented to generate automatic alarm filters by using statistical learning methods. Suggested algorithms are tested on Turkey's biggest GSM Company's alarm history. In this study, two main areas are focused: Filtering of transient alarms and filtering of correlated alarms.

To produce transient alarm filters, two non-parametric density estimation approaches are used: *Histogram Analysis* and *Parzen Window Analysis*. By investigating alarm history, cumulative alarm lifetime histograms and density functions are produced for each alarm type. By analyzing calculated cumulative alarm lifetime histograms and density functions, transient alarm types and suitable transient alarm filter parameters are estimated. In the literature, there is no similar work, so suggested both approaches are firsts of its kinds. Learning performance of *Histogram Analysis* and *Parzen Window Analysis* are tested with comparision. Results show that *Histogram Analysis* and *Parzen Window Analysis* methods are successful to detect transient alarm types and estimate suitable transient alarm filter parameters. On the other hand, *Parzen Window Analysis* shows better results with inefficient number of alarm sample because of Kernel function's smoothing effect, and *Histogram Analysis* has better results with efficient number of alarm sample. In addition, *Histogram Analysis* is faster than *Parzen Window Analysis*.

To produce alarm filters which can filter correlated alarms, we used probabilistic relationships between different alarm types. Historical alarms are investigated by using sliding time window method to calculate alarm types co-occurrences counts. To be able to detect correlated alarm types, six most common similarity measurement types of *Market Basket Analysis* are used. These similarity measurements are *Lift* similarity, *Maximum Confidence* similarity, *Minimum Confidence* similarity, *Coherence* similarity, *Cosine* similarity, and *Kulczynski* similarity. Experimental results show that six similarity measurements of *Market Basket Analysis* are successful to detect correlated alarm types. To combine six different similarity measurements, and to be able to produce more successful experimental results, *Logistic Regression* is used to determine correlated alarm types, and results are better than each similarity type. In this study, to determine correlated alarm types, *Logistic Regression* is suggested because this method can combine power of each similarity measurement and similarity thresholds can be learned by experiences.

1. GSM/CEP TELEFONU ŞEBEKESİNDE AKSAKLIK YÖNETİMİ

Japonya'da 1979 yılında NTT firması tarafından dünyada ilk defa cep telefonu hizmetinin verilmeye başlamasından bu yana teknoloji hızla gelişerek mobil hizmetler hayatımızın ayrılmaz birer parçası haline geldi. 2010 yılı itibariyle dünya üzerindeki cep telefonu kullanıcı sayısı 3,5 milyarın üzerine çıkmıştır. Artık cep telefonları sadece konuşmak için kullanılan cihazlar değillerdir. Değişen müşteri ihtiyaçları ve gelişen teknoloji ile mobil şebekeler üzerinden verilen hizmetlerin sayısında bir patlama yaşanmıştır. Günümüzde cep telefonları ile SMS/MMS gibi gelişmiş mesajlar gönderebilmekteyiz. İnternete bağlanabilmekte, istediğimiz yerde elektronik postalarımızı kontrol edebilmekteyiz. Sevdiklerimizle görüntülü görüşmeler yapıp, çocuklarımızın gün içinde nerelere gitmiş olduklarını öğrenebilmekteyiz. Sevdiğimiz müzikleri cep telefonlarımıza indirip dinleyebilmekte, çektiğimiz video ve resimleri sosyal paylaşım sitelerine yükleyip arkadaşlarımızla paylaşabilmekteyiz. Resmi işlemlerde ıslak imza yerine mobil imza kullanıp, internet üzerinden yaptığımız bankacılık işlemlerini bize özel SMS mesajlarındaki şifrelerle güvenli bir şekilde onaylayabilmekteyiz. Alışveriş ödemelerimizi cep telefonları ile yapıp, bilgilendirme servisleri ile spor, ekonomi ve hava durumu haberlerini güncel bir şekilde temin edilebilmekteyiz. Yeni nesil mobil hizmetlerin sayısı her geçen gün artmakta ve çeşitlenmektedir. Kısacası cep telefonu şebekesi üzerinden verilen hizmetler artık günlük yaşantımızın vazgeçilmez bir parçası haline gelmiştir.

Günümüzde verilen hizmetlerin artması ve çeşitlenmesine paralel olarak müşterilerin bir şebeke işletmecisi firmadan ve verdiği hizmetlerden beklentileri de yükselmiştir. Bundan 50 sene önce sabit telefon hatları ile şehirlerarası görüşme yapmak için günlerce bekleyen müşteri profili, günümüzde bir görüşmenin başlamasının birkaç saniye gecikmesine tahammül edemeyen talepkar bir profile dönüşmüştür. Şebeke işletmecisi firmalar arasında yoğun bir rekabet söz konusudur. Verilen bir hizmetin kesilmesi çok büyük kazanç kayıplarına neden olduğu gibi şebeke işletmecisi firmaların prestijlerini düşürmektedir. Müşteriler verilen mobil hizmetlerden

memnun kalmazlarsa numaralarını değiştirmeden rakip şebeke işletmecisi firmalardan hizmet almayı seçebilmektedirler. Kesintisiz ve kaliteli mobil hizmetlerin verilebilmesi için şebeke işletmecisi firmaların şebekelerinin problemsiz ve verimli çalışması gerekmektedir. Aksaklıklar mümkünse oluşmadan engellenmeli, oluştuysa da en kısa sürede çözüme kavuşturulmalıdır. Bu nedenle şebeke işletmecisi firmalar içinde bulunan aksaklık yönetim departmanları şirket için kritik öneme sahip bölümler haline gelmektedir.

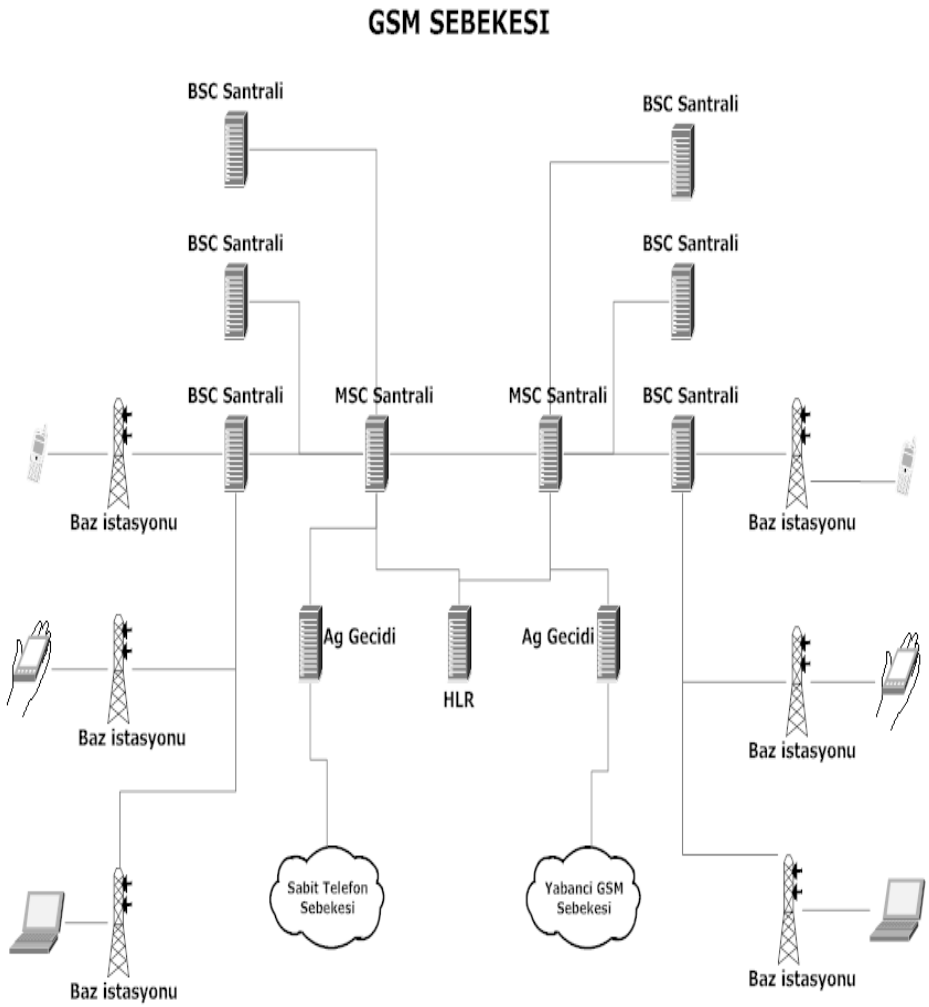
Tez çalışması kapsamında temel olarak odaklanılan konu, GSM şebekelerinin aksaklık yönetimi süreçleri ve bu süreçleri zorlaştıran ilgilenilmesi gereken yüksek alarm sayısı probleminin istatistiksel öğrenme yöntemleri ile alternatif çözümleridir. Çalışmanın 1. bölümünde genel olarak GSM şebekelerinin alt yapıları, karşılaşılan aksaklık çeşitleri ve bu aksaklıklarla ilgilenirken karşılaşılan zorluklar hakkında bilgiler verilmektedir. Bu bölümde ayrıca aksaklık yönetimi ile ilgili temel kavramlar anlatılıp, bütün dünyada kabul görmüş aksaklık yönetimi süreci aşamaları ile anlatılmıştır. Çalışmanın 2. bölümünde yüksek alarm sayısı probleminin bir çözümü olan alarm filtreleme konusu anlatılıp, şebeke alarmları üzerinde kullanılan temel alarm filtresi çeşitleri paylaşılmıştır. 3. bölümde alarm ilintilendirmesi hakkındaki genel kavramlar ve alarm ilintilendirmenin teorik çeşitleri incelenmiştir. Aynı bölümde aksaklık yeri saptama hakkındaki genel kavramlar ve kullanılan yöntem çeşitleri de incelenmiştir. 4. bölümde deneysel çalışmalarımızda kullandığımız veri kümesi ayrıntıları ile anlatılmıştır. 5. bölümde geçici alarmların oluşturduğu alarm kirliliğini engellemek için birikimli histogram analizi ve Parzen penceresi analizi yöntemleri ile otomatik bekletme filtresi üretme algoritmalarımızın detayları anlatılmakta ve veri kümemiz üzerinde aldığımız sonuçlar paylaşılmaktadır. Son bölümde alarm tarihçesi üzerinden alarm ilintilendirme kuralları üretimi konusunda pazar sepet analizi benzerlik ölçütlerinin kullanımı incelenmiş, incelenen benzerlik ölçütlerini beraber kullanabilmek için S biçimli sınıflandırma yöntemi irdelenmiş ve veri kümemiz üzerinde aldığımız sonuçlar paylaşılmmıştır.

1.1 GSM Şebekelerinin Genel Yapısı

GSM şebekelerindeki temel yapı taşlarını aşağıdaki gibi altı gruba ayırabiliriz:

- Mobil İstasyonlar

- Baz İstasyonları
- BSC Santralleri
- MSC Santralleri
- Transmisyon Altyapısı
- Diğer Birimler



Şekil 1.1: GSM Şebekesi Alt Yapısı

Şekil 1.1'de GSM şebekelerininde bulunan birimler ve aralarındaki bağlantılar gösterilmiştir. Bu birimlerin detayları aşağıdaki açıklanmaktadır.

Mobil İstasyonlar: Müşterilerin mobil hizmetler almasını sağlayan cihazlara mobil istasyonlar denmektedir. Cep telefonları, PDA cihazları, GSM internet modemleri, mobil POS cihazları en yaygın kullanılan mobil istasyon türleridir.

Baz İstasyonları: GSM şebekelerindeki temel hizmet birimleri baz istasyonlarıdır. Baz istasyonları mobil istasyonlar ile sürekli irtibat halinde olan ve müşterilerin santrallerle bağlantısını sağlayarak hizmet verilmesini sağlayan temel şebeke birimleridir. Baz istasyonlarında genel olarak kablosuz sinyalleşmeyi sağlayan ve farklı yönlere bakan antenler, antenlerden gelen sinyalleri yöneten elektronik kartlar, elektronik kartların içinde bulunduğu kasalar, elektrik kesintisi durumunda verilen hizmetin devam edebilmesi için aküler, ortamın aşırı ısınması veya soğuması durumunda ekipmanların çalışmasının kötü yönde etkilenmesini önlemek için klima ve problemler karşısında şebeke işletmecisi firmayı uyarmak üzere çeşitli sensörler bulunmaktadır (hırsız alarmı, ısı sensörleri, vs.). Baz istasyonlarının farklı yönlere bakan antenleri farklı elektromanyetik frekans setleri kullanmaktadır. Bu nedenle GSM şebeke yönetiminde baz istasyonlarının altında hücre adı verilen sanal alt birimler tanımlanmıştır. Bir baz istasyonunda bir veya daha fazla hücrenin ekipmanları bulunabilmektedir.

BSC Santralleri: Baz istasyonlarının çalışmasını kontrol eden, kendisine bağlı baz istasyonlarının servis bölgelerinde yer değiştiren müşterilerin servis aldığı baz istasyonlarının değişmesini sağlayan santrallerdir.

MSC Santralleri: BSC santrallerinin bağlı olduğu temel GSM santralleridir. Diğer MSC santralleri ve ait olduğu şebeke işetmecisi firma dışındaki diğer GSM ve PSTN şebekelere görüşmeleri yönlendirmeyi sağlayan ağ geçitlerine bağlıdır.

Transmisyon Alt Yapısı: Baz istasyonlarının BSC santrallerine, BSC santrallerin MSC santrallerine, MSC santrallerinin diğer MSC santralleri ve ağ geçitlerine bağlanmasını sağlayan alt yapılardır. Transmisyon alt yapısında kullanılan teknolojiler çok çeşitlidir. Fiber optik kablo alt yapısının mevcut olduğu durumlarda baz istasyonları için genelde çeşitli kapasitelerde fiber optik bağlantılar kullanılmaktadır. Fiber optik alt yapısı bulunmayan yerlerde veya maliyetinin yüksek olduğu yerlerde baz istasyonlarındaki transmisyon hizmeti radyolink ekipmanları ile verilmektedir. Radyolink ekipmanları 30 km mesafeye kadar transmisyon hizmeti verebilmektedirler. Fiber optik kablo alt yapısının olmadığı ve radyolink cihazlarının kullanımının elverişli olmadığı durumlarda transmisyon hizmeti uydu antenleri üzerinden de alınabilmektedir.

Diğer Temel Düğümler: GSM şebekesinin en yaygın kullanılan diğer temel birimleri güncel kullanıcı bilgilerinin tutulduğu HLR adı verilen sunucular, SMS/MMS gibi çeşitli hizmetlerin verilmesine destek olan sunucular ve GSM şebekesinin diğer GSM ve PSTN şebekelerine bağlanmasını sağlayan ağ geçitleridir.

1.2 GSM Şebekelerinde Karşılaşılan Temel Aksaklıklar

Kaliteli ve kesintisiz hizmet verebilmek için şebekedeki bütün birimlerin sorunsuz çalışması gerekmektedir. GSM şebekelerinde karşılaşılan problemler kaynak tiplerine göre 12 temel gruba ayrılabilmektedirler:

Ekipman Alarmları: Baz istasyonlarında bulunan ekipmanlarda karşılaşılan problemler için yaratılan alarmlardır. Ekipman alarmlarına neden olan aksaklıkların etkileri çeşitlilik gösterse de oluştukları baz istasyonunun kısmi veya tamamen servis dışı kalmasına varan ciddi sonuçlara neden olabilmektedir. Aşağıda en sık karşılaşılan ekipman alarm çeşitlerine örnekler bulunmaktadır.

Fan Arızası: Baz istasyonlarındaki elektronik devrelerin soğumasını sağlayan fanlar bozulabilmektedir. Elektronik kartların aşırı ısınmadan bozulmaması için soğutucu fanların yeniden çalışır hale getirilmesi gerekmektedir. Fan arızaları çok acil arızalar değildir. Çünkü baz istasyonunda soğutma için ek olarak klima bulunmaktadır. Ancak yazın sıcak bölgelerimizde klimalar soğutma için yetersiz kalabildiği için fan arızaları çözüm bulunması gereken öncelikli problemler haline gelmektedir.

SNMP Erişim Hatası: Ekipmanların yönetiminde kullanılan SNMP protokolü ile bazı zamanlarda ilgili donanımlara komutlar gönderilemeyebilmektedir. SNMP iletişimi sağlanamayan donanımlar için bu alarmlar üretilmektedir.

Ulaşılamayan Ekipman Hatası: Bağlantının koptuğu ve yönetim sisteminin hiçbir şekilde iletişim kuramadığı donanımlar için üretilen alarmlardır.

Hücre Alarmları: Baz istasyonlardaki hizmet alt birimleri olan hücrelerde verilen servislerle ilgili problemler oluşabilmektedir. Hücre alarmlarına neden olan aksaklıkların etkileri çeşitlilik gösterse de oluştukları hücrenin servis dışı kalmasına varan ciddi sonuçlara neden olabilmektedirler. Aşağıda sık karşılaşılan hücre alarm örnekleri bulunmaktadır.

Servis Dışı Kalan Hücre Alarmı: Çeşitli nedenlerle hücreler servis dışı kalabilmektedirler. Bu durumlarda var ise komşu hücreler servis dışı kalan hücrelerin vermesi gereken hizmeti daha düşük kalite ile vermektedirler. Ama komşu hücrelerin hizmet vermesi trafik yoğunluklarını arttırdığı için kendi servis alanlarındaki hizmet kalitesi de düşebilmektedir. Servis dışı kalan hücre problemleri acil çözüm bulunması gereken problemlerdendir.

Mobil Sinyalleşme Hataları: Mobil cihazlar ile hücre donanımları sürekli sinyalleşme halindedir. Bu sinyalleşmelerde hizmet kalitesini etkileyecek hatalar oluşabilmektedir. Bu hataların miktarının artması önemli problemlere işaret edebilmektedir.

Kanal Çakışmaları: Komşu hücreler mobil cihazlarla iletişim için farklı trafik kanal setleri kullanmaktadırlar. Aynı trafik kanal setleri uzakta bulunan hücreler tarafından da kullanılabilmektedir. Birbirine uzakta bulunan ve aynı trafik kanal setlerini kullanan hücrelerin aynı trafik kanalından aynı anda hizmet vermesi bazen problemlere neden olabilmektedir.

Baz istasyonu Alarmları: Baz istasyonu alarmlarına neden olan aksaklıkların etkileri çeşitlilik gösterse de oluştukları baz istasyonunun servis dışı kalmasına varan ciddi sonuçlara neden olabilmektedirler. Aşağıda sık karşılaşılan baz istasyonu alarm örnekleri bulabilirsiniz.

Açık Kapı Alarmları: Baz istasyonlarında klima ve akü hırsızlıklarına sık rastlanmaktadır. Bu nedenle izinsiz kapı açılması durumunda gerekli önlemlerin alınması için alarm üretilir.

Redresör Arızaları: Baz istasyonlarındaki cihazların önemli bir kısmı sabit akım ile çalışır. Elektrik dağıtım şebekesinden alınan alternatif akımı sabit akıma çeviren redresör cihazlarında sıkça problem görünmektedir.

Yüksek Sıcaklık Alarmları: Klimaların ve elektronik devrelerdeki fanların yetersiz kalması veya çalışmaması durumlarında baz istasyonunun içindeki sıcaklık çok yükselebilmektedir. Yüksek sıcaklıklar baz istasyonundaki cihazları bozabildikleri gibi yangınlara da neden olabilmektedirler. Bu nedenle baz istasyonunun içindeki sıcaklık belirli bir derecenin üstüne çıktığında gerekli önlemlerin alınması için alarm alarmları üretilir.

BSC Santral Alarmları: BSC santral alarmlarına neden olan aksaklıkların etkileri çeşitlilik gösterse de oluştukları BSC santraline bağlı bütün baz istasyonlarının servis dışı kalmasına varan ciddi sonuçlara neden olabilmektedirler. Aşağıda sık karşılaşılan BSC Santral alarm örneklerini bulabilirsiniz.

Bağlantı Yolu Hataları: BSC santraller yönetiminden sorumlu oldukları baz istasyonlarına düzenli aralıklarla IP ping komutları yollamaktadırlar. Bazen ping komutları başarılı sonuçlar vermeyebilir. Bu durumda BSC Santralden baz istasyonuna doğru olan bağlantıda problem olduğu varsayılarak alarm üretilmektedir.

Bit-Hata Oranı Alarmları: BSC santralleri transmisyon alt yapısı ile MSC santrallerine ve birçok baz istasyonuna bağlıdırlar. Bu transmisyon bağlantılarının kalitelerini ölçmek için çeşitli kontrol yöntemleri vardır. Bu kontrol yöntemlerine göre transmisyon aşamasındaki mesajlardaki bit-hata oranları belirli bir derecenin üstüne çıkarsa gerekli önlemlerin alınması için alarm üretilir.

MSC Santral Alarmları: MSC santral alarmlarına neden olan aksaklıkların etkileri çeşitlilik gösterse de oluştukları MSC santralinden hizmet alan bütün baz istasyonlarının servis dışı kalmasına varan ciddi sonuçlara neden olabilmektedirler. Aşağıda sık karşılaşılan MSC Santral alarm örneklerini bulabilirsiniz.

Sinyalleşme Link Hataları: MSC santralleri mobil kullanıcıların başlatmak istedikleri görüşmeleri başlatmak ve yönetmek için başka MSC santralleri ve ağ geçitleri ile sinyalleşmektedir. Farklı protokoller kullanılan farklı sinyalleşme linkleri bazen hizmet dışı kalabilmektedir. Bu durum görüşmelerin başlatılma süresini uzatabileceği gibi bazen tamamen engelleyebilmektedir. Bu nedenle sinyalleşme linklerinde yaşanan problemler için alarmlar üretilmektedir.

Çağrı Sonlandırma Hataları: Farklı GSM ve PSTN şebekelerindeki kullanıcılar aranmak istendiğinde MSC santraller ağ geçitleri üzerinden çağrı başlatma istekleri göndermektedirler. Bu isteklerin reddedilmeye başlanması durumunda gerekli önlemlerin alınması için alarmlar üretilmektedir.

Tıkanıklık Alarmları: Yüksek görüşme trafiği olduğu durumlarda kullanılan bağlantılarda tıkanıklıklar oluşabilmektedir. Tıkanıklıklardan oluşabilecek hizmet kalitesini düşürebilecek problemlerden kaçınabilmek için tıkanıklık alarmları üretilir.

Radyolink Transmisyon Alarmları: Fiber optik transmisyon alt yapısının olmadığı veya maliyetinin yüksek olduğu yerlerde bulunan baz istasyonlarının transmisyon

ihtiyacı radyolink sistemleri ile karşılanmaktadır. Fiber optik transmisyon hizmetini yüksek kapasite ve düşük maliyetle alabilecek noktalar seçilerek bu toplama noktası ile komşu istasyonlar arasında radyolink antenleri ile bağlantı kurularak düşük maliyetli bir transmisyon imkanı sağlanabilmektedir. Radyolink sistemlerinde oluşan aksaklıkların etkileri çok çeşitlilik gösterse de aksaklığın oluştuğu radyolinkin transmisyon hizmeti sağladığı bir veya daha fazla baz istasyonunun servis dışı kalmasına varan sonuçları olabilir. Radyolink transmisyon sistemlerinde sık karşılaşılan problem örneklerini aşağıda bulabilirsiniz.

Kapasite Eşik Değeri Alarmları: Radyolink antenlerin bağlantı halinde oldukları radyolink vericilerinden alabilecekleri sinyal bant genişliği sabittir. Eğer radyolink sistemlerinin alıcılarına gelen sinyalin bant genişliği belirli bir eşik değerini aşarsa oluşabilecek tıkanıklık problemleri için erken önlem alabilmek amacıyla alarmlar üretilir.

Bit-Hata Oranı Alarmları: Transmisyon sırasında oluşan bit hatalarının miktarı belirli bir eşik değerini aştığında transmisyon kalitesini arttırıcı önlemler alınması için alarmlar üretilmektedir.

Görüş Çizgisi Kaybı Alarmları: Radyolink sistemleri ile transmisyon sağlanan iki noktadaki antenlerin aralarında bir şey olmadan birbirlerine dönük olmaları gerekmektedir. Buna görüş çizgisi denmektedir. Sisli, yağmurlu ve karlı havalarda görüş çizgisi kalitesi düşebilmektedir. Rüzgârla sallanan ağaç dalları, yeni yapılan binalar gibi etkenlerde görüş çizgisi kalitesini etkileyebilmektedirler. Kaliteli transmisyon hizmeti vermeye devam edebilmek için görüş çizgisi kalitesi düştüğünde gerekli önlemlerin alınabilmesi için alarmlar üretilmektedir.

Fiber Optik Transmisyon Alarmları: Birçok baz istasyonunun ve radyolink transmisyon toplama noktalarının BSC santrallerle olan transmisyonları ve santrallerin kendi aralarındaki transmisyon hizmetleri fiber optik transmisyon sistemleri ile gerçekleşmektedir. Fiber optik transmisyon sistemlerinde sık karşılaşılan problemlere örnekleri aşağıda bulabilirsiniz.

Alarm Bildirim Sinyalleri: Transmisyon linkinde oluşan kalite problemleri için AIS adı verilen bir sinyal üretilir. AIS sinyalleri için transmisyon sistemi alarmlar üretmektedir.

Bit-Hata Oranı Alarmları: Transmisyon sırasında oluşan bit hatalarının miktarı belirli bir eşik değerini aştığında transmisyon kalitesini arttırıcı önlemler alınması için alarmlar üretilmektedir.

Kontrol Kanalı Alarmları: Yüksek hızda veri iletimi için kontrol kanalları üzerinden sinyalleşmeler gerçekleştirilmektedir. Fiber optik transmisyon sistemlerinde bazı zamanlarda kontrol kanallarında problemler oluşmaktadır. Bu durum verilen transmisyon hizmetinin kalitesini düşürmektedir. Bu nedenle gerekli önlemlerin alınması için alarmlar üretilmektedir.

Diğer Transmisyon Alarmları: Radyolink ve fiber optik transmisyon sistemleri dışında yer alan transmisyon altyapısı da alarmlar üretmektedir.

Düşük Sinyal Seviyesi: Transmisyon linkindeki sinyal seviyesi düştüğünde gerekli önlemlerin alınması için alarmlar üretilir.

Alarm Bildirim Sinyalleri: Transmisyon linkinde oluşan kalite problemleri için AIS adı verilen bir sinyal üretilir. AIS sinyalleri için transmisyon sistemi alarmlar üretmektedir.

Bit-Hata Oranı Alarmları: Transmisyon sırasında oluşan bit hatalarının miktarı belirli bir eşik değerini aştığında transmisyon kalitesini arttırıcı önlemler alınması için alarmlar üretilmektedir.

STP Sinyalleşme Alarmları: Santraller müşterilerin istedikleri görüşmeleri başlatmak, yönetmek ve sonlandırmak için birbirlerine çeşitli protokollerde sinyaller göndermektedirler. Sinyalleşmeler sırasında çıkan problemler verilen hizmetin kalitesi konusunda çok önemli ip uçları içermektedir. SS7 protokolündeki mesajlar STP adı verilen düğümler ile taşınmaktadır. Sık karşılaşılan STP sinyalleşme alarmlarına örnekleri aşağıda bulabilirsiniz.

Tıkanıklık Alarmları: STP düğümleri arasında sinyalleşme linklerinde yoğunluk çok arttığında bu alarmlar üretilmektedir. Gerekli önlemler alınmazsa yeni görüşme hizmetleri verilemeyebilir.

Sinyal Yönlendirme Hataları: STP düğümlerine gelen sinyallerin yönlendirileceği adreslerin bulunamaması durumlarında bu alarmlar üretilmektedir.

Sinyalleşme Linklerinin Hizmet Dışı Kalması: STP düğümlerine gelen sinyallerin yönlendirilmesinde kullanılacak linklerin hizmet dışı kalma durumlarında bu alarmlar üretilmektedir.

Örneklerden anlaşılabileceği gibi GSM şebekesinde çok çeşitli yerlerde çok çeşitli aksaklıklar oluşabilmektedir. Sıkça karşılaşılan aksaklıklar olduğu gibi daha önceden hiç karşılaşılmamış, nedenleri ve sonuçları kestirilemeyen yeni çeşit aksaklıklarla da karşılaşılması mümkündür. Bu nedenle aksaklıklar karşısında uygulanacak süreçler en beklenmedik problemlerde de uygulanacak şekilde tasarlanmalıdır.

1.3 GSM Şebekelerinde Aksaklık Yönetimi

Aksaklık yönetimi, hizmet veren bir sistemin en az kesinti ve problemle çalışabilmesi için gözlem altına alınması, çıkan problemlere en kısa sürede en az zararla müdahale edilip hizmet vermeye kaliteli bir şekilde devam edilmesi süreçleridir.

Aksaklık yönetimindeki temel kavramlar aşağıdaki gibidir.

Alarm: Gözlemlenen sistemin donanım veya yazılımında sıra dışı bir durum gerçekleştiğinde üretilen bilgilendirici mesajlara alarm denmektedir. Alarmlarda bulunması gereken en temel üç bilgi aşağıdaki gibidir [1]:

- Alarmın gerçekleşme zamanı
- Alarmın kaynağı
- Alarmın açıklayıcı mesajı

Ama alarmların kullanıldığı alanlardaki ihtiyaçlara göre alarmlara onlarca farklı bilgi de eklenebilmektedir.

Aksaklık: Alarmlara neden olan ama başka problemlerden kaynaklanmayan temel probleme aksaklık denir [2]. Kök neden olarak da adlandırılır. Aksaklıklar var oluş sürelerine göre üç gruba ayrılabilirler.

Kalıcı aksaklıklar: Bir tamir işlemi gerçekleşene kadar devam eden aksaklıklara kalıcı aksaklık denir.

Periyodik aksaklıklar: Düzenli aralıklarla tekrarlayarak oluşup kendiliğinden düzelen aksaklıklara periyodik aksaklıklar denmektedir. Bu tip aksaklıklar uzun sürmeseler de çok sık karşılaşıldıkları için servis kalitesine önemli zararlar vermektedirler.

Geçici aksaklıklar: Verilen servis kalitesine önemli etkileri olmayan ve kısa süre içinde kendiliğinden düzelen aksaklıklara geçici aksaklık denir.

Hata: Hesaplanan, gözlemlenen veya ölçülen bir değerin veya durumun doğru, belirtilmiş veya teorik olarak olması gereken değerde veya durumda olmamasına hata denir.

Yönetilen nesne: Aksaklık yönetiminde alarmların geldiği, gözlemlenen alt birim veya cihazlara yönetilen nesne denmektedir. Alarmların kaynakları bu nesnelerdir.

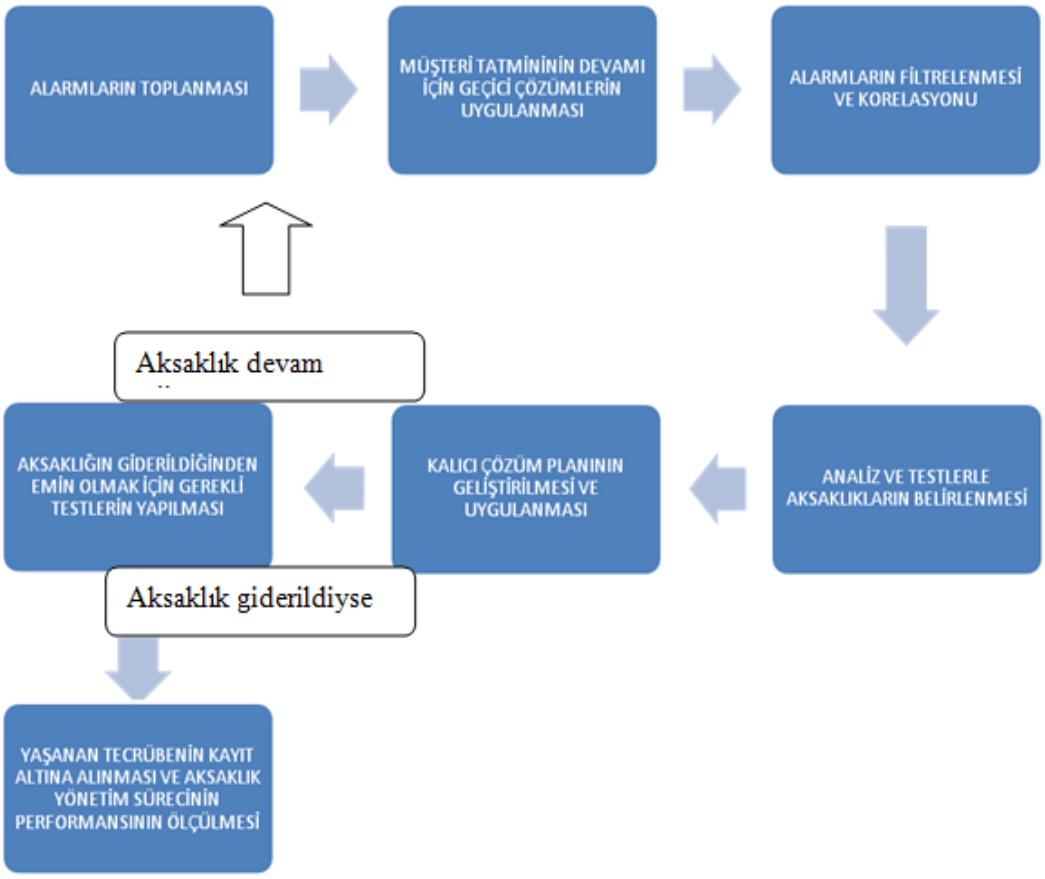
Aksaklık yönetimi süreçleri kesintisiz ve kaliteli hizmet vermenin önem kazandığı çok farklı sektörlerde uygulanmaktadır. Aksaklık yönetimi süreçlerinin en yaygın olarak kullanıldığı alan bilgisayar ve haberleşme ağlarının yönetimidir [1-17]. Teknolojinin gelişmesi, yeni teknolojilerin hayatın vazgeçilmez birer parçası haline gelmesi, yepyeni cihazların kullanılmaya başlanması, hizmet veren ağ alt yapılarının her geçen gün büyümesi ve çeşitlenmesi beraberinde karşılaşılan problem ve aksaklıkları arttırmakta ve çeşitlendirmektedir. Bu nedenlerle bilgisayar ve haberleşme ağlarındaki aksaklık yönetimi süreçlerinin önemi günden güne artmaktadır.

Enerji ihtiyacının her geçen gün arttığı dünyada nükleer santrallerin sayısı her geçen gün artmaktadır. Nükleer enerjiden elektrik enerjisinin en güvenli şekilde üretilebilmesi için nükleer santrallerde de çok titiz bir şekilde aksaklık yönetimi süreçleri uygulanmaktadır [18,19].

Hizmet kalitesinin önem kazandığı elektrik dağıtım şebekelerinde [20], lojistik hizmet veren dağıtım firmalarında [21], uçaklarına düzenli kontrol ve bakımlar yaptıran hava yolu firmalarında [22], meteoroloji merkezlerinin hava durumu tahmininde kullandıkları dağıtık kablosuz sensör ağlarında [23,24], güvenlik hizmeti veren firmalarda da [25-27] aksaklık yönetimi süreçleri etkin bir şekilde kullanılmaktadır.

1.3.1 Aksaklık Yönetimi Süreci

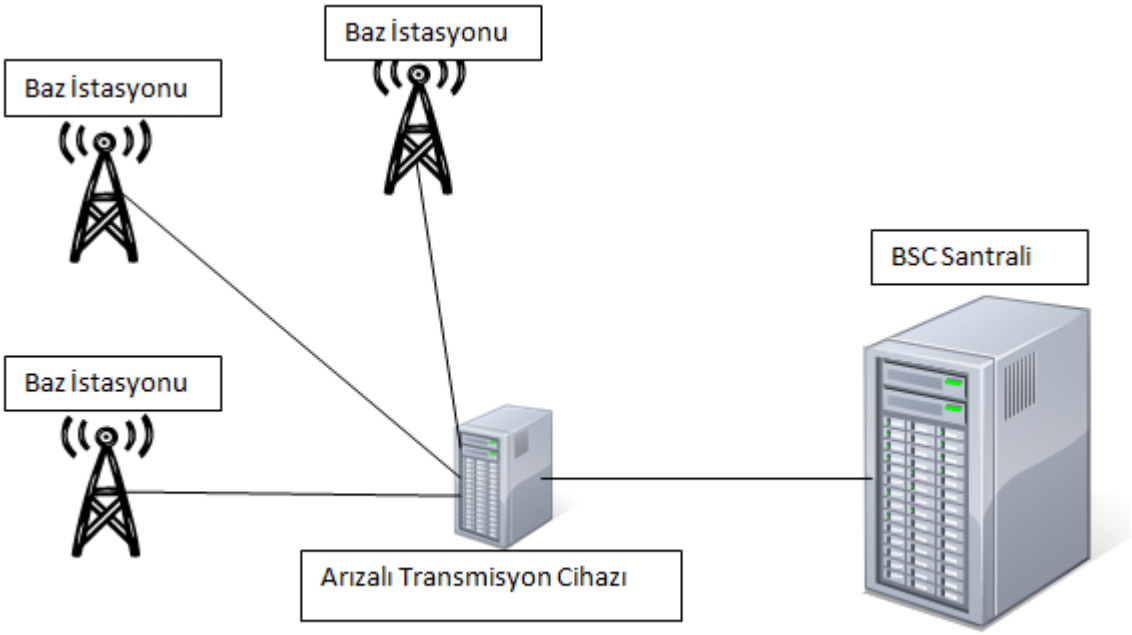
Aksaklık yönetimi süreçleri temel olarak yedi alt sürece ayıralabilir [4]. Şekil 1.2'de aksaklık yönetimi sürecinin evreleri gösterilmektedir:



Şekil 1.2: Temel Aksaklık Yönetimi Süreci

Süreçleri incelerken örnek olarak GSM ağlarından alınan bir problem senaryosu kullanılacaktır.

Problem Senaryosu: Üç tane baz istasyonunu bir BSC santraline bağlayan transmisyon aktarma noktası cihazının önemli bir kartı yüksek voltaj nedeniyle yanarak servis dışı kalır. Şekil 1.3'de problem senaryosunda bahsedilen birimlerin birbirleriyle bağlantısal ilişkileri gösterilmektedir.



Şekil 1.3: Örnek Problem Senaryosu

Alarmların toplanması: Aksaklık yönetiminin ilk aşamasında sistemde yönetilen nesneler tarafından üretilen alarmlar tek bir sistemde toplanır. Problem senaryosunda bahsedilen transmisyon noktasında yüksek voltaj alarmı ile servis dışı cihaz alarmı üretilir. Transmisyon noktasının bağlı olduğu santralde üç tane ulaşılamayan istasyon alarmı üretilir. Aksaklık yönetimi sistemi ilk iş olarak bu alarmların hepsini toplar.

Gelen sistem alarmları doğrultusunda müşteri tatmininin devamı için gerekli aksiyonların hızlıca alınması: Yönetilen sistemler için alarmlar geldiğinde müşterilere sunulan hizmetlerin kaliteleri konusunda sıkıntı ihtimali varsa aksaklıkların nedenleri ve çözümleri bulunana kadar geçici çözümler uygulanmalıdır. Problem senaryosunda ulaşılamayan baz istasyonları müşteriye verilen hizmetin durması anlamına gelmektedir. Bu nedenle hizmetin devamı için ilgili baz istasyonu servis sahalarına acil olarak mobil baz istasyonları gönderilip yeniden hizmet verilmesi sağlanarak müşteri tatmini garanti edilir.

Alarmların filtrelenmesi ve birbirleriyle ilintilendirilmesi: Alarm filtreleme süreci çok sayıda alarmın analiz edilerek gereksiz alarmların elenmesidir. Örnek olarak aynı alarmın aynı anda birden fazla gelmesi durumunda bir tanesi bırakılıp geri kalanı elenebilir. Problem senaryosunda servis dışı kalan her baz istasyonu için birden fazla ulaşılamaz baz istasyonu alarmı oluştuysa fazlalık alarmlar bu aşamada elenir. Alarm ilintilendirmesi ise beraber gelen birçok alarmın birbirleriyle

ilişkilendirilerek alarmlara yeni anlamlar yükleyip, yeni bir alarmın yaratılmasıdır. Problem senaryosunda ulaşılamaz baz istasyonu alarmları ile transmisyon noktasından gelen alarmlar ilişkilendirilerek tek bir alarm haline getirilir (alarm ilintilendirme).

Analiz ve testlerle aksaklıkların saptanması: Alarmlar filtrelenip ilintilendirmeye tabi tutulduktan sonra çıkan sonuçlar analiz edilir. Gerekli sistem testleri yapılır ve ilgili sistemlerin durum değişimleri gözlemlenerek aksaklığın nedeni bulunur. Problem senaryosunda filtrelenmiş ve ilintilendirmeye tabi tutulmuş alarmlar incelendikten sonra aksaklığın nedeninin transmisyon noktasından kaynaklandığı ihtimaline karşı bu cihaz üzerinde uzaktan performans testleri koşturulmaya başlanır. Testler sonucunda aksaklığın nedeni olarak yüksek voltajdan yanmış bir kartın olduğu bulunur.

Alternatif çözüm planlarının oluşturulması ve uygulanması: Aksaklığın nedeni bulunduktan sonra alternatif aksaklık giderim planları oluşturulur. Seçenekler incelenerek en uygun çözüm planı seçilir. Seçilen plan doğrultusunda aksaklık giderilir. Problem senaryosunda aksaklığın nedeni yüksek voltaj nedeniyle yanmış bir karttır. Aksaklık bozulmuş bir kart ile yüksek voltaja dayanıklı daha pahalı bir kartın değişimi ile giderilebilir. Alternatif olarak yanmış kart standart bir kart ile değiştirilebilir ve yüksek voltaja karşı koruyucu olarak transmisyon noktasına yeni bir cihaz eklenebilir. En uygun senaryo seçilerek transmisyon noktasında yeniden hizmet verilmesi sağlanır.

Aksaklığın giderildiğinden emin olmak için gereken testlerin yapılması: Aksaklığı gidermek için çözüm senaryosu uygulandıktan sonra sistem üzerinde problemin devam edip etmediğinden emin olabilmek için testler koşturulmaya başlanır. Problem senaryosunda transmisyon noktası üzerinde rutin testlerin koşturulması dışında, hizmet dışı kalan baz istasyonlarında yeniden hizmet verilmeye başlanıp başlanmadığı kontrol edilir.

Süreçlerdeki temel bilgilerin kaydedilerek geri besleme ile aksaklık yönetimi süreçlerinin geliştirilmesi: Aksaklık süreçlerinin her aşamasındaki her bilgi kaydedilerek süreçlerde bir yavaşlık veya problem var ise geliştirilmesi için gerekli aksiyonlar alınır. Problem senaryosunda karşılaşılan yanmış kart problemleri sık

karşılaşılan bir durum ise ilgili kişilere raporlanarak GSM ağındaki benzer kartların hepsinin değişimi sağlanabilir.

1.3.2 Aksaklık Yönetimi Süreçlerinde Yaşanan Zorluklar

Aksaklık yönetimi süreçleri aşağıdaki temel sebepler nedeniyle uygulaması zor süreçlerdir [2,12]:

Devasa boyutlara ulaşabilen bilgisayar, haberleşme ağları ve çok çeşitlilik içeren alarm mesajları nedeniyle aksaklığı bulmak çok zorlaşabilir. Oluşabilecek aksaklık çeşitleri çok yüksek sayılara ulaşabilir.

Alarmları gözlemlemekten sorumlu uzman personelin gelen alarmlar için ne yapacağına karar vermesi konusunda çok az zamanı vardır.

Bilgisayar ve haberleşme ağlarında kullanılan donanım ve yazılım teknolojileri çok hızlı gelişmektedir. Ağlara eklenen yeni cihazlar ve yazılımları güncellenen eski cihazlar oluşan alarmların içeriklerini ve karakteristiklerini değiştirmektedir. Alarmları gözlemlemekten sorumlu personelin oluşabilecek her yeni durum için uygulayacağı uygun çözüm yöntemlerini öğrenmek için yeterli vakti olmayabilir.

Bir cihaz tek bir aksaklık nedeniyle çok sayıda ve çok farklı çeşitlerde alarmlar üretebilir. Bu durum ilgilenilmesi gereken alarm sayısını arttırdığı gibi aksaklığın gerçek nedeninin bulunmasını güçleştirebilir.

Bazı aksaklıklar ağdaki çok sayıdaki farklı cihazlardan yakın zamanlı gelen farklı alarmların incelenmesiyle bulunabilir.

Bir cihazdaki aksaklık farklı cihazları da etkileyerek onlarda da aksaklıklara neden olabilir. Bu duruma aksaklık yayılımı denmektedir. Bu durum ilgilenilmesi gereken aksaklık miktarını arttırıp problemlere neden olan temel aksaklığın bulunma süresini arttırır.

Aksaklık yönetimi uygulanan sistemler çoğunlukla dağıtık yapılı sistemler olduğu için bu durum aksaklık yönetimi süreçlerini de zorlaştırmaktadır. Dağıtık bir sistemin aksaklık yönetiminin gözlemlendiği bir uygulamada aşağıdaki özelliklerin bulunması gerekmektedir [8]:

Coğrafi yayılım: Yönetilen ağların boyutu ve coğrafi yayılımı, yönetim sisteminde alarmların hiyerarşik ve coğrafi olarak gruplanabilme ihtiyacını doğurmaktadır. Bu

nedenle aksaklık yönetimi sisteminin farklı çeşitteki topolojilerle uyum içinde çalışabilmesi gerekmektedir.

Büyüklük: Aksaklık yönetimi sistemi aynı anda çok sayıda gözlemci personelinin kullanabileceği bir yapıda olmalıdır. Ve çok yüksek sayıda yönetilen nesnenin gözlemlenebilmesine olanak sağlayabilmelidir.

Farklı teknolojilere kolay uyum: Aksaklık yönetimi sistemi farklı mimari yaklaşımlara ve bütünleşme çeşitlerine (OSI, SNMP, CORBA, vs.) sahip sistemlerle kolayca entegre olabilmelidir. Bu sayede çok farklı teknolojilere sahip alt yapı cihazlarının aksaklık yönetimi tek bir merkezden yapılabilmektedir.

Erişim güvenliği: Aksaklık yönetimi sistemi kötü niyetli ve hatalı kullanıcılara karşı korumalı olmalıdır.

Ölçeklendirilebilirlik: Ağların boyutları ve içerikleri her geçen gün değişmektedir. Aksaklık yönetimi sistemi ağın büyümesi, konfigürasyon değişimi ve teknolojik değişimlere karşı uyumlu olmalıdır.

1.3.3 Aksaklık Yönetiminde Yapay Zeka Çözümlerinin Önemi

Çok sayıda alarmın çok kısa sürede incelenip aksaklıkların nedenlerinin bulunması ve gerekli aksiyonların en hızlı şekilde alınması çok yüksek iş gücü gerektirdiği için aksaklık yönetimi sistemlerinde uzun zamandan beri uzman sistem çözümleri kullanılmaktadır.

Alarmları gözlemlemekten sorumlu personelin işlerini kolaylaştırmak için uzmanlıklarına başvurularak sık karşılaştıkları durumlar ve bu durumlar karşısında yapılması gerekenler belirlenir. Sık karşılaşılan durumlar ve yapılması gerekenler uzman sistem içinde uzman kurallara çevrilir. Bu sayede önemli miktarda alarm daha az insan iş gücü ile incelenmiş ve gerekli aksiyonlar alınmış olur.

GSM sektöründen örnekler vermek gerekirse baz istasyonlarındaki ekipmanlardan gelen bazı problemler ekipmanın yeniden başlatılması ile çözülebilmektedir. Yazılan uzman kurallar ile insan faktörü kullanılmadan gözlemlenen farklı alarm tipleri için ilgili ekipmanlara farklı komutlar gönderilerek problemler giderilebilmektedir. Benzer şekilde uzman kurallar ile farklı arıza alarmları için ilgili ekiplere otomatik SMS ve e-posta mesajları gönderilip ilgili tamir aksiyonunun en hızlı şekilde alınması sağlanabilmektedir. Uzman sistemlerin kullanılmaya başlanması ile

aksaklık yönetiminde alarmları gözlemlemekten sorumlu personel ihtiyacı %70-80 mertebelerine varacak şekilde düşüşler gösterebilmektedir.

Uzman sistemler aksaklık yönetiminde çok faydalı olmalarına rağmen yetersiz kaldıkları alanlar bulunmaktadır [4]:

Uzman sistemler yeni ve değişen bilgiler ışığında çözümler üretemezler. Uzman kurallar sadece daha önceden tanımlanmış durumlarda çalışırlar. Yeni gelmeye başlayan alarm çeşitleri ve değişen topoloji bilgileri durumunda yetersiz kalırlar.

Uzman sistemler geçmiş tecrübeden dersler çıkarıp kendilerini güncelleyemezler.

Uzman sistemler değişimler karşısında yüksek bakım maliyetleri gerektirmektedir. Yeni uzman kuralların geliştirilmesi ve var olan uzman kuralların değişen koşullar karşısında güncellenmesi veya silinmeleri gerekmektedir.

Uzman sistemler ihtimaller ve belirsizlikler karşısında yetersiz kalmaktadır. Fuzzy uzman kurallar geliştirilebilir. Ama bu kurallarda da yukarıdaki problemler gözlemlenmeye devam edecektir.

Uzman sistemler yüksek miktardaki ilintisiz, açık olmayan ve eksik bilginin incelenmesi konusunda zorluklar çekmektedir. Uzman sistemlerde problem uzayının çok iyi anlaşılmış olması gerekmektedir. Ama aksaklık yönetimi gibi bir alanda bu imkânsız gibidir.

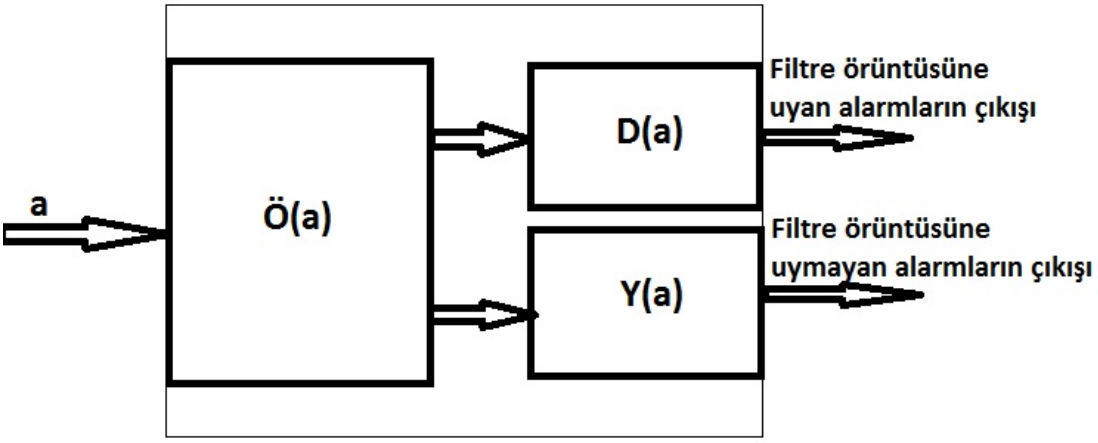
Yukarıdaki problemlere çözüm olarak son dönemlerde aksaklık yönetiminde uzman sistemlere tamamlayıcı olarak yapay zeka çözümleri araştırılmakta ve geliştirilmektedir. Aksaklık yönetimi sisteminde karşılaşılan alarmlar ve problemler üzerinden kendini eğiten ve güncelleyen, yeri geldiğinde otomatik olarak yeni uzman kurallar yazıp eskilerini güncelleyen çözümler aksaklıkların bulunması ve çözülmesi süreçlerinde insan gücünden tasarruf sağlayıp problemlerin çok daha kısa sürede çözülmesine imkan tanıyabilmektedir.

Literatüre baktığımızda, zamansal olarak birbiriyle ilişkili alarm tipleri için uzman kurallar yazılarak bahsedilen tiplerden alarmların gelmesi durumunda bu alarmları birleştirip bileşik alarmlar üreten uygulama örnekleri bulunmaktadır [3]. Bu çalışmada uzman kural bazlı alarm korelasyonu örneklerle güzel bir şekilde anlatılmasına rağmen bu kuralların üretilmesi için korelasyona tabi tutulacak alarm tiplerinin belirlenmesi kapsam dışı tutulmuştur.

2. ALARM FİLTRELEME

2.1 Amaç ve Temel Alarm Filtre Yapısı

Alarm filtresi kendisine gelen alarmları kontrol edip istenilen koşulları sağlayıp sağlamamasına göre bekleten, silen, gizleyen veya istenilen başka bir aksiyonu gerçekleştiren uygulamaya denmektedir. Alarm filtreleme, aksaklık yönetimi sistemlerinde alarm sayısını azaltma konusunda en çok başvurulan çözüm yöntemidir. GSM şebekelerinde çok çeşitli alarm filtreleri kullanılmaktadır. Alarm filtreleri geleneksel analog ve sayısal sinyal filtreleri ile benzerlikler göstermekle beraber birçok farklılıklara da sahiptir. Temel farklılık filtrelerin girdileridir. Alarmlar birçok düz yazı, sayı ve bayrak gibi tiplerde bilgiler içeren karmaşık ve homojen olmayan girdilerdir. Alarm filtrelerinin gerçekleştirmesi istenen aksiyonlar her zaman analog ve sayısal sinyal filtreleri gibi matematiksel olarak modellenemeyebilmektedir. Şekil 2.1'de GSM şebekelerinde kullanılan filtrelerin genelleştirilmiş bir hali bulunmaktadır.



Şekil 2.1: Genel Alarm Filtre Yapısı

- *a:* Filtreye giren alarmları simgelemektedir.
- *Ö(a):* Filtrenin odaklanacağı alarmları belirleyen örüntü fonksiyonudur.
- *D(a):* Filtrenin odaklanacağı alarm örüntüsüne uyan alarmlar için alınacak aksiyonları gerçekleştiren fonksiyondur.

- *Y(a):* Filtrenin alarm örüntüsüne uymayan alarmlar için alınacak aksiyonları gerçekleştiren fonksiyondur.

GSM şebekelerinde kullanılan alarm filtreleri temel olarak üç bölümden oluşmaktadır. Birinci bölüm alarm filtresinin odaklanmak istediği alarmları belirleyen alarm örüntüsü tanıma kısmıdır. Bu bölüm alarmın çeşitli bilgilerini kontrol ederek alarmın istenilen örüntüye uyup uymadığını mantıksal bir sonuç olarak belirler. İkinci bölüm alarm örüntüsüne uygun doğru alarmlar için istenilen aksiyonların alındığı bölümdür. Bu bölümde alarmın bekletilmesi, içeriğinin değiştirilmesi, başka alarmlarla ilişkilendirilmesi gibi çok farklı işlemler yapılabilmektedir. Üçüncü bölüm alarm örüntüsüne uymayan alarmlar için istenilen aksiyonların alındığı bölümdür. Genelde alarm filtresinin örüntüsüne uymayan alarmlar üzerinde herhangi bir işlem yapılmadığı için bu bölümde alarm geldikleri gibi iletilirler. Ama filtrenin alarm örüntüsü koşuluna uymayan alarmlar üzerinde işlem yapılan örneklerde bulunmaktadır.

2.2 Temel Alarm Filtresi Çeşitleri

Aksaklık yönetiminde en sık kullanılan temel filtre çeşitlerini sekiz gruba ayırabiliriz [14]:

2.2.1 Eleme Filtresi

Eleme filtrelerine basitçe açma-kapama filtreleri diyebiliriz. Filtrenin içerdiği alarm örüntüsü fonksiyonu *Ö(a)*'ya uyan alarmlar yok edilerek filtre çıkışına verilmez. Yani filtre alarm örüntüsüne uyan alarmlar için gerekli aksiyonları alan *D(a)* fonksiyonu kendine gelen alarmları elemek ile sorumludur. Filtrenin alarm örüntüsüne uymayan alarmlar *Y(a)* fonksiyonu tarafından geldikleri gibi herhangi bir değişikliğe uğramadan filtrenin çıkışına yönlendirilmektedir.

2.2.2 Boole Filtresi

Boole filtreleri alarmların üzerinde herhangi bir manipulasyon yapmayan, sadece girdi alarmlarını filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya göre iki gruba ayıran filtrelerdir. Filtredeki *D(a)* ve *Y(a)* fonksiyonları alarmları geldikleri gibi geçirmektedirler. Ama bu iki fonksiyonun çıkışları farklı sistemlere bağalanarak

alarmlarda ayrıştırılma yapılabilmektedir. Boole filtreleri karmaşık filtrelerin tasarımlarında faydalı alt birimlerdir.

2.2.3 Eşik Filtresi

Eşik filtreleri, seyrek zamanlı geldiklerinde önemsiz sayılarak filtrelenmek istenen ama sık gelmeye başladıklarında filtrelenmemesi gereken alarmlar için üretilen alarm filtreleridir. Filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya uyan alarmlar *D(a)* fonksiyonuna yönlendirilirler. Eşik filtrelerinde *D(a)* fonksiyonu iki temel karakteristik bilgi içermektedir. Bu bilgiler incelecek zaman penceresi genişliği *w* ve alarm sayısı eşik değeri t_e'den oluşmaktadır. Filtrenin alarm örüntüsüne uyan alarmlar *D(a)* fonksiyonunda *w* kadar süre için bekletilmektedir. Herhangi bir anda *D(a)* fonksiyonunda bekletilen alarm sayısı eşik değeri t_e'yi geçerse bekletilen alarmlar *D(a)* fonksiyonunun çıkışına yönlendirilirler. Eşik değeri aşılmazsa bekletilen alarmlar hala aktif ise *w* süresi sonunda elenerek filtrelenir. Filtrenin alarm örüntüsüne uymayan alarm *Y(a)* fonksiyonu tarafından herhangi bir işlem yapılmadan filtrenin çıkışına yönlendirilir. Eşik filtreleri sayesinde çok az miktarlarda geldiklerinde önemsiz olan ama sık gelmeye başladıklarında daha önemli problemlerin varlığı konusunda bilgi veren alarmlar etkili bir şekilde filtrelenir.

2.2.4 Geçici Bekletme Filtresi

Geçici bekletme filtreleri, yaşam süreleri kısa olan, sık oluşup yok olan ve önemli problemlere işaret etmemelerine rağmen incelenmesi gereken alarm sayılarını yükselten alarmları filtrelemeyi sağlayan kullanışlı filtrelerdir. Filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya uyan alarmlar *D(a)* fonksiyonuna yönlendirilirler. Geçici bekletme filtrelerinde *D(a)* foksiyonu alarm bekletmetme süresi *w* olarak adlandırılan karakteristik bir bilgi içermektedir. Filtrenin alarm örüntüsüne uyan alarmlar *D(a)* fonksiyonunda *w* kadar süre için bekletilmektedir. Eğer bekletilen alarmlar *w* süresi içinde kendiliğinden sonlandıysa alarmlar otomatik olarak filtrelenmiş olur. Ama *w* süresi sonunda bekletilen alarmlar hala aktif ise *D(a)* fonksiyonu tarafından alarm filtresinin çıkışına yönlendirilir. Filtrenin alarm örüntüsüne uymayan alarm *Y(a)* fonksiyonu tarafından herhangi bir işlem yapılmadan filtrenin çıkışına yönlendirilir.

2.2.5 Eş Alarm Filtresi

Eş alarm filtreleri aynı problem için birbirine yakın zaman aralıklarında üretilen çok fazla sayıda alarmları filtrelemek için kullanılan bir filtre çeşididir. Filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya uyan alarmlar *D(a)* fonksiyonuna yönlendirilirler. Eş alarm filtrelerinde *D(a)* foksiyonu alarm ilişkilendirme süresi *w* olarak adlandırılan karakteristik bir bilgi içermektedir. Filtrenin alarm örüntüsüne uygun bir alarm, *D(a)* fonksiyonuna geldiğinde herhangi bir değişikliğe uğramadan filtrenin çıkışına yönlendirilir. Bu esnada *D(a)* fonksiyonu içinde *w* süresine sahip bir zaman sayacı başlatılır. Bu süre içinde *D(a)* fonksiyonuna gelen alarmlar elenir. Sayaç süresi dolduktan sonra gelen ilk alarm için aynı süreç tekrarlanır. Filtrenin alarm örüntüsüne uymayan alarm *Y(a)* fonksiyonu tarafından herhangi bir işlem yapılmadan filtrenin çıkışına yönlendirilir.

2.2.6 Alarm Yığını Filtresi

Alarm yığını filtreleri şebekede gözlemlenen alarmlar üzerinde istatistiksel hesaplamalar yaparak önemli problemlere işaret edebilecek yeni alarmlar üreten özel bir filtre çeşididir. Filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya uyan alarmlar *D(a)* fonksiyonuna yönlendirilirler. Alarm yığını filtrelerinde *D(a)* fonksiyonu üç temel karakteristik bilgi içermektedir. Bu bilgiler incelecek zaman penceresi genişliği *w*, alarm sayaç değeri *c* ve alarm sayısı eşik değeri t_e'den oluşmaktadır. *D(a)* fonksiyonuna gelen her alarm için alarm sayaç değeri *c* bir yükseltilir. Gelen alarm elenmeden filtrenin çıkışına yönlendirilir. İncelenecek zaman penceresi *w* içinde alarm sayaç değeri *c* alarm sayısı eşik değeri t_e'yi geçerse filtre tarafından yeni bir alarm oluşturulur. Filtrenin alarm örüntüsüne uymayan alarm *Y(a)* fonksiyonu tarafından herhangi bir işlem yapılmadan filtrenin çıkışına yönlendirilir. Alarm yığını şebekede gözlemlenen alarmlar hakkında istatistiksel bilgiler içeren faydalı alarmlar üretip önemli kronik problemlerin farkedilmesini sağlayabilmektedirler.

2.2.7 Onarım Filtreleri

Onarım filtreleri filtre koşullarına uyan alarmları alarak içeriklerinde değişiklikler yapan filtrelerdir. Filtrenin alarm örüntü fonksiyonu *Ö(a)*'ya uyan alarmlar *D(a)* fonksiyonuna yönlendirilirler. *D(a)* fonksiyonu alarmların içeriklerinde güncellemeler ve değişiklikler yapıp manipule edilmiş alarmı filtrenin çıkışına yönlendirilir. Filtrenin alarm örütüsüne uymayan alarmların *Y(a)* fonksiyonu içinde

manipule edildiği onarım filtre örnekleri var olmakla birlikte genelde örüntüye uymayan alarmlar herhangi bir değişikliğe uğratılmadan filtrenin çıkışına yönlendirilirler. Onarım filtreleri sayesinde içerikleri bozulmuş alarmların içerikleri düzeltilebildiği gibi farklı sistemler tarafından üretilen ve aksaklık yönetimi sisteminin altyapısına uygun olmayan içerikteki alarmların altyapıya uygun hale getirilmesi sağlanabilir.

2.2.8 Hibrid Filtreler

Önceki bölümlerde anlatılan filtre çeşitleri aslında sadece filtre yapıtaşlarıdır. Yukarıda bahsedilen çeşitlerden filtreler birbirine bağlanarak karmaşık filtreler üretebilmek mümkündür.

3. ALARM İLİNTİLENDİRMESİ VE AKSAKLIKLARIN YERİNİN SAPTANMASI

3.1 Amaç

Alarm ilintilendirmesi çok sayıda alarmın değiştirilerek ve birleştirilerek daha anlamlı bilgiler içeren tek bir alarma dönüştürülmesine denmektedir [17]. Alarm ilintilendirmesi ile başlangıçtaki alarmlara birçok yeni anlam yüklenmesi mümkündür. Alarm ilintilendirme kuralları ile aksaklığın temel nedenleri ve tam olarak yeri bulunabilir.

3.2 Alarm İlintilendirme Çeşitleri

Aksaklık yönetiminde kullanılan alarm ilintilendirme çeşitlerini altı temel grup altında toplanabilir [10-12]:

3.2.1 Sıkıştırma

Sıkıştırma alarm ilintilendirmesi bir alarmın birden fazla tekrarlanmasının tek bir alarma indirgenmesidir. Bölüm 2.2.5'te açıklanan eş alarm filtrelerinin temel olarak yaptığı alarmların sıkıştırma ilintilendirmesidir. Sıkıştırma tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

$$[a, a, \dots, a] \rightarrow a \qquad \textbf{(3.1)}$$

- *a:* Oluşma anları, kaynakları ve alarm tipleri aynı olan alarmları simgelemektedir.

Sıkıştırma alarm ilintilendirme kurallarının kullanım alanlarına GSM şebekelerinden MSC santrallerinden alınan ulaşılamayan link alarmları örnek gösterilebilir. Eğer herhangi bir nedenle iki santral arasındaki transmisyon linki çalışamaz hale gelirse bu iki santral arasındaki sesli görüşme isteklerine cevap verilemeyeceği için bir anda yüzlerce ulaşılamayan link alarmı oluşabilir. Bu alarmların hepsi aynı problemi bildirdiği için alarm gözlem gruplarının ekranına tek alarm olarak düşmeleri alarm kirliliğini engelleyecektir.

3.2.2 Baskılama

Baskılama alarm ilintilendirmesi, yüksek öneme sahip bir alarm ile ilişkili olarak gelen düşük öneme sahip alarmların elenmesine denir. Alarm maskelemesi olarak da adlandırılmaktadır. Baskılama tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

$$[a, b, p(a) < p(b)] \rightarrow b \qquad \textbf{(3.2)}$$

- *a ve b:* Aynı kaynaktan aynı anda gelen, alarm tipleri farklı ama oluşma nedenleri ilişkili iki alarmı simgelemektedir.
- *p(a) ve p(b):* Bu iki alarmın öncelik değerlerini simgelemektedir.

Baskılama tipi alarm ilintilendirmesinin kullanım alanlarına GSM şebekelerinden örnek olarak önemli BSC santral alarmları verilebilir. BSC santralleri baz istasyonlarının yönetiminden sorumlu oldukları için BSC'de karşılaşılacak bir sorun aynı anda onlarca bağlı baz istasyonunda servis kalitesi problemlerine neden olabilir. Böyle bir durumda BSC santralindeki temel alarm önceliklendirilip bu probleme bağlı olarak baz istasyonlarında oluşan alarmlar maskelenir.

3.2.3 Gruplama

Gruplama alarm ilintilendirmesinde bir alarmın belirtilen bir sayıda gelmesi durumunda gelen alarmlar elenerek yerine tek bir yeni alarm üretilir. Baskılama alarm ilintilendirmesine çok benzemektedir. Baskılama alarm ilintilendirmesinde alarmlar filtrelenerek tek bir alarm bırakılır. Gruplamada aynı alarmların hepsi filtrelenerek yerlerine 1 adet farklı çeşit bir alarm oluşturulur. Düşük öneme sahip alarmlar sık gelmeye başladıklarında daha önemli problemlerin belirtisi olabilmektedirler. Gruplama tipi alarm ilintilendirmesi bu tarz problemlerin saptanmasında çok faydalı bir yöntemdir. Gruplama tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

$$[nxa] \rightarrow a \qquad \textbf{(3.3)}$$

- *a:* Gözlemlenen düşük öneme sahip alarmları simgelemektedir.
- *b:* Gözlemlenen alarm grubunu temsilen üretilen yeni yapay alarmı simgelemektedir.

Gruplama tipi alarm ilintilendirmesinin kullanım alanlarına GSM şebekelerinden örnek olarak radyolink transmisyon cihazlarında gelen kalite alarmları verilebilir. Radyolink cihazlarında anlık problemler nedeniyle düşük öncelikli kalite alarmları oluşabilmektedir. Bu alarmlar nadiren ve kısa süreli oluşup yok oluyorsa önemsizdirler. Ama kısa süre içinde çok sayıda oluşuyorlarsa radyolink cihazında bir problem olma ihtimali bulunmaktadır. Gruplama tipi alarm ilintilendirme ile bu tarz dolaylı olarak anlaşılan problemlerin alarmları yapay olarak oluşturulabilir.

3.2.4 Genelleme

Genelleme alarm ilintilendirmesinde gözlemlenen çok spesifik alarm tiplerinine sahip alarmların yerlerine daha genel alarm tiplerine sahip üst sınıflarından yeni alarmlar yaratılır. Alarm gözlem gruplarındaki insanların çok detaylı bilgilere ihtiyaç duymadıkları durumlarda genelleme alarm ilintilendirmesi gözlemlenen alarmları daha anlaşılır kılmaktadır. Genelleme tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

$$[a, a \in b] \rightarrow b \qquad \textbf{(3.4)}$$

- *a:* Gözlemlenen daha spesifik bir problemi anlatan alarmı simgelemektedir.
- *b:* Gözlemlenen alarmın yerine yaratılan ve gözlemlenen alarmın tipinin üst sınıfından üretilmiş alarmı simgelemektedir.

Genelleme tipi alarm ilintilendirmesinin kullanım alanlarına GSM şebekelerinden örnek olarak baz istasyonu ekipmanlarından gelen arıza alarmları verilebilir. Baz istasyonlarındaki ekipmanlar çok farklı nedenler ile arızalanabilmektedirler. Farklı nedenler ile farklı tipte ekipman arıza alarmları üretilmektedir. Nedeni ne olursa olsun ekipman arızası oluştuğunda bakımdan sorumlu ekiplerin baz istasyonuna gidip ilgili ekipmanı kontrol etmeleri gerektiği için oluşan spesifik alarmların yerine daha genel ekipman arızası alarmı oluşturulması alarm gözlem gruplarının karşılarındaki alarmların sadeleşmesini sağlamaktadır.

3.2.5 Özelleme

Özelleme alarm ilintilendirmesinde gelen alarmlar elenerek yerlerine daha özel alt sınıflardan alarmlar yaratılır. Genelleme alarm ilintilendirme yönteminin tam tersi bir yöntemdir. Özellikle alarmların oluşma nedenlerine ihtiyaç duyulduğu önemli

problemlerde kullanışlı bir yöntemdir. Özelleme tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

$$[a, a \ni b] \rightarrow b \quad \textbf{(3.5)}$$

- *a:* Gözlemlenen ve problemi daha genel açıklayan, problemin ayrıntılı detaylarını içermeyen alarmı simgelemektedir.
- *b:* Gözlemlenen alarmın yerine yaratılan ve gözlemlenen alarmın tipinin alt sınıfından daha spesifik bir problemi belirten alarmı simgelemektedir.

Özelleme tipi alarm ilintilendirmesinin kullanım alanlarına GSM şebekelerinden örnek olarak baz istasyonlarından gelen arıza alarmları verilebilir. Bu alarmlar baz istasyonu aksaklık tipinde oluşturulurlar. Oluşan problemin kodu alarmın içeriğinde bulunmaktadır. Bu problem kodu okunup gözlemlenen alarm yerine daha spesifik tipte alarmlar üretilebilmektedir.

3.2.6 Boole

Boole tipi alarm ilintilendirmesinde belirtilen bir boole koşuluna göre farklı tiplerde alarmlar aynı anda gelince gelen alarmlar elenerek yerine yeni bir alarm üretilmektedir. Bu ilintilendirme yöntemi farklı alarm tiplerinin eş zamanlı gözlemlenmesi ile saptanabilen aksaklıkların belirlenmesinde çok faydalıdır. Boole tipi alarm ilintilendirmesi aşağıdaki gibi modellenebilir:

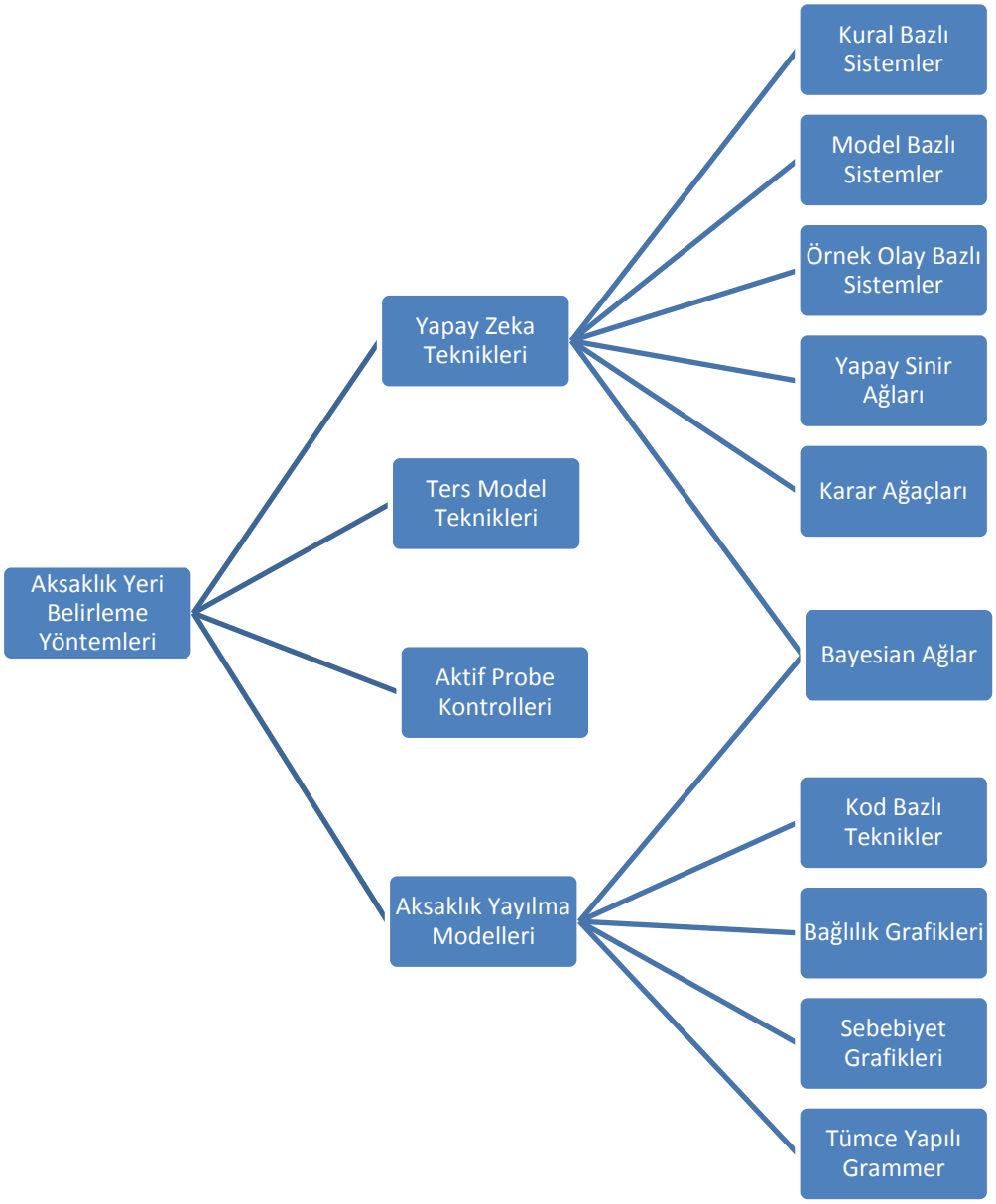
$$[A, B, \dots, T] \rightarrow C \quad \textbf{(3.6)}$$

- *A, B,..., T:* Gözlemlenen farklı tipteki alarmları simgelemektedirler.
- *C:* Gözlemlenen alarm grubu yerine yaratılan ve spesifik bir probleme işaret eden yeni alarmı simgelemektedir.

Boole tipi alarm ilintilendirmesinin kullanım alanlarına GSM şebekelerinden transmisyon alarmları örnek verilebilir. Bir transmisyon düğümünün arızalandığı ve bu arızaya dair alarm üretemediği durumlar olabilmektedir. Böyle zamanlarda şebekede bu düğümle ilişkili cihazlar çok farklı tiplerde alarmlar üretebilmektedir. Bu yöntemler gözlemlenen alarm tipi grubuna istinaden ulaşılamayan transmisyon düğümü için yeni bir alarm üretilebilmektedir.

3.3 Aksaklık Yeri Saptama Yöntemleri

Aksaklıkların yerinin saptanması bozuklukların tam kaynağının gözlemlenen alarmlar ile bulunma sürecidir. Aksaklıkların yerlerinin otomatik olarak saptanma teknikleri Şekil 3.1'de belirtildiği gibi gruplara ayrılabilir [2]:

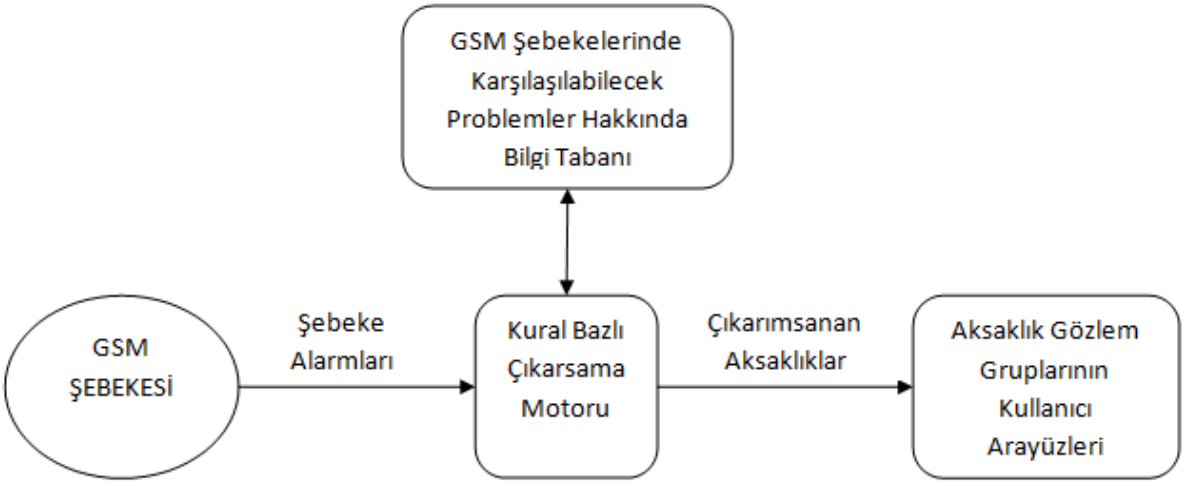


Şekil 3.1: Aksaklık Yeri Saptama Yöntemleri

3.3.1 Yapay Zeka Teknikleri

Kural Bazlı Sistemler

Aksaklık yönetimi sistemlerinde aksaklıkların yerinin ve nedenlerinin bulunmasında en yaygın olarak kullanılan çözüm kural bazlı sistemlerdir. Kural bazlı çözümler uzman sistemler üzerinde uzman kuralların tanımlanıp kullanılması ile yaratılmaktadır. Kural bazlı sistemler belirli alanlardaki problemlerin çözümlerinde o alanda uzman kişilerin tecrübelerini kullanarak çözümler üretmeye çalışan otomatik sistemlerdir. Alan uzmanlarının bilgileri ve tecrübeleri kural tanımlama dilleri ile yazılarak uzman sistemin bilgi tabanı oluşturulur. Aksaklık yerinin bulunması için uzman sistem üzerinde bulunan çıkarsama motoru bilgi tabanındaki kuralları döngüsel bir şekilde ateşleyerek uzman kişilerin uzmanlığını taklit etmeye çalışır ve kural bazlı muhakeme ile aksaklığın yerini ve sebeplerini bulmaya çalışır. Aşağıdaki şekilde GSM şebekeleri için kural bazlı sistemlerin teorik grafiği verilmiştir.



Şekil 3.2: GSM Şebekeleri İçin Kural Bazlı Sistem

Kural bazlı sistemler çok yaygın olarak kullanılmalarına rağmen önemli eksiklikleri olduğu için aksaklık yeri saptama konusunda alternatif çözüm yöntemlerinin geliştirilmesi aktif araştırmaların yapıldığı bir alandır. Kural bazlı sistemler kendi kendine tecrübelerden ders çıkarıp öğrenen sistemler değillerdir. Daha önceden karşılaşılmamış durumlara ve öngörülememiş problemlere çözüm getiremezler. Aksaklık yeri saptamada çok faydalı bilgiler olan ağ konfigürasyon ve topoloji

bilgileri genellikle kuralların kodları içinde statik tanımlanmaktadır. Değişen koşullar karşısında kuralların yazılım bakım maliyetleri yüksektir. Değişimler ve yeni durumlar karşısında yeni kuralların yazılması ve var olan kuralların güncellenmesi gerekmektedir. Bu nedenle aksaklık yönetiminde farklı yapay zeka çözümleri de geliştirilmeye çalışılmıştır.

Model Bazlı Sistemler

Model bazlı aksaklık belirleme çözümleri de uzman sistemler üzerinde gerçeklenen ama uzman kurallar yazılırken problem uzayındaki sistem modelleri referans alınarak değişimlere karşı daha dinamik kuralların yazıldığı bir yaklaşımdır. Modeller genellikle nesneye dayalı yaklaşımla tanımlanırlar ve bu modeller genellikle sistem içerisinde birbirine bağımlı bileşenlerin ilişkilerini içermektedir [2]. Aksaklıkların bulunmaya çalışıldığı problem uzayları çok farklılıklar gösterebildiği için model bazlı aksaklık belirleme sistemlerinde kullanılan modeller de çok farklılıklar gösterebilmektedir.

Aksaklık belirleme sistemlerinde model bazlı yapay zeka çözümlerini daha iyi anlayabilmek için örnek olarak GTE laboratuarlarında geliştirilmiş olan IMPACT (Intelligent Management Platform for Alarm Correlation Tasks) sistemini inceleyebiliriz [11]. IMPACT sisteminde kullanılan modelde iki temel bileşen kullanılmaktadır: Yapısal bileşen ve davranışsal bileşen. Yapısal bileşende ilgili ağ bileşenlerinin bilgileri, birbirleriyle bağlantıları ve hiyerarşik ilişkileri bulunmaktadır. Davranışsal bileşende gelen alarmların bilgileri, alarm sınıflarının hiyerarşik ilişkileri ve alarm sınıflarının ilişkileri bulunmaktadır. Model bazlı yazılan uzman kurallar ile aksaklık yönetimi sistemine gelen alarmlar, alarmların geldiği ağ elementleri ve elementlerin arasındaki ilişkiler ile alarmlar ilintilendirilip aksaklığın yeri saptanabilmektedir.

Model bazlı sistemlere başka bir örnek FLAMES sistemidir [29]. Bu sistemin amacı ATM ağlarındaki aksaklıkların saptanmasıdır. Sistemde kullanılan model, ATM ağındaki cihazların yapısı ve cihazların bileşenlerinden beklenen doğru davranışlardan oluşmaktadır. FLAMES sisteminde modele göre beklenen davranışlar dışındaki davranışların tamamı aksaklık olarak algılanmaktadır. Bu sistemde modelin tasarımı Fuzzy uzman sistem kullanılarak yapılmıştır.

Aksaklık yönetimi yapılan fiber optik transmisyon ağının topoloji bilgisi kullanılan araştırmalar yapılmaktadır [6]. Komşu olan ağ elementleri saptanarak gelen alarmların direk bir aksaklıktan mı yoksa bir aksaklığın yankısından mı geldiği saptanıp aksaklığın tam yeri bulunmaya çalışılmaktadır.

GSM şebekeleri için geliştirilen çalışmalar da bulunmaktadır [30]. Model tasarımlarında baz istasyonu, BSC ve MSC gibi farklı ağ elementleri ayrı davranış beklentileri ile modellenmiştir. Herhangi bir durumda sistemden beklenen davranış ile sistem tarafından gerçekleştirilen davranış karşılaştırılarak aksaklıkların saptanmasına çalışılmaktadır.

Model bazlı sistemler kural bazlı sistemlere göre daha esnek ve kullanışlı olsalar da kullanılan modellerin güncel tutulması zor bir iştir. Modelin ağ yapısının hiyerarşisi hakkındaki kısmı geliştirilen entegrasyonlarla güncel olarak bir konfigürasyon veri tabanından çekilerek modelin güncel tutulması kısmi olarak kolaylaşabilmektedir.

Örnek Olay Bazlı Sistemler

Örnek olay bazlı sistemler, kararların yaşanmış tecrübeler ve geçmişte karşılaşılan olaylara göre alındığı özel bir uzman sistem çeşididir [2,7,12]. Geçmişte karşılaşılan olaylar ve getirilen çözüm bilgilerini kullanarak karşılaşılan yeni problemlere çözüm önerileri getirmektedirler.

Örnek olay bazlı sistemler çok farklı alanlarda aksaklık yeri ve nedenlerini belirlemekte kullanılmaktadır. Bilgisayar ağları aksaklık yönetiminde, hem aksaklıkların saptanması hem de saptanan aksaklıklara çözümler getirilmesinde örnek olay kütüphanesi kullanılabilmektedir [4]..

Örnek olay bazlı sistemler yazılım geliştirme süreçlerinde aksaklık yeri belirleme konusunda başarılı bir şekilde kullanılabilmektedirler [31]. Yazılım geliştirme süreçlerinin analiz, geliştirme ve test gibi farklı aşamalarında karşılaşılan problemler örnek olay olarak kaydedilip yazılım geliştirme süreçlerinde karşılaşılan yeni aksaklıkların yerlerinin ve nedenlerinin çok daha kısa sürede saptanıp çözümler üretilmesi sağlanmaktadır.

Genelde haberleşme ağlarında aksaklık yönetimi fiziksel kaynaklarına göre yönetilirken, çalışmasında servis merkezli bir aksaklık yönetimi için algoritmalar bulunan örnek olay bazlı sistemler de bulunmaktadır [7]. Çalışmada önerilen kural

bazlı ve örnek olay bazlı hibrid alarm korelasyon algoritması ile servislerde gerçekleşen aksaklıklar saptanıp kaliteli hizmetin devamı için gerekli çözüm yolları sistem tarafından tavsiye edilmektedir.

Aksaklık yönetimi sisteminde aşağıdaki koşullar bulunuyorsa örnek olay bazlı sistemlerin kullanılması çok uygun bir çözüm haline gelmektedir [12]:

- Problem uzayı modelinin üretilmesinin zor veya imkânsız olması
- Sistemin değişimler karşısında sürekli yazılım bakımı gerektirmesi
- Geçmişte karşılaşılan problemlerin çözümlerinin kayıtlarının tutulması
- Çözüm getirilen problemlere benzer problemlerin gözlemlenmeye devam etmesi

Örnek olay bazlı sistemlerin faydaları aşağıdaki gibidir [4,12]:

- Kısmen anlaşılmış problem uzaylarındaki problemlerin çözümünü sağlayabilirler.
- Problemlerin benzerliklerini saptama ve kullanma yetkinliklerine göre yeni veya değişmiş durumların üstesinden gelebilirler.
- Karşılaşılan yeni olayların incelenmesi ile tecrübelerden ders alıp kendilerini geliştirebilirler.
- Değişimlere karşı çok yüksek yazılım bakımı gerektirmezler.
- Karşılaşılan durumların nedenlerini geçmiş durumlarla benzerliklerini etkin olarak kullanarak bulabilirler.
- Normal uzman kural geliştirme süreçlerinden çok daha az zamana mal olan otomatik bilgi çıkarım yöntemlerini kullanabilirler.
- Uzman kural kütüphanesi yerine karşılaşılan olay kütüphanesi üretmek çok daha kolaydır.
- Geçmiş olaylardan kazanılan bilgilerin tutulma biçimi uzman kuralların tutulma biçimlerinden daha serbestçe yapılmakta ve belli kalıplar içerisinde bulunma zorunlulukları olmamaktadır.
- Karşılaşılabilecek durum çeşitlerinin çok yüksek sayıda olduğu büyük problem uzaylarına uyum konusunda çok başarılılardır. Kaydedilen tecrübe

bilgilerinin tutulma yöntemlerinin izin vermesi ile karşılaşılan olay kayıtları parçalanarak veya birleştirilerek yeni bilgilere ulaşılabilir.

- Bu sistemler tavsiye edilen çözüm yönteminin başarı bilgisini simülasyon ile ve/veya geçmiş olay kütüphanelerini kullanarak belirleyebilir.

Geçmiş olay bazlı sistemlerin yetersiz kaldığı durumlarda olmaktadır [4,12]:

- Karşılaşılan yeni durumların geçmişte yaşanan olaylarla benzerliği yok ise başarılı bir çözüm üretemez.
- Tavsiye edilen çözümler için ayrıntılı açıklamalar sunamaz.
- Karşılaşılan olaylar ve getirilen çözüm bilgileri kolay elde edilebilir bilgiler değilse olay kütüphanesinin yaratılması çok uzun zaman alır.

Çalışma şekli zaman alıcı olduğu için gerçek zamanlı alarm ilintilendirmesinde başarılı sonuçlar veremeyebilir.

Yapay Sinir Ağları

Yapay sinir ağları nöron adı verilen birbirine bağlı düğümler kullanılarak insan beyninin çalışma şeklinin taklit edilmeye çalışıldığı sistemlerdir. Aksaklık yönetimi sistemlerinde alarmların korelasyonunda ve aksaklıkların yerinin saptanmasında kullanılan bir çözüm yöntemidir [2,4,22].

Literatürde, uçak motorlarındaki sensörlerden gelen sinyaller kullanılarak aksaklık yeri saptayan yapay sinir ağı çözüm örnekleri bulunmaktadır [22]. Analog sinyaller yapay sinir ağları tarafından işlenerek motor aksaklıkları belirlenmektedir.

Yapay sinir ağlarının aksaklık yeri saptama konusunda aşağıdaki avantajları bulunmaktadır [4]:

- Yapay sinir ağları daha önceden çözümü bilinen durumlara benzer durumları saptayabilmektedir (örüntü eşleştirme).
- Yeterli sayıda nöron kullanılırsa yapay sinir ağları her türlü fonksiyonu ve sınıflandırıcıyı üretebilmektedir. Bu durum yapay sinir ağlarına farklı alarm örüntüleri için eğitilebilirlik konusunda büyük esneklik vermektedir.
- Yapay sinir ağları problem uzayı hakkında ayrıntılı bilgilere sahip olmadan kolaylıkla genellemeler yapabilir ve kendini eğiterek verilen bir fonksiyonun

yakınsamasını kolaylıkla üretebilir. Bu özellikler sürekli gelişen ve değişen yeni teknolojilerin aksaklık yönetimi sistemlerinde büyük avantaj sağlamaktadır.

- Gelen alarmların analizi konusunda hızlı ve etkili bir çözüm yöntemi sunarlar.

Eksik, açık olmayan ve kötü bilgilerin üstesinden kolaylıkla gelebilmektedirler.

Karar Ağaçları

Karar ağaçları uzman bilgi birikiminin aksaklıkların yerinin ve nedenlerinin bulunması konusunda kullanıcılara rehberlik etmesini sağlayan özel bir gösterim çeşididir. Ama başarıları gürültülü ve kirli bilgiler olduğunda düşmekte ve uygulanabilirlikleri uygulama bağımlı oldukları için düşük olmaktadır [2].

3.3.2 Ters Model Teknikleri

Aksaklık yönetiminde ters model teknikleri bilgisayar ve haberleşme ağlarında bulunan varlıkların aralarındaki ilişkileri kullanan tekniklerdir. Bu ilişkiler göz önüne alınarak gelen problem alarmları incelenir, alarmlar ilintilendirilerek aksaklığın yeri tespit edilir [2,32]. Ters model teknikleri, gözlemlenen sistemlerin nesneye dayalı modellerini kullanırlar. Bu tekniklerde alarm korelasyonu genellikle alarm bazlı tetiklenmektedir. Gözlemlenen her alarm için modeldeki yönetilen nesnelerin aralarındaki ilişkiler özyinelemeli olarak araştırılmaktadır. Bu araştırmalar sonucunda aksakların tam yerleri bulunabilmektedir. Ters model teknikleri ağ yapısındaki sık karşılaşılabilen konfigürasyonel değişimlerden kolay etkilenmezler. Aksaklık yeri belirleme süreçlerinde otomatik yönetilen nesne testleri kullanılıyorsa ters model teknikleri özellikle faydalı olabilirler. Eğer ağdaki nesneler arasındaki ilişkiler grafiksel olarak gösterilebiliyorsa ve bu ilişkilerin güncel hallerini elde etmek kolay ise ters model teknikleri çok kullanışlı olurlar.

3.3.3 Aktif Kontrol Teknikleri

Aktif kontrol teknikleri aksaklıkların yerinin bulunması konusunda etkili çözümler geliştirmemize yardımcı olan bir çeşit aktif gözlemleme yöntemidir. Geleneksel aksaklık yönetimi sistemleri pasif gözlemleme yöntemleri kullanmaktadır. Problemler oluştuğunda alarmlar üretilir. Üretilen alarmlar bir merkezde toplanıp

aksaklıkların yeri saptanmaya çalışılmaktadır. Aktif kontrol tekniklerinde aksaklıkların belirlenmesi için alarm gelmesi beklenmez. Çalışan sistem üzerinde testler yapılmaktadır. Bu testler bir kaynaktan başka bir kaynağa gönderilen basit ping komutlarından seri halde yapılan kompleks performans testlerine kadar çeşitlilik gösterebilmektedir. Pasif gözlemleme tekniklerinin aksine aktif kontrol yöntemlerinde yönetilen ağlarda ek bir trafik oluşmaktadır. Bu durum aktif kontrol tekniklerinin en temel dezavantajıdır. Bu etkiyi azaltmak için aktif kontroller en az kaynak harcayacak şekilde tasarlanmaya çalışılır. Yönetilen ağın farklı yerlerinde gerçek zamanlı uygulanan aktif kontroller ile bir aksaklık durumunda aksaklığın yeri bulunabilmektedir [28,33].

Örnek olarak bir GSM şebeke işletmecisi firmanın transmisyon alt yapısında kilit durumda olan bir transmisyon düğümü arızalanıp vermesi gerekenden daha düşük performansta hizmet vermeye başlayabilir. Bu durumda bu düğümün düşen bant genişliği nedeniyle uçtan uça birçok hizmet aksayabilmektedir. Aktif kontroller ile uçtan uca testlerinde kötü sonuçlar alınan senaryolar için transmisyon şebekesinde adım adım kontroller yapılarak aksaklık tam olarak saptanabilmektedir.

Aktif kontrollerin çok faydalı olduğu bir başka örnek kara delik aksaklıklarıdır [34]. Ağda bulunan bazı düğümler kendilerine gelen paketleri göndermeleri gereken yeren göndermeyip bir de bu problem için alarm üretmeyebilirler. Oluşmaları ile birlikte hiçbir alarm üretmeyen ve pasif gözlem yöntemleri ile saptanamayan aksaklıklara kara delik aksaklıkları denmektedir. Aktif kontrol yöntemleri uçtan uca gerçek zamanlı bir çok test uyguladıkları için bu aksaklıkları kolayca saptayabilmektedir.

3.3.4 Aksaklık Yayılma Modelleri

Bilgisayar ve haberleşme ağlarında yer alan düğümlerden birisinde bir aksaklık oluştuğunda bu aksaklıktan çevresinde ilişkili olduğu düğümlerde etkilenebilmektedir. Bir temel aksaklık nedeniyle komşu düğümlerde yeni aksaklıkların oluşması aksaklık yayılması olarak adlandırılmaktadır. Oluşan her yeni aksaklık yeni alarm mesajları üretmektedir. Yayılan aksaklıklar ve belirtileri ile aksaklıkların kök nedenlerini bulmak için kullanılan yöntemlere aksaklık yayılma modelleri denmektedir. Aksaklık yayılımı üzerinden temel aksaklığı bulma yöntemleri temel olarak beş grup altında toplanabilmektedir.

Kod Bazlı Teknikler

Kod bazlı teknikler aksaklık yeri saptamasını kolaylaştırmak için bilgi teorisini kullanan tekniklerdir. Bu tekniklerde aksaklık yayılma örüntüleri kod bazlı tekniklerle kod rehberi şeklinde tutulmaktadırlar. Kod bazlı tekniklerde alarmlar ve bu alarmlara neden olan kök nedenler bir matris üzerinde gösterilmektedir. Bu matrisler bağlılık grafiklerinin işlenmesi ve optimize edilmesi ile üretilirler[7]. Haberleşme ağlarındaki alarmları incelerken kod bazlı teknikleri kullanan uygulamalara örnek olarak SMARTS adlı ürünü gösterebiliriz [9,16]. Bu uygulamada haberleşme ağ yapısı MODEL adı verilen nesneye dayalı dille modellenmektedir. Alarm korelasyon motoru kod bazlı teknik ile çalışmaktadır. Gelen alarmlara ve gözlemlere kodlar üretilip kod rehberindeki kayıtlarla Hamming uzaklıkları hesaplanarak aksaklıklar saptanmaktadır.

Bayesian Ağlar

Bayesian ağları, aksaklık yeri saptamasında belirsizliğin üstesinden gelebilmek için olasılıksal hesaplamalar kullanan başarılı tekniklerdir. Bayesian ağları düğümlerden ve düğümlerin arasında belirsiz neden sonuç ilişkilerinden oluşan ağlardır. Düğümlerin arasındaki ilişkiler istatistiksel ihtimallerle belirtilmektedir. Bayesian ağlar aynı zamanda aksaklık yeri belirleme yöntemlerinden yapay zeka teknikleri altında da yer almaktadır.

Aksaklık yeri saptamada Bayesian ağlara örnek olarak Shrink adı verilen uygulama gösterilebilir [35]. Uygulama optik bir katman üzerinde çalışan bir IP ağında aksaklık yeri saptamasında kullanılmaktadır. Alarm tarihçesi ve topoloji bilgilerinden üretilen istatistiksel bilgiler ile Bayesian ağ oluşturulup güncel alarmlar bu ağ ile işlenip aksaklık yeri saptamaları yapılmaktadır.

Aksaklık yeri saptanmasında Bayesian ağların aşağıdaki avantajları bulunmaktadır [4]:

- Bayesian ağları, haberleşme ağlarının fonksiyonlarını haberleşme ağlarındaki elementlerin, bilgisayar ağının davranışlarının ve aksaklıkların aralarındaki ilişkilerin neden sonuç ilişkileri ile modelleyebilmektedir.
- Bayesian ağı üzerindeki hesaplamalarla ağ üzerindeki aksaklıklar bulunabilmektedir.

- Bayesian ağlar olasılık teorisini kullandıkları için gürültülü, geçici ve belirsiz bilgileri kullanabilmektedir.
- Bayesian ağları diğer olasılık metotları ile kıyaslandıklarında kolay anlaşılır, modüler ve kompakt bir yapıya sahiptirler.
- Bayesian ağları kompakt ve iyi tanımlanmış bir problem uzayı sunmaktadır. Çünkü bütün delil veya aksaklık setleri için aynı çözüm yöntemini kullanmaktadır.

Aksaklıkları belirleyen bir Bayesian ağı üretebilmek için problem uzayındaki neden sonuç ilişkilerini çok iyi anlamak gerekmektedir. Bu bilgilerin uzmanlar tarafından verilmesi gerekmektedir. Bu hem bir avantaj hem de bir dezavantajdır. Bu bir avantajdır çünkü bilgi yapay sinir ağlarındaki gibi kara kutu şeklinde gösterilmemektedir. Bu bir dezavantajdır. Çünkü problem uzaylarında bu bilgilerin temin edilmesi çok zor bir iştir.

Bağlılık Grafikleri

Bağlılık grafikleri düğümlerin birbirlerine göre bağımlılıklarını gösteren yönlü grafiklerdir. $G=(O,D)$ şeklinde modellenebilmektedir.. O değişkeni belirli sayıda obje içeren bir seti simgelemektedir. D ise bu objelerin kendi aralarındaki yönlü ilişkileri içermektedir. $(o_i,o_j) \epsilon O$ ilişkisi o_i objesinde gerçekleşen bir aksaklığın o_j objesinde de bir aksaklığa neden olabileceğini belirtmektedir. Alarm tarihçesi ayrıntılı analiz edilerek oluşturulan bağlılık grafikleri kullanılarak, yeni oluşan alarmlar ile aksaklık yerleri saptanabilmektedir.

Sebebiyet Grafikleri

Sebebiyet grafikleri düğümlerin neden sonuç ilişkileri içerdiği, yönlü ve çevrimsiz grafiklerdir. $G_c(E,C)$ şeklinde grafiksel olarak modellenebilmektedirler. E ilgili alarmları ve C bu alarmların arasındaki neden sonuç ilişkilerini içermektedir. $(e_i,e_j) \epsilon C$ şeklindeki sebebiyet grafiği ilişkisi e_i alarmının e_j alarmına neden olduğunu simgelemektedir ($e_i \rightarrow e_j$). Alarm tarihçesi ayrıntılı analiz edilerek sebebiyet grafikleri oluşturulup aksaklık yeri saptanabilmektedir.

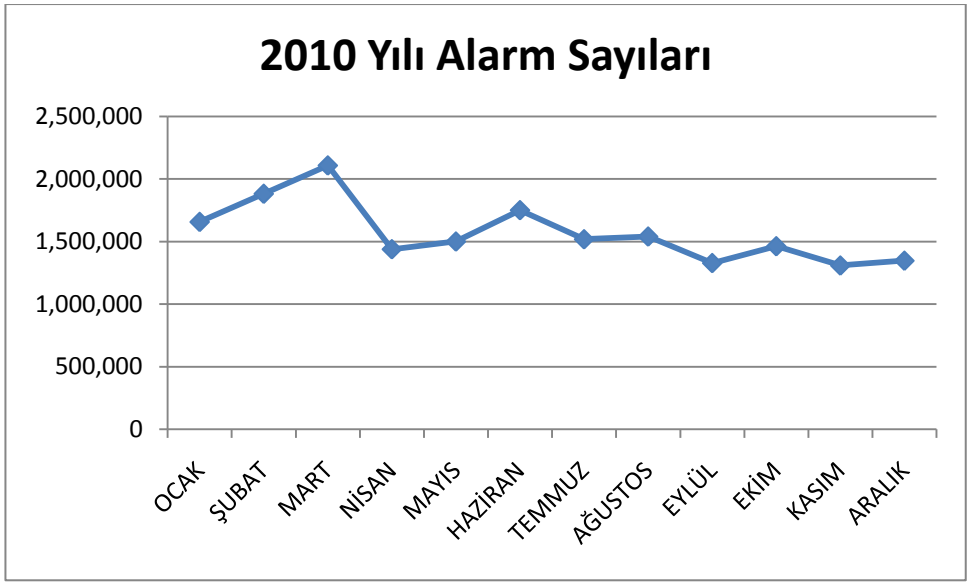
Tümce Yapılı Gramerler

Grafiksel bağlantıların, ilişkilerin tümce yapılı gramer kullanılarak ifade edildiği çözümlerdir.

4. ÇALIŞMADA KULLANILAN VERİ KÜMESİ

4.1 Ham Alarm Veri Kümesi

Tez çalışması kapsamında iki farklı konuda uygulamalı olarak yeni yöntemler geliştirilmiştir. Her iki çalışmada da aynı veri kümesi kullanılmıştır. Veri kümemiz Türkiye'nin en büyük GSM şebeke işletmecisi Turkcell İletişim Hizmetleri AŞ'nin aksaklık yönetimi sistemine 01.01.2010-31.12.2010 tarihleri arasında gelen bir yıllık alarmlardan oluşmaktadır. Şekil 4.1'de bu veri kümesindeki aylık alarm sayıları grafiği gösterilmektedir.



Şekil 4.1: Veri Kümesindeki Aylık Alarm Sayıları

Veri kümemizde 104.094 kaynak tarafından üretilmiş 3400 farklı alarm tipinde toplam 18.842.887 alarm bulunmaktadır. Çizelge 4.1'de karşılaşılan alarm, kaynak ve alarm tipi sayılarının aylara göre dağılımı yer almaktadır:

Çizelge 4.1: Veri Kümesindeki Alarmlar

	Kaynak Sayısı	Alarm Tipi Sayısı	Alarm Sayısı
Ocak	55.237	889	1.657.219
Şubat	67.629	900	1.881.684
Mart	64.743	1.166	2.107.949
Nisan	59.397	1.112	1.438.950
Mayıs	62.525	1.237	1.500.395
Haziran	69.492	1.460	1.750.816
Temmuz	63.601	1.759	1.518.524
Ağustos	66.924	1.788	1.540.150
Eylül	67.389	1.630	1.328.627
Ekim	73.784	1.662	1.462.800
Kasım	64.710	1.374	1.308.614
Aralık	69.549	1.328	1.347.159
2010 Toplam	104.094	3400	18.842.887

Veri kümesinde bulunan her alarm 20 farklı parametre içermektedir.

- Alarm Id: Aksaklık yönetimi sisteminin alarma verdiği ayırt edici numara
- Notification Id: Alarma alarmın üretildiği sistem tarafından verilen ayırt edici numara
- Severity: Alarmın önem derecesi
- Alarm Type: Alarmın tipi
- Alarm Header: Alarmın başlığı
- Probable Cause: Alarmın muhtemel nedeni
- Managed Object: Alarmın kaynağı
- Additional Text: Alarm hakkında ek bilgiler
- User Text: Aksaklıkları gözlemleyen personel için ek bilgilendirme alanı
- Creation Time: Alarmın yaratılma zamanı
- Event Time: Alarmın aksaklık yönetimi sistemine geliş zamanı
- Clearance Time: Alarmın sona erme zamanı
- Clearance Report Flag: Alarmın düzeldi bilgisinin tutulduğu bayrak
- Cell Name: Alarm bir GSM hücresi geliyorsa ilgili hücrenin ismi
- BTS Name: Alarm bir GSM baz istasyonu veya bu istasyona bağlı bir alt cihazdan geliyorsa ilgili baz istasyonunun ismi

- Node: Alarm bir GSM santrali veya bu santrale bağlı bir alt birimden geliyorsa ilgili santralin ismi
- Acknowledgement User: Alarmın incelemesini yapan personelin ismi
- Acknowledgement Time: Alarmın incelenme zamanı
- Handled User: Alarmı çözen personelin ismi
- Handle Time: Alarmın çözüm zamanı

4.2 Alarm Tipi Veri Kümeleri

Tez çalışması kapsamında GSM şebekelerinde karşılaşılan geçici alarm tipleri ve ilintili alarm tiplerinin belirlenmesi için istatistiksel makine öğrenmesi yöntemleri önerilmiştir. Önerilen yöntemlerin başarımının ölçümlendirilebilmesi için Turkcell Şebeke Kontrol Merkezinde çalışan uzmanların tez çalışmamız için ürettiği geçici alarm tipi veri kümesi ve ilintili alarm tipi veri kümesi kullanılmıştır.

4.2.1 Geçici Alarm Tipi Veri Kümesi

Alarm veri kümesinde gözlemlenme sayısı 2000'den büyük 358 alarm tipi, alarm gözleme uzmanları tarafından incelenerek geçici alarm tipi olup olmadıklarına karar verilmiştir. Geçici alarm tipleri yaşam süreleri birkaç dakikayı geçmeyen ve verilen hizmet konusunda önemli problemlere işaret etmeyen alarm tipleridir. Çalışmamızda geçici alarm tiplerinin belirlenmesi konusunda önerilen yöntemlerin başarılarının ölçümlendirilmesinde bu veri kümesi kullanılmıştır. Çizelge 4.2'de veri kümesinde yer alan geçici ve kalıcı alarm tipi sayıları yer almaktadır.

Çizelge 4.2: Geçici Alarm Tipi Veri Kümesi

Geçici Alarm Tipi Sayısı	Kalıcı Alarm Tipi Sayısı	İncelenen Alarm Tipi Sayısı
85	273	358

Çizelge 4.3'de geçici alarm tipi veri kümesinde yer alan geçici ve kalıcı alarm tipleri örnekleri bulunmaktadır.

Çizelge 4.3: Geçici ve Kalıcı Alarm Tipi Örnekleri

Alarm Tipi	Alarm Tipi Durumu
Pool Capacity Degraded	Geçici Alarm Tipi
Huawei Tch Mht Low	Geçici Alarm Tipi
Path Forward Congested	Geçici Alarm Tipi
Ccit7 Destination Inaccessible	Kalıcı Alarm Tipi
Cell Out Of Service	Kalıcı Alarm Tipi
Gtp Tunnel Path Broken	Kalıcı Alarm Tipi

4.2.2 İlintili Alarm Tipi Veri Kümesi

Alarm veri kümesinde eş zamanlı gözlemlenme sayıları 1000'den büyük olan 320 alarm tipi ikilisi, alarm gözleme uzmanları tarafından incelenerek ilintili alarm tipleri olup olmadıklarına karar verilmiştir. Çalışmamızda ilintili alarm tiplerinin belirlenmesi konusunda önerilen yöntemlerin başarılarının ölçümlendirilmesinde bu veri kümesi kullanılmıştır. Çizelge 4.4'de veri kümesinde yer alan ilintili ve ilintisiz alarm tipi ikililerinin sayıları yer almaktadır.

Çizelge 4.4: İlintili Alarm Tipi Veri Kümesi

İlintili Alarm Tipi İkilileri Sayısı	İlintisiz Alarm Tipi İkilileri Sayısı	İncelenen Alarm Tipi İkilileri Sayısı
141	179	320

Çizelge 4.5'de ilintili alarm tipi veri kümesinde yer alan, ilintili ve ilintisiz alarm tipi ikililerinden örnekler bulunmaktadır.

Çizelge 4.5: İlintili Alarm Tipi Veri Kümesi

Alarm Tipi 1	Alarm Tipi 2	İlinti Durumu
Ap Not Redundant	Ap Fault	İlintili
Cell Out Of Service	Cell Ps Service Faulty	İlintili
Ncp Faulty Alarm	Sctp Link Down	İlintili
Rectifier Under V	Ac Failure	İlintili
Ap Fault	Heartbeat Failure	İlintisiz
Rectifier Under V	Door Opened	İlintisiz
High Temperature	Rectifier Mains	İlintisiz
Door Opened	Free Cooling Failure	İlintisiz

5. ÖZDEVİMLİ GEÇİCİ BEKLETME FİLTRELERİ ÜRETİMİNDE İSTATİSTİKSEL ÖĞRENME YÖNTEMLERİ

GSM şebekelerinde karşılaşılan alarmların büyük bir kısmı geçici alarm olarak adlandırılan kısa ömürlü ve düşük öncelikli alarmlardır [37]. Geçici alarmlar önemli problemlere işaret etmemelerine rağmen sayıları çok yüksek olduğu için GSM şebekelerinde aksaklık yönetiminden sorumlu personelin incelemesi gereken problem sayılarını arttırdıkları için iş gücü kaybına ve önemli problemlere geç müdahale edilmesine neden olmaktadırlar. Geçici alarmlarla mücadelede en yaygın kullanılan yöntem alarm tiplerine göre hazırlanmış alarm bekletme filtreleridir [14]. Alarmlar alarm gözlem sistemine geldiklerinde filtrede tanımlanan bekletme süresi kadar bekletilirler. Bu süre içerisinde ilgili alarmın belirttiği problem çözülürse alarm ekrana yansımadan elenmiş olur. Ancak problem hala devam ediyorsa bu alarmın geçici bir alarm olmadığı anlaşılıp gözlem ekranına aktarılır. Alarm bekletme filtreleri uzman kişiler tarafından GSM şebekesinde geçmişte gözlemlenmiş alarm örneklerine göre yaratılmaktadırlar. Tez çalışması kapsamında alarm bekletme filtrelerinin otomatik olarak yaratılması ve var olan filtrelerin güncellenmesi için GSM şebekesinde geçmişte gözlemlenmiş alarm bilgilerini kullanan iki yeni istatistiksel öğrenme yöntemi önerilmiştir. Önerilen her iki yöntemin temelinde, geçici alarm tiplerinin yaşam sürelerini istatistiksel dağılımlarının düşük değerlerde yoğunlaştığı varsayımı yatmaktadır. Geçici alarm tiplerinin belirlenmesinde önerilen yöntemler Histogram Analizi ve Parzen Penceresi Analizi yöntemleridir.

5.1 Algoritma Detayları

Çalışmamızda geçici alarm tiplerinin belirlenmesi için önerilen her iki yöntemde de alarm tarihçesinde yer alan alarmların yaşam sürelerinin alarm tiplerine göre birikimli yoğunluk fonksiyonları üretilmektedir. Üretilen istatistiksel fonksiyonlar incelenerek alarm tiplerinin geçici alarm tipi olup olmadığına karar verilip, geçici alarm tipleri için uygun alarm bekletme süreleri tavsiye edilmektedir. Önerilen iki yöntem arasındaki fark sadece alarmların yaşam sürelerinin birikimli yoğunluk fonksiyonlarının hesaplama yöntemlerinin farklılığıdır.

5.1.1 Alarm Modeli

GSM şebekelerinde gözlemlenen alarmların içeriğinde yaratılmalarına neden olan problem ile ilgili çok çeşitli bilgiler bulunabilmektedir. Bu çalışmada önerilen yöntemlerde alarmların iki temel bilgisi ön plana çıkmaktadır. Bu iki temel bilgi alarmın tipi ve yaşam süresidir. Alarm tarihçesindeki alarmlar aşağıdaki gibi modellenebilmektedir:

$$a_i = (e_i, t_i) \quad \textbf{(5.1)}$$

- $\boldsymbol{a_i}$**:** Gözlemlenen alarmı simgelemektedir.
- $\boldsymbol{e_i}$**:** Gözlemlenen alarmın tip bilgisidir.
- $\boldsymbol{t_i}$**:** Alarmın saniye olarak yaşam süresidir ($t_i > 0$).

Alarm tarihçesindeki ham alarm bilgileri alarm modeline uygun şekilde sadeleştirildiğinde kullanılan veri kümesi aşağıdaki gibi iki değişkenli üyeler içeren bir küme olarak modellenebilmektedir:

$$A = \{a_i\}_{i=1}^{N} \quad \textbf{(5.2)}$$

5.1.2 Histogram Analizi ile İstatistiksel Yoğunluk Hesaplama

Histogram analizi, dağılımdan bağımsız olasılık kestirimi konusunda kullanılan en eski ve yaygın yöntemdir. Bu yöntemde girdi uzayı eşit boyda kutucuklara bölünmektedir. Bir sıfır noktası t_0 ve kutu genişliği h verildiğinde kutucuklar, artı ve eksi m tamsayıları için, $[t_0+mh,\ t_0+(m+1)h)$ aralıklarını kapsar ve kestirim, kutucuk içine düşen örneklerin oranıdır [38]:

$$\hat{p}(t) = \frac{\#\{t\ ile\ aynı\ kutucuğa\ düşen\ t_i\}}{Nh} \quad \textbf{(5.3)}$$

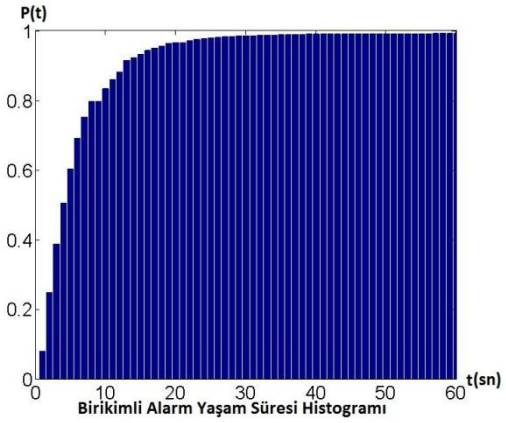
- t: Dağılımdan bağımsız olasılık kestirimi yapılan değişkendir. Çalışmamızda alarm yaşam süresini simgelemektedir.
- $\hat{p}(t)$: t değişkeninin dağılımdan bağımsız hesaplanmış yoğunluk fonksiyonudur.
- N**:** Hesaplamada kullanılan t değişkenine ait gözlemlerin toplam sayısıdır. Çalışmamızda alarm veri kümesinde incelenen alarm tipine sahip alarm örneği sayısıdır.
- h: Histogramı oluşturan kutucukların genişliğidir. Çalışmamızda bu değer 1 saniye olarak kullanılmıştır.

Histogram analizi yöntemi ile bir değişkenin birikimli yoğunluk fonksiyonu hesaplanmak istenirse formül 5.3'ün manipule edilmesi ile üretilen formül 5.4 kullanılabilir:

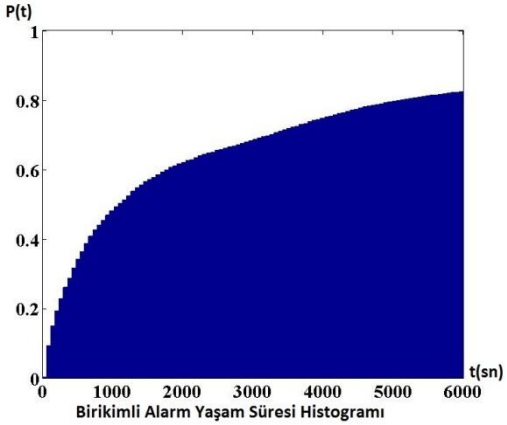
$$P(t) = \frac{\#\{t \text{ ile aynı veya daha önceki kutucuklara düşen } t_i\}}{Nh} \quad \textbf{(5.4)}$$

- $P(t)$: t değişkeninin dağılımdan bağımsız hesaplanmış birikimli yoğunluk fonksiyonudur.

Çalışmamızda formül 5.4 kullanılarak alarm veri kümesinde yer alan alarm tiplerinin yaşam sürelerinin birikimli yoğunluk fonksiyonları hesaplanmaktadır. Şekil 5.1'de geçici alarm tiplerine örnek olarak "Pool Capacity Degraded" alarm tipinin birikimli yaşam süresi histogramı verilmiştir. Şekil 5.2'de kalıcı alarm tiplerine örnek olarak "Cell Out Of Service" alarm tipinin yaşam süresi birikimli yoğunluk histogramı bulunmaktadır. Bu iki histogram şekil olarak birbirlerine benzeselerde yaşam süresi konusunda geçici alarm tipi örneğindeki dağılım kalıcı alarm tipindeki dağılımdan çok daha düşük yaşam sürelerinde yoğunlaşmaktadır. Şekil 5.1'de geçici alarm tipi histogram örneğinin 0-60 saniye arasındaki kısmı gösterilirken, Şekil 5.2'de kalıcı alarm tipi histogram örneğinin 0-6000 saniye arasındaki kısmı gösterilmektedir.



Şekil 5.1: Geçici Alarm Tipi Histogram Örneği



Şekil 5.2: Kalıcı Alarm Tipi Histogram Örneği

5.1.3 Parzen Penceresi Analizi ile İstatistiksel Yoğunluk Hesaplama

Parzen penceresi yöntemi, bir değişkenin istatistiksel yoğunluk fonksiyonunun keskin hatları olmadan yumuşak bir şekilde üretildiği parametrik olmayan bir yöntemdir [37]. Yoğunluk fonksiyonunun yumuşak bir şekilde üretilmesi için formül 5.5'de gösterilen Gaussian çekirdek fonksiyonu kullanılmaktadır:

$$K(u) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{u^2}{2}\right) \tag{5.5}$$

Bu yöntemde incelenen değişkene ait gözlem değerleri belirtilen Gaussian çekirdek fonksiyonundan geçirilerek değişkenin yoğunluk fonksiyonu elde edilir. Parzen penceresi yöntemi ile üretilen yoğunluk fonksiyonunun formülü formül 5.6'da gösterilmiştir:

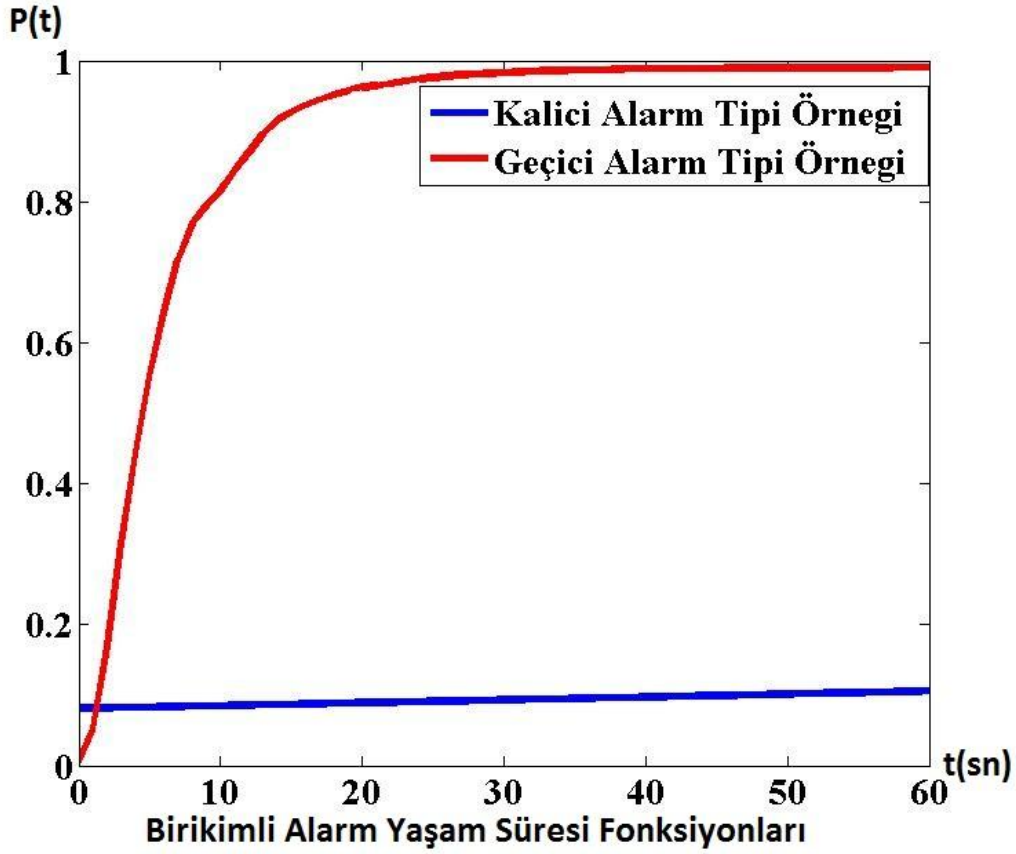
$$p(t) = \frac{1}{Nh} \sum_{i=1}^{N} K\left(\frac{t - t_i}{h}\right) \tag{5.6}$$

- *p(t):* t değişkeninin Parzen penceresi yöntemi ile hesaplanmış yoğunluk fonksiyonudur.
- *N:* t değişkenine ait mevcut gözlem sayısıdır.
- *K:* Formül 5.5'de verilen Gaussian çekirdek fonksiyonudur.
- t_i*:* t değişkenine ait gözlem değeridir (Gözlemlenen alarmın yaşam süresi).
- *h:* Parametrik olmayan yoğunluk hesaplama yönteminin karmaşıklığını kontrol eden parametredir (Keskin hatların yumuşatılmasını etkiler).

Parzen penceresi yöntemine göre bir değişkenin birikimli yoğunluk fonksiyonu formül 5.7 ile hesaplanabilmektedir:

$$P(T) = \int_{-\infty}^{T} \frac{1}{Nh} \sum_{i=1}^{N} K\left(\frac{t - t_i}{h}\right) \partial t \qquad \textbf{(5.7)}$$

Şekil 5.3'de geçici alarm tiplerinden "Pool Capacity Degraded" ve kalıcı alarm tiplerinden "Cell Out Of Service" alarm tiplerinin Parzen penceresi yöntemi ile hesaplanmış yaşam süresi birikimli yoğunluk fonksiyonları gösterilmektedir. Şekilde görüldüğü gibi geçici alarm tipi örneğinin birikimli yoğunluk fonksiyonu çok hızlı bir şekilde artış gösterirken, kalıcı alarm tipi örneğinin yaşam sürelerinin birikimli yoğunluk fonksiyonu daha yatay bir artış göstermektedir.



Şekil 5.3: Parzen Penceresi Yaşam Süresi Birikimli Yoğunluk Fonksiyonları

5.1.4 Özdevimli Geçici Bekletme Filtrelerinin Üretimi

Alarm bekletme filtreleri iki parametre ile yaratılan özel filtrelerdir. Bekletilecek alarm tipi ve bekletme süresi. Çalışmamızda önerilen yöntemlerde, filtre üretilecek alarm tiplerine ve üretilecek filtrelerin bekletme sürelerine karar vermek için alarm tiplerinin yaşam sürelerinin birikimli yoğunluk fonksiyonları kullanılmaktadır. Bir alarm tipi için tavsiye edilebilecek bekletme süresinin alt ve üst limit değerlerini

hesaplamak için aşağıdaki iki temel kıstas kullanılmaktadır. Bu iki kıstas sisteme uzmanlar tarafından girdi olarak verilmektedir.

Maksimum bekletme süresi eşiği ($t_{ü}$): Üretilen filtrelerde kabul edilebilir en yüksek bekletme süresidir. Tavsiye edilebilecek bekletme süresinin üst eşik değeridir.

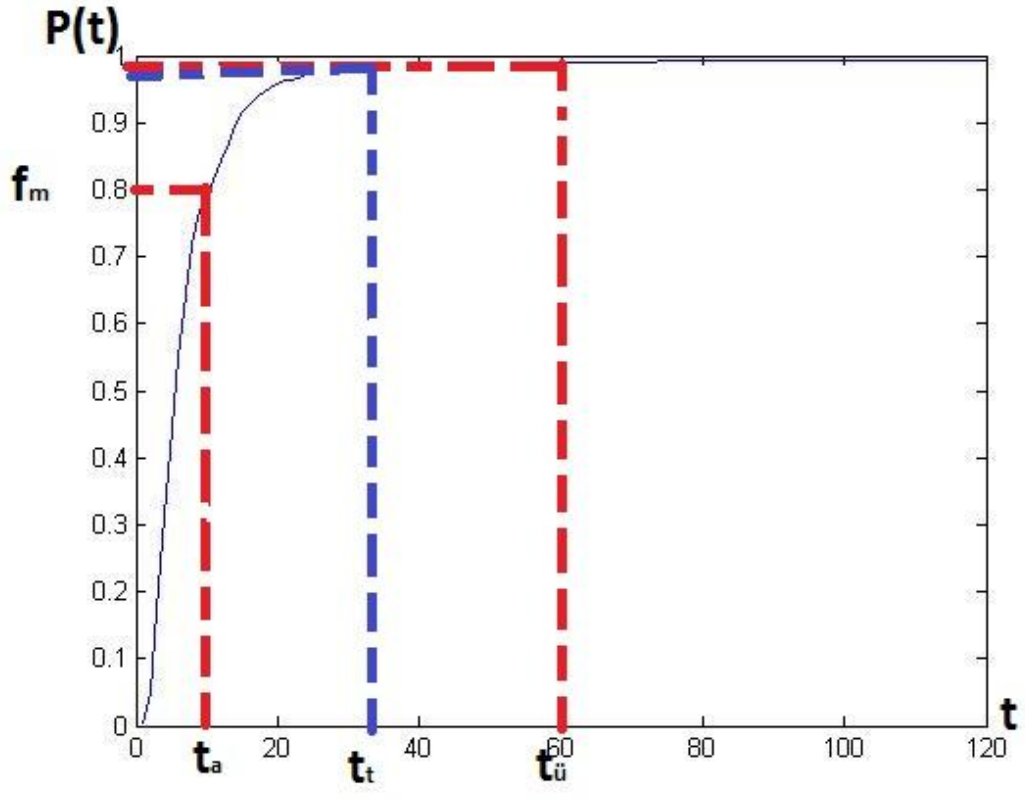
Minimum alarm filtreleme yüzdesi (f_m): Üretilen filtreler için kabul edilebilir en düşük alarm filtreleme yüzdesidir. Bir filtrenin alarm filtreleme yüzdesi, ilgili filtrenin incelenen veri kümesi üzerinde test edilmesi ile hesaplanmaktadır.

Birikimli yoğunluk fonksiyonunda f_m filtreleme yüzdesi eşik değerine denk gelen bekletme süresi değeri (t_a) tavsiye edilebilecek bekletme süresinin alt eşik değeridir. Geçici alarm tiplerine karar vermek için her alarm tipinin yaşam süresi birikimli yoğunluk fonksiyonları üretilerek f_m filtreleme yüzdesi eşik değerine denk gelen bekletme süresi değeri (t_a) hesaplanır. Eğer hesaplanan bekletme süresi alt eşik değeri t_a, tavsiye edilebilecek maksimum bekletme süresi eşiği $t_{ü}$ değerinden büyük ise bu alarm tipinin geçici alarm tipi olmadığına karar verilir. Çünkü bu alarm tipi için maksimum bekletme süresi eşiğinde bir filtre yaratılsa bile bir filtreden beklenecek minimum alarm filtreleme yüzdesine ulaşılamayacaktır. Eğer $t_{ü}$ değeri t_a değerinden büyük ise incelen alarm tipinin geçici alarm tipi olduğuna karar verilip üretilecek filtre için bekletme süresi olarak $t_{ü}$ ve t_a'nın ortalaması tavsiye edilir. Formül 5.8'de karar verme süreci özetlenmektedir:

$$t_f(e) = \begin{cases} \frac{t_a + t_{ü}}{2}, & t_a \le t_{ü} \\ 0, & t_a > t_{ü} \end{cases} \qquad \textbf{(5.8)}$$

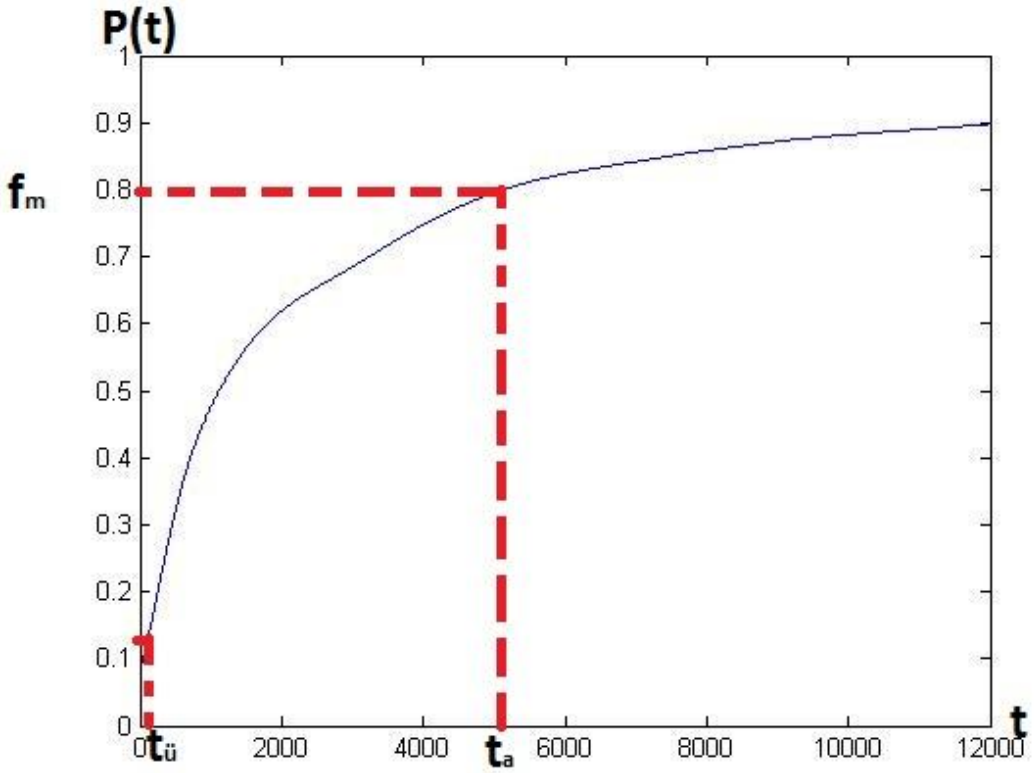
- t_f: Tavsiye edilen filtre için alarm bekletme süresidir.
- e: Filtre üretilmek üzere incelenen alarm tipidir.
- t_a: Minimum alarm filtreleme yüzdesi eşiği (f_m) ile hesaplanan bekletme süresi alt eşik değeridir.
- $t_{ü}$: Bekletme süresi üst eşik değeridir.

Formül 5.8 kalıcı alarm tipleri için 0 sonucunu dönmektedir. Eğer bu formül 0'dan farklı bir değer dönerse incelenen alarm tipi geçici alarm tipi olarak önerilmektedir. Dönen sonuç ise önerilecek filtrede kullanılacak alarm bekletme süresidir.



Şekil 5.4: Geçici Alarm Tipinin ve Filtre Bekletme Süresinin Çıkarımı

Şekil 5.3'de örnek bir geçici alarm tipinin yaşam süresi birikimli yoğunluk fonksiyonu verilmiştir. Maksimum alarm bekletme süresi($t_{ü}$) 60 saniye ve minimum alarm filtreleme yüzdesi(f_m) %80 limitleri verildiğinde alarm tarihçesinden üretilen yaşam süresi birikimli yoğunluk fonksiyonu ile f_m değerine karşılık minimum bekletme süresi alt limit değeri t_a 12 saniye olarak hesaplanmaktadır. Çalışmamızda önerilen karar fonksiyonu t_a 12 saniye ve $t_{ü}$ 60 saniye olduğu için bu alarm tipinin geçici alarm tipi olduğuna karar vermektedir. Bekletme süre t_t olarakta t_a ve $t_{ü}$'nün ortalaması 36 saniye tavsiye etmektedir. Tavsiye edilen 36 saniyelik bekletme süresine birikimli yoğunluk fonksiyonunda karşılık gelen alarm filtreleme yüzdesi %98 olmaktadır.



Şekil 5.5: Kalıcı Alarm Tipinin Belirlenmesi

Şekil 5.5'de örnek bir kalıcı alarm tipinin yaşam süresi birikimli yoğunluk fonksiyonu verilmiştir. Maksimum alarm bekletme süresi($t_{ü}$) 60 saniye ve minimum alarm filtreleme yüzdesi(f_m) %80 limitleri verildiğinde alarm tarihçesinden üretilen yaşam süresi birikimli yoğunluk fonksiyonu ile f_m değerine karşılık minimum bekletme süresi alt limit değeri t_a 5250 saniye olarak hesaplanmaktadır. Sistemden beklenen minimum alarm filtreleme yüzdesini sağlayacak alarm bekletme süresi alt limit değeri t_a, alarm bekletme süresi $t_{ü}$'nün çok üzerinde olduğu için karar fonksiyonumuz bu alarm tipini kalıcı alarm tipi olarak önermektedir.

5.2 Deneysel Gözlem Sonuçlarının Başarı Ölçümlendirilmesi

Çalışmamız kapsamında geçici alarm tiplerinin belirlenmesi için önerdiğimiz histogram analizi ve Parzen penceresi analizi yöntemleri alarm veri kümesi üzerinde test edilmiştir. Kullanılan alarm veri kümesi 2010 yılında Turkcell GSM şebekesinde gözlemlenen alarmlardan oluşmaktadır. Bölüm 4.1'de kullanılan alarm veri kümesi hakkında ayrıntılı bilgiler bulunmaktadır. Elde edilen sonuçların başarısının ölçümü için Turkcell alarm gözlem uzmanları tarafından üretilmiş geçici alarm tipi veri

kümesi kullanılmıştır. Geçici alarm tipi veri kümesi en sık karşılaşılan 358 alarm tipini ve bu alarm tiplerinin geçicilik/kalıcılık durumlarını içermektedir. Veri kümesinde bulunan 358 alarm tipinden 85 tanesi geçici, 273 tanesi kalıcı alarm tiplerinden oluşmaktadır (Bölüm 4.2.1).

Başarım ölçümleme metriklerinin hesaplanmasında kullanılan temel bilgiler Çizelge 5.1'de verilmektedir:

Çizelge 5.1: Alarm Tipi Belirlenmesinde Hata Dizeyi

	Tahmin Edilen Sınıf	
Gerçek Sınıf	Geçici Alarm Tipi	Kalıcı Alarm Tipi
Geçici Alarm Tipi	DP	YN
Kalıcı Alarm Tipi	YP	DN

- **DP (Doğru Pozitif):** Sınıfı doğru şekilde belirlenmiş geçici alarm tipi sayısıdır.
- **YP (Yanlış Pozitif):** Geçici alarm tipi olarak önerilen kalıcı alarm tipi sayısıdır.
- **YN (Yanlış Negatif):** Kalıcı alarm tipi olarak önerilen geçici alarm tipi sayısıdır.
- **DN (Doğru Negatif):** Sınıfı doğru şekilde belirlenmiş kalıcı alarm tipi sayısıdır.

Önerilen yöntemlerin başarımının ölçümlendirilmesinde üç temel metrik kullanılmıştır. Kullanılan metrikler başarılı tavsiye sayısı, tavsiye kesinliği ve sınıflandırma başarısı metrikleridir.

- **Başarılı Tavsiye Sayısı:** Sınıfı doğru şekilde belirlenmiş geçici alarm tipi sayısıdır. Çizelge 5.1'de belirtilen DP sayısına eşittir.
- **Tavsiye Kesinliği:** Önerilen geçici alarm tiplerinin doğruluk başarısının ölçümüdür. Formül 5.9 ile hesaplanmaktadır.

$$Kesinlik = \frac{DP}{DP+YP} \quad \textbf{(5.9)}$$

- **Sınıflandırma Başarısı:** Önerilen geçici ve kalıcı alarm tiplerinin doğruluk başarısının ölçümüdür. Bu ölçümleme metriğinde önerilen geçici alarm tiplerinin kesinliği dışında önerilen kalıcı alarm tiplerinin kesinliği de dikkate alınmaktadır. Formül 5.10 ile hesaplanmaktadır.

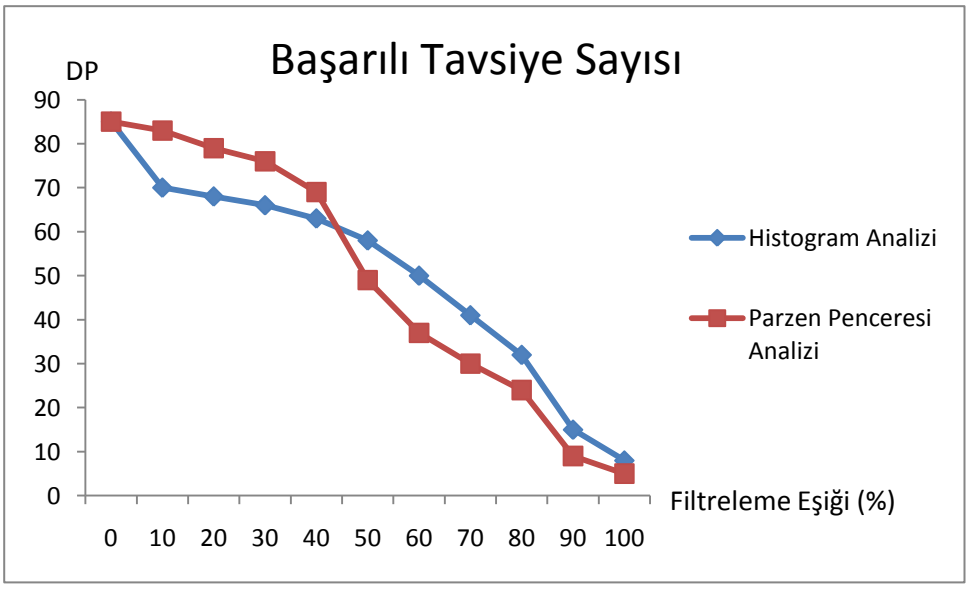
$$Başarı = \frac{DP+DN}{DP+YP+DN+YN} \quad \textbf{(5.10)}$$

5.3 f_m ve $t_ü$ Değerlerinin Değişimine Göre Deneysel Sonuçlar

Çalışmamızda önerilen iki yöntemde bekletilecek alarm tiplerine karar verilirken sisteme girdi olarak minimum alarm filtreleme yüzdesi eşiği(f_m) ve maksimum alarm bekletme süresi eşiği($t_ü$) değerleri verilmektedir. Bu değerler yaşam süresi birikimli yoğunluk fonksiyonu incelenen alarm tipi için tavsiye edilebilecek bekletme süresinin alarm tarihçesindeki gözlemlere dayalı alt ve üst eşik değerlerinin belirlenmesinde kullanılır. Geçici alarm tipi veri kümesinde bulunan 358 alarm tipinin yaşam süresi birikimli histogramları ve Parzen penceresi yöntemi ile üretilmiş birikimli yoğunluk fonksiyonları kullanılarak başarılı tavsiye sayısı, tavsiye kesinliği ve sınıflandırma başarılarının farklı f_m ve $t_ü$ değerlerine göre değişimi incelenmiştir.

5.3.1 Başarılı Tavsiye Sayılarının f_m ve $t_ü$ Değerlerine Göre Değişimi

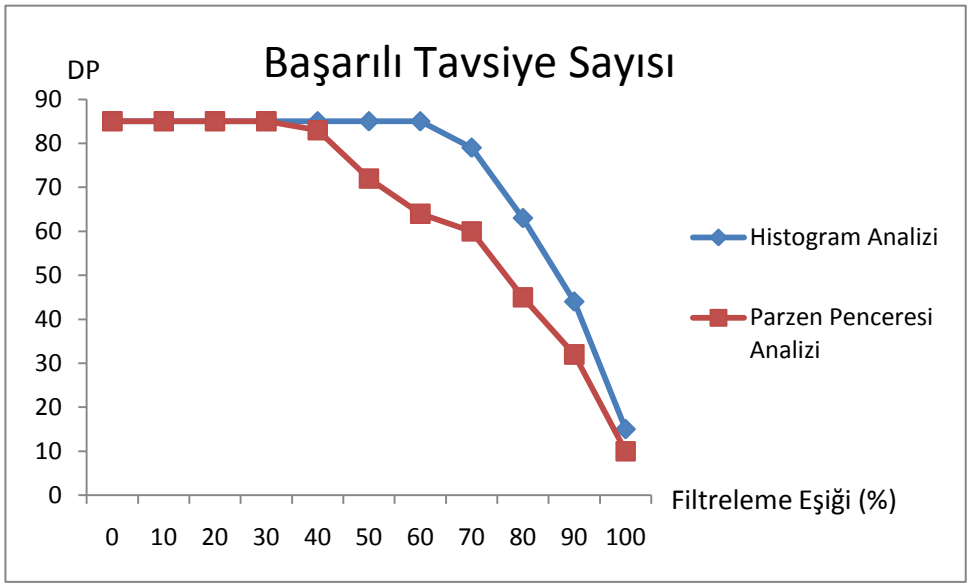
Başarılı tavsiye sayısı, sınıfı doğru şekilde tahmin edilmiş geçici alarm tipi sayısıdır. Başarılı tavsiye sayısının yüksekliği daha çok sayıda başarılı geçici alarm bekletme filtresi üretilebileceğini göstermektedir.



Şekil 5.6: Başarılı Tavsiye Sayısı ($t_ü$=60 saniye)

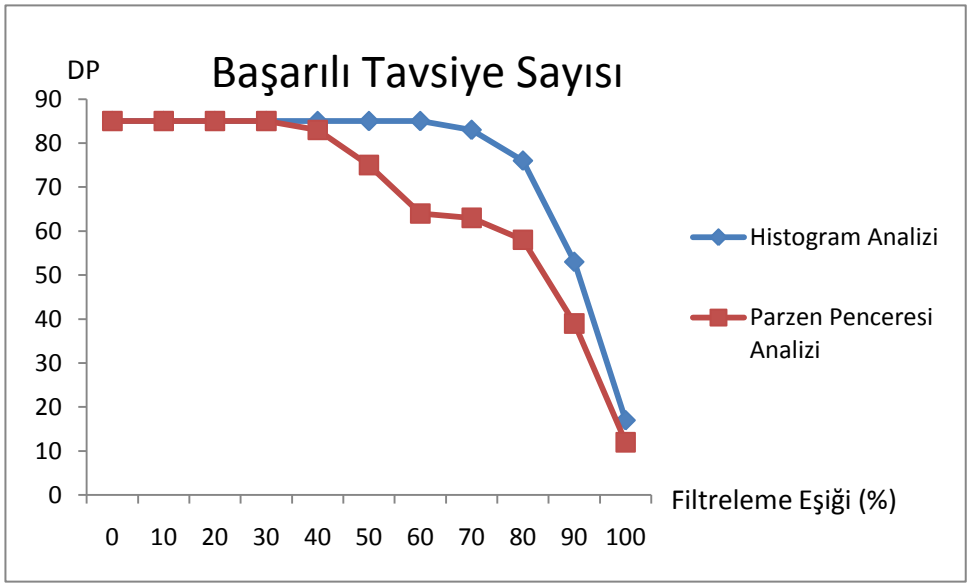
Şekil 5.6'da maksimum alarm bekletme süresi eşiği($t_ü$) değeri 60 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile başarılı

geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.7: Başarılı Tavsiye Sayısı ($t_{ü}$=300 saniye)

Şekil 5.7'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 300 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.8: Başarılı Tavsiye Sayısı($t_{ü}$=600 saniye)

Şekil 5.8'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 600 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile

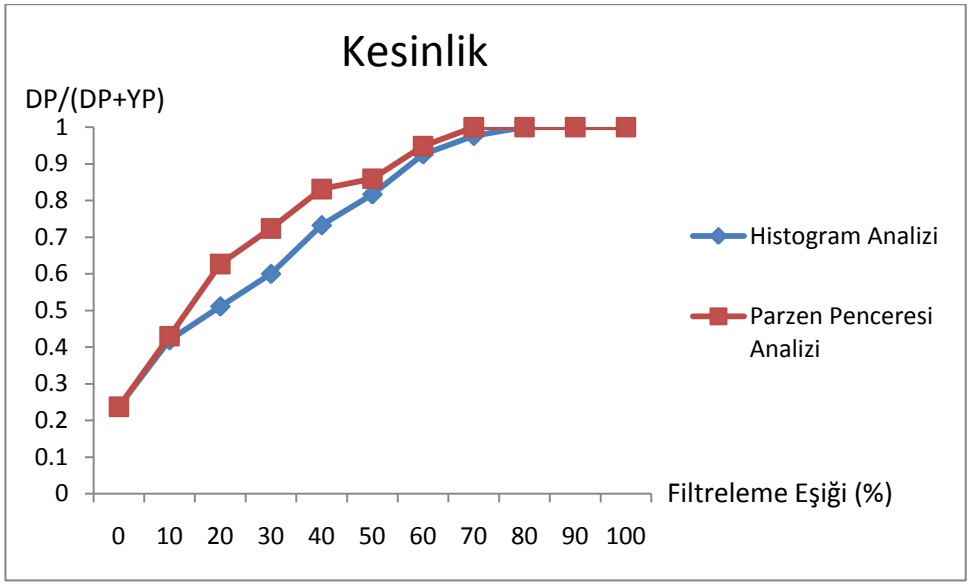
başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

Şekil 5.6, Şekil 5.7 ve Şekil 5.8 karşılaştırılmalı şekilde incelendiğinde başarılı tavsiye sayısı konusunda Histogram Analizi kullanımının daha başarılı sonuçlar verdiği görünmektedir. Düşük f_m değerleri(%0-%50 arası) için Parzen Penceresi Analizi ve Histogram Analizi yöntemlerinin başarılı tavsiye sayısı sonuçları birbirine yakınken, yüksek f_m değerleri(%50-%100 arası) için Histogram Analizi yönteminin başarılı tavsiye sayısı çok daha yüksektir. Diğer iki şekilden farklı olarak Şekil 5.6'da düşük f_m değerleri(%0-%50 arası) için Parzen Penceresi Analizi yönteminin başarılı tavsiye sayısı Histogram Analizi yönteminin başarılı tavsiye sayısından daha yüksektir. Şekil 5.6'da $t_ü$ değeri Şekil 5.7 ve Şekil 5.8'deki $t_ü$ değerlerinden çok daha düşüktür. Bu üç şekilden aşağıdaki iki sonuç çıkarılabilmektedir:

- Minimum alarm filtreleme yüzdesi eşiği değeri(f_m) yükseldikçe başarılı tavsiye sayısı düşmektedir.
- Maksimum alarm bekletme süresi eşik değeri($t_ü$) ve minimum alarm filtreleme yüzdesi eşik değeri(f_m) düşük değerlerdeyse($t_ü$=60 saniye f_m=%40 gibi), Parzen Penceresi Analizi yönteminin başarılı tavsiye sayısı daha yüksektir. Diğer durumlarda Histogram Analizi yöntemi daha yüksek sayıda başarılı tavsiyede bulunmaktadır.

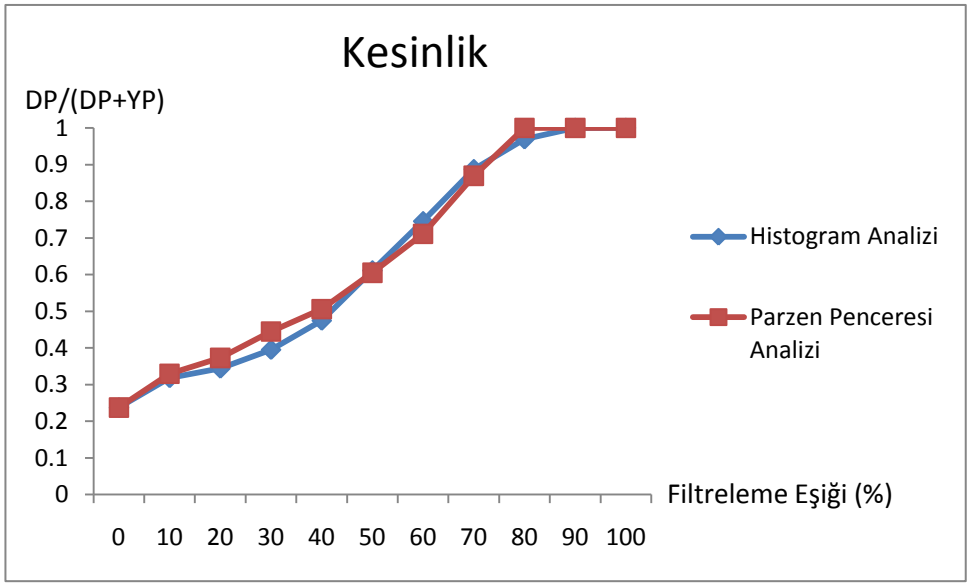
5.3.2 Tavsiye Kesinliğinin f_m ve $t_ü$ Değerlerine Göre Değişimi

Geçici alarm tiplerinin belirlenmesinde başarılı tavsiye sayısı önemli bir gösterge olmasına rağmen tek başına bir anlam ifade etmemektedir. Başarılı tavsiye sayısı yüksek olsa bile başarısız tavsiye sayısı da yüksek ise tavsiyelerin güvenilirliği düşmektedir. Bu nedenle tavsiyelerin güvenilirliğini ölçmek için formül 5.10 ile hesaplanan tavsiye kesinliği ölçümü kullanılmıştır.



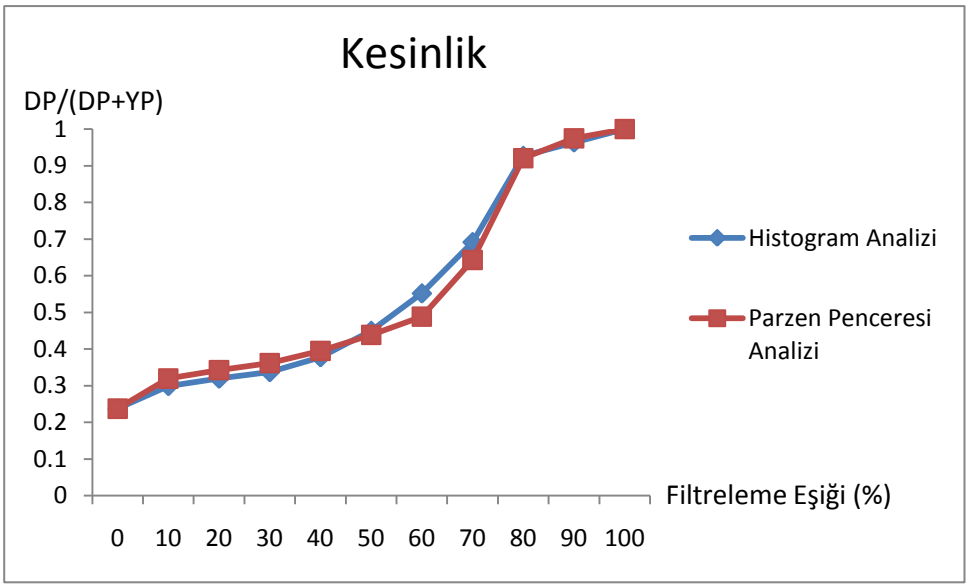
Şekil 5.9: Tavsiye Kesinliği ($t_{ü}$=60 saniye)

Şekil 5.9'da maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.10: Tavsiye Kesinliği ($t_{ü}$=300 saniye)

Şekil 5.10'da maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 300 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.11: Tavsiye Kesinliği ($t_{ü}$=600 saniye)

Şekil 5.11'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 600 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

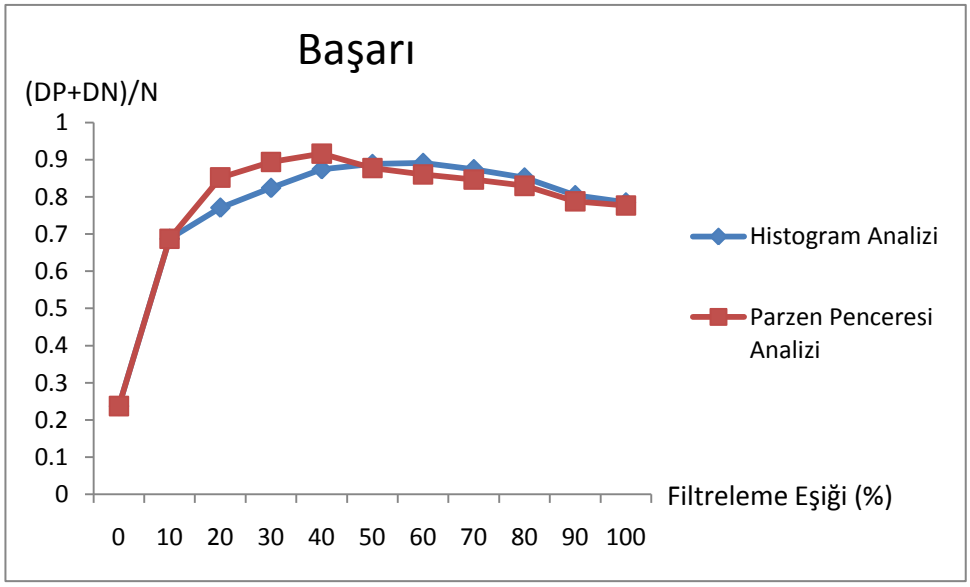
Şekil 5.9, Şekil 5.10 ve Şekil 5.11 karşılaştırılmalı şekilde incelendiğinde tavsiye kesinliği konusunda her iki yöntemde benzer sonuçlar sergilemiştir. Her üç şekilde de minimum alarm filtreleme yüzdesi değeri(f_m) yükseldikçe tavsiye kesinliği yükselmektedir. Şekil 5.10 ve Şekil 5.11'de görüldüğü gibi maksimum alarm bekletme süresi değeri($t_{ü}$) 300 ve 600 saniye iken önerilen her iki yöntemin tavsiye kesinliği her f_m değeri için birbirlerine çok yakındırlar. Şekil 5.9 incelendiğin $t_{ü}$ değeri daha 60 saniye iken Parzen Penceresi yönteminin tavsiye kesinliği Histogram Analizi yönteminin tavsiye kesinliğinden çok daha başarılıdır. Bu üç şekil incelendiğinde aşağıdaki iki sonuç çıkarılabilmektedir:

- Minimum alarm filtreleme yüzdesi eşiği değeri(f_m) yükseldikçe tavsiye kesinliği yükselmektedir.

- Maksimum alarm bekletme süresi eşik değeri($t_{ü}$) düşük bir değerdeyse (60 saniye gibi), Parzen Penceresi analizi yönteminin deneysel sonuçlarının tavsiye kesinliği Histogram Analizi yönteminin sonuçlarından daha yüksektir. $t_{ü}$ değeri yükselirse her iki yöntemin tavsiye kesinliği sonuçları birbirlerine yaklaşmaktadır.

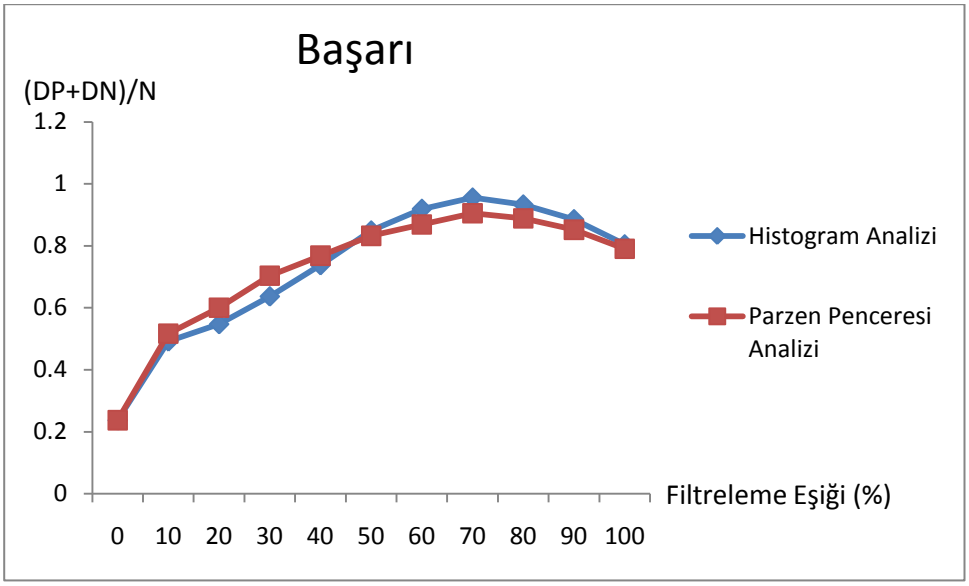
5.3.3 Sınıflandırma Başarısının f_m ve $t_{ü}$ Değerlerine Göre Değişimi

Tavsiye kesinliği ölçümü ile sadece geçici alarm tipi önerilerinin başarısı ölçümlenmektedir. Bu nedenle çalışmamızda geçici alarm tiplerinin belirlenmesi için önerilen iki yöntemin performansları başarılı tavsiye sayıları ve tavsiye kesinlikleri beraber incelenerek ölçümlenebilmektedir. Formül 5.11'de belirtilen sınıflandırma başarısı ölçümünde hem geçici hemde kalıcı alarm tipi önerilerinin başarıları beraber göz önüne alınmaktadır.



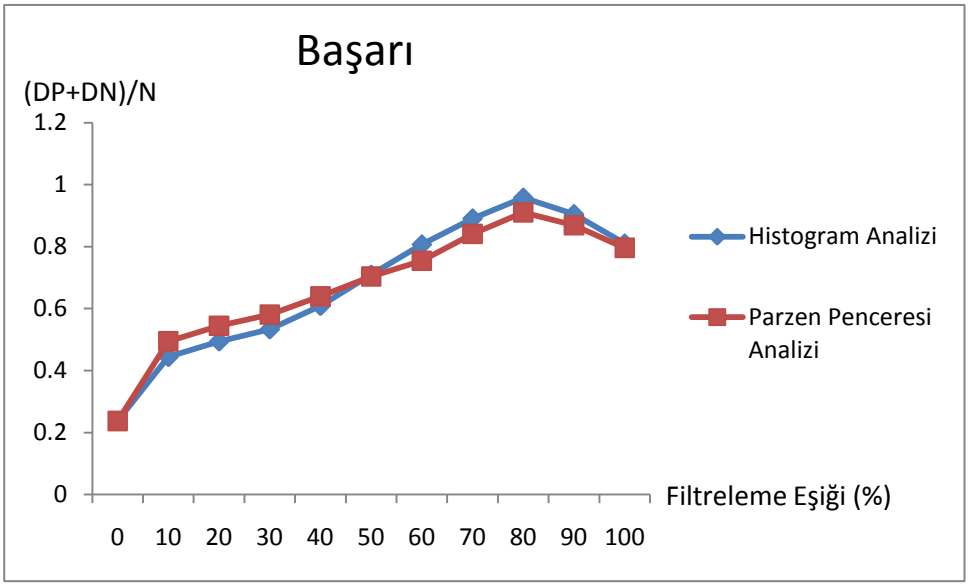
Şekil 5.12: Sınıflandırma Başarısı ($t_{ü}$=60 saniye)

Şekil 5.12'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.13: Sınıflandırma Başarısı ($t_{ü}$=300 saniye)

Şekil 5.13'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 300 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.14: Sınıflandırma Başarısı ($t_{ü}$=600 saniye)

Şekil 5.14'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 600 saniye olarak kabul edildiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

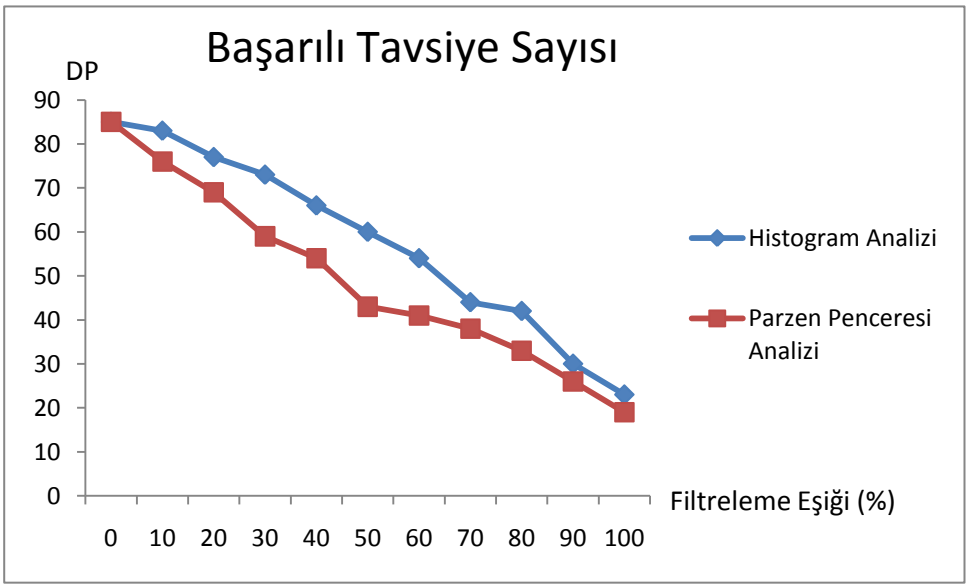
Şekil 5.12, Şekil 5.13 ve Şekil 5.14 karşılaştırılmalı şekilde incelendiğinde sınıflandırma başarısı konusunda her iki yöntemde benzer sonuçlar sergilemiştir. Her üç şekilde de minimum alarm filtreleme yüzdesi değeri(f_m) yükseldikçe tavsiye kesinliği önce hızlıca yükselip, sonra yavaşça düşmüştür. Bu üç şekil incelendiğinde aşağıdaki sonuç çıkarılabilmektedir:

- Önerilen her iki yöntemdede sınıflandırma başarısının f_m değerinin değişimine göre en yüksek olduğu değerler bulunmaktadır. Sınıflandırma başarısının en yüksek olduğu f_m değeri $t_ü$ değeri yükseldikçe yükselmektedir.

5.4 Örnek Alarm Sayısına Göre Deneysel Sonuçların Değişimi

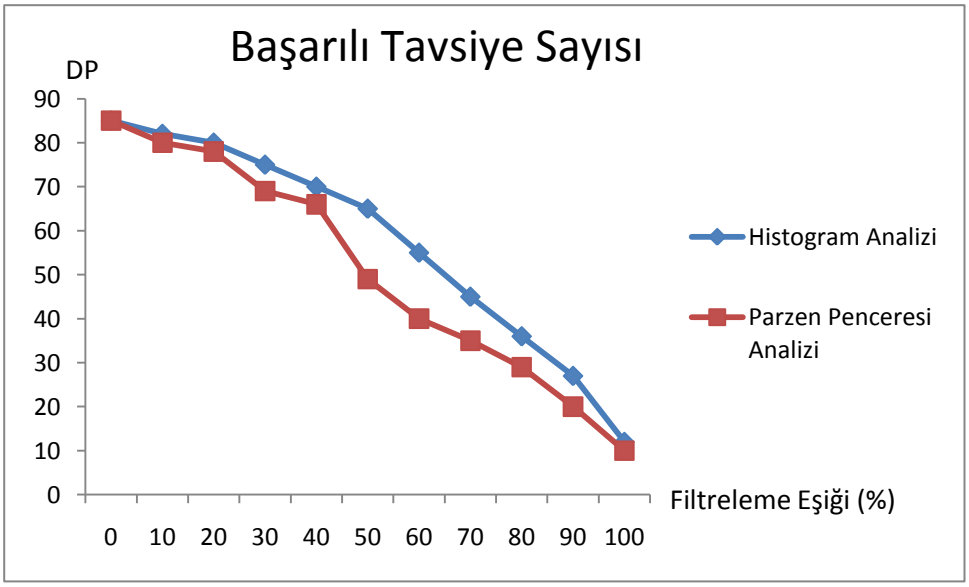
İstatistiksel makine öğrenmesi çalışmalarında karşılaşılan en önemli güçlüklerden birisi yeterli örnek verinin her zaman temin edilememesidir. Deneysel çalışmalarımızı yaptığımız geçici alarm tipi veri kümesinde yer alan alarm tipleri sık karşılaşılan alarm tipleri oldukları için böyle bir problem yaşanmamıştır. Geçici alarm tipi veri kümesinde bulunan her alarm tipi alarm veri kümesinde en az 2000 defa gözlemlenmiş alarmlardan oluşmaktadır. Önerilen yöntemlerin düşük alarm örneklerindeki başarısını ölçebilmek için alarm kümesinde karşılaşılan ilk *S* sayısı kadar örnek incelenerek geçici alarm tipleri bulunmaya çalışılmıştır. *S* değeri olarak 10,100 ve 1000 değerleri kullanılmıştır. Bu bölümde başarılı tavsiye sayısı, tavsiye kesinliği ve sınıflandırma başarısının alarm tarihçesinde incelenen alarm örneği sayısı *S*'e göre değişimleri gösterilmiştir.

5.4.1 Başarılı Tavsiye Sayılarının Örnek Alarm Sayısına Göre Değişimi



Şekil 5.15: Başarılı Tavsiye Sayısı ($t_{ü}$=60 saniye, S=10 alarm)

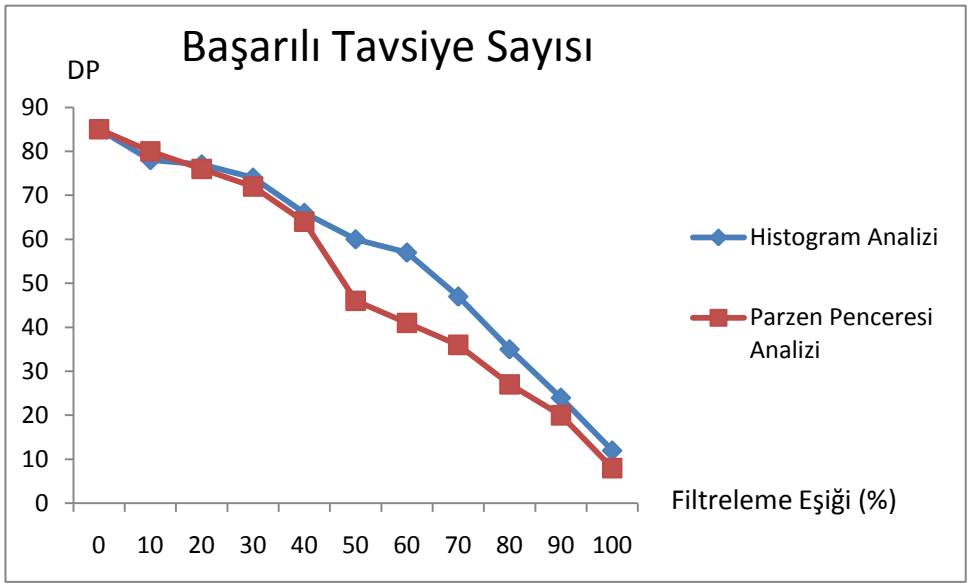
Şekil 5.15'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 10 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.16: Başarılı Tavsiye Sayısı ($t_{ü}$=60 saniye, S=100 alarm)

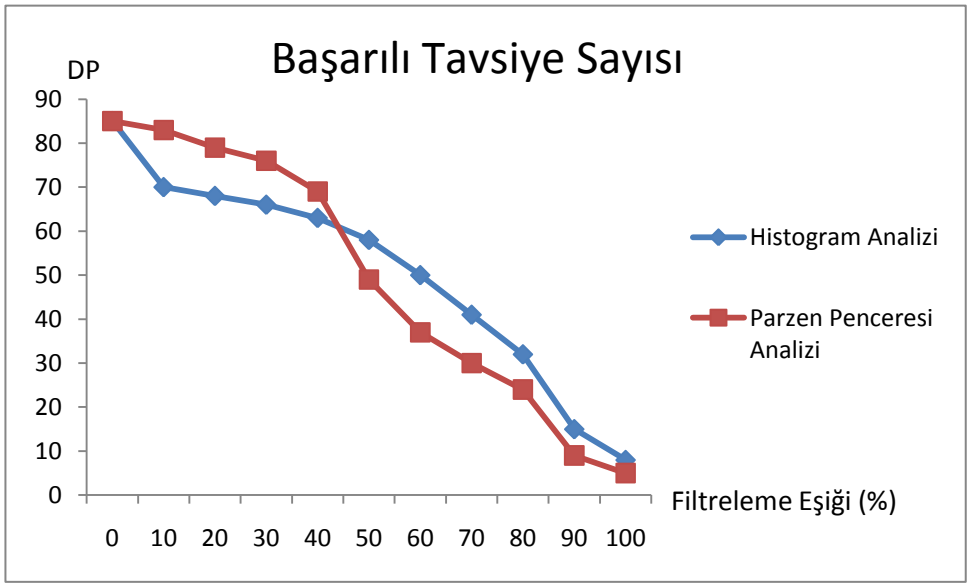
Şekil 5.16'da maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 100 alarm incelendiğinde Histogram Analizi ve

Parzen Pencereresi Analizi yöntemleri ile başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.17: Başarılı Tavsiye Sayısı ($t_{ü}$=60 saniye, S=1000 alarm)

Şekil 5.17'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 1000 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



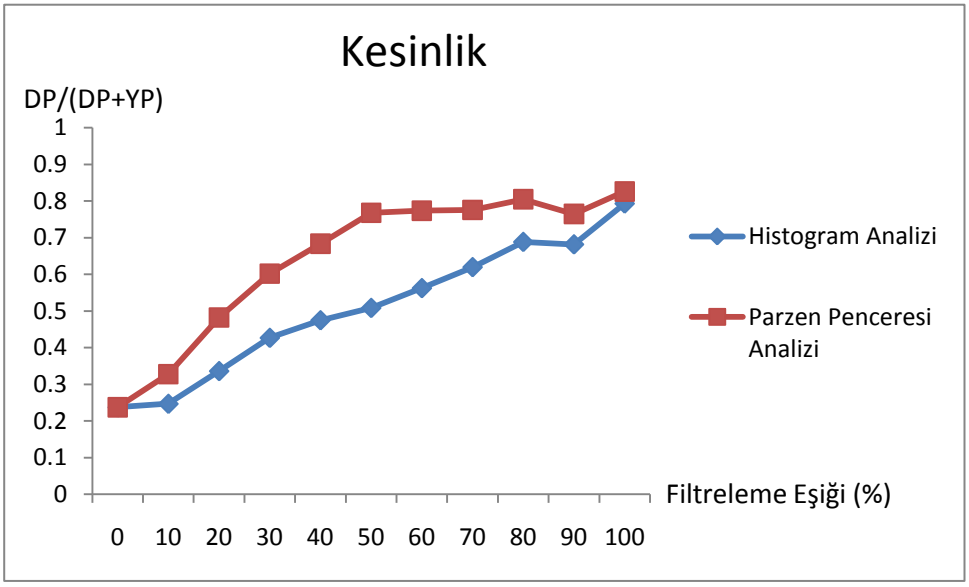
Şekil 5.18: Başarılı Tavsiye Sayısı ($t_{ü}$=60 saniye, S=Tüm veri kümesi)

Şekil 5.18'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki bütün alarmlar incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile başarılı geçici alarm tipi tavsiye sayılarının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

Şekil 15, Şekil 16, Şekil 17 ve Şekil 18 beraber incelendiğinde aşağıdaki sonuç çıkarılabilmektedir:

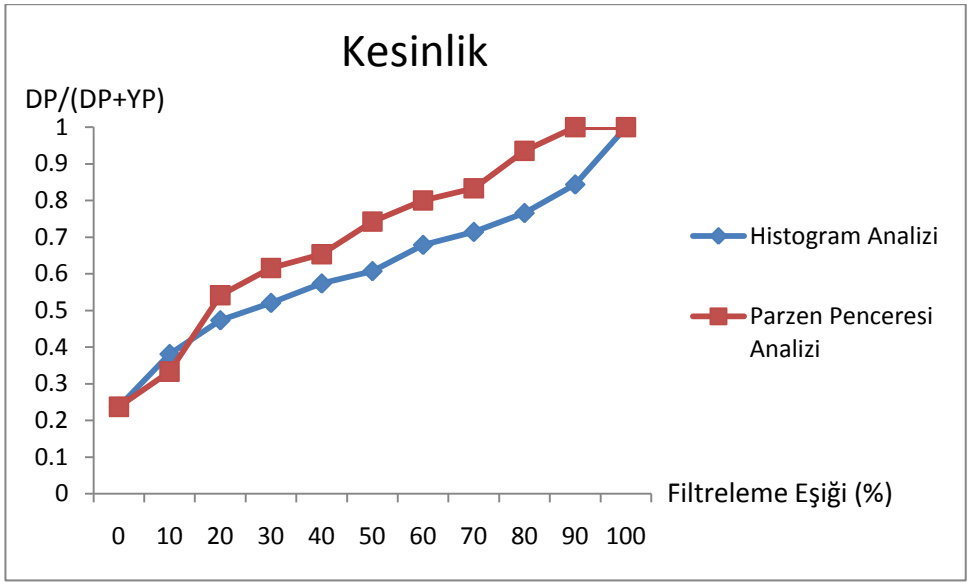
- Başarılı tavsiye sayısı örnek alarm sayısı *S*'in değişiminden önemli ölçüde etkilenmemektedir.

5.4.2 Tavsiye Kesinliğinin Örnek Alarm Sayısına Göre Değişimi



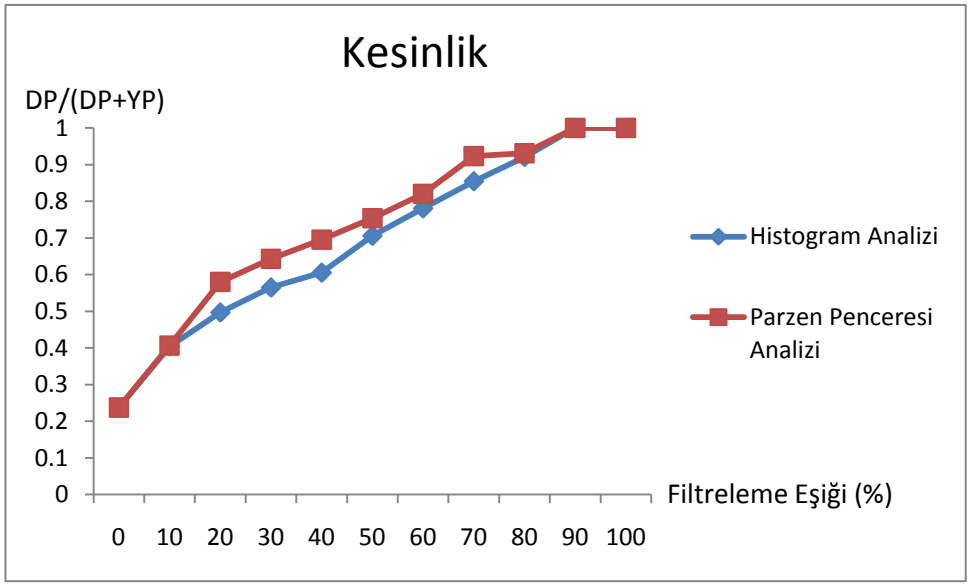
Şekil 5.19: Tavsiye Kesinliği ($t_{ü}$=60 saniye, *S*=10 alarm)

Şekil 5.19'da maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 10 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



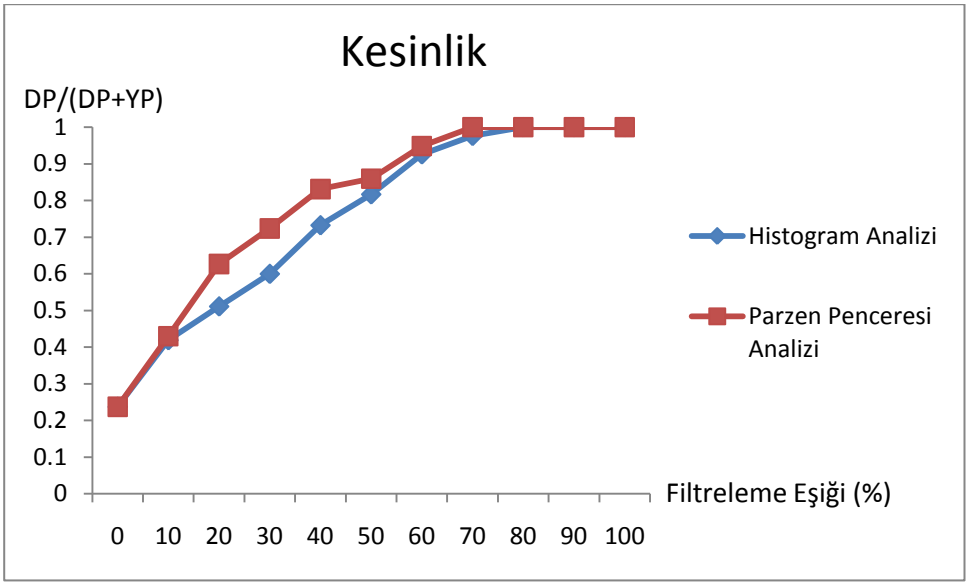
Şekil 5.20: Tavsiye Kesinliği ($t_{ü}$=60 saniye, S=100 alarm)

Şekil 5.20'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 100 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.21: Tavsiye Kesinliği ($t_{ü}$=60 saniye, S=1000 alarm)

Şekil 5.21'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 1000 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.22: Tavsiye Kesinliği ($t_{ü}$=60 saniye, S=Tüm veri kümesi)

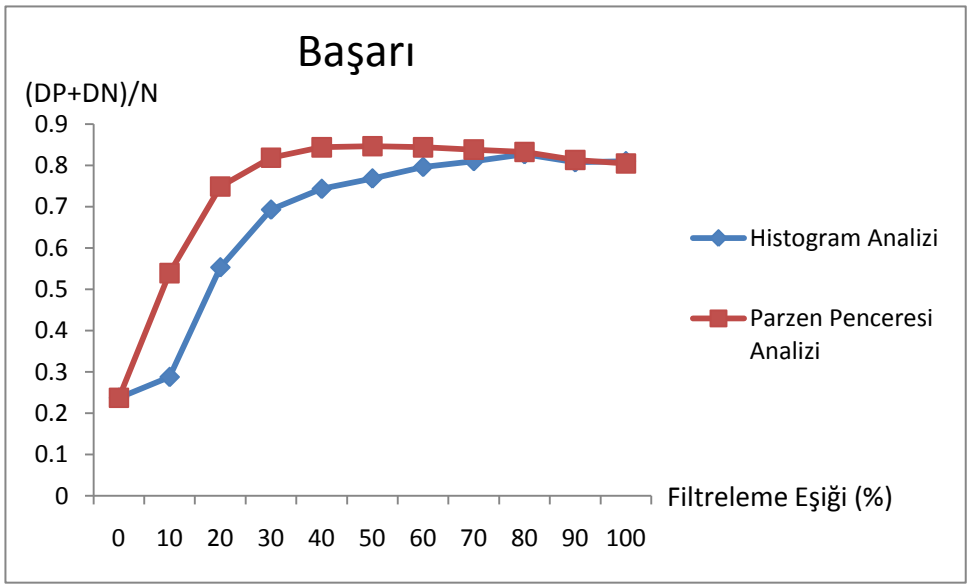
Şekil 5.22'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki bütün alarm örnekleri incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile tavsiye kesinliğinin minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

Şekil 19, Şekil 20, Şekil 21 ve Şekil 22 beraber incelendiğinde aşağıdaki iki sonuç çıkarılabilmektedir:

- Eğer incelenen örnek alarm sayısı S düşük değerlerdeyse, yetersiz örnek veri nedeniyle tavsiye kesinlikleri düşük değerlerdedir. İncelenen örnek alarm sayısı arttıkça tavsiye kesinliği yükselmektedir.

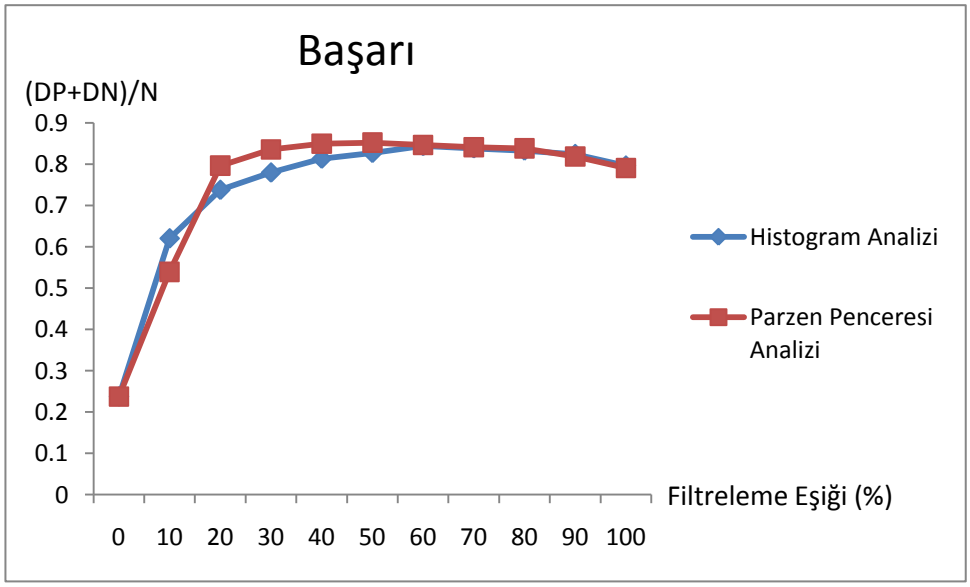
- Parzen Penceresi analizi yönteminin küçük S değerleri için tavsiye kesinliği Histogram Analizi yönteminin sonuçlarından çok daha başarılıdır.

5.4.3 Sınıflandırma Başarısının Örnek Alarm Sayısına Göre Değişimi



Şekil 5.23: Sınıflandırma Başarısı ($t_{ü}$=60 saniye, S=10 alarm)

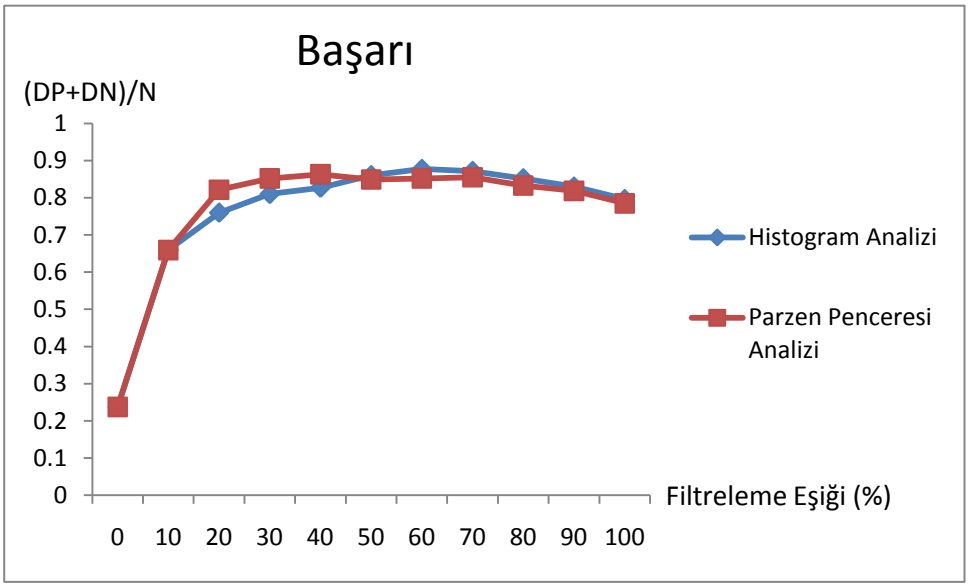
Şekil 5.23'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 10 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarısının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.24: Sınıflandırma Başarısı ($t_{ü}$=60 saniye, S=100 alarm)

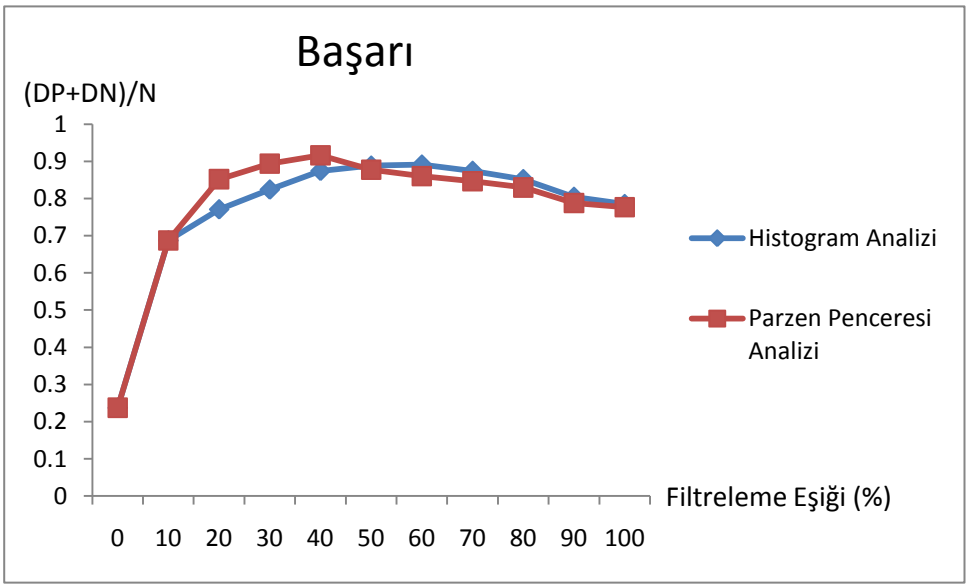
Şekil 5.24'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 100 alarm incelendiğinde Histogram Analizi ve

Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarısının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.25: Sınıflandırma Başarısı ($t_{ü}$=60 saniye, S=1000 alarm)

Şekil 5.25'de maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki ilk 1000 alarm incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarısının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.



Şekil 5.26: Sınıflandırma Başarısı ($t_{ü}$=60 saniye, S=Tüm veri kümesi)

Şekil 5.26'da maksimum alarm bekletme süresi eşiği($t_{ü}$) değeri 60 saniye olarak kabul edilip, alarm tarihçesindeki bütün alarm örnekleri incelendiğinde Histogram Analizi ve Parzen Pencereresi Analizi yöntemleri ile sınıflandırma başarısının minimum alarm filtreleme yüzdesi eşik(f_m) değerine göre değişimi verilmiştir.

Şekil 23, Şekil 24, Şekil 25 ve Şekil 26 beraber incelendiğinde aşağıdaki iki sonuç çıkarılabilmektedir:

- Eğer incelenen örnek alarm sayısı *S* düşük değerlerdeyse, yetersiz örnek veri nedeniyle sınıflandırma başarısı düşük değerlerdedir. İncelenen örnek alarm sayısı arttıkça sınıflandırma başarısı yükselmektedir.

- Parzen Penceresi analizi yönteminin küçük *S* değerleri için sınıflandırma başarısı Histogram Analizi yönteminin sonuçlarından çok daha başarılıdır.

5.5 SONUÇ

Deneysel çalışmalarımızın sonuçlarını gösteren şekiller alarm veri kümesi üzerinde farklı f_m, $t_{ü}$ ve *S* değerleri için yapılmış 60 farklı deneyin sonuçlarını içermektedir. Yapılan deneysel çalışmalarımızın sonuçları GSM şebekelerinde gözlemlenen geçici alarm tiplerinin belirlenmesinde alarm yaşam sürelerinin dağılımdan bağımsız olasılık kestirimi yöntemlerinin kullanılabileceğini göstermiştir. Alarm tiplerinin yaşam sürelerinin birikimli istatistiksel yoğunluk fonksiyonları incelenerek geçici alarm tipleri başarıyla tahmin edilip önerilecek filtre için uygun bekletme süresi tavsiye edilebilmektedir. Alarm yaşam sürelerinin birikimli yoğunluk fonksiyonlarının hesaplanması için önerilen Histogram Analizi ve Parzen Penceresi yöntemlerinin sonuçları birbirine yakın ve her ikisi de kullanışlıdır. İki yöntemi kıyasladığımızda her birisinin artıları ve eksileri bulunmaktadır. Yöntemlerin birbirlerine göre avantajları ve dezavantajları aşağıdaki dört temel konuda belirginleşmektedir:

- **Başarılı Tavsiye Sayısı:** Histogram Analizi yönteminde önerilen başarılı tavsiye sayısı istisna durumlar dışında hep daha yüksek gözlemlenmiştir. Yapılan 60 deneyden 56'sında Histogram Analizi yöntemi başarılı tavsiye sayısı konusunda Parzen Penceresi yönteminin önündedir. Sadece $t_{ü}$'nün 60 saniye olduğu deneylerde f_m'inde %50'den düşük olduğu 4 durumda Parzen Penceresi

yönteminin tavsiye ettiği başarılı tavsiye sayısı küçük bir farkla öne geçmiştir. Deneysel sonuçlara göre eğer sistemden öncelikli istenen başarılı tavsiye sayısının yüksekliği ise Histogram Analizi yönteminin kullanılması daha uygun olacaktır.

- **Tavsiye Kesinliği:** Parzen Penceresi yönteminde önerilen tavsiyelerin kesinliği daha yüksektir. Tavsiye kesinliği konusunda 60 deneyden sadece 5'inde Histogram Analizi yönteminin sonuçları daha başarılıdır. Deneysel sonuçlara göre eğer sistemden öncelikli istenen kesinliği yüksek tavsiyeler ise Parzen Penceresi yönteminin kullanılması daha uygun olacaktır.

- **Yetersiz Alarm Örneği Sayısı:** Yapılan deneylerden 20 tanesi düşük alarm sayısı içeren alarm veri kümeleri ile yapılmıştır. Bu deneylerin yarısı S=10 alarm, diğer yarısı da S=100 alarm olmak üzere gerçekleştirilmiştir. Yetersiz sayıda alarm örneği olduğu durumlarda Parzen Penceresi yönteminin tavsiye kesinliği ve sınıflandırma başarısı öne çıkmıştır. Yapılan 20 deneyden sadece 1 tanesinde Histogram Analizi yönteminin tavsiye kesinliği ve sınıflandırma başarısı daha iyiydi. Deneysel sonuçlara göre eğer incelenen alarm tipi için alarm örnek sayısı düşük ise Parzen Penceresi yönteminin kullanılması daha uygun olacaktır.

- **Harcanan Zaman, İşlemci ve Bellek Kapasiteleri:** Yapılan deneysel çalışmalarda kullanılan işlemci, bellek kapasiteleri ve harcanan zaman ölçümlenmemiştir. Ama genel olarak Histogram Analizi yönteminin gerektirdiği zaman, işlemci ve bellek kapasitelerinin daha düşük olduğu gözlemlenmiştir. Eğer sistemden öncelikli istenen daha hızlı hesaplama ve sunucunun kaynaklarının daha tutumlu kullanılması ise Histogram Analizi yönteminin kullanılması daha uygundur.

Sonuç olarak geçici alarm filtrelerinin istatistiksel öğrenme ile otomatik olarak üretilmesi konusunda önerilen her iki yöntemde başarılı sonuçlar vermesine karşın sistemden istenilen öncelikli beklentilere göre kullanılması uygun olan yöntem değişebilmektedir.

6. SEPET ANALİZİ İLE ALARM İLİNTİLENDİRME KURALLARININ OTOMATİK ÜRETİMİ

GSM şebekelerinde aynı kök neden sebebiyle birden fazla ilişkili alarm oluşabilmektedir. Alarm sayısının yükselmesi, alarmları inceleyen uzmanların çalışma süresini arttırmakta ve bazen önemli problemlerin alarmlarının daha geç fark edilmesine neden olmaktadır. Bu nedenle uzmanlar, alarm tarihçesini inceleyerek ilişkili alarm tiplerini belirleyerek alarm ilintilendirme filtreleri oluşturmaktadırlar. Alarm tarihçesinde milyonlarca alarm bulunabildiği için ilişkili alarm tiplerini belirlemek GSM şebeke uzmanlarının çok zamanını almaktadır ve birçok ilişkili alarm tipi gözden kaçabilmektedir. Çalışmamız kapsamında alarm ilintilendirme filtrelerinde kullanılacak ilişkili alarm tiplerinin otomatik olarak belirlenmesi için pazar sepet analizi tekniklerinin kullanılması önerilmiştir.

Pazar sepet analizi, aktivitelerin beraber gözlemlenme ilişkilerini keşfeden bir veri analizi ve madenciliği tekniğidir [41,42]. Pazar sepet analizi tekniği, satış yapılan mağazalarda müşterilerin sınıflandırmasında [43], satışları arttırmak için hangi ürünlerin beraber raflara yerleştirilmesine karar verilmesinde [44], ve özellikle internet alışverişlerinde satın alınacak ürünlerin yanında ilişkili başka ürünlerin tavsiyesinde [42] aktif olarak kullanılan bir tekniktir. Müşteri bağlılığı programlarının hazırlanması, promosyon kampanyalarının içeriğinin belirlenmesi ve indirim planlarına karar verilmesi gibi konularda faydalı bilgilerde vermektedir [Wikipedia2011]. Pazar sepet analizi tekniğinin satış ve pazarlama alanları dışında da birçok farklı kullanım alanı bulunmaktadır. Kütüphanelerdeki kitap ve dokümanların tasnifinden [45], genetik alanında gen dizilerinin ilişkilerinin saptanmasına [46] kadar farklı alanlarda kullanılabilmektedir.

Çalışmamız kapsamında kayan zaman penceresi yöntemi ile hesaplanan alarm tiplerinin beraber gözlemlenme frekansları kullanılarak alarm tipleri arasındaki ilişkiler pazar sepet analizinde kullanılan benzerlik ölçütleri ile bulunmaya çalışılmıştır. Alarm ilintilendirme kurallarının çıkarımında kullandığımız sepet analizi benzerlik ölçütleri şunlardır:

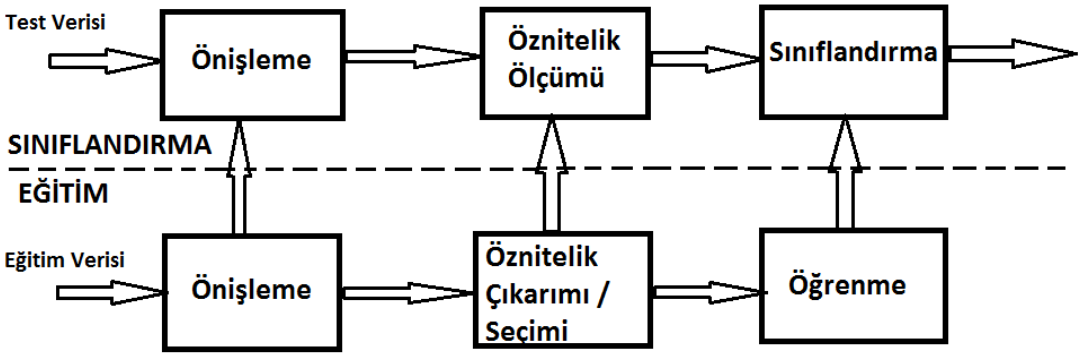
- *Etki* benzerliği [41,44,47].
- *Maksimum Güven* benzerliği [43,48].

- *Minimum Güven* benzerliği [49].
- *Tutarlılık* benzerliği [48,50].
- *Cosine* benzerliği [50].
- *Kulczynski* benzerliği [51,52].

İncelenen benzerlik ölçütleri ile hesaplanan benzerlik öznitelikleri S biçimli sınıflandırma tekniği [39] kullanılarak ilintili ve ilintisiz alarm tiplerinin sınıflandırılması yapılmıştır.

6.1 Algoritma Özeti

Çalışmamız kapsamında önerilen ilintili ve ilintisiz alarm tiplerinin sınıflandırılması istatistiksel örüntü tanıma uygulamalarına iyi bir örnektir. Şekil 6.1'de istatistiksel örüntü tanıma sürecinin genel bir modeli verilmektedir [53]:



Şekil 6.1: Alarm İlintilendirme Kurallarının Öğrenme Süreci

Önerilen algoritma eğitim ve sınıflandırma olarak iki bölüme ayrılmaktadır:

Eğitim bölümü üç aşamadan oluşmaktadır. İlk aşama olan ön işleme aşamasında veri kümesindeki ham veriler sadeleştirilip gerekli olmayan kısımlar alarmlar verilerinden çıkarılmaktadır. Alarmlar bölüm 6.2'de açıklanan alarm modeline göre sadeleştirilmektedir. Eğitim bölümünün ikinci aşaması olarak sadeleştirilmiş alarm bilgilerinden öznitelik çıkarımları yapılmaktadır. Bu öznitelikler pazar sepet analizinde kullanılan incelediğimiz benzerliklerdir. Eğitimin son aşaması olarak üretilen öznitelikler ile ilintili alarm tiplerine karar verilmesini sağlayacak

sınıflandırma modeli üretilir. Sınıflandırma modelinin üretilmesinde S biçimli sınıflandırma yöntemi kullanılmıştır [39].

Sınıflandırma bölümü eğitim bölümü gibi üç aşamadan oluşmaktadır. İlk aşama olan önişleme aşamasında veri kümesindeki ham veriler sadeleştirilir. İkinci aşamada öznitelik ölçümleri yapılır. Öznitelik olarak incelenen altı benzerlik ölçütü hesaplanır. Sınıflandırmanın son aşamasında ilintili ve ilintisiz alarm tipi ikilileri sınıflandırılır. Sınıflandırma işleminde hesaplanan öznitelikler eğitim bölümünün son aşamasında üretilmiş olan sınıflandırma modeline göre incelenerek ilintili ve ilintisiz alarm tiplerine karar verilir.

6.2 Alarm Modeli

Alarmların içerisinde üretilme nedenleri ve ilgili oldukları problemler hakkında çok değişik bilgiler bulunabilmektedir. Alarm ilintilendirmesi söz konusu olduğunda alarmların üç temel bilgisi ön plana çıkmaktadır. Sistem için alarmlar özetle aşağıdaki gibi modellenebilir:

$$a = (e, s, t) \quad \textbf{(6.1)}$$

- ***a:*** Alarmı simgelemektedir.
- ***e:*** Alarmın tip bilgisidir.
- ***s:*** Alarmın oluştuğu kaynağın bilgisidir.
- ***t:*** Alarmın yaratılma zaman bilgisidir.

Alarmları üç değişken ile modelledikten sonra ilintilendirme kurallarının keşfedilmesi için kullanılacak alarm tarihçesi aşağıdaki gibi üç değişkenli üyeler içeren bir küme olarak modellenebilmektedir:

$$A = \{a_i\}_{i=1}^{N} \quad \textbf{(6.2)}$$

6.3 Gözlem Frekansı Ölçümleri

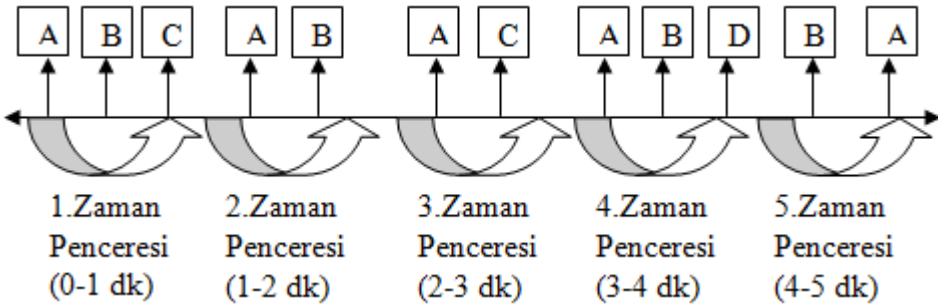
Gözlem frekansı bir alarm tipi grubu ve o alarm tipi grubunun alarm tarihçesinde beraber gözlemlenme sayısını içeren bir ölçümdür. Gözlem frekansı ölçümleri benzerlik özniteliklerinin hesaplanmasında kullanılmaktadır. Gözlem frekansı ölçümü aşağıdaki gibi modellenebilmektedir:

$$f(E) = \#_E \quad \textbf{(6.3)}$$

- ***f(E):*** E alarm tipi grubunun gözlem frekansı ölçümünü simgelemektedir.
- ***E:*** Özniteliğe konu olan, aynı kaynaktan eş zamanlı olarak gözlemlenen alarm tipi kümesidir (e_i ε E).
- ***$\#_E$:*** İncelenen veri kümesinde ölçüme konu olan alarm tipi grubunun eş zamanlı olarak gözlenme frekansıdır.

6.3.1 Kayan Zaman Penceresi Yöntemi

Pazar sepet analizi yaklaşımı ile alarm tipleri arasındaki ilişkilendirme kurallarının üretimi söz konusu olduğunda incelenen alarm veri kümesindeki alarmların oluşma zamanları önem kazanmaktadır. Gözlem frekansı ölçümleri alarm tiplerinin aynı kaynaktan eş zamanlı gözlemlenme miktarları sayılarak hesaplanmaktadır. Ama aynı kök nedenden alarmlar oluşurken alarmların oluşma zamanları arasında onlarca saniye fark olabilmektedir. Alarmlar genelde problemlerin semptomları ile oluşmaktadır ve semptomların gözlemlenme zamanları arasında fark olabilmektedir. Bu nedenle eş zamanlı alarmları, aynı kaynaktan aynı saniye içinde oluşan alarmlar diye tanımlamak yerine aynı kaynaktan belirli bir zaman aralığı içinde oluşan alarmlar olarak tanımlamaktayız. İncelen zaman aralığı zaman penceresi olarak adlandırılmaktadır. Kayan zaman penceresi yönteminde, incelen alarm veri kümesinde yaratılma zamanı en eski olan alarmın yaratılma zamanı t_0 anı olarak kabul edilir. Aynı kaynakta oluşan alarmların eş zamanlı olarak kabul edilmesi için uygun bir zaman aralığına karar verilir. Karar verilen bu aralık *h* ile gösterilir ve zaman penceresinin genişlik bilgisidir. Alarm tarihçesinin başlangıcından itibaren *m* tamsayı değerleri için sırayla $[t_0+mh, t_0+(m+1)h]$ zaman aralıkları yani pencereleri incelenmeye başlanır. İncelenen zaman penceresinde aynı kaynakta oluşan alarm tipleri sayılarak gözlem frekansı ölçümleri üretilmektedir.



Şekil 6.2: Alarmların Kayan Zaman Penceresi İle İncelenmesi

Şekil 6.2 kayan pencere yöntemini açıklamak için verilmiştir. Temsili şekilde, bir *K* kaynağının beş dakika içinde ürettiği alarmlar zaman ekseni üzerinde gösterilmektedir. İncelenen zaman aralığı içinde *K* kayanğında dört tipte alarm oluşmuştur (*A*,*B*,*C*,*D*). Zaman penceresi genişliği *h* bir dakika olarak kabul edilip gözlemlenen alarm veri kümesi birer dakikalık ardışıl beş alt kümeye ayrılmıştır. Ardışıl beş zaman penceresi incelendikten sonra gözlem ölçümleri aşağıdaki gibi hesaplanmaktadır:

- $\#_A$= 5 (*A* alarm tipi beş zaman penceresinde gözlemlenmiştir)
- $\#_B$= 4 (*B* alarm tipi dört zaman penceresinde gözlemlenmiştir)
- $\#_C$= 2 (*C* alarm tipi iki zaman penceresinde gözlemlenmiştir)
- $\#_D$= 1 (*D* alarm tipi bir zaman penceresinde gözlemlenmiştir)
- $\#_{A,B}$= 4 (*A* ve *B* alarm tipleri dört zaman penceresinde beraber gözlemlenmiştir)
- $\#_{A,C}$= 2 (*A* ve *C* alarm tipleri iki zaman penceresinde beraber gözlemlenmiştir)
- $\#_{A,D}$= 1 (*A* ve *D* alarm tipleri bir zaman penceresinde beraber gözlemlenmiştir)
- $\#_{B,C}$= 1 (*B* ve *C* alarm tipleri bir zaman penceresinde beraber gözlemlenmiştir)
- $\#_{B,D}$= 1 (*B* ve *D* alarm tipleri bir zaman penceresinde beraber gözlemlenmiştir)
- $\#_{C,D}$= 0 (*C* ve *D* alarm tipleri her hangi bir zaman penceresinde beraber gözlemlenmemiştir)
- *G*= 5 (Alarm tarihçesinde kayan pencere yöntemi ile yapılan toplam gözlem sayısıdır)

Bu yaklaşım ile incelemeye kayan zaman penceresi yöntemi olarak adlandırılmasının nedeni incelen zaman aralıklarının ardışıl olması ve zaman ekseni üzerinde kayarak yeni zaman pencerelerinin incelenmesidir. Kayan zaman penceresi yönteminde istenirse sınırları belirli oranlarda örtüşen zaman pencereleri kullanılabilir. Ama çalışmamızda bitişik zaman pencereleri kullanılmıştır.

6.4 Benzerlik Öznitelikleri

Pazar sepet analizi tekniği ilişkilendirme kurallarının üretimini sağlayan bir tekniktir. İlişkilendirme kuralı, X → Y biçiminde bir gerektirmedir. Burada X öncel ve Y ardıl olarak anılmaktadır. Sepet analizi ile ilişkilendirme kurallarının öğrenilmesinde yoğun olarak kullanılan iki ölçüt bulunmaktadır [40]:

- X → Y ilişkilendirme kuralının *destek* değeri:

$$Destek(X,Y) \equiv P(X,Y) = \frac{\#\{X\ ve\ Y\ almış\ müşteriler\}}{\#\{müşteriler\}} \quad \textbf{(6.4)}$$

Kayan zaman penceresi yöntemi ile elde edilen gözlem frekansı öznitelikleri kullanılarak alarm tipleri arasındaki *Destek* Formül 6.5 ile hesaplanmaktadır:

$$Destek(X,Y) \equiv P(X,Y) = \frac{\#_{X,Y}}{G} \quad \textbf{(6.5)}$$

- $\#_{X,Y}$**:** X ve Y alarm tiplerinin beraber gözlem frekansıdır.
- ***G:*** İncelen toplam zaman penceresi sayısıdır.

- X → Y ilişkilendirme kuralının *güven* değeri:

$$Güven(X \rightarrow Y) \equiv P(Y|X) = \frac{P(X,Y)}{P(X)} = \frac{\#\{X\ ve\ Y\ almış\ müşteriler\}}{\#\{X\ almış\ müşteriler\}} \quad \textbf{(6.6)}$$

Kayan zaman penceresi yöntemi ile elde edilen gözlem frekansı öznitelikleri kullanılarak alarm tipleri arasındaki *Güven* Formül 6.7 ile hesaplanmaktadır:

$$Güven(X \rightarrow Y) \equiv P(Y|X) = \frac{\#_{X,Y}}{\#_X} \quad \textbf{(6.7)}$$

- $\#_{X,Y}$**:** X ve Y alarm tiplerinin beraber gözlem frekansıdır.
- $\#_X$**:** X alarm tipinin gözlem frekansıdır.

Bu iki ölçüt kullanılarak daha karmaşık başka ilişkilendirme ölçütleri üretilebilmektedir. Çalışmamızda sepet analizi literatüründe daha önceden kullanılmış altı temel benzerlik ölçütü kullanılmıştır:

6.4.1 Etki Benzerliği:

Etki benzerliği iki alarm tipinin beraber desteklerinin ayrı ayrı destekleri çarpımına oranıdır. Formül 6.8 ile hesaplanmaktadır:

$$Lift(X,Y) \equiv \frac{Destek(X,Y)}{Destek(X)Destek(Y)} \quad \textbf{(6.8)}$$

Etki benzerliği formülü formül 6.9'daki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$Lift(X,Y) \equiv \frac{{}^{\#_{X,Y}}/_{G}}{{}^{\#_X}/_{G}\ {}^{\#_Y}/_{G}} = \frac{\#_{X,Y}\ G}{\#_X\ \#_Y} \quad \textbf{(6.9)}$$

Etki benzerliği [0,∞] aralığında bir değer alabilmektedir. Özellikle frekansı çok yüksek alarm tiplerinin frekansı çok düşük alarm tipleri arasındaki ilintinin hesaplanmasında başarılı bir benzerliktir.

6.4.2 Maksimum Güven Benzerliği:

Maksimum güven benzerliği iki alarm tipinin ortak desteğinin alarm tiplerinden desteği küçük olana oranıdır. Formül 6.10 ile hesaplanmaktadır:

$$MaxConf(X,Y) = max\ \{Güven(X \rightarrow Y), Güven(Y \rightarrow X)\} \quad \textbf{(6.10)}$$

Maksimum güven benzerliği formülü formül 6.11'deki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$MaxConf(X,Y) = max\ \{\frac{\#_{X,Y}}{\#_X}, \frac{\#_{X,Y}}{\#_Y}\} \quad \textbf{(6.11)}$$

Maksimum güven benzerliği [0,1] aralığında bir değer alabilmektedir. Alarm tipleri arasında tek yönlü ilintilerin belirlenmesinde başarılı bir benzerliktir.

6.4.3 Minimum Güven Benzerliği:

Minimum güven benzerliği iki alarm tipinin ortak desteğinin alarm tiplerinden desteği büyük olana oranıdır. Formül 6.12 ile hesaplanmaktadır:

$$AllConf(X,Y) = min\ \{Güven(X \rightarrow Y), Güven(Y \rightarrow X)\} \quad \textbf{(6.12)}$$

Minimum güven benzerliği formülü formül 6.13'deki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$AllConf(X,Y) = min\{\frac{\#_{X,Y}}{\#_X}, \frac{\#_{X,Y}}{\#_Y}\} \quad \textbf{(6.13)}$$

Minimum güven benzerliği [0,1] aralığında bir değer alabilmektedir. Alarm tipleri arasında çift yönlü ilintilerin belirlenmesinde başarılı bir benzerliktir.

6.4.4 Tutarlılık Benzerliği:

Tutarlılık benzerliği formül 6.14 ile hesaplanmaktadır:

$$Coherence(X,Y) = \frac{Destek(X,Y)}{Destek(X)+Destek(Y)-Destek\,(X,Y)} \quad \textbf{(6.14)}$$

Tutarlılık benzerliği formülü formül 6.15'deki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$Coherence(X,Y) = \frac{\#_{X,Y}/_G}{\#_X/_G + \#_Y/_G - \#_{X,Y}/_G} = \frac{\#_{X,Y}}{\#_X+\#_Y-\#_{X,Y}} \quad \textbf{(6.15)}$$

Tutarlılık benzerliği [0,1] aralığında bir değer alabilmektedir. Alarm tipleri arasındaki çift yönlü ilintilerin belirlenmesinde başarılı bir benzerliktir.

6.4.5 Cosine Benzerliği:

Cosine benzerliği formül 6.16 ile hesaplanmaktadır:

$$Cosine(X,Y) = \frac{Destek(X,Y)}{\sqrt{Destek(X)Destek(Y)}} \quad \textbf{(6.16)}$$

Cosine benzerliği formülü formül 6.17'deki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$Cosine(X,Y) = \frac{\#_{X,Y}/_G}{\sqrt{\#_X/_G \#_Y/_G}} = \frac{\#_{X,Y}}{\sqrt{\#_X\#_Y}} \quad \textbf{(6.17)}$$

Cosine benzerliği [0,1] aralığında bir değer alabilmektedir.

6.4.6 Kulczynski Benzerliği:

Kulczynski benzerliği formül 6.18 ile hesaplanmaktadır:

$$Kulc(X,Y) = \frac{Destek(X,Y)}{2}\left(\frac{1}{Destek(X)} + \frac{1}{Destek(Y)}\right) \quad \textbf{(6.18)}$$

Kulczynski benzerliği formülü formül 6.19'daki gibi sadeleştirilerek gözlem frekansı öznitelikleri ile hesaplanacak hale getirilebilmektedir:

$$Kulc(X,Y) = \frac{\#_{X,Y}/_G}{2}\left(\frac{1}{\#_X/_G} + \frac{1}{\#_Y/_G}\right) = \frac{\#_{X,Y}}{2}\left(\frac{1}{\#_X} + \frac{1}{\#_Y}\right) \quad \textbf{(6.19)}$$

Kulczynski benzerliği [0,1] aralığında bir değer alabilmektedir.

6.5 Alarm İlintilendirme Kurallarının Üretimi

GSM şebekelerinde alarm ilintilendirme filtreleri uzman sistemler üzerinde oluşturulan uzman kurallar ile yaratılmaktadır. Bir alarm ilintileme uzman kuralı özetle belirli bir zaman aralığı içinde aynı kaynaktan ilintili olduğunu bilinen alarm tiplerinden gelen birden fazla alarmı tek bir alarma indirgeyerek alarm sayısını azaltmaya yardımcı olur. Çalışmamız kapsamında ilintili alarm tiplerinin saptanması hedeflenmektedir. İlintili alarm tiplerinin belirlenmesi için incelenen benzerlik ölçütleri tek başlarına kulllanılabildikleri gibi beraber de kullanılabilmektedirler. Çalışmamız kapsamında incelenen altı benzerlik ölçütün tek başlarına ilintili alarm tiplerini belirleme performansları karşılaştırılmış ve S biçimli sınıflandırma ile beraber kullanıldıklarındaki başarı performansları incelenmiştir.

6.5.1 Bir Çeşit Benzerlik İle İlinti Kurallarının Öğrenilmesi

Alarm tipi ikilileri için hesaplanmış altı benzerlikten herhangi birisi ile ilinti alarm tiplerinin belirlenmesi Formül 6.20 ile sağlanmaktadır:

$$C(X,Y,b,t_b) = \begin{Bmatrix} 1, t_b \le b \\ 0, t_b > b \end{Bmatrix} \quad \textbf{(6.20)}$$

- C: İliniti ilişkisi belirleme fonksiyonudur. Sonucu 1 ise alarm tipleri ilintili, 0 ise ilintisizdir.

- *X,Y:* İlintili olup olmadıkları belirlenmek isteyen alarm tipleridir.

- *b: X* ve *Y* alarm tipleri için çalışmamızda önerilen altı benzerlik özniteliğinden herhangi birisidir.

- t_b*:* Benzerlik eşiğidir. Eğer *X* ve *Y* alarm tipleri için b benzerlik değeri t_b'nin üzerinde ise alarm tiplerinin ilintili olduğuna karar verilir.

Benzerlik öznitelikleri ile ilintili alarm tiplerinin öğrenilmesi mümkün olmakla beraber bu yaklaşımın önemli bir eksiği bulunmaktadır. Formül 6.20'de yer alan ve incelenen alarm ikilisinin ilintili veya ilintisiz olduğunun kestiriminin yapılmasını sağlayan t_b benzerlik eşiği değeri formüle girdi olarak verilmektedir. Özetle bir çeşit benzerlik ile ilintili alarm tiplerinin öğrenilmesinde eğitim ve test süreçleri bulunmamaktadır. Girdi olarak verilen benzerlik eşiğine göre alarm tarihçesi incelenerek öğrenme işlemi yapılır.

6.5.2 S Biçimli Sınıflandırma İle İlinti Kurallarının Öğrenilmesi

Alarm tipi ikililerinin alarm tarihçesi üzerinden hesaplanmış benzerlik özniteliklerinin herhangi bir benzerlik eşiğine ihtiyaç duyulmadan beraber kullanılabilmeleri için çalışmamız kapsamında S biçimli sınıflandırma yöntemi kullanılmıştır [39,54]. S biçimli sınıflandırmada $p(x|C_i)$ sınıf dağılımları yerine dağılımların oranları modellenmektedir. Formül 6.21'de iki sınıflı bir sınıflandırmanın doğrusal olduğu varsayılan log olabilirlik oranı verilmektedir:

$$log\frac{p(x|C_1)}{p(x|C_2)} = w^T x + w_0^o \quad \textbf{(6.21)}$$

Formül 6.22 ve 6.23'de Bayes kuralı ile sonsal olasılık formülleri verilmiştir:

$$logit(P(C_1|x)) = log\frac{P(C_1|x)}{1-P(C_1|x)} = log\frac{p(C_1|x)}{p(C_2|x)} + log\frac{P(C_1)}{P(C_2)} = w^T x + w_0 \quad \textbf{(6.22)}$$

$$w_0 = w_0^o + log\frac{P(C_1)}{P(C_2)} \quad \textbf{(6.23)}$$

Formüller incelenince $\boldsymbol{P(C_1|x)}$ sonsal olasılığının S biçimli bir sigmoid işlevi kullanılarak elde edildiği görülmektedir. Formül 6.24'de bu durum görünmektedir:

$$y = P(C_1|x) = \frac{1}{1+exp[-(w^T x + w_0)]} \quad \textbf{(6.24)}$$

İki sınıflı bir sınıflandırmada modelin eğitilmesi $\boldsymbol{w}$ ve $\boldsymbol{w_0}$ve parametrelerinin öğrenilmesidir. Elimizde iki sınıflı bir $\boldsymbol{X=\{x^t, r^t\}}$ örneklemi olsun ($x \in C_1$ ise $r^t=1$, $x \in C_2$ ise $r^t=0$). r^t rastlantısal değişkeninin Bernoulli ve olasılığının $\boldsymbol{y^t \equiv P(C_1|x^t)}$ olduğunu varsayıyoruz. Bu varsayımlarla örneklemin olabilirliği Formül 6.25'te verilmektedir:

$$l(w, w_0|X) = \prod_t (y^t)^{(r^t)}(1-y^t)^{(1-r^t)} \quad \textbf{(6.25)}$$

Bu durum için tanımlanacak *çapraz düzensizlik hatası*($E=-logl$) Formül 6.26'da gösterilmektedir:

$$E(w, w_0|X) = -\sum_t r^t log y^t + (1-r^t) log(1-y^t) \quad \textbf{(6.26)}$$

Öğrenilmek istenen katsayılar çapraz düzensizlik hatasının türevi alınarak bulunabilmektedir:

$$\Delta w_j = -\eta \frac{\partial E}{\partial w_j} = \eta \sum_t \left(\frac{r^t}{y^t} - \frac{1-r^t}{1-y^t}\right) y^t(1-y^t)x_j^t = \eta \sum_t (r^t - y^t)x_j^t \quad (j=1,\ldots,d)$$

$$\Delta w_0 = -\eta \frac{\partial E}{\partial w_0} = \eta \sum_t (r^t - y^t) \quad \textbf{(6.27)}$$

Öğrenilmek istenen katsayılara düşük başlangıç değerleri verilip, aşağıdaki algoritma ile yakınsama elde edilene kadar döngüsel işlemler yapılarak öğrenme işlemi tamamlanır:

Tüm $j=0,\ldots,d$

$w_j \leftarrow$ rand(-0.01,0.01)

Yinele

Tüm $j=0,\ldots,d$

$\Delta w_j \leftarrow 0$

Tüm $t=1,\ldots,N$

$o \leftarrow 0$

Tüm $j=0,\ldots,d$

$o \leftarrow o + w_j \boldsymbol{x}_j^t$

$y \leftarrow S(o)$

Tüm $j=0,\ldots,d$

$\Delta w_j \leftarrow \Delta w_j + (r^t - y)\, \boldsymbol{x}_j^t$

Tüm $j=0,\ldots,d$

$w_j \leftarrow w_j + \eta \Delta w_j$

Yakınsamaya dek

Şekil 6.3: S biçimli sınıflandırma ile öğrenme

6.6 Deneysel Sonuçlar

Çalışmamız kapsamında ilintili alarm tiplerinin belirlenmesi için önerdiğimiz benzerlik metrikleri ve S biçimli sınıflandırma yöntemi alarm veri kümesi üzerinden test edilmiştir. Kullanılan alarm veri kümesi 2010 yılında Turkcell GSM şebekesinde gözlemlenen alarmlardan oluşmaktadır. Bölüm 4.1'de kullanılan alarm veri kümesi hakkında ayrıntılı bilgiler bulunmaktadır. Elde edilen sonuçların başarısının ölçümü için Turkcell alarm gözlem uzmanları tarafından üretilmiş ilintili alarm tipi veri kümesi kullanılmıştır. İlintili alarm tipi veri kümesi en sık beraber gözlemlenmiş 320 alarm tipi ikilisini ve bu alarm tiplerinin ilintililik durumlarını içermektedir. Veri

kümesinde bulunan 320 alarm tipi ikilisinden 141 tanesi ilintili, 179 tanesi ilintisiz alarm tipi ikilisinden oluşmaktadır (bölüm 4.2.2).

S biçimli sınıflandırmanın deneysel testleri için eğitim ve test veri kümeleri alarm tarihçesi işlenerek üretilmiştir. 2010 yılı alarm veri kümesi birer aylık 12 alt veri kümesine bölünmüştür. Ocak-Kasım ayları arasındaki 11 aylık dönemde ilintili alarm tipi veri kümesindeki alarm tipi çiftlerinin aylık beraber gözlemlenme miktarı 100'den fazla olduğu 2551 durum için alarm tipi çiftlerinin 6 tane benzerlik ölçütü hesaplanarak bir eğitim veri kümesi hazırlanmıştır. Hazırlanan veri kümesinde her kayıt için ilgili alarm tipi çiftinin ilintililik bilgisi etiket olarak eklenmiştir. Aralık ayı için alarm tipi veri kümesinde bulunan 320 alarm tipi çiftinin 6 tane benzerlik ölçümü yapılarak test veri kümesi elde edilmiştir.

Başarım ölçümleme metriklerinin hesaplanmasında kullanılan temel bilgiler Çizelge 6.1'de verilmektedir:

Çizelge 6.1: İlintili Alarm Tipleri Belirlenmesinde Hata Dizeyi

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	DP	YN
İlintisiz Alarm Tipi Grubu	YP	DN

- DP: Başarılı şekilde tahmin edilmiş ilintili alarm tipi grubu sayısıdır. Doğru pozitif tahmin sayısıdır.

- YP: Gerçekte ilintisiz olan ama ilintili olarak tahmin edilmiş alarm tipi grubu sayısıdr. Yanlış pozitif tahmin sayısıdır.

- YN: Gerçekte ilintili olan ama ilintisiz olarak tahmin edilen alarm tipi grubu sayısıdır. Yanlış negatif tahmin sayısıdır.

- DN: Başarılı şekilde tahmin edilmiş ilintisiz alarm tipi grubu sayısıdır. Doğru negatif tahmin sayısıdır.

Önerilen yöntemlerin başarımının ölçümlendirilmesinde üç temel metrik kullanılmıştır. Kullanılan metrikler başarılı tavsiye sayısı, tavsiye kesinliği ve sınıflandırma başarısı metrikleridir.

Başarılı Tavsiye Sayısı: Başarılı şekilde tahmin edilmiş ilintili alarm tipi grubu sayısıdır. Çizelge 6.1'de belirtilen DP sayısına eşittir.

Tavsiye Kesinliği: Önerilen ilintili alarm tipi gruplarının doğruluk başarısının ölçümüdür. Formül 6.28 ile hesaplanmaktadır.

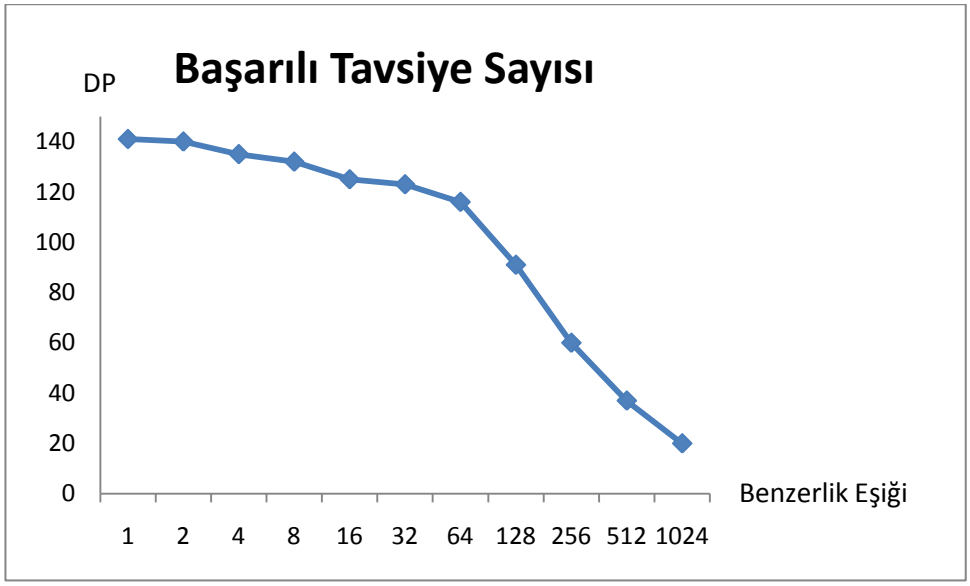
$$Kesinlik = \frac{DP}{DP+YP} \quad \textbf{(6.28)}$$

Sınıflandırma Başarısı: Önerilen ilintili ve ilintisiz alarm tipi gruplarının doğruluk başarısının ölçümüdür. Bu ölçümleme metriğinde önerilen ilintili alarm tipi grubu kesinliği dışında önerilen ilintisiz alarm tipi grubu kesinliği de dikkate alınmaktadır. Formül 6.29 ile hesaplanmaktadır.

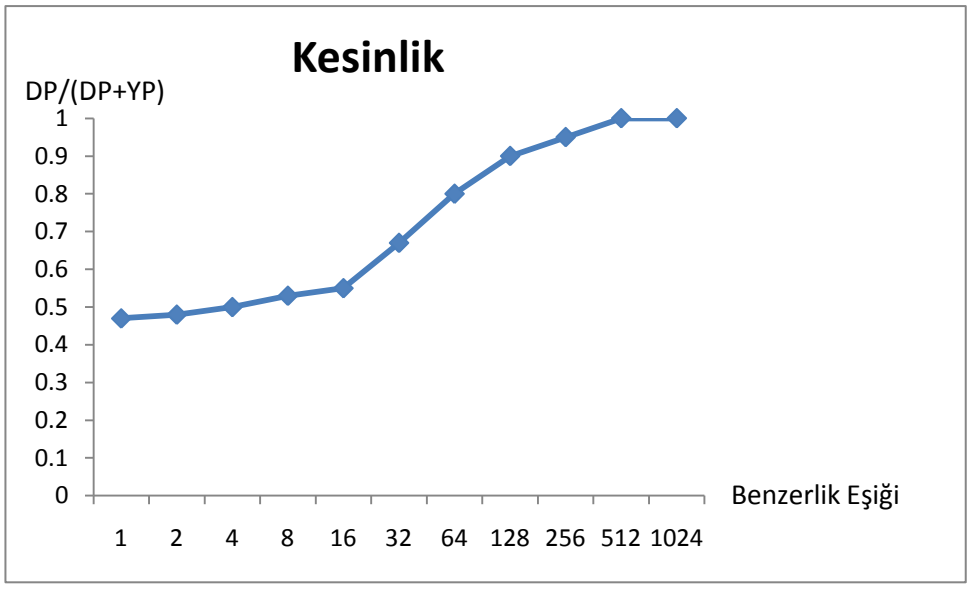
$$Başarı = \frac{DP+DN}{DP+YP+DN+YN} \quad \textbf{(6.29)}$$

6.6.1 Etki Benzerliği Deneysel Sonuçları

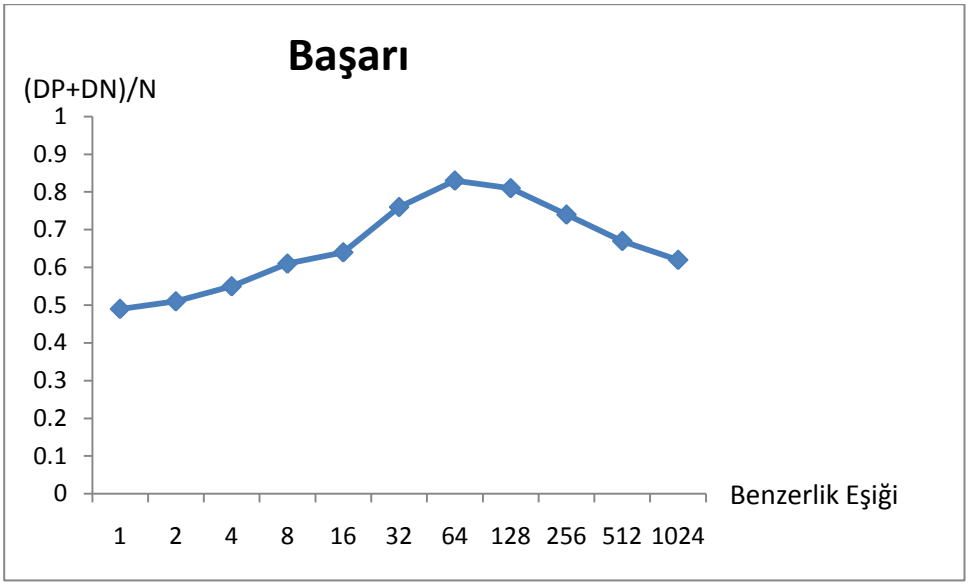
Alarm veri kümesi üzerinde etki benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.4'de etki benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine göre değişimi verilmektedir. Şekil 6.5'de etki benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.6'da etki benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir.



Şekil 6.4: Başarılı Tavsiye Sayısı (Etki Benzerliği)



Şekil 6.5: Tavsiye Kesinliği (Etki Benzerliği)



Şekil 6.6: Sınıflandırma Başarısı (Etki Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde etki benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 128 kabul edilip, etki benzerliği 128'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.2'de gösterilmiştir:

Çizelge 6.2: Etki Benzerliği İçin Yanılsama Matrisi (b=128)

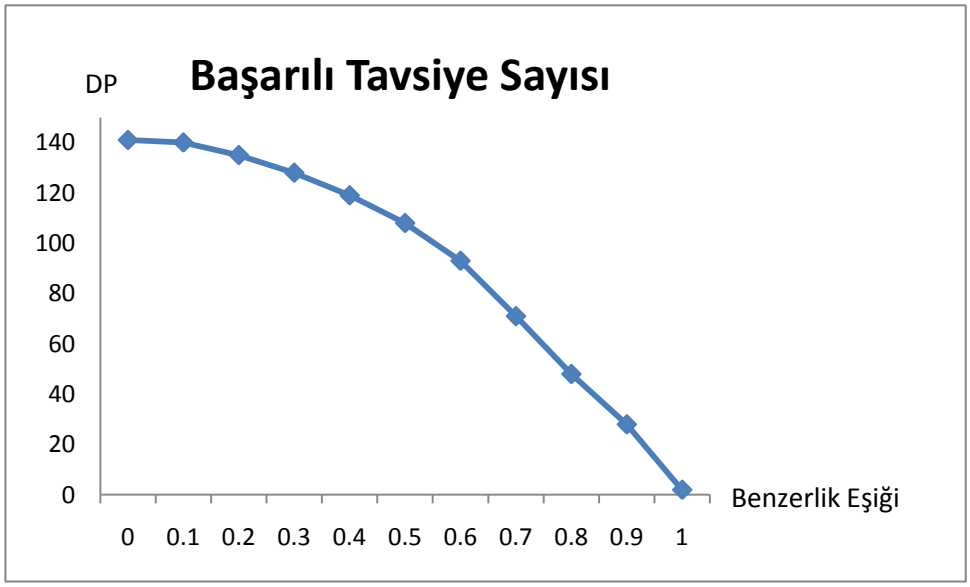
	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	91	50
İlintisiz Alarm Tipi Grubu	10	169

Çizelge 6.2'de görüldüğü gibi 91 tane ilintili alarm tipi grubu %90 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %65'i belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

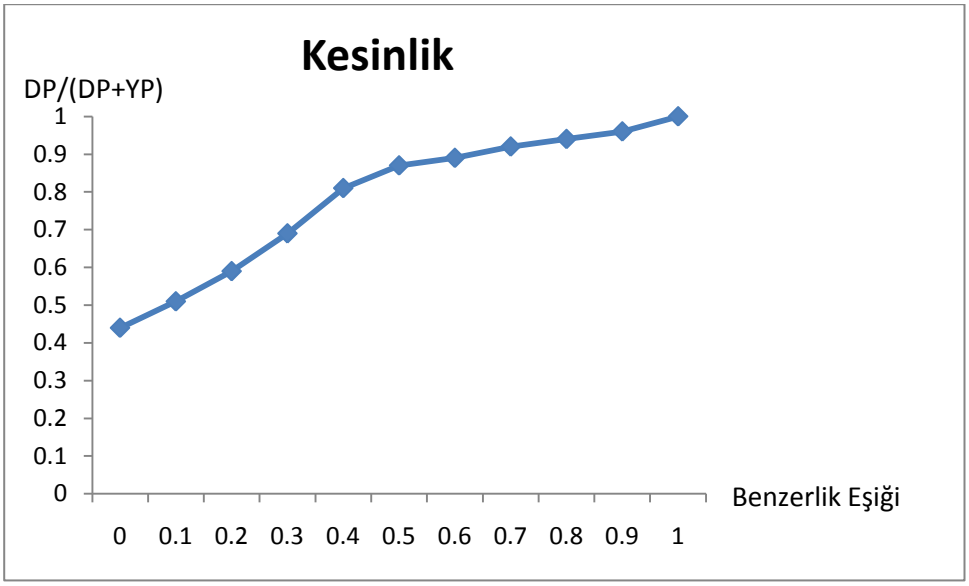
6.6.2 Maksimum Güven Benzerliği Deneysel Sonuçları

Alarm veri kümesi üzerinde maksimum güven benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.7'de maksimum güven benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine

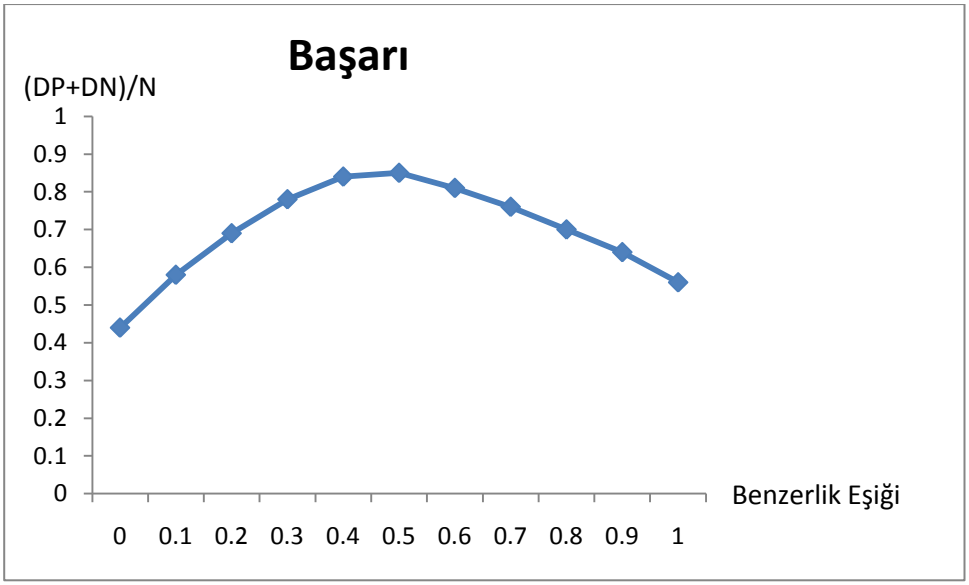
göre değişimi verilmektedir. Şekil 6.8'de maksimum güven benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.9'de maksimum güven benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir.



Şekil 6.7: Başarılı Tavsiye Sayısı (Maksimum Güven Benzerliği)



Şekil 6.8: Tavsiye Kesinliği (Maksimum Güven Benzerliği)



Şekil 6.9: Sınıflandırma Başarısı (Maksimum Güven Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde maksimum güven benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 0.5 kabul edilip, maksimum güven benzerliği 0.5'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.3'de gösterilmiştir:

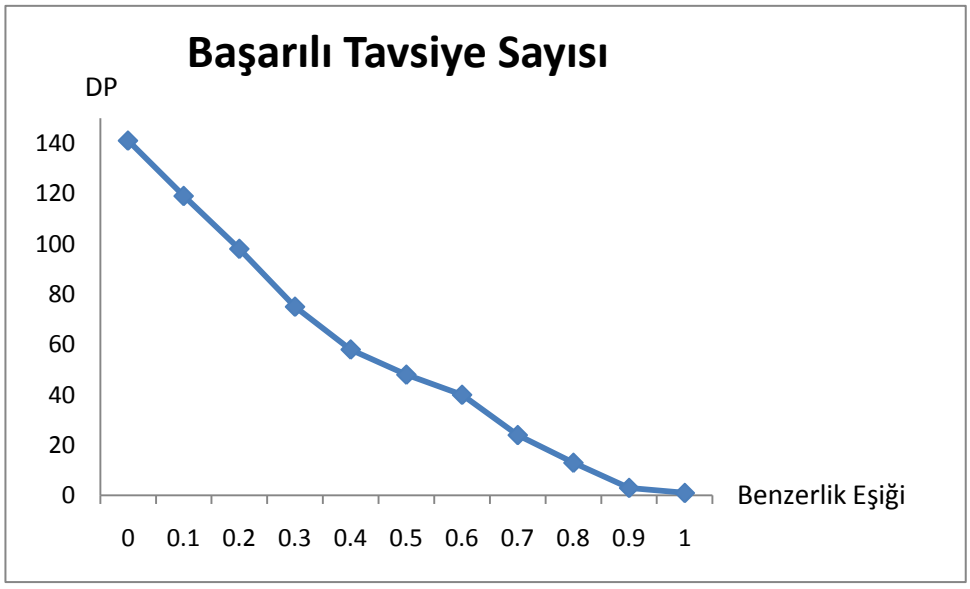
Çizelge 6.3: Maksimum Güven Benzerliği İçin Yanılsama Matrisi (b=0.5)

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	108	33
İlintisiz Alarm Tipi Grubu	16	163

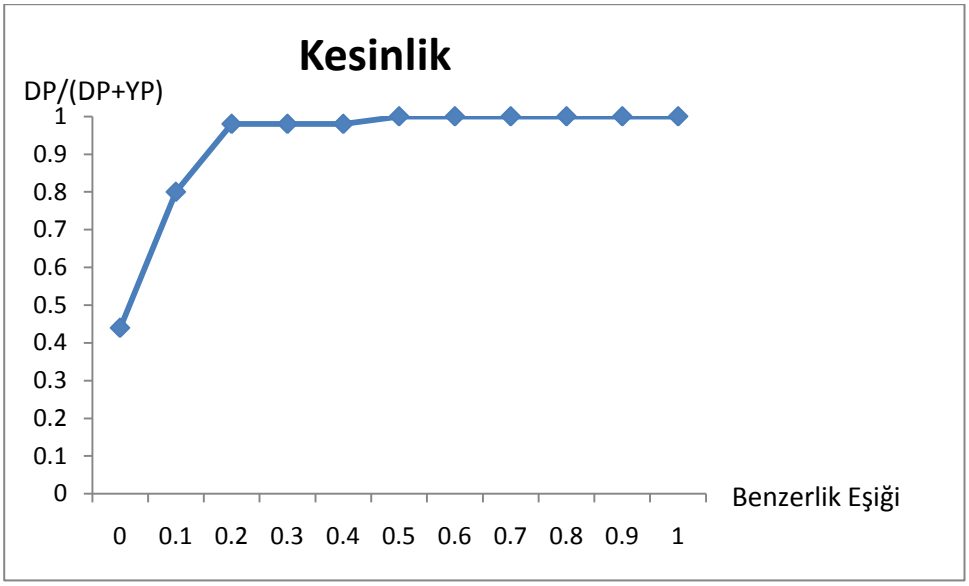
Çizelge 6.3'de görüldüğü gibi 108 tane ilintili alarm tipi grubu %87 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %77'si belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

6.6.3 Minimum Güven Benzerliği Deneysel Sonuçları

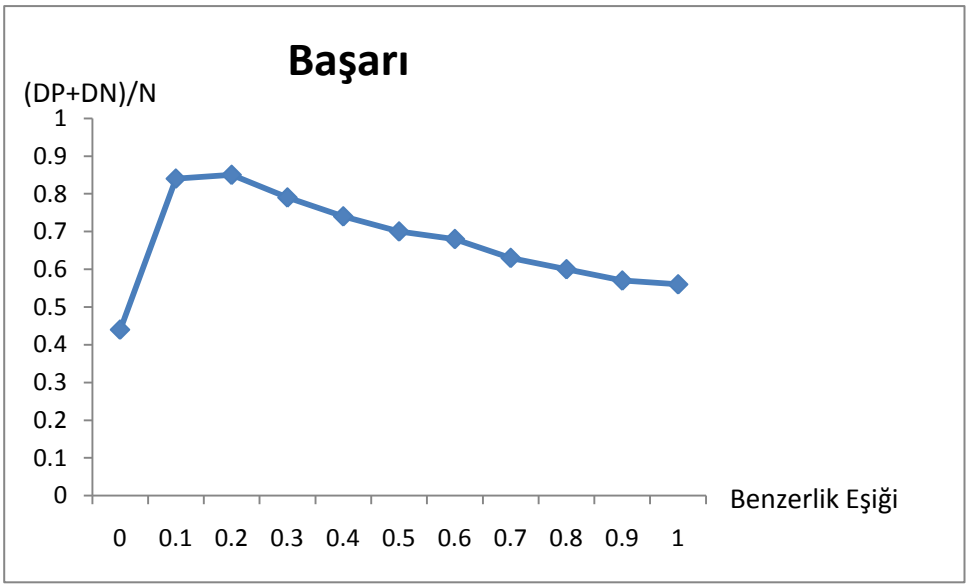
Alarm veri kümesi üzerinde minimum güven benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.10'da minimum güven benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine göre değişimi verilmektedir. Şekil 6.11'de minimum güven benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.12'de minimum güven benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir.



Şekil 6.10: Başarılı Tavsiye Sayısı (Minimum Güven Benzerliği)



Şekil 6.11: Tavsiye Kesinliği (Minimum Güven Benzerliği)



Şekil 6.12: Sınıflandırma Başarısı (Minimum Güven Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde minimum güven benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 0.2 kabul edilip, minimum güven benzerliği 0.2'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.4'de gösterilmiştir:

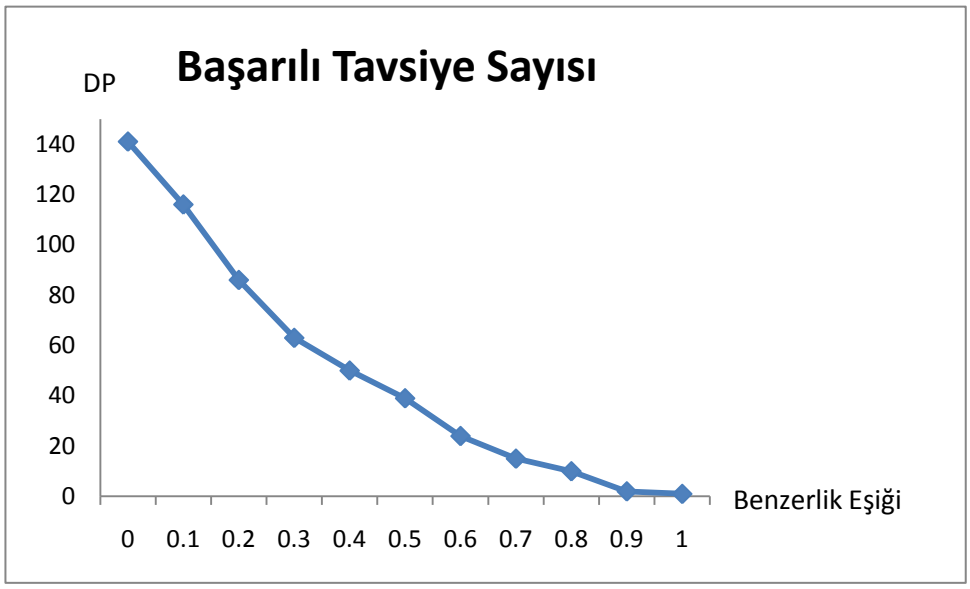
Çizelge 6.4: Minimum Güven Benzerliği İçin Yanılsama Matrisi (b=0.2)

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	98	43
İlintisiz Alarm Tipi Grubu	2	177

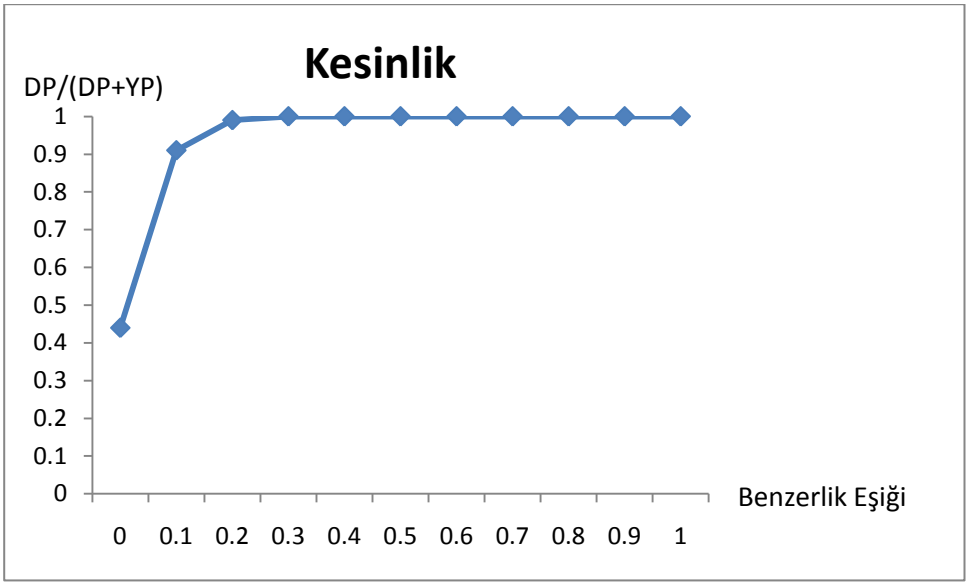
Çizelge 6.4'de görüldüğü gibi 98 tane ilintili alarm tipi grubu %98 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %70'i belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

6.6.4 Tutarlılık Benzerliği Deneysel Sonuçları

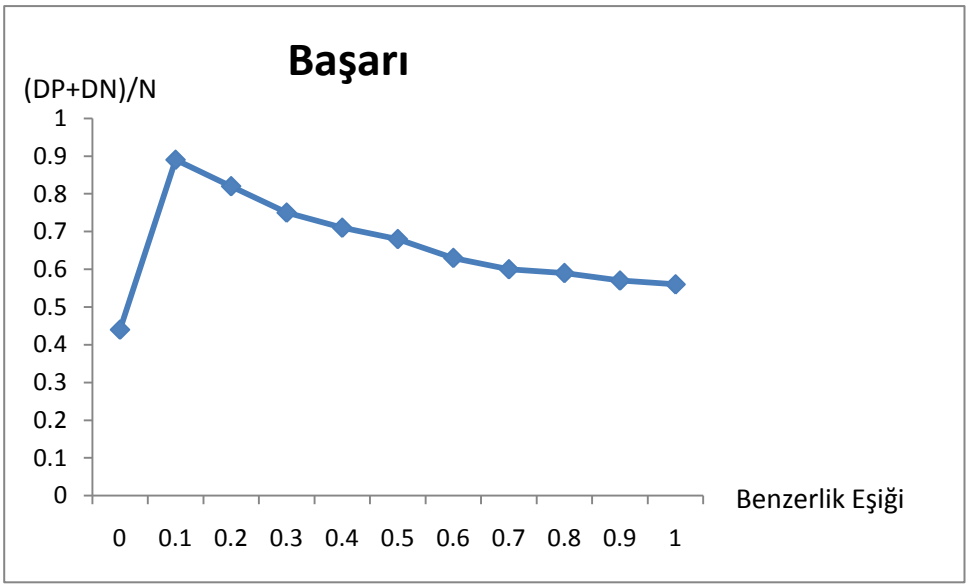
Alarm veri kümesi üzerinde tutarlılık benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.13'de tutarlılık benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine göre değişimi verilmektedir. Şekil 6.14'de tutarlılık benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.15'de tutarlılık benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir.



Şekil 6.13: Başarılı Tavsiye Sayısı (Tutarlılık Benzerliği)



Şekil 6.14: Tavsiye Kesinliği (Tutarlılık Benzerliği)



Şekil 6.15: Sınıflandırma Başarısı (Tutarlılık Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde tutarlılık benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 0.2 kabul edilip, tutarlılık benzerliği 0.2'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.5'de gösterilmiştir:

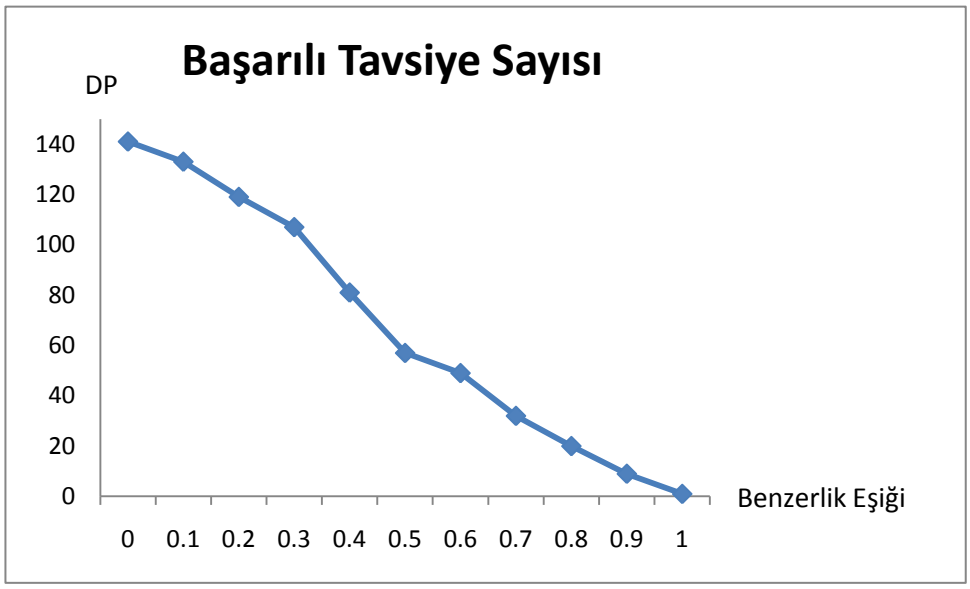
Çizelge 6.5: Tutarlılık Benzerliği İçin Yanılsama Matrisi (b=0.2)

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	86	55
İlintisiz Alarm Tipi Grubu	1	178

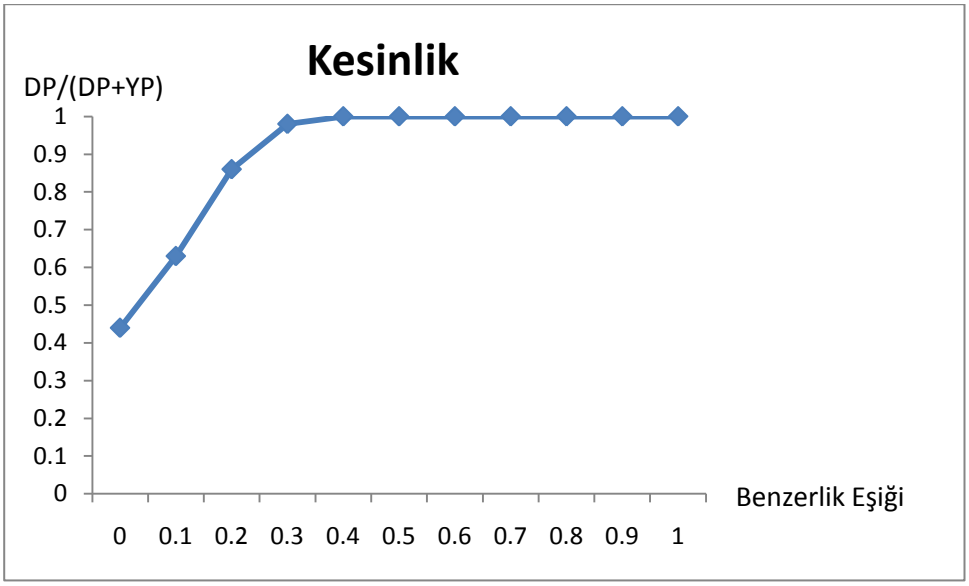
Çizelge 6.5'de görüldüğü gibi 86 tane ilintili alarm tipi grubu %99 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %61'i belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

6.6.5 Cosine Benzerliği Deneysel Sonuçları

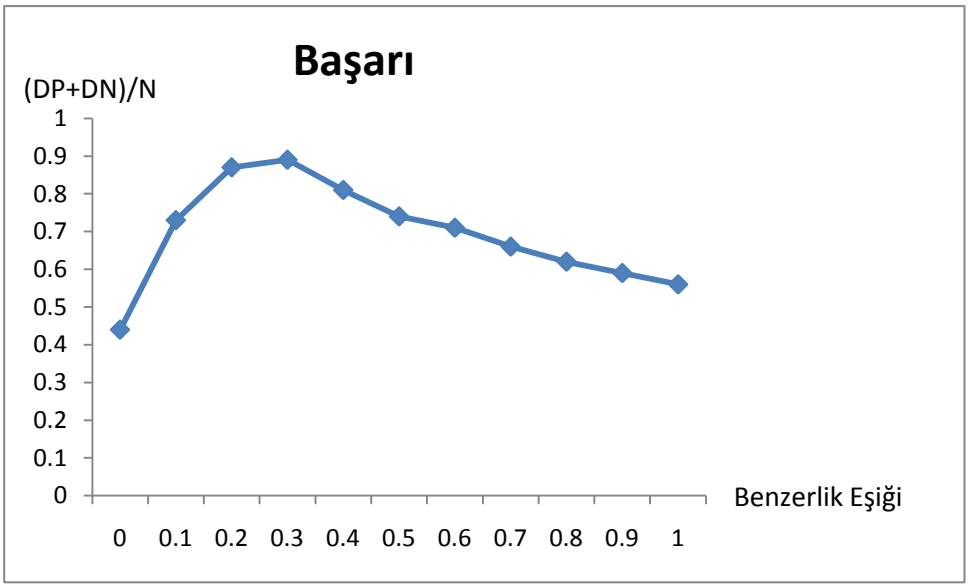
Alarm veri kümesi üzerinde cosine benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.16'da cosine benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine göre değişimi verilmektedir. Şekil 6.17'de cosine benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.18'de cosine benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir



Şekil 6.16: Başarılı Tavsiye Sayısı (Cosine Benzerliği)



Şekil 6.17: Tavsiye Kesinliği (Cosine Benzerliği)



Şekil 6.18: Sınıflandırma Başarısı (Cosine Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde cosine benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 0.3 kabul edilip, cosine benzerliği 0.3'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.6'da gösterilmiştir:

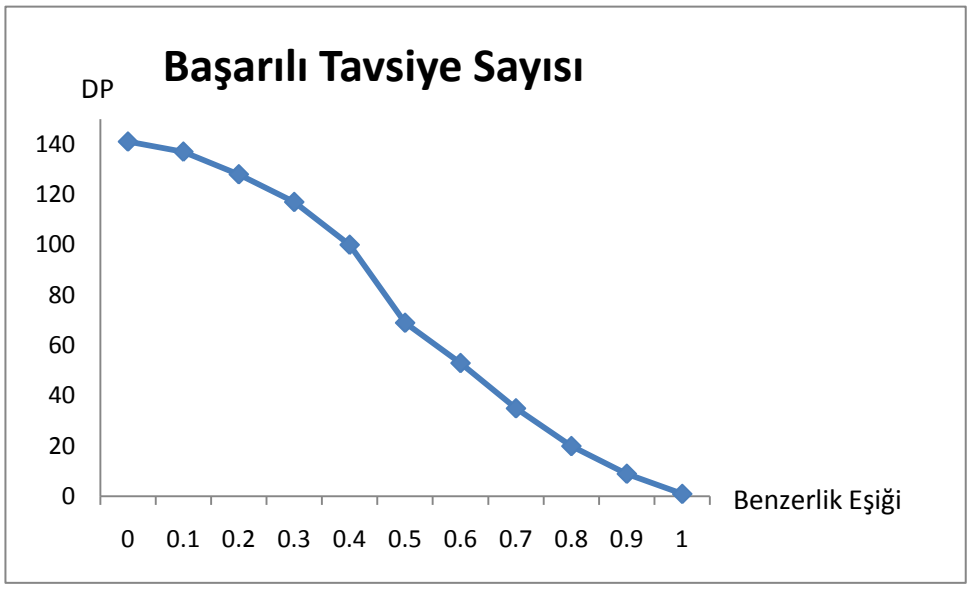
Çizelge 6.6: Cosine Benzerliği İçin Yanılsama Matrisi (b=0.3)

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	107	34
İlintisiz Alarm Tipi Grubu	2	177

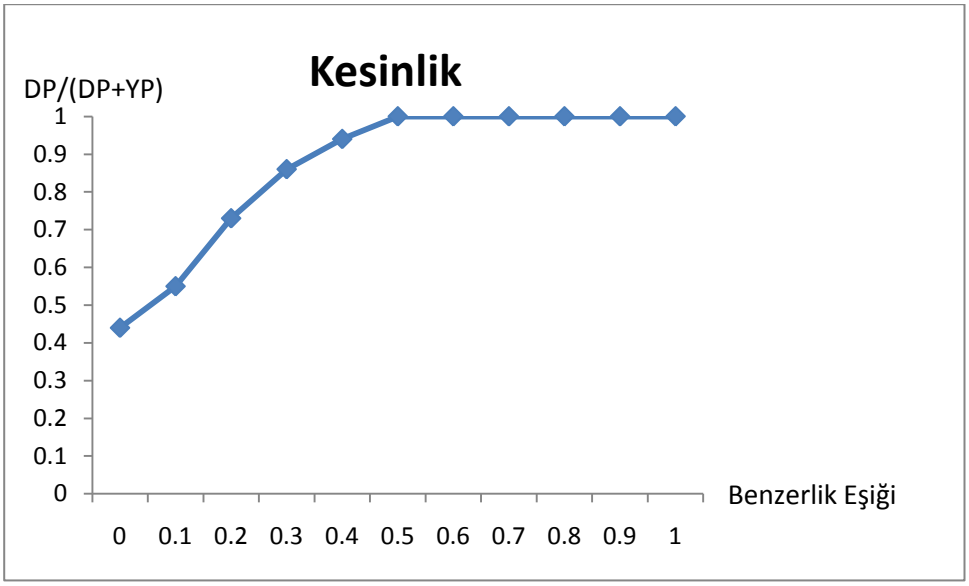
Çizelge 6.6'da görüldüğü gibi 107 tane ilintili alarm tipi grubu %98 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %76'sı belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

6.6.6 Kulczynski Benzerliği Deneysel Sonuçları

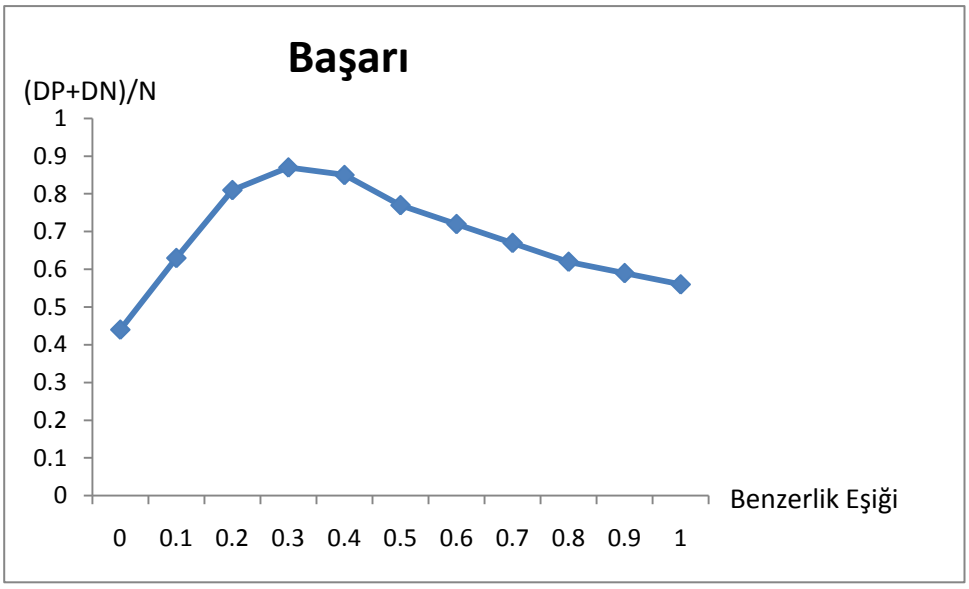
Alarm veri kümesi üzerinde Kulczynski benzerliği kullanılarak yapılan deneysel testlerin sonuçları aşağıdaki şekillerde gösterilmektedir. Şekil 6.19'da Kulczynski benzerliği ile önerilen başarılı tavsiye sayısının benzerlik eşiğine göre değişimi verilmektedir. Şekil 6.20'de Kulczynski benzerliği kullanılarak yapılmış ilintili alarm tipi ikilisi tavsiyelerinin kesinliğinin benzerlik eşiğine göre değişimi bulunmaktadır. Şekil 6.21'de Kulczynski benzerliği kullanılarak önerilen ilintili ve ilintisiz alarm tipi ikililerinin sınıflandırma başarısının benzerlik eşiğine göre değişimi verilmektedir



Şekil 6.19: Başarılı Tavsiye Sayısı (Kulczynski Benzerliği)



Şekil 6.20: Tavsiye Kesinliği (Kulczynski Benzerliği)



Şekil 6.21: Sınıflandırma Başarısı (Kulczynski Benzerliği)

Şekiller incelendiğinde uygun benzerlik eşiği seçildiğinde Kulczynski benzerliği ile çok sayıda ilintili alarm ikililerinin yüksek tahmin kesinliği ile saptanabildiği görülmektedir. Benzerlik eşiği 0.4 kabul edilip, Kulczynski benzerliği 0.4'den büyük olan alarm tipi ikilileri ilintili alarm tipleri olarak tavsiye edilirse ortaya çıkacak yanılsama matrisi Çizelge 6.7'da gösterilmiştir:

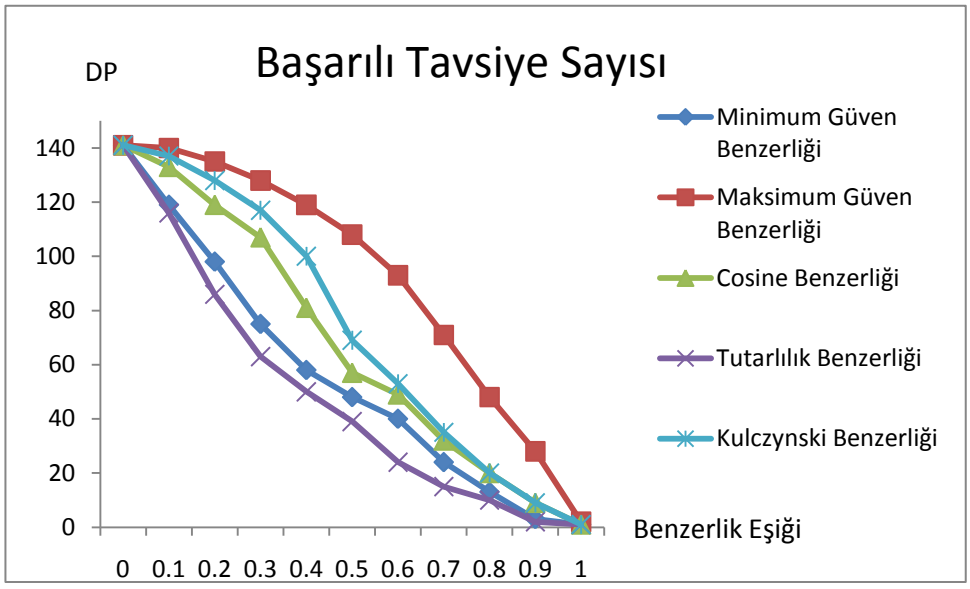
Çizelge 6.7: Kulczynski Benzerliği İçin Yanılsama Matrisi (b=0.4)

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	100	41
İlintisiz Alarm Tipi Grubu	6	173

Çizelge 6.7'de görüldüğü gibi 100 tane ilintili alarm tipi grubu %94 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %71'i belirlenebilmiştir. İlintili alarm tiplerinin öğrenilmesi konusunda mevcut bir yöntem bulunmadığı için bu oran başarılı bir sonuçtur.

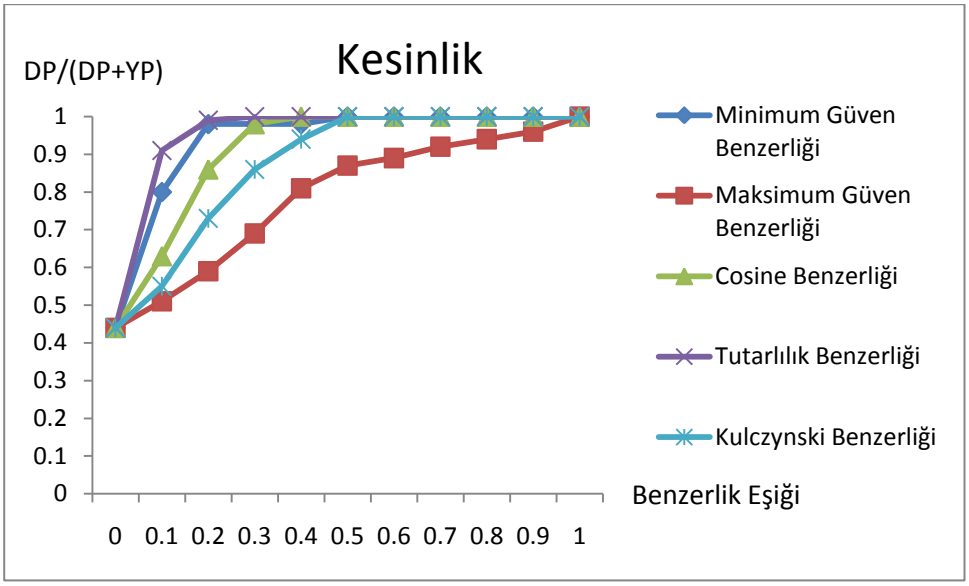
6.6.7 Kullanılan Benzerlik Çeşitlerinin Karşılaştırılması

Çalışmamızda önerilen 6 benzerlik metriğinden 5 tanesi [0,1] aralığında değerler almaktadır. Önerilen benzerlik metriklerinin performanslarını birbirleri ile kıyaslamak için aşağıdaki şekiller üretilmiştir.



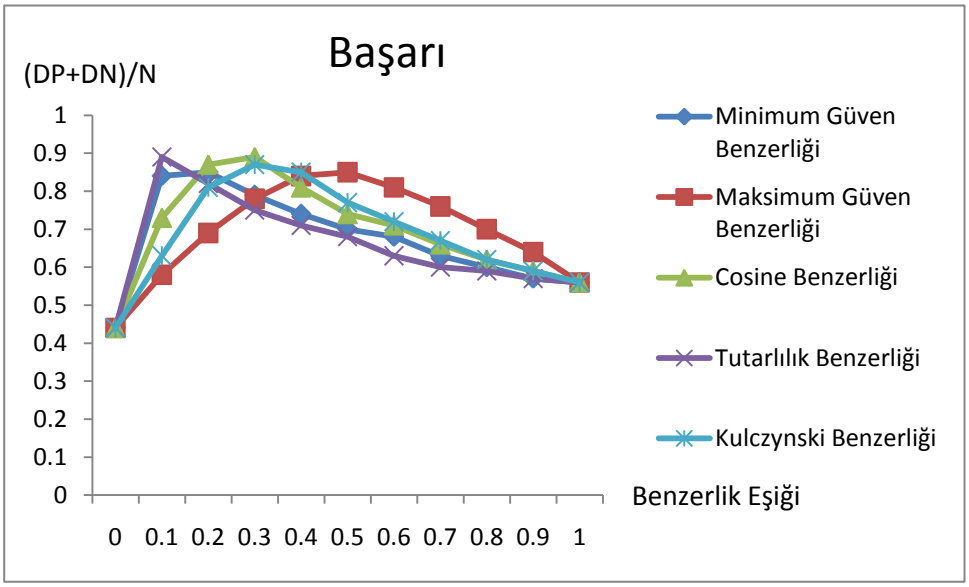
Şekil 6.22: Başarılı Tavsiye Sayıları

Şekil 6.22'de benzerlik metrikleri kullanılarak önerilen başarılı ilintili alarm tipi grubu sayısının benzerlik eşik değerine göre değişimi verilmiştir.



Şekil 6.23: Tavsiye Kesinliği

Şekil 6.23'de benzerlik metrikleri kullanılarak önerilen tavsiyelerin kesinliğinin benzerlik eşik değerine göre değişimi verilmiştir.



Şekil 6.24: Sınıflandırma Başarısı

Şekil 6.24'de benzerlik metrikleri kullanılarak elde edilen sınıflandırma başarısının benzerlik eşik değerine göre değişimi verilmiştir.

Şekil 6.22, Şekil 6.23 ve Şekil 6.24 karşılaştırmalı olarak incelendiğinde aşağıdaki sonuçlara varılabilmektedir:

- Aynı benzerlik değerleri için benzerlik tiplerinin başarılı tavsiye sayısına göre sıralaması büyükten küçüğe şu şekildedir: Maksimum güven benzerliği, Kulczynski benzerliği, cosine benzerliği, minimum güven benzerliği ve tutarlılık benzerliğidir.

- Aynı benzerlik değerleri için benzerlik tiplerinin tavsiye kesinliğine göre sıralaması büyükten küçüğe doğru şu şekildedir: Tutarlılık benzerliği, minimum güven benzerliği, cosine benzerliği, Kulczynski benzerliği ve maksimum güven benzerliği. Bu sıralama başarılı tavsiye sayısına göre yapılan sıralamanın tam tersidir.

- Başarılı tavsiye sayısının yüksekliği daha önemli ise maksimum güven benzerliği daha başarılı bir benzerlik metriğidir. Ama yapılan tavsiyelerin kesinliği daha önemli ise en başarılı benzerlik metriği tutarlılık benzerliğidir.

6.6.8 S Biçimli Sınıflandırmanın Deneysel Sonuçları

İncelenen benzerlik ölçütleri ilintili alarm tiplerinin belirlenmesinde tek başlarına başarılı olmalarına rağmen ilintili alarm tiplerine karar vermeyi sağlayan benzerlik eşik değerlerinin dışarıdan girdi olarak verilmesi ihtiyacı bulunmaktadır. Bu benzerlik eşiklerine ihtiyaç duymadan farklı tipteki benzerlik ölçütlerinin beraber kullanılması için çalışmamız kapsamında *S Biçimli Sınıflandırma* kullanılmıştır.

Çizelge 6.8'de bu eğitim ve test veri kümeleri kullanılınca elde edilen test sonuçları görülmektedir.

Çizelge 6.8: S Biçimli Sınıflandırma Sonuçları

	Tahmin Edilen İlişki	
Gerçek İlişki	İlintili Alarm Tipi Grubu	İlintisiz Alarm Tipi Grubu
İlintili Alarm Tipi Grubu	116	25
İlintisiz Alarm Tipi Grubu	10	169

Çizelge 6.8'de görüldüğü gibi 116 tane ilintili alarm tipi grubu %92 tavsiye kesinliği ile belirlenebilmektedir. İlintili alarm tiplerinin %82'si belirlenebilmiştir. Sınıflandırma başarısı %89'dur. Bu değer Şekil 6.24'de gösterilen her bir benzerliğin en yüksek başarısından daha yüksek bir değerdir. Bu sınıflandırma başarısına

herhangi bir benzerlik eşik değerine ihtiyaç duymadan ulaşılması önemli bir başarıdır.

İlintili alarm tiplerinin belirlenmesinde *Pazar Sepet Analizi* literatüründe kullanılan benzerlik ölçütleri tek başlarına dışarıdan girdi olarak verilen benzerlik eşik değerleri ile başarılı sonuçlar vermektedir. Ama bu benzerlikler *S Biçimli Sınıflandırma* için eğitici öznitelikler olarak kullanıldığında her bir benzerlik çeşidinden daha yüksek başarılar elde edilmektedir.

7. SONUÇ

Ülkemizin GSM şebeke işletmecisi firmalarından Turkcell'in 2010 yılına ait şebeke alarmlarını içeren veri kümesi üzerindeki deneysel çalışmalarımızın sonunda alarm tarihçesinin incelenmesi ile elde edilen istatistiksel bilgiler ile çok sayıda başarılı alarm filtresinin üretilebildiği gözlemlenmiştir.

Çalışmamız kapsamında istatistiksel öğrenme yöntemleri ile otomatik öğrenilmesi hedeflenen ilk filtre çeşidi geçici alarm filtreleridir. Alarm veri kümesinde yer alan örneklerin yaşam süreleri dağılımdan bağımsız olasılık kestirimi yöntemleri ile incelenince geçici alarm filtrelerinin üretimi için gerekli geçici alarm tiplerine karar verilmesi ve uygun alarm bekletme sürelerinin belirlenmesi mümkün olmuştur. Karşılaştırmalı olarak incelenen dağılımdan bağımsız olasılık kestirimi yöntemlerinden *Parzen Penceresi Analizi* ve *Histogram Analizi* yöntemleri %90'ların üzerinde tavsiye kesinliği başarısı ile önemli miktarda geçici alarm filtresi tavsiyeleri üretebilmişlerdir. İki yöntem karşılaştırılınca *Parzen Penceresi Analizi* yöntemi düşük sayıda alarm örneğinin bulunduğu durumlarda daha başarılı filtre tavsiyelerinin üretilmesini sağlamıştır. Aynı zamanda bu yöntemin tavsiye kesinlikleri *Histogram Analizi* yönteminin sonuçlarından daha başarılıdır. *Histogram Analizi* yönteminin en önemli avantajları hızı ve öğrenme işleminin gerçekleştirildiği sunucuda kullandığı düşük kaynak miktarıdır. *Histogram Analizi* yönteminin tavsiye kesinliği başarısı *Parzen Penceresi* yöntemi ile kıyaslanınca düşük olmasına rağmen başarılı tavsiye sayısı daha yüksektir. Bunun yanında incelenen veri kümesindeki alarm örneği sayısı arttıkça *Histogram Analizi* yönteminin tavsiye kesinliği ve sınıflandırma başarısı da *Parzen Penceresi* yönteminin sonuçlarına yakınsamaktadır. Sonuç olarak, geçici alarm filtrelerinin öğrenilmesi konusunda alarm örneği sayısı düşük olan alarm tipleri için *Parzen Penceresi Analizi*, alarm örneği sayısı yüksek olan alarm tipleri için *Histogram Analizi* yöntemini kullanan hibrid bir çözüm minimum zaman ve kaynağı kullanıp maksimum başarı performansı sağlayabilir.

Çalışmamız kapsamında istatistiksel öğrenme yöntemleri ile otomatik öğrenilmesi hedeflenen ikinci filtre çeşidi alarm ilintilendirme filtreleridir. Bu amaçla *Pazar Sepet Analizi* yöntemlerinde çok sık kullanılan altı benzerlik ölçütü ayrıntılı bir şekilde incelenmiştir. İncelenen benzerlikler *Maksimum Güven*, *Minimum Güven*, *Tutarlılık*, *Cosine*, *Etki* ve *Kulczynski* benzerlikleridir. Bu benzerlikler alarm

tiplerinin beraber gözlemlenme frekansları ile hesaplanmaktadır. Dışarıdan girdi olarak verilen benzerlik eşiği değerlerinin alarm tipleri arasındaki istatistiksel benzerlik ölçümleri ile beraber kullanılması sayesinde her bir benzerlik çeşidi ilintili alarm tipi filtrelerinin öğrenilmesine olanak vermektedir. Ama benzerlik eşik değerleri uygun seçilmezse alarm ilintilendirme filtre tavsiyelerinin başarıları önemli ölçüde düşmektedir. Bu probleme çözüm olarak çalışmamız kapsamında hesaplanan bütün benzerlik çeşitlerini kullanıp güçlerini birleştirebilen ve herhangi bir eşik değerine girdi olarak ihtiyaç duymayan *S Biçimli Sınıflandırma* yöntemi kullanılmıştır. Bu sınıflandırma yöntemi ile incelenen ilintili alarm tipi grupları %90 civarında bir başarı ile sınıflandırılabilmiştir. Bu başarı oranı incelenen benzerlik çeşitlerinin tek başlarına sağlayabildikleri maksimum başarının biraz üstündedir. Bu başarıya herhangi bir eşik değeri girdisine ihtiyaç duymadan ulaşabilmek önemli bir kazanımdır. Çalışmanın sonunda alarm ilintilendirme filtrelerinin otomatik üretiminde kullanılabilecek ideal yöntemin farklı benzerlik çeşitlerini girdi olarak kullanan *S Biçimli Sınıflandırma* olduğuna karar verilmiştir.

GSM şebekelerinde aksaklık yönetimi kapsamından istatistiksel öğrenme yöntemleri gelecek vaat eden bir araştırma alanıdır. İncelenen iki çeşit alarm filtresinin otomatik öğrenilmesi dışında diğer filtre çeşitlerinin de makine öğrenmesi yöntemleri ile geliştirilmesi yeni araştırma alanları açabilir. Filtrelerin üretimi dışında alarm tarihçesi üzerinde geliştirilecek öğrenme algoritmalarıyla önemli problemlerin oluşmadan belirlenmesi ve gerekli aksiyonların alınması konusunda yapılacak çalışmalar GSM sektörüne önemli katkılar sağlayabilir. Ülkemizde bulunan telekomünikasyon şebeke işletmecisi firmalar Türkiye'nin en büyük veri tabanlarını bünyelerinde barındırmaktadırlar. Altyapılarında karşılaşılan birçok problem bu veri tabanları üzerinde uygulanacak akıllı veri madenciliği yaklaşımlarıyla çözülebilir.

KAYNAKLAR

[1] **Klemettinen, M., Mannila, H. and Toivonen, H.,** December 1999: Rule discovery in telecommunication alarm data. In *Journal of Network and Systems Management*, 7(4), pp.395–423.

[2] **Steinder, M. and Adarshpal, S.S**., October 2004: Probabilistic Fault Localization in Communication Systems Using Belief Network. In IEEE/ACM Transactions on Networking, 12(5), pp.809-822.

[3] **Liu, G., Mok A. K. and Yang, E. J.,** May 1999: Composite events for network event correlation. In *Integrated Network Management* VI, Boston, MA.

[4] **Gürer, D., Khan, I., Ogier, R. and Keffer, R**., 2007: An Artificial Intelligence Approach to Network Fault Management. SRI International, Menlo Park, California, USA.

[5] **Mao, Y., Jamjoom, H., Tao, S. and Smith, J.M.,** October 2007: NetworkMD: Topology inference and failure diagnosis in the last mile. *In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement (IMC)*, San Diego, California, USA, pp.189-202.

[6] **Mas, C., Le Boudec, Jean-Yves,** 1997: An alarm filtering algorithm for optical communication networks. In International Conference on Management of Multimedia Networks and Services, July 08-10, pp.205-218.

[7] **Hanemann, A. and Marcu, P.,** April 2008: Algorithm Design and Application of Service-Oriented Event Correlation. In *Proceedings of the 3rd IFIP/IEEE International Workshop on Business Driven IT Management (BDIM 2008)*, Salvador Bahia, Brazil.

[8] **Jardin, P.,** 1996: Supporting Scalability and Flexibility in a Distributed Management Platform, *Distributed Systems Engineering 3*, The British Computer Society, IEE and IOP Publishing Ltd.

[9] **Hasan, M., Sugla, B. And Viswanathan, R.,** May 1999: A conceptual framework for network management event correlation and filtering systems.

In *Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Management*, 21, pp.233-246.

[10] **Sterritt, R., Marshall, A., Shapcott, C. and McClean, S.,** September 2000: Exploring dynamic bayesian belief networks for intelligent fault management system. In *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp.3646-3652.

[11] **Jakobson, G. & Weissman, M.D**., 1993: Alarm correlation: Correlating multiple network alarms improves telecommunications network surveillance and fault management. In *IEEE Network*, November, pp.52-59.

[12] **Amani, N., Fathi, M. and Dehghan, M.,** 2005**:** A Case-Based Reasoning Method for Alarm Filtering and Correlation in Telecommunication Networks. Retrieved on September, 21st 2010. Available at http://ieeexplore.ieee.org/iel5/10384/33117/01557421.pdf?arnumer=1557421.

[13] **He, Z., Niu, Q. and Tang, T.**, December 2008: Research on alarm system in wireless network based on mining association rules. In *International Conference on Computer Science and Software Engineering*, IEEE Computer Society, Wuhan, Hubei, pp. 598 – 601.

[14] **Malowidzki, M.,** 2000: Advanced Event Filtering Approach For CODA-Based Management Systems. In *IEEE/IFIP Network Operations and Management Seminar* (NOMS), pp. 45-58.

[15] **Mannila, H., Toivonen, H. And Verkamo, A.I.,** 1997: Discovery of Frequent Episodes in Event Sequences. In *Data Mining and Knowledge Discovery*, 1, pp.259-289.

[16] **Yemini, S. A., Kliger, S., Mozes, E., Yemini, Y. and Ohsie, D.,** May 1996: High speed and robust event correlation. In *IEEE Communications Magazine*, 34(5), pp.82–90.

[17] **Zheng, Q., Xu, K., Lv, W. and Ma, S.,** April 2002: Intelligent Search of Correlated Alarms from Database Containing Noise Data. In *Proceedings of the 8th IFIP/IEEE International Network and OperationsManagement Symposium (NOMS)*, Florence, Italy, pp. 405–419.

[18] **Choi, S. S., Kang, K. S., Kim, H. G., and Chang, S. H.,** August 1995: Development of an On-Line Fuzzy Expert System for Integrated Alarm

Processing in Nuclear Power Plants. In *IEEE Transactions on Nuclear Science*, **42**(4), pp.1406–1418.

[19] **Ghariani, A., Toguyéni, A.K.A. and Craye, E.** 2002: A Functional Graph Approach for Alarm Filtering and Fault Recovery for Automated Production Systems. In *Proceeding of Sixth International Workshop on Discrete Event Systems (WODES),* IEEE Computer Society, Spain, pp.1-6.

[20] **Lampley, G. C.,** 2009 : Permanent and Temporary Faults: Fault analysis on an electrical distribution system. In *Industry Applications Magazine*, Sept-Oct, pp.25-31.

[21] **Hinze, A. and Bittner, S.,** 2002: Efficient distribution-based event filtering. In *Proceedings of the 22nd IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW),* Vienna, Austria, pp.525-532.

[22] **Volponi, A.J., DePold, H., Ganguli, R. and Daguang C**., 2003: The Use of Kalman Filter and Neural Network Methodologies in Gas Turbine Performance Diagnostics: A Comparative Study. *Journal of Engineering for Gas Turbines and Power*, 125, pp.917-924.

[23] **Yu, M., Mokhtar, H. and Merabti, M.,** 2007: A Survey on Fault Management in Wireless Sensor Networks. In *PGNET Conference,* 2007.

[24] **Paradis, L. and Han, Q,** June 2007: A Survey of Fault Management in Wireless Sensor Networks, *Journal of Network and Systems Management*, 15(2), pp.171-190.

[25] **Julisch, K.,** 2003: Clustering Intrusion Detection Alarms to Support Root Cause Analysis, *ACM Transactions on Information and System Security,* 6(4), pp.443-471.

[26] **Manganaris, S., Christensen, M. Zerkle, D. and Hermiz, K**., 1999: A datamining analysis of RTID alarms. In *2nd International workshop on recent advances in intrusion detection*, West Lafayette, Indiana, USA, 7–9 September. Purdue University, CERIAS.

[27] **Shehab, M., Mansour, N. and Faour, A.,** May 2008: Growing Hierarchical Self-Organizing Map for Filtering Intrusion Detection Alarms. In *the International Symposium on Parallel Architectures, Algorithms, and Networks,* IEEE Computer Society, Sydney, NSW, pp.167-172.

[28] **Natu, M. and Sethi A.S.,** April 2006: Active probing approach for fault localization in computer networks. *In Proceedings of 4th End-to-End Monitoring Techniques and Services (E2EMON),* IEEE/IFIP Workshop, Vancouver, Canada, pp.25–33.

[29] **Mohamed, F., Marzouki, M. and Touati, M.,** March 1996: FLAMES: A fuzzy logic ATMS and model-based expert system for analog diagnosis. In *Proceedings of the European Design and Test Conference*, 96, pp.259-263.

[30] **Fröhlich, P., Jobmann, K., Nejdl, W. and Wietgrefe, H**., 1997: Model based alarm correlation in cellular phone networks. In Proceedings of the International Symposium on Modelling Analysis and Simulation of Computers and Telecommunications Systems (MASCOTS), pp.197-204.

[31] **Leszak, M., Perry, D. E. and Stoll, D. ,** 2000: A case study in root cause defect analysis. In *International Conference on Software Engineering*, Limerick, Ireland, ACM Press, pp.428-437.

[32] **Gruschke, B.,** 1998: Integrated Event Management: Event Correlation Using Dependency Graphs. In *9th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM),* Newark, Delaware, USA.

[33] **Natu, M. and Sethi A.S.,** July 2005: Efficient Probing Techniques for Fault Diagnosis. *In 2nd Intl. Conference on Internet Monitoring and Protection (ICIMP),* IEEE, pp.20-26.

[34] **Kompella, R., Yates, J., Greenberg, A. And Snoeren A.C.,** May 2007: Detection and Localization of network black holes. In Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM), pp.2180-2188.

[35] **Kandula, S., Katabi, D. and Vasseur, J.P.,** August 2005: Shrink: A tool for failure diagnosis in IP networks. *In Proceedings of ACM SIFCOMM MineNet Workshop on Mining network data,* New York, NY, USA, pp. 173-178.

[36] **Ravindranath, L., Bahl, P., Chandra, R., Maltz, D.A., Padhye, J. and Patel, P.,** 2009: Change is Hard: Adapting Dependency Graph Models For Unified Diagnosis in Wired / Wireless Networks. *In Proceedings of the 1st ACM workshop on Research on Enterprise networking,* New York, NY, USA, pp.83-92.

[37] **Sarkan, M. O., Çataltepe, Z.,** 2011: Parzen Penceresi Yöntemi İle Geçici Alarm Filtreleri Üretimi. *IEEE 19. Sinyal İşleme ve İletişim Uygulamaları Kurultayı.*

[38] **Alpaydın, E**., Mart 2011: Yapay Öğrenme. *Boğaziçi Üniversitesi Yayınevi.* İstanbul, pp.44-45, 136-139, 418-421.

[39] **Alpaydın, E**., Mart 2011: Yapay Öğrenme. *Boğaziçi Üniversitesi Yayınevi.* İstanbul, pp.44-45, 136-139, 418-421.

[40] **Alpaydın, E**., Mart 2011: Yapay Öğrenme. *Boğaziçi Üniversitesi Yayınevi.* İstanbul, pp.44-45, 136-139, 418-421.

[41] **Brin, S., Motwani, R. and Silverstein, C.** 1997: Beyond Market Basket: Generalizing Association Rules to Correlations. *In Proceedings of ACM SIGMOD,* AZ, USA, pp.265-276.

[42] **Chen, Y., Tang, K., Shen, R., Hu, Y.,** August 2005: Market Basket Analysis In A Multiple Store Environment. In *Journal of Elsevier Decision Support Systems,* pp.339-354.

[43] **Hilderman, R. J., Carter, C. L., Hamilton, H. J., Cercone, N.,** April 1998: Mining Market Basket Data Using Share Measures And Characterized Itemsets. In *Second Pacific-Asia Conference on Knowledge Discovery and Data Mining,* pp.159-173.

[44] **Brijs, T., Swinnen, G., Vanhoof, K., Wets, G.,** 1999: Using Association Rules for Product Assortment Decisions: A Case Study. In *Proceedings of the fifth International Conference on Knowledge Discovery and Data Mining,* pp.143-150.

[45] **Cunningham, S.J., Frank,E.,** November 1999: Market Basket Analysis of Library Circulation Data. In *International Conference on Neural Information Processing,* pp.825-830.

[46] **Creighton, C., Hanash, S.,** July 2002: Mining Gene Expression Databases For Association Rules. In *Journal of Oxford Bioinformatics,* pp. 79-86.

[47] **Hilderman, R. J., Hamilton, H. J.,** 2001: Knowledge Discovery and Measures of Interest. Kluwer Academic Press.

[48] **Tan, P.N., Kumar, V., Srivastava, J.,** 2002: Selecting The Right Interestingness Measure for Association Patterns. In *Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,* pp.32-41.

[49] **Srikant, R., Vu, Q., Agrawal, R.,** 1997: Mining Association Rules with Item Constraints. In *Proceedings of Third International Conference on Knowledge Discovery and Data Mining.*

[50] **Omiecinski, E.,** 2003: Alternative Interest Measures for Mining Associations. In *IEEE Transaction on Knowledge abd Data Engineering,* pp.57-69.

[51] **Kulczynski, S.,** 1927: Die Panzenassoziationen der Pieninen. In *Bulletin International de l'Academie Polonaise des Sciences et des Lettres, Classe des Sciences Mathematiques et Naturelles*, pp.57-203.

[52] **Segond, M., Borgelt, C., Yang, X.,** May 2011: Itemset Mining Based On Cover Similarity. In *15th Pacific-Asia Conference on Knowledge Discovery and Data Mining.*

[53] **Jain, A. K., Duin, R. P. W., Mao, J.,** 1999: Statistical Pattern Recognition: A Review. In *Pattern Analysis and Machine Intelligence.* Volume 22, Pp.4-37.

[54] **Agrawal, R. and Srikant, R.,** June 1994: Fast Algorithms for Mining Association Rules. IBM Research Report RJ9839i IBM Almaden Research Center, San Jose, California.

[55] **Allan, L. G.,** 1980: A note on measurements of contingency between two binary variables in judgment tasks. *Bulletin of the Psychonomic Society,* 15, pp.147-149.

[56] **Allan, L. G.,** 1993: Human Contingency Judgements: Rule based or associative? *Psychological Bulletin,* 114(3), pp.435-448.

[57] **Alonso, C. J. and Rodriguez, J. J**., 2004: Boosting interval based literals: Variable length and early classification. In *Data Mining in Time Series Databases*, World Scientific.

[58] **Alpaydın, E**., Mart 2011: Yapay Öğrenme. *Boğaziçi Üniversitesi Yayınevi.* İstanbul, pp.44-45, 136-139, 418-421.

[59] **Armengol, J., Vehl, J., Sainz, M.A.,** March 2001: Application of Multiple Sliding Time Windows to Fault Detection Based on Interval Models. *In 12th International Workshop on Principles of Diagnosis,* pp.9-16.

[60] **Bouloutas, A.T., Calo, S. and Finkel, A.**, February 1994: Alarm Correlation and Fault Identification in Communication Networks. In IEEE Transactions on Communications, 42(234), pp.523–533.

[61] **Böhm, C., Läer, L., Plant, C. and Zherdin, A,** 2009: Model-based Classification of Data with Time Series-valued Attributes. In *BTW*, 144GI, pp. 287-296.

[62] **Brunet, R., 1998:** Temporal Alarm Correlation in Communication Networks. Master's thesis, Faculty of Engineering, Carleton University, Ottawa, Ohio.

[63] **Burns, L., Hellerstein, J. L., Ma, S., Perng, C. S., Rabenhorst, D. A. and Taylor, D.,** 2001: A Systematic Approach to Discovering Correlation Rules For Event Management. In *Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management,* pp.345-359.

[64] **Chen, M., Zheng, A.X., Jordan, M.I. and Brewer, E.,** May 2004: Failure Diagnosis UsingDecision Trees. In *International Conference on Autonomic Computing* (ICAC), New York, NY, pp.36-42.

[65] **Chib, S. and Greenberg, E,** 1998: Analysis of multivariate probit models. Biometrika, 85, pp.347-361.

[66] **Cho, K.B., Song, S.K. and Youn, H.Y.,** August 2007: Publisher-side Event Filtering for QoS-Awareness in Ubiquitous Computing. In *Fifth International Conference on Computational Science and Applications (ICCSA)*, IEEE Computer Society, Kuala Lumpur, Malaysia, pp.361-366.

[67] **Chu, S., Keogh, E., Hart, D. and Pazzani, M.,** 2002: Iterative Deepening Dynamic Time Warping for Time Series. In Proceedings of 2nd SIAM International Conference on Data Mining, pp.195-212.

[68] **Cotofrei, P. and Stoffel, K.,** 2002: Rule Extraction from Time Series Database using Classification Trees. In *Proceedings of IASTED International Conference*, Insbruck, Austria, pp.327-332.

[69] **Cotofrei, P. and Stoffel, K., 2007:** Stochastic processes and temporal data mining. In *Proceedings of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Datamining (KDD),* New York, NY, pp.183–190.

[70] **Das, G., Lin, K., Mannila, H.,** 1998: Rule Discovery From Time Series. In *Proceedings of The 4th National Conference on Knowledge Discovery and Data Mining,* pp.16-22.

[71] **De la Rosa, J. J. G., Lloret, I., Moreno, A., Puntonet, C. G., and Górriz, J. M.,** 2006: Wavelets and wavelet packets applied to detect and characterize transient alarm signals from termites. *Measurement (Ed. Elsevier),* 39(6), pp.553–564.

[72] **Donchin E. and Heffley E.,** 1978: Multivariate analysis of event-related potential data: a tutorial review. In D. Otto (Eds.), *Multi-disciplinary perspectives in event-related brain potential research,* Washington, D.C., U.S. Government Printing Office, pp.555-572.

[73] **El-Darieby, M. and Bieszczad, A.,** May 1999: Intelligent Mobile Agents: Towards Network Fault Management Automation. In In *Proceedings of the 6th IFIP/IEEE International Symposium on Integrated Network Management,* Boston, MA, USA, pp.611 – 622.

[74] **Fraiwan, M. and Manimaran, G.,** May 2008: Localization of IP Links Faults Using Overlay Measurements. In *Proceedings of IEEE International Conference on Communications (ICC),* Beijing, pp.5629-5633.

[75] **Fröhlich, P., Nejdl, W., Schroeder, M., Damasio, C., Pereira, L.M.,** 1999: Using extended logic programming for alarm-correlation in cellular phone networks. In *12th International Conference. on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE),* LNCS 1611, Cairo, Egypt, pp.343-352.

[76] **Griffth, R., Hellerstein, J., Kaiser, G. and Diao, Y.**, June 2006: Dynamic adaptation of temporal event correlation for qos management in distributed systems. In *Quality of Service, IWQoS, 14th IEEE International Workshop*, pp. 290-294.

[77] **Han, J., Pei, J., Yın, Y. and Mao, R.,** 2004: Mining Frequent Patterns without Candidate Generation: A Frequent-Pattern Tree Approach. In *Data Mining and Knowledge Discovery,* 8, pp.53-87

[78] **Isermann, R.,** 1984: Process fault detection based on modelling and estimation methods: A survey, Automatica., 20, pp. 387-404.

[79] **Jiang, G. and Cybenko, G.,** 2004: Temporal and spatial distributed event correlation for network security. In *Proceedings of the IEEE, 2004 IEEE American Control Conference,* 2, pp.996–1001.

[80] **Julisch, K. and Dacier, M.,** July 2002: Mining intrusion detection alarms for actionable knowledge. In *The 8th ACM International Conference on Knowledge Discovery and Data Mining*, pp.366 – 375.

[81] **Kadous, M. W.,** 1999: Learning comprehensible descriptions of multivariate time series. In *Proceedings of 16th International Machine Learning Conference*, pp 454-463.

[82] **Keogh, E. and Pazzani, M.,** 2000: Scaling up Dynamic Time Warping for Datamining Applications. In *Proceedings of 21st International Conference on Very Large Databases,* Boston, MA, pp.285-289.

[83] **Keogh, E. and Ratanamahatana, A.,** August 2002: Exact indexing of dynamic time warping. In *Knowledge and Information Systems*, 7 (3), pp.358-386.

[84] **Kıcıman, E. and Subramanian, L.,** June 2005: Root Cause Localization in Large Scale Systems. *In Proceedings of the First Workshop on Hot Topics in System Dependability (HotDep).*

[85] **Kovar, K., Fürnkranz, J. F., Petrak, J., Pfahringer, B., Trappl, R. and Widmer, G.,** 2000: Searching for patterns in political event sequences: Experiments with the KEDS database. Cybernetics and Systems, 31(6), pp. 649-668.

[86] **Lee, P.P.C., Misra, V. and Rubenstein, D.,** May 2007: Toward Optimal Network Fault Correction via End-to-End Inference. *In Proceedings of the 6th IEEE International Conference on Computer Communications,* Anchorage, AK, pp.1343-1351.

[87] **Markopoulou, A., Iannaccone, G., Bhattacharyya, S., Chuah,C.N and Diot, C.,** August 2008: Characterization of Failures in an IP Backbone Network. *In Proceedings of IEEE / ACM Transactions on Networking*, 16(4), pp.749-762.

[88] **Meira, D. M.,** 1997: A Model for Alarm Correlation in Telecommunication Networks. PhD thesis, Universidade Federal de Minas Gerais, Belo Horizonte, Brazil.

[89] **Mörchen, F.,** 2006: Time Series Knowledge Mining. PhD Thesis, Philipps University, Marburg, Germany

[90] **Natu, M. and Sethi A.S.,** 2007: Probabilistic fault diagnosis using adaptive probing. *In Proceedings of Distributed systems: operations and management (DSOM)*, Springer-Verlag Berlin, Heidelberg, pp.38-49.

[91] **Oliner, A.J., Kulkarni, A.V. and Aiken, A.,** 2010: Using correlated surprise to infer shared influence. *In Dependable Systems and Networks (DSN),* IEEE / IFIP International Conference, Chicago, IL, pp.191-200.

[92] **Ozden, B., Ramaswamy, S., Sillberschatz, A.,** February 1998: Cyclic Association Rules. In *Proceedings of 14th International Conference on Data Engineering,* pp.412-421.

[93] **Rodriguez, J. J., Alonso, C. J., and Boström, H,** 2000: Learning First Order Logic Time Series Classifiers. In *Proceedings of Work-in-Progress Track at the 10th International Conference on Inductive Logic Programming,* pp. 260–275.

[94] **Rodríguez, J. J., Alonso, C. J., and Boström, H.,** 2001: Boosting interval based literals. In *Intelligent Data Analysis,* 5(3), pp.245-262.

[95] **Steinder, M. and Sethi, A.,** November 2002: Increasing robustness of fault localization through analysis of lost, spurious and positive symptoms. In *Proceedings of 21st Joint Conference of the IEEE Computer and Communications Societies, INFOCOM,* New York, NY, 1, pp. 322 – 331.

[96] **Steinder, M. and Sethi, A.S.,** March 2003: Probabilistic Event-driven Fault Diagnosis Through Incremental Hypothesis Updating. *In Proceedings of 8th Integrated Network Management,* IFIP / IEEE International Symposium, pp. 635 – 648.

[97] **Steinder, M. and Sethi, A. S.,** 2004: A survey of fault localization techniques in computer networks. Science of Computer Programming, 53, pp.165-194.

[98] **Sterritt, R.,** December 2002: Towards autonomic computing: Effective event management. In *27th Annual IEEE / NASA Software Engineering Workshop (SEW),* IEEE Computer Society, Maryland, USA, pp.40–47.

[99] **Sterritt, R., Shapcott, M., Adamson, K. and Curran, E.,** 2000: High Speed Network First- Stage Alarm Correlator. In *International Conference on Intelligent Systems and Control.*

[100] **Tang, Y., Al-Shaer, E. and Boutaba, R.,** May 2005: Active Integrated Fault Localization in Communication Networks. In *Proceedings of the 9th IFIP / IEEE International Symposium on Integrated Network Management (IM),* Nice, France, pp.543–556.

[101] **Tiffany, M.**, May 2002: A Survey of Event Correlation Techniques and Related Topics. Retrieved on October 13, 2010 from http://www.tiffman.net/netman/netman.pdf

[102] **Trindade, J.P.P,** 2007: Fault diagnostics and reporting in mobile services. Master's thesis, Faculty of Information and Computer, Technical University of Lisboa, Spain.

[103] **Turner, D., Levchenko, K., Snoeren, A.C. and Savage, S.,** October 2010: California Fault Lines: Understanding the Causes and Impact of Network Failures. *In Proceedings of ACM SIGCOMM Computer Communication Review*, 40(4), New York, NY, USA, pp.315-326.

[104] **Vaarandi, R.** October 2003: A Data Clustering Algorithm for Mining Patterns from Event Logs. In Proceedings of the 2003 IEEE Workshop on IP Operations and Management (IPOM), pp.119 – 126.

[105] **Vautier, A., Cordier, M.O. and Quiniou, R.,** 2005 :An Inductive Database for Mining Temporal Patterns in Event Sequences. In *Proceedings of workshop on Mining Spatial and Temporal Data*, pp. 1640-1641.

[106] **Weiss, G.M.,** 2005: Data Mining in Telecommunications. In *The Data Mining and Knowledge Discovery Handbook*, pp. 1189-1201.

[107] **Wietgrefe, H.,** 2002: Investigation and practical assessment of alarm correlation methods for the use in GSM access networks. In Network Operations and Management Symposium (NOMS), IEEE / IFIP, pp.391–403.

[108] **Wietgrefe, H., Tuchs, K.D., Jobmann, K., Carls, G., Froelich, P., Nejdl, W. And Steinfeld, S.,** 1997: Using neural networks for alarm correlation in cellular phone network. In *International Workshop on Applications of Neural Networks in Telecommunications* (IWANNT).

[109] **Zhang, H., Ho, T.B., Lin, M.S. and Huang, W,** 2005: Combining the Global and Partial Information for Distance-Based Time Series Classification and Clustering. In *Journal of Advanced Computational Intelligence & Intelligent Informatics*, Fuji Technology Press Ltd., 10 (1), pp.69-76.

[110] **Zhu, D. and Sethi, A. S.,** 2001: SEL, a new event pattern specification language for event correlation. In Proceedings of the IEEE Intl. Conference (ICCCN), pp.586–589.

[111] **Zurutuza, U. and Uribeetxeberria, R**., 2004: Intrusion Detection Alarm Correlation: A Survey. Computer Science Department, Mondragon University, Gipuzkoa Spain.

ÖZGEÇMİŞ

Ad Soyad: Mehmet Onur Sarkan

Doğum Yeri ve Tarihi: Adana 9 Nisan 1981

Adres: Ağaoğlu Eltes Güneşi Sitesi C5 Blok Daire 41 Yukarıdudullu Ümraniye İstanbul

Lisans Üniversite: Sabancı Üniversitesi Telekomünikasyon Mühendisliği

Yayın Listesi:

- **Sarkan, M. O.,** Çataltepe, **Z.,** 2011: Parzen Penceresi Yöntemi İle Geçici Alarm Filtreleri Üretimi. *IEEE 19. Sinyal İşleme ve İletişim Uygulamaları Kurultayı.*

Patent Başvuru Listesi:

- Bir otomatik filtre üretim sistemi ve yöntemi. Başvuru numarası: 2010/10287
- GSM sistemleri için bir otomatik alarm filtreleme sistemi ve yöntemi. Başvuru numarası: 2010/11178
- Parzen Penceresi Yöntemi ile Otomatik Alarm Filtresi Üretim Sistemi ve Yöntemi, Başvuru numarası: 2011/06503